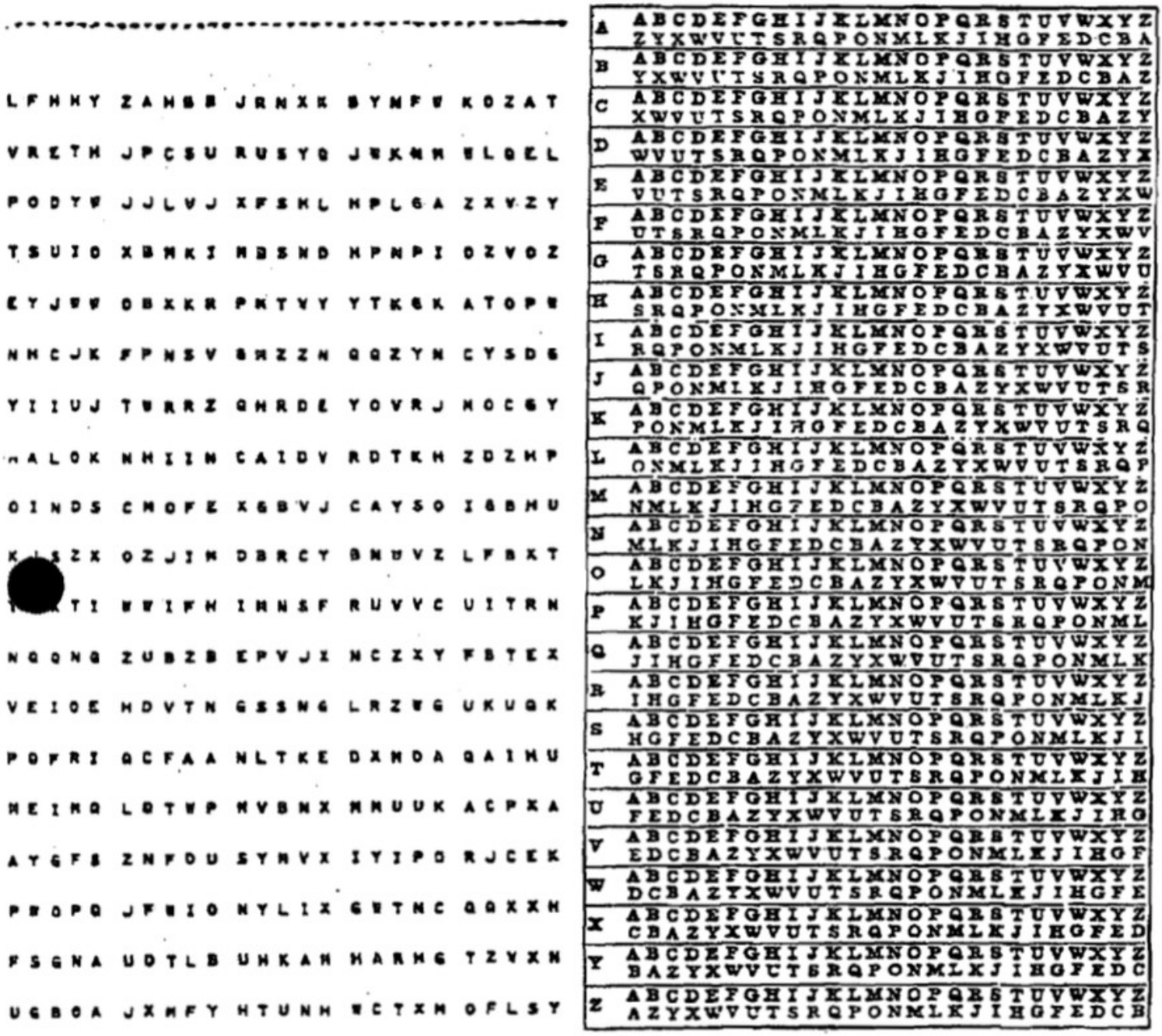
Understanding The Process Of Operational Intelligence Analysis



Compiled And Edited By

David Childers

Foreward

The Intelligence analysis process is the ability to examine and evaluate information; based upon a formal structured process. This evaluation process incorporates several vital questions, which include:

- The validity of the data.
- The accuracy of the data.
- How data from various sources are related.
- The relevance of the data to the required information objective.
  (What needs to be known.)

Peer review of Intelligence analysis summary reports is should also be incorporated as an essential process step. This process allows a fresh insight into data received, techniques used, and drawn conclusions. A second party review can provide the opportunity to find or question data not observed before.

It is crucial to determine the initial information requirements to alleviate the duplication of staffing or resources. This determination focuses staffing and resources on collecting only the relevant information required. Intelligence data is also typically acquired from multiple sources, which allows the analyst to have the opportunity to cross-checking information. Having information requirements or objectives enables the analyst to focus on what is required.

It is my sincere wish that the reader will gain both insight and knowledge from the contents of this publication.

David Childers

Non Ducor, Duco!

15 February 2021

If you know the enemy and know yourself you need not fear the results of a hundred battles.

Sun Tzu

Cover Image

https://commons.wikimedia.org/wiki/File:NSA_DIANA_one_time_pad.tiff

Dedication

To the Heroes and Zeroes of the blacker boxes.

Understanding Intelligence is neither a trivial pursuit nor a fool's game.
You must excel to achieve the mastery of this critical skill.

Oberstleutnant Günther von Mittelbiberach
Hauptverwaltung Aufklärung
Ministerium für Staatssicherheit
Deutsche Demokratische Republik

Copyright Information

All documents contained within this publication are conditionally used under the auspices of 17 U.S. Code § 105, hereby referred to as "Subject matter of copyright: United States Government works."

This publication is licensed under the
Attribution-ShareAlike 4.0 International
(CC BY-SA 4.0)
Creative Commons License.

www.creativecommons.org/licenses/by-sa/4.0/

Executive Summary

This publication aims to provide reference material that establishes a methodology and process outline for qualitative analysis of operational intelligence data.

Index

Publication Title	Page Number
Marine Corps Warfighting Publication MCWP 2-1 Intelligence Operations Department Of The Navy Headquarters United States Marine Corps Washington, D.C. September 2003	12
Field Manual FM 3-55 Information Collection Headquarters, Department of the Army April 2012	101
Army Techniques Publication ATP 2-33.4 Intelligence Analysis United States Army January 2020	188
Marine Corps Doctrinal Publication MCTP 2-10B MAGTF Intelligence Production and Analysis Department Of The Navy Headquarters United States Marine Corps Washington, D.C. April 2018	363
Technical Manual TM 32-250 Air Force Manual AFM 100-80 Fundamentals Of Traffic Analysis (Radio-Telegraph) Department Of The Army Department Of The Airforce October 1948	645
Airforce Handbook No. 14-133 Intelligence Analysis United States Air Force September 2017	754
Field Manual FM 34-8-2 Intelligence Officers Handbook Headquarters, United States Army March 1990	859
A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis Prepared by the US Government March 2009	1072

Analyst Toolbox 1118
A Toolbox For The Intelligence Analyst
United States Department of Justice

Intelligence Analysis in Theater Joint Intelligence Centers: 1131
An Experiment In Applying Structured Methods
Occasional Paper Number Seven
By MSgt Robert D. Folker, Jr. (USAF)
Joint Military Intelligence College
Washington, DC
January 2000

Intelligence Essentials For Everyone 1182
Occasional Paper Number Six
By Lisa Krizan
Joint Military Intelligence College
Washington, DC
June 1999

Bringing Intelligence About 1273
Practitioners Reflect on Best Practices
Russell G. Swenson, Editor
Joint Military Intelligence College
Washington, DC
May 2003

Critical Thinking and Intelligence Analysis 1432
Occasional Paper Number Fourteen
David T. M oore
National Defense Intelligence College
Washington, DC
March 2007

Analytic Culture In The US Intelligence Community 1592
An Ethnographic Study
Dr. Rob Johnston
Center For The Study Of Intelligence
Central Intelligence Agency
Washington DC
2005

Studies in Intelligence 1766
Journal of the American Intelligence Professional
Unclassified articles from Studies in Intelligence Volume 55, Number 2
Center for the Study of Intelligence
Central Intelligence Agency
Washington DC
June 2011

Advanced Analysis Cognition: 1870
Improving The Cognition Of Intelligence Analysis
Christina M. Kampman
Charles A. Mangio
Melinda Marsh
Air Force Research Laboratory
711 Human Performance Wing
Wright-Patterson AFB OH
September 2013

Intelligence Analysis for Problem Solvers 2279
John E. Eck and Ronald V. Clarke
with contributions by Gohar Petrossian
Community Oriented Policing Services
United States Department Of Justice
September 2013

Curing Analytic Pathologies: 2424
Pathways to Improved Intelligence Analysis
Jeffrey R. Cooper
Center for the Study of Intelligence
Central Intelligence Agency
Washington, DC 20505
December 2005

Defence And Intelligence Abreviations And Acronyms 2502
Joint Military Intelligence College
United States Secretary of Defense (Public Affairs)
Washington, DC
November 1997

Special Operations and International Studies 2756
Political Military Analysis Handbook
U.S. Army Regional Studies Course
John F. Kennedy Special Warfare Center and School
United States Army
Fort Bragg, North Carolina
2004

The Role of Rhetorical Theory in Military Intelligence Analysis 2907
A Soldier’s Guide to Rhetorical Theory
Gary H. Mills
Major, USAF
Fairchild Paper
Air University Press
United States Air Force
Maxwell Air Force Base, Alabama
August 2003

Employing The Intelligence Cycle Process 2981
Model Within The Homeland Security Enterprise
Roger L. Stokes
Naval Postgraduate School
Monterey, CA
December 2013

Sources in Cryptologic History 3099
Volume4
A Collection of Writings on Traffic Analysis
Vera R. Filby
Center For Cryptologic History
National Security Agency
1993

Directorate of Intelligence 3350
A Compendium of Analytic Tradecraft Notes
Volume I
(Notes 1-10)
Central Intelligence Agency
February 1997

Psychology Of Intelligence Analysis 3410
Richards J. Heuer, Jr
Center For The Study Of Intelligence
Central Intelligence Agency
1999

Masters Of Analytical Tradecraft: 3625
Certifying The Standards And Analytic Rigo Of Intelligence Products
Lt Col USAF J. Tucker Rojas
Air Command And Staff College
Air University
Maxwell Air Force Base, Alabama
April 2016

Using Industry Analysis For Strategic Intelligence 3663
Capabilities And Strategic Intent
Discussion Paper 17
Chuck Howe
Center For Strategic Intelligence Research
National Intelligence University
Washington, DC
January 2015

Sensemaking 3796
A Structure For An Intelligence Revoluion
David T. Moore
National Intelligence College
Washington, DC
March 2011

The Applied Critical Thinking Handbook 4030
Red Teaming Handbook v7
Training And Doctrine Command
Headquarters, United States Army
2015

Introductory Guide to Crime Analysis and Mapping 4281
Written by:
Rachel Boba, Ph.D.
Community Orientated Policing Services
U.S. Department Of Justice
November 2001

Law Enforcement Intelligence: 4356
A Guide for State, Local, and Tribal Law Enforcement Agencies
Second Edition
David L. Carter, Ph.D.
Community Orientated Policing Services
U.S. Department Of Justice
January 2009

Additional Reference Information 4853

This Page Is Intentionally Left Blank

MCWP 2-10
(Formerly MCWP 2-1)

Intelligence Operations

US Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 143 000036 00

CD&I (C 116)

2 May 2016

ERRATUM

to

MCWP 2-1

INTELLIGENCE OPERATIONS

1. Change all instances of MCWP 2-1, *Intelligence Operations*, to MCWP 2-10, *Intelligence Operations.*

2. File this transmittal sheet in the front of this publication.

PCN 143 000036 80

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes that will improve it. Recommendations may be sent directly to Commanding General, Marine Corps Combat Development Command, Doctrine Division (C 42), 3300 Russell Road, Suite 318A, Quantico, VA 22134-5021 or by fax to 703-784-2917 (DSN 278-2917) or by E-mail to **morgann@mccdc.usmc.mil**. Recommendations should include the following information:

- Location of change
  - Publication number and title
  - Current page number
  - Paragraph number (if applicable)
  - Line number
  - Figure or table number (if applicable)
- Nature of change
  - Add, delete
  - Proposed new text, preferably double-spaced and typewritten
- Justification and/or source of change

Additional copies: A printed copy of this publication may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status.* An electronic copy may be obtained from the Doctrine Division, MCCDC, world wide web home page which is found at the following universal reference locator: **http://www.doctrine.usmc.mil**.

Unless otherwise stated, whenever the masculine gender is used, both men and women are included.

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, DC 20380-1775

10 September 2003

FOREWORD

Marine Corps Warfighting Publication (MCWP) 2-1, *Intelligence Operations*, builds on the doctrinal foundation established in Marine Corps Doctrinal Publication (MCDP) 2, *Intelligence*. It provides tactics, techniques, and procedures (TTP) for Marine air-ground task force (MAGTF) intelligence operations. This publication is intended for commanders, other users of intelligence, and intelligence personnel who plan and execute intelligence operations.

This publication supersedes MCWP 2-1, *Intelligence Operations,* dated 19 February 1998.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

EDWARD HANLON, JR.
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command

Publication Control Number: 143 000036 00

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

MCWP 2-1, INTELLIGENCE OPERATIONS

TABLE OF CONTENTS

Chapter 1. Fundamentals

Intelligence Objectives 1-1
Maneuver Warfare 1-2
Developing Intelligence 1-2
    Data, Information, and Intelligence 1-2
    The Intelligence Cycle 1-3
Intelligence Operations 1-4
    Relationship to Command and Control 1-4
    Relationship to Operations 1-5
Principles of Intelligence Operations 1-5
Intelligence Functions 1-6
    Support the Commander's Estimate 1-6
    Develop the Situation 1-7
    Provide Indications and Warning 1-7
    Support Force Protection 1-7
    Support Targeting 1-7
    Support Combat Assessment 1-7
The Commander's Role in the Intelligence Process 1-8
    Focus the Intelligence Effort 1-8
    Participate in the Intelligence Process 1-8
    Use Intelligence in Decisionmaking 1-8
    Support the Intelligence Effort 1-8
    Evaluate the Results of Intelligence Activities 1-9
Information Operations 1-9
    Planning 1-9
    Intelligence Preparation of the Battlespace 1-9
    IO-Related Force Protection 1-9
    The Role of Intelligence in IO is Continual 1-10
Required Intelligence Capabilities 1-10

Chapter 2. Command and Control

Decisionmaking 2-1
    Observe, Orient, Decide, and Act Loop 2-1
    Intelligence and the OODA Loop 2-2
    Decisionmaking Approaches: Analytical and Intuitive 2-2

The Planning, Decision, Execution, and Assessment Cycle 2-3
Intelligence Support to Planning 2-3
Planning Models 2-3
Mission Analysis 2-4
COA Development 2-5
COA War Game 2-6
Orders Development 2-6
Execution 2-7
Resource Allocation 2-8
Linkage to Operations 2-8
Generation of Tempo 2-8

Chapter 3. Developing Intelligence

Intelligence Requirements 3-2
Priority Intelligence Requirement 3-4
Characteristics 3-4
Planning and Direction 3-4
Requirements Development 3-4
Requirements Management 3-5
Directing the Intelligence Effort 3-6
Collection Management 3-7
Production Management 3-7
Dissemination Management 3-7
Planning the Intelligence Support System 3-7
Collection 3-7
Imagery Intelligence 3-8
Signals Intelligence 3-8
Human Intelligence 3-9
Measurement and Signature Intelligence 3-9
Open-Source Intelligence 3-9
Counterintelligence 3-10
Processing and Exploitation 3-10
Production 3-10
Intelligence Preparation of the Battlespace 3-10
Levels of Production 3-11
Dissemination 3-12
Form 3-12
Delivery 3-13
Channels 3-14
Architectures 3-15
Utilization 3-15
Application of the Intelligence Cycle 3-17
Counterintelligence 3-17
Responsibilities 3-17
CI Planning 3-18
CI Measures 3-19

Chapter 4. Concept of MAGTF Intelligence Support

Role of the Organic Intelligence Section 4-2
The Unit Intelligence Officer 4-2
The Unit Intelligence Section 4-3
Required Capabilities 4-3
The MAGTF Intelligence Section 4-3
MAGTF Intelligence Officer 4-3
Special Staff Officers under Staff Cognizance of G-2 Officer 4-4
MAGTF Intelligence Units 4-9
Organization of MAGTF-Level Intelligence Units 4-9
Employment of MAGTF Intelligence Units 4-11
Focused Intelligence Support 4-12
Intelligence Nodes 4-12
Split-basing 4-12
Task Organization of Intelligence Support Units 4-13
Intelligence DSTs 4-13
Intelligence Coordination 4-13
External Intelligence Support to the MAGTF 4-14
MARFOR Component Intelligence Section 4-14
National, Theater, Joint, and Other Service Intelligence Support 4-16
Augmentation 4-17
Supporting Establishment 4-17
Marine Corps Intelligence Activity 4-17
Marine Cryptologic Support Battalion 4-18
Navy Marine Corps Intelligence Training Center 4-18
Personnel Augmentation 4-18
Marine Corps Forces Reserve 4-18

Chapter 5. Operational Maneuver from the Sea

Required Intelligence Capabilitites 5-1
Planning and Direction 5-1
Collection 5-2
Processing, Exploitation, and Production 5-2
Dissemination 5-3
Utilization 5-3
Planning and Direction 5-3
Collection 5-4
Processing, Exploitation, and Production 5-4
Dissemination 5-4
Utilization 5-5

Chapter 6. Sustained Operations Ashore

Required Intelligence Capabilities 6-1
Planning and Direction 6-1
Collection 6-2

Processing, Exploitation, and Production 6-3
Dissemination 6-3
Utilization 6-4

Chapter 7. Military Operations Other Than War

Required Intelligence Capabilities 7-1
Planning and Direction 7-2
Collection 7-2
Processing, Exploitation, and Production 7-3
Dissemination 7-3
Utilization 7-3

Chapter 8. Joint Operations and Multinational Operations

JFC and Component Commander Responsibilities 8-1
Joint Intelligence Structure 8-1
Procedures 8-2
Marine Intelligence Section and Unit Responsibilities 8-2
MARFOR Component Headquarters or
MAGTF CE as a JTF Headquarters 8-2
Multinational Operations 8-2

Appendices

A. Glossary A-1
B. References B-1

List of Figures

1-1. The Information Hierarchy 1-3
1-2. Key Considerations of the Intelligence Cycle 1-3
1-3. Relationship Between Intelligence Functions and Operations 1-7

2-1. The Observe, Orient, Decide, and Act Loop 2-1
2-2. Intelligence Support to Planning 2-4

3-1. The Marine Corps Intelligence Cycle 3-1
3-2. The Intelligence Cycle—Macro View 3-2
3-3. The Intelligence Cycle—Micro View 3-2
3-4. Intelligence Development and the Intelligence Cycle 3-3
3-5. Planning and Direction Phase Functions 3-4
3-6. Intelligence Requirements Management 3-5
3-7. Requirements Satisfaction 3-6
3-8. MAGTF Primary Organic Collection Assets 3-8
3-9. Intelligence Preparation of the Battlespace 3-11
3-10. Graphic Climatology Study 3-13
3-11. Graphic Intelligence Estimate 3-14
3-12. Notional Marine Expeditionary Force Intelligence Architecture 3-16

3-13. Application of the Intelligence Cycle 3-18
3-14. The Counterintelligence Process 3-20

4-1. Special Staff Officers and Relationships under the Staff Cognizance of the MEF G-2 4-5
4-2. AC/S G-2's Principal Subordinate Staff Officers and their Responsibilities 4-7
4-3. Intelligence Battalion 4-10
4-4. Intelligence Operations Center 4-14
4-5. The National Intelligence Community 4-16

5-1. Intelligence Considerations During OMFTS 5-2

6-1. Intelligence Considerations During Sustained Operations Ashore 6-2

7-1. Intelligence Factors in MOOTW 7-2

CHAPTER 1
FUNDAMENTALS

Intelligence is knowledge of the battlespace and of the threat forces in that battlespace. Knowledge is generated in support of the commander's decisionmaking process and is the result of the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat.

Intelligence Objectives

Intelligence has two objectives: to reduce uncertainty by providing accurate, timely, and relevant knowledge about the threat and the surrounding environment, and to assist in protecting friendly forces (to include Department of Defense [DOD] personnel, family members, resources, facilities and critical information) through counterintelligence (CI).

Uncertainty pervades the battlespace—it is a fundamental attribute of war. First and foremost, intelligence should support the commander's decisionmaking process by reducing uncertainty about the hostile situation. Intelligence should accomplish the following actions to achieve this objective:

- Identify and evaluate existing conditions and capabilities.
- On the basis of those existing conditions and capabilities, estimate possible enemy courses of action (COAs) and provide insight into possible future actions.
- Aid in identifying friendly critical vulnerabilities that the threat may exploit.
- Assist in developing and evaluating friendly COAs.

The fog and friction of war will never allow the commander to have a perfect picture of the battlespace. Because intelligence deals with the greatest number of unknowns—questions about an unfamiliar area and a hostile enemy who is actively trying to conceal information about his forces and intentions—there will almost always be gaps in intelligence, and the knowledge provided will lack the desired degree of detail and reliability. Intelligence cannot provide absolute certainty. It attempts to reduce the uncertainty facing the commander to a reasonable level by collecting relevant information, placing it in context to provide knowledge, and conveying it in the form of images to enhance understanding.

CI is information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, foreign persons or international terrorist activities.

CI activities consist of active and passive measures, functions, and services. CI measures, functions, and services are intended to deny a potential adversary information that might increase the effectiveness of hostile operations against friendly forces; detect and neutralize foreign intelligence collection; and deceive the enemy as to friendly capabilities and intentions. In so doing, CI increases uncertainty for the enemy, thereby making a significant contribution to the success of operations. CI services identify friendly vulnerabilities, evaluate security measures, and assist in implementing appropriate plans to enhance a unit's force protection posture against the threats of sabotage, subversion, and terrorism.

Maneuver Warfare

The essence of war is a violent clash between independent wills, each trying to impose itself on the other. War's defining attributes of friction, uncertainty, fluidity, disorder, and complexity combine with the various dimensions of human nature to make war a fundamentally unpredictable activity. To succeed in war, Marines must be able to operate effectively in this uncertain, chaotic, complex, and fluid environment.

The Marine Corps philosophy for winning under these conditions is based on rapid, flexible, and opportune maneuver. MCDP 1, *Warfighting*, states that, "Maneuver warfare is a warfighting philosophy that seeks to shatter the enemy's cohesion through a variety of rapid, focused, and unexpected actions which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope." Maneuver warfare requires maneuver in time and space to achieve superiority over the enemy. It concentrates on those actions that present the enemy with a series of dilemmas where events happen unexpectedly and faster than the enemy can react. Concepts central to executing maneuver warfare follow:

- **Orienting on the enemy.** Maneuver warfare attacks the enemy "system," the combination of physical, moral, and mental components that make up an enemy or an enemy force. This means focusing outward on the particular characteristics of the enemy.
- **Centers of gravity (COG) and critical vulnerabilities.** COG are sources of moral or physical strength, power or resistance that are critical to the enemy's ability to resist. Critical vulnerabilities are components of the enemy system that are both crucial to the functioning of the system and vulnerable to exploitation. Identifying and exploiting an enemy's COG and critical vulnerabilities help focus combat power toward a decisive aim.
- **Main effort.** The main effort is the unit assigned responsibility to accomplish the key mission within the command. It is directed where there is the best opportunity to succeed and at the objective that will have the most significant effect on the enemy, normally a critical vulnerability.
- **Commander's intent.** Commander's intent describes the purpose behind the task assigned in a mission. It provides continuing guidance when the tactical situation changes and permits the exercise of initiative in harmony with the commander's desires.
- **Mission tactics.** Mission tactics assign subordinates a task without specifying how it must be accomplished. They permit subordinates to exercise initiative in adapting to ever-changing situations.
- **Tempo.** Tempo keeps the enemy off balance, thereby increasing his friction. Speed, initiative, and flexibility generate and maintain a tempo that the enemy cannot match.

Accurate and timely intelligence is a prerequisite for success in maneuver warfare. Maneuver warfare is based on a firm focus on the enemy and on taking action that avoids enemy strengths and exploits enemy critical vulnerabilities. It means acting in a manner and at a time and place that the enemy does not expect and is not prepared. It requires decision and action based on situational awareness—a keen understanding of the factors that make each situation unique. Intelligence provides the knowledge of the enemy and the battlespace that permits the commander to reduce uncertainty, identify opportunities for success, assess risk, outline intent, and make decisions that provide focus, generate speed and tempo, and achieve decisive results.

Developing Intelligence

Data, Information, and Intelligence

Intelligence is not simply another term for information. Intelligence is more than an element of

data or a grouping of information; it is a body of knowledge. Knowledge occupies a unique place in the information hierarchy, which is a framework to distinguish between various classes of information. (See figure 1-1.)

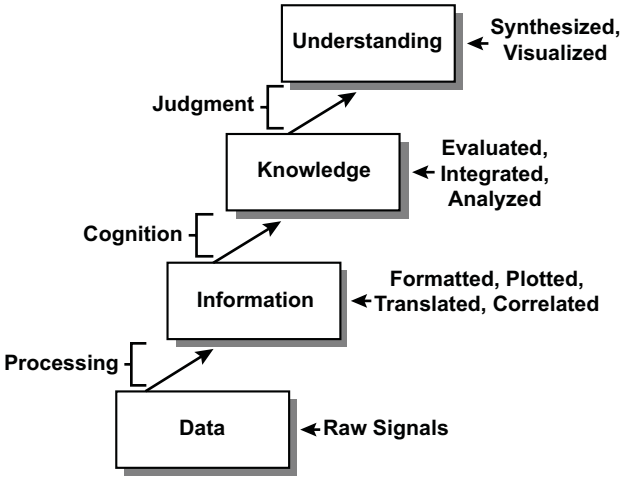


Figure 1-1. The Information Hierarchy.

There is a clear and important distinction between raw data, information, and intelligence. Intelligence is not a mass of unfocused data or even a collection of related facts. In fact, giving a commander every piece of data without providing meaning can increase uncertainty by overloading the commander with incomplete, contradictory or irrelevant information. To be intelligence, data must be placed in context to provide an accurate and meaningful image of the hostile situation. Intelligence is developed by analyzing and synthesizing data and information to produce knowledge about the threat and the environment. The commander combines this knowledge with knowledge of the friendly situation and employs experience, judgment, and intuition to understand the situation. The commander then applies this understanding in making decisions.

The Intelligence Cycle

Intelligence is the output of a process that converts data and information into knowledge that applies to a specific military decision. The process used to develop intelligence is called the intelligence cycle. This cycle is the process by which information is planned for, obtained, assembled, converted through analysis into intelligence, provided to decisionmakers, and, ultimately, used in making decisions. (See figure 1-2.)

Intelligence Cycle	Key Considerations
Planning and direction.	Identify intelligence requirements. Plan intelligence operations and activities. Support the formulation of the commander's estimate of the situation.
Collection.	Develop the required intelligence structure. Use organic, attached, and supporting intelligence sources to collect intelligence.
Processing, exploitation, and production.	Conversion of raw data and information into a suitable form of intelligence.
Dissemination.	Timely provision of intelligence, in appropriate form, to those who need it.
Utilization.	Use of intelligence.

Figure 1-2. Key Considerations of the Intelligence Cycle.

The intelligence cycle consists of a series of related activities that translate the need for intelligence about a particular aspect of the battlespace or threat into a knowledge-based product that is provided to the commander for use in the decisionmaking process. In this sequence, intelligence needs are identified and a plan is developed for satisfying those needs. Data are collected, processed into information, and converted into intelligence through analysis and synthesis. The resulting knowledge is then provided to the commander as an intelligence product that is used in making decisions. The information used to produce intelligence is derived from a variety of sources. Intelligence information; i.e., information used to generate intelligence, is commonly drawn from three types of data: intelligence, sensor or combat.

Intelligence data is derived from assets primarily dedicated to intelligence collection; e.g., imagery systems, electronic intercept equipment or human intelligence (HUMINT) sources.

Sensor data is derived from sensors whose primary mission is surveillance or target acquisition; e.g., air surveillance radars, counterbattery radars, and remote ground sensors.

Combat data is derived from reporting by operational units. Because of their highly perishable or critical nature, combat data and sensor data are sometimes used to effect decisions without being converted into intelligence. Although the demands of the ongoing battle may require rapid action, decisions based on raw, unprocessed data or single pieces of data should be avoided.

Processing, analysis, and synthesis of data and information into intelligence can be accomplished rapidly at all levels. We seek knowledge—*accurate intelligence, not incomplete, unfocused, or unevaluated information*—to enhance our understanding and base our decisions. The intelligence cycle works continuously to satisfy intelligence shortfalls and confirm or refute fragmentary information. Once collected and processed, information is converted into intelligence through the application of experience and judgment. Information is analyzed to determine its significance and is synthesized with other relevant information to build a coherent picture of existing conditions and capabilities. This picture is then used to predict possible outcomes of environmental conditions and enemy actions. Results are conveyed to the commander in an intelligence product. Because humans understand situations best as images—mental pictures—intelligence is produced and disseminated in graphic form whenever possible. The process is completed when the knowledge provided is applied to influence decisionmaking.

Intelligence Operations

Intelligence personnel and organizations perform a number of separate and distinct activities and functions that are collectively known as intelligence operations. Intelligence operations are conducted to provide intelligence in support of the decisionmaking process of commanders down to the small-unit level. The primary focus of Marine Corps intelligence operations is generating *tactical intelligence*; i.e., intelligence that supports the planning and conduct of tactical actions. Although the focus is on tactical intelligence, the Marine Corps must draw on both strategic and operational intelligence resources and, in certain circumstances, be prepared to conduct intelligence operations at the operational and even strategic level. Intelligence reduces uncertainty and supports the decisionmaking process by—

- Describing the battlespace.
- Identifying key factors in the battlespace that can influence operations.
- Defining and evaluating threat capabilities.
- Identifying the enemy's COG and critical vulnerabilities.
- Assessing enemy intentions.

Relationship to Command and Control

Intelligence is a fundamental component of command and control (C2). C2 is the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. A principal aim of C2 is to enhance the commander's ability to make sound and timely decisions. Intelligence facilitates the commander's decisionmaking process by making a major contribution to the understanding of the battlespace and the threat. Intelligence is also an

integral element of the process through which the commander implements decisions. Inadequate or imperfect intelligence can significantly inhibit the ability of a commander or subordinates to carry out these decisions. Lack of a continuous, effective intelligence effort also degrades the quality of feedback to the commander about the unfolding situation; it is this feedback that allows the commander to modify the actions of the command as needed.

Because intelligence is crucial to success on the battlefield, it must be given command attention. The commander drives intelligence by focusing the intelligence effort through the definition of the mission, articulation of his intent, and designating priority intelligence requirements (PIRs). A PIR is an intelligence requirement (IR) associated with a decision that will critically affect the overall success of the command's mission. PIRs are a subset of commander's critical information requirements (CCIRs) and are focused on the environment and the threat.

Relationship to Operations

Intelligence is inseparable from operations. Intelligence drives operations by shaping the planning and execution of operations. It provides a menu of factors that the commander considers when making a decision. Specifically, intelligence—

- Identifies potential advantages offered by the environment.
- Describes limitations imposed by the environment.
- Ascertains and assesses enemy strengths to be avoided.
- Uncovers enemy critical vulnerabilities that can be exploited.
- Recommends COAs based on factors of the battlespace and threat.
- Enables rapid decisionmaking and generating and maintaining tempo.

Operational actions develop logically from intelligence. A commander with effective intelligence knows the nature of the terrain, weather conditions, the composition and status of the infrastructure in the area of operations, the makeup and attitude of the population that will be encountered, and how the combined effects of these factors will influence mission accomplishment. Intelligence provides knowledge of threat capabilities, strengths, COG, and critical vulnerabilities, along with insight into the enemy's intentions. Integrating intelligence on the threat and the battlespace helps to provide the commander with situational awareness, which is used to determine the decisive time and place to strike.

Intelligence and operations must be linked throughout the planning, decision, execution, and assessment (PDE&A) cycle at all levels. Intelligence shapes the plan and provides the knowledge that facilitates execution. It identifies changes in the situation that require modification of the plan or that trigger decisions during the conduct of the operation. At the same time, the nature of the mission and the concept of operations focus and shape the intelligence effort; intelligence that is not relevant to the mission is useless. IRs and intelligence operations are continually evaluated to ensure that they are focused on supporting mission accomplishment.

Principles of Intelligence Operations

- **The focus is on tactical intelligence.** The focus of Marine Corps intelligence operations is on the generation of tactical intelligence. However, there are no sharp boundaries between levels of intelligence; they merge and form a continuum. In some instances Marine Corps tactical intelligence operations will support operational and strategic IRs.
- **Intelligence is focused downward.** Intelligence must be available to commanders at all

levels. Although the management of intelligence collection and production is centralized in the MAGTF command element (CE), the focus is on providing the intelligence needed to plan and execute the mission to every unit involved in the operation. Requirements of the entire force will be considered in directing the intelligence effort. Critical products will be *pushed* down to the tactical commander, who will be able to *pull* additional intelligence support as needed.

- **Intelligence drives operations.** The Marine Corps' warfighting philosophy depends on timely, accurate intelligence for success. Intelligence is the critical underpinning for each phase of the PDE&A cycle.
- **Intelligence activities require centralized management.** Good intelligence is the result of the integration of many separate and specialized collection, processing, and analytical resources. The scarcity of these assets, coupled with the requirement to focus on the commander's PIRs, creates the need for centralized coordination and management. This centralization will be done in the MAGTF CE, under the direction of intelligence officers who are trained and experienced in the management of multidiscipline, all-source intelligence operations. (All-source intelligence is intelligence that incorporates all available sources of information in the development of the finished intelligence product.) *Although centralized coordination and management is required for efficient and effective use of intelligence assets, it is critical for the commander who is exercising centralized control to allocate appropriate resources to ensure that needs of subordinate commands that are crucial to mission accomplishment are properly addressed.*
- **The G-2/S-2 facilitates use of intelligence.** The intelligence officer enables effective use of intelligence throughout the command. As the principal disseminator of intelligence, the intelligence officer ensures that the full implications of the intelligence picture are understood. To do this, the intelligence officer must be a *full and continuous* participant in the planning process.
- **Intelligence must be tailored and timely.** Intelligence must be tailored to the requirements of the user, provided in a useful format, and received in time to affect the decisionmaking process. Delivery of the right intelligence—not simply data or information—to the right place at the right time must be the guiding principle of all dissemination efforts.
- **Utilization is the final step of the intelligence cycle.** Intelligence has no inherent value; its value is derived from its support of decisionmaking. The intelligence cycle is not complete until the intelligence that has been developed is used to plan and/or execute operations.

Intelligence Functions

All six functions are carried out continually during the PDE&A cycle at all levels throughout the force. However, particular functions may be stressed more during one phase of the cycle. Different units may emphasize one or two functions over the others based on individual missions. (See figure 1-3.)

Support the Commander's Estimate

Intelligence supports the formulation and subsequent modification of the commander's estimate of the situation by providing as accurate an image of the battlespace and the threat as possible. Intelligence supports initial planning and decisionmaking. One of the principal tools used in this function is intelligence preparation of the battlespace (IPB). IPB is a systematic, continuous process of analyzing the threat and environment in a specific geographic area. IPB helps to provide an appreciation for the characteristics of the area of operations and the enemy capabilities, weaknesses, and COAs. This knowledge affords the commander an understanding of the battlespace and the opportunity to exploit enemy critical vulnerabilities.

Intelligence Functions	Decisionmaking	Operational Activities
Support to commander's estimate.	Plan a mission.	Develop and analyze COAs.
Situation development.	Execute the mission.	Monitor execution. Modify plan as necessary.
Indications and warning.	Orient on contingencies.	Increase readiness. Develop contingency plans.
Support to force protection.	Force protection.	Support operations security (OPSEC). Nuclear, chemical, and biological defense. Support deception plan.
Support to targeting.	Plan fire support.	Attack targets.
Support to combat assessment.	Reorient forces. Plan future operations.	Consolidate, pursue, exploit. Reattack targets.

Figure 1-3. Relationship Between Intelligence Functions and Operations.

Develop the Situation

Situation development provides continuing knowledge of unfolding events to help update the estimate of the situation. It is a dynamic process that assesses the current situation and confirms or denies the adoption of specific COAs by the enemy. It helps refine our understanding of the battlespace and reduces uncertainty and risk. Situation development occurs during execution and provides the basis for adapting plans or exploiting opportunities.

Provide Indications and Warning

Indications and warning (I&W) serve a protective purpose, providing early warning of potential hostile action. They help prevent surprise and reduce risk from enemy actions that run counter to planning assumptions.

Support Force Protection

Force protection is the set of comprehensive security measures, collection activities, and operations that are undertaken to guard the force against the effects of enemy action. Intelligence supports force protection by identifying, locating, and countering foreign intelligence collection, sabotage, subversion, and terrorism capabilities. Support to force protection requires detailed and accurate assessments of threat force capabilities and intentions and facilitates efforts to deny the enemy the opportunity to take offensive action against our forces.

Support Targeting

Intelligence supports targeting by identifying target systems, critical nodes, and high-value and high-payoff targets as well as by providing the intelligence required to most effectively engage these targets.

Support Combat Assessment

Combat assessment is the process used to determine the overall effectiveness of military operations and identify requirements for future actions. Intelligence supports the entire combat assessment process and is directly responsible for battle damage assessment (BDA), which is one of the principal components of combat assessment. BDA is the timely and accurate estimate of the damage resulting from the application of military force. BDA estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations.

The Commander's Role in the Intelligence Process

Intelligence is an inherent and essential responsibility of command. Commanders must come to think of command and intelligence as inseparable, just as they commonly think of command and operations as inseparable. They must study and understand the theory and the practice of intelligence doctrine. They must be personally involved in the conduct of intelligence activities, and provide guidance, supervision, judgment, and authority to ensure a timely and useful product.

Focus the Intelligence Effort

The commander must provide the guidance and direction necessary for the effective conduct of intelligence activities. Intelligence assets will rarely be sufficient to satisfy every requirement. Thus, the intelligence effort must be focused on clearly articulated priorities that drive the concept of intelligence support and the collection, production, and dissemination efforts. The commander provides this focus through articulating the commander's intent, planning guidance, and the command's PIRs.

Participate in the Intelligence Process

Although the intelligence officer manages the intelligence effort for the commander, the commander is responsible for the results. Effective participation requires an understanding of the practical capabilities and limitations of intelligence personnel, equipment, procedures, and products. The commander should supervise the process, interjecting guidance and direction at key points to ensure that the process is responding to the commander's intent; e.g., the commander should define the scope of the IPB effort, identify the preferred intelligence product format, and establish priorities among subordinate commands' IRs.

Use Intelligence in Decisionmaking

Intelligence exists for the primary purpose of aiding the commander's decisionmaking process. Although the intelligence officer facilitates the use of intelligence throughout the command by providing timely dissemination of the intelligence product and ensuring that the meaning of the intelligence is understood, the commander makes the judgment of its operational impact. The commander makes a personal analysis of the intelligence product and arrives at the estimate of the situation that serves as the basis for the decision. This act is the responsibility of the commander and no one else.

Support the Intelligence Effort

Intelligence is a team effort. Good intelligence is the result of integrating many separate and specialized collection, processing, and analytical resources. Some of these resources are organic to the unit; many are provided by units or agencies outside the command. Intelligence operations by organic assets normally cannot succeed without support from throughout the command. Reconnaissance teams must be inserted, sensors implanted, and communications assets provided for dissemination. Timely and effective intelligence dissemination requires dedicating significant C2 assets. Once an operation begins, nearly every Marine will have the occasion to observe significant facts about the enemy and environment. All personnel should understand and carry out their responsibility to collect and report information. The commander must ensure that all members of the unit understand the importance placed on intelligence and the requirement to support the intelligence effort. External support must be requested and coordinated. The intelligence staff executes the procedures to obtain the required support, but does so in the name of the commander. When the command's support requirements go unsatisfied, the commander must intervene, lending command authority to obtain the support.

Evaluate the Results of Intelligence Activities

The commander must provide feedback to the intelligence support system. Feedback should identify where the intelligence provided met expectations and where and how it fell short. Key areas to evaluate include product content, presentation, timeliness, and overall usefulness. Meaningful evaluation of the intelligence effort provides the basis for its continual improvement.

Information Operations

Intelligence support is required to conduct information operations (IO). Specific intelligence is required for planning and deconfliction and for employing military disciplines available to achieve IO effects. Intelligence is inextricably linked to facilitating core and supporting IO disciplines in offensive or defensive postures. As a product, intelligence supports IO in the same manner provided to all operations. Planning for IO cannot be conducted without intelligence on adversary information and information systems, perceptions, and critical vulnerabilities in their C2 process. Each capability used in an IO context will have separate and continuous intelligence support requirements. The psychological profiles of adversary commanders and forces are themselves an important element within the overall assessment process.

Planning

Intelligence support to IO planning is conducted as part of the IPB process. One of the key outputs from IPB is an analysis of the desired objectives and/or end states of stakeholders. These desires are usually categorized relative to broad capability. The categories may be elements of national power such as politics, economics, military, and society. Capability analysis processes within IPB also provide detail on stakeholder capacity and intent to conduct or sustain defensive and offensive IO. Intelligence support will aim to define critical nodes and vulnerabilities within the adversary's information structure; these include the key personnel, equipment, procedures and protocols involved in the transfer of information required for successful C2. Such intelligence support will orient key aspects of the operation plan towards the systematic disruption of critical nodes and information bearers. Friendly force staff advice, linked to intelligence advice on adversary COAs and CI advice on the threats to security, provide the operations planning process with the background to decide the protective measures required for own nodes and information bearers. Accurate, timely, and directed intelligence provides the foundation that IO decisions are based.

Intelligence Preparation of the Battlespace

IPB is a continuous process used to develop a detailed knowledge of the adversary's use of information and information systems. Intelligence support for IO planning builds upon traditional IPB and provides the essential basis for planning IO through the following considerations:

- The adversary commander's freedom of action and the freedom of action allowed to subordinates (decisionmaking process). This includes adversary perceptions of the situation (political, social, and cultural influences) and developments.
- Adversary IO capability, intent, morale, and vulnerability to offensive IO.
- C2 aspects such as key personnel, target audiences, headquarters, communications nodes, databases or intelligence collection systems. C2 nodes that appear in more than one adversary COA should be highlighted for targeting.
- Technical knowledge of a wide array of information, C2, intelligence, and media systems.
- Assessments of friendly vulnerability to adversary IO.

IO-Related Force Protection

Knowledge of the threat—adversaries, their intent, and capabilities—is a key consideration in the risk

management process. CI and counterreconnaissance contribute directly to force protection by denying critical information to potential adversaries. Many IO IRs require significant lead-time to develop collection sources, access, and databases. Potential intelligence collection sources should be developed as early as possible; a clear statement of MAGTF IRs is essential. IO will require development of extensive intelligence analytical products to obtain a detailed knowledge of cultural factors, and adversary use of information and information systems.

The Role of Intelligence in IO is Continual

Changes in attitudes, actions, operating patterns, and enemy information systems must be detected, analyzed, and reported to ensure that IO continues to achieve the desired operational effect. Assessing ongoing IO activities is a crucial and extremely challenging responsibility of intelligence as targets must be monitored to determine the effectiveness of the IO efforts. To achieve complete synthesis, IO must be incorporated into the MAGTF's intelligence, BDA, and targeting cycles. The impact of many IO actions may be difficult to measure. Indicators of success or failure must be carefully crafted in advance. Since IO will often not produce the same directly observable effects used for traditional BDA, IO execution will challenge the intelligence system to develop other measures of effectiveness. Once detected, these indicators should be integrated into operational planning and targeting systems, and appropriate action can be taken.

Intelligence enables the planning and execution of successful operations. MAGTF operations are characterized by unity of effort, high tempo, timely decisionmaking, rapid execution, and the relentless exploitation of opportunities. Intelligence operations must have the flexibility, agility, and sustainability to support these types of operations. Expeditionary Maneuver Warfare, as the Marine Corps' current capstone concept, lays the foundation for MAGTF operations. MAGTF operations include--

- Operational maneuver from the sea (OMFTS).
- Sustained operations ashore.
- Military operations other than war (MOOTW).
- Joint.
- Multinational.

Each operation presents unique challenges and considerations for intelligence support. Many MAGTF operations will be executed as joint operations and with allies, coalition or multinational partners. Intelligence activities in joint and multinational operations require special planning and coordination.

Required Intelligence Capabilities

As a warfighting function, intelligence applies broadly across the full range of military operations. The following required intelligence capabilities are common to all operations:

- Conduct intelligence planning and direction.
- Perform intelligence collection management.
- Process and exploit intelligence.
- Produce intelligence.
- Disseminate intelligence.
- Facilitate intelligence's use.
- Perform intelligence, surveillance, reconnaissance, and CI operations.

CHAPTER 2
COMMAND AND CONTROL

C2 aims to reduce the amount of uncertainty that commanders must accept—to a reasonable point— to make sound decisions. Intelligence is a principal component of C2. Intelligence is a process conducted specifically to aid the commander in decisionmaking by reducing this uncertainty. Intelligence operations support the commander's PDE&A cycle by helping to build situational awareness and providing insight into the nature of the problem facing the commander.

Intelligence provides knowledge concerning the environment and the enemy while furnishing an estimate of potential enemy activities. This knowledge is used by the commander to devise workable, flexible plans; make sound and timely decisions; monitor events to ensure proper execution; and modify decisions quickly in response to changing situations or to exploit fleeting opportunities.

Decisionmaking

The principal aim of C2 is to enhance the commander's ability to make sound and timely decisions. Decisionmaking is a time-competitive process that depends in part on the availability of the right elements of information at the right time and place. Without the information that provides the basis of situational awareness, no commander can make sound decisions. Intelligence operations focus on providing the right elements of information concerning the threat and the environment; i.e, intelligence, required to generate situational awareness and fuel the decisionmaking process.

Observe, Orient, Decide, and Act Loop

A simple model that is known as the observe, orient, decide, and act (OODA) loop is used to describe the C2 process. (See figure 2-1.)

The OODA loop applies to any two-sided conflict, whether combatants are individuals or large military formations. When engaged in conflict, participants—

- **Observe.** Take in information about the environment, the friendly status, and the threat.
- **Orient.** Make estimates, assumptions, analyses, and judgments about the situation to create a cohesive mental image.
- **Decide.** Determine what needs to be done, whether it is an immediate reaction or a deliberate plan.
- **Act.** Put the decision into action.

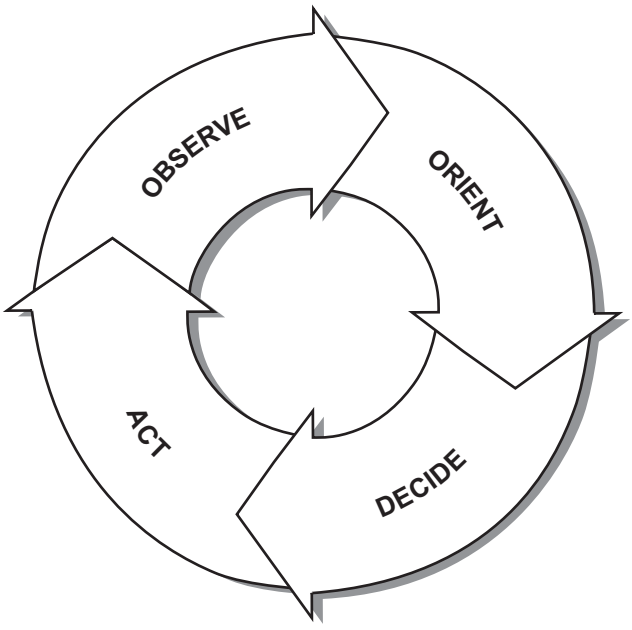


Figure 2-1. The Observe, Orient, Decide, and Act Loop.

The OODA loop reflects how decisionmaking is a continual, cyclical process. In any conflict, the participant who can consistently and effectively cycle through the OODA loop faster—who can maintain a higher tempo of action—gains an increasing advantage with each cycle. The essential lesson of the OODA loop is the importance of generating and maintaining tempo.

Intelligence and the OODA Loop

Intelligence supports all phases of the OODA loop. Intelligence operations facilitate the exercise of C2 by helping to reduce the uncertainty confronting the commander, providing a significant part of the knowledge needed to reach the decision, and assisting in monitoring the implementation and effects of that decision.

- **Observe.** Intelligence collection operations observe threat activity and current environmental conditions. All-source analysis of the collected intelligence information is provided to enhance the commander's situational awareness and understanding of the battlespace.
- **Orient.** The image of the battlespace presented by intelligence, coupled with the predictive analysis of the IPB process, helps orient the commander. It aids in comparing the current situation to the desired end state and in identifying COAs to achieve that end state.
- **Decide.** Intelligence enables decisionmaking by helping define what is operationally possible and most advantageous. It provides the framework for assessing the potential COAs against existing environmental conditions and threat capabilities, vulnerabilities, and likely responses.
- **Act.** Intelligence supports execution by providing a shared picture of the battlespace to all levels of command and by meeting the intelligence needs of all levels of commanders involved in the conduct of operations. Once the concept of operations has been formulated, the focus of intelligence activities shifts from developing the wide-scope intelligence required for COA selection to providing detailed, tailored intelligence to support mission planning and execution. Intelligence is also critical to generating and maintaining tempo in C2. During execution, supporting intelligence operations are conducted to monitor enemy reactions, protect the force from enemy counteraction, and assess the effects of ongoing operations. The continuing intelligence development effort aids the commander in effectively cycling through the OODA loop faster to gain an increasing advantage over the enemy.

Decisionmaking Approaches: Analytical and Intuitive

In analytical decisionmaking, several options for solving the problem at hand are identified, studied, and compared to arrive at the best solution. In intuitive decisionmaking, the commander assesses the situation to recognize a pattern. Once a pattern is identified, experience and judgment guide the commander in evaluating the key elements of the problem and rapidly determining a satisfactory solution. Each approach has different strengths and weaknesses; although conceptually distinct, the two are rarely mutually exclusive.

Intelligence supports analytical decisionmaking by helping to identify the options available and provide the framework (in the form of estimates and studies focused on the threat and key factors of the battlespace) for analysis and comparison of those options. Intelligence supports intuitive decisionmaking by providing the knowledge that helps the commander to recognize emerging patterns. The same methodology is used to develop intelligence support for both decisionmaking approaches. Application of that methodology will vary based on the specifics of each situation and the decisionmaking style of the supported commander. The goal remains the same: to provide a knowledge-based intelligence product that can be applied to make a sound decision.

The Planning, Decision, Execution, and Assessment Cycle

The PDE&A cycle provides a framework for implementing C2. It translates the cognitive process of the OODA loop into a concrete series of actions taken by the commander and the staff to plan and execute an operation. To be effective, intelligence operations must be linked to the commander's decisionmaking process and the resulting operational activity. Therefore, intelligence operations are integrated with the PDE&A cycle. Specific intelligence tasks are carried out to support each phase of this cycle. While the level of command, time available, and specific tactical situation will influence how the PDE&A cycle is carried out and the degree of detail applied in performing intelligence activities, the same basic intelligence development process is employed in deliberate and rapid planning scenarios and supports analytical and intuitive decisionmaking.

Intelligence support to planning begins with providing a basic description of the environmental conditions and enemy situation in the projected area of operations (AO). As plans are developed and refined, the intelligence effort becomes more narrowly focused on identifying the enemy's critical vulnerabilities and potential COAs and generating mission-specific intelligence products that support detailed planning and execution of specific operational activities. Finally, during mission execution, intelligence operations concentrate on the satisfaction of requirements linked to key operational decisions and the recognition of exploitable opportunities as they arise in the battlespace.

Intelligence Support to Planning

Planning is the process of developing practical schemes for taking future actions. It represents an effort to project operational concepts and designs forward in time and space. During the planning process, the commander assesses the situation, builds a vision of the battlespace, and develops the desired outcome of the battle or campaign. Planning is oriented on the future because the primary objective of intelligence is to reduce uncertainty about the future. Intelligence makes a critical contribution to this process. Much of the intelligence effort is "front loaded" to support planning; a substantial portion of intelligence development must be completed during this phase. Intelligence provides a comprehensive image of the battlespace and the threat and helps commanders to provide for constant or predictable aspects of the environment, come to an understanding on the general direction of future actions, and anticipate possible threat force actions and reactions.

Planning Models

The choice of planning model is made on the basis of a variety of factors, including the mission, level of command, command relationships, time available, and preferences of individual commanders. All planning models have the same basic elements in common. They—

- Determine what needs to be done.
- Identify one or more COAs to accomplish the required tasks.
- Study the COAs to test feasibility, identify support requirements, and select the most promising alternative.
- Convey instructions to subordinates to execute the plan.

Intelligence development follows the same basic process, no matter which planning model is used. While the specific steps and sequence used in planning may vary, the requirement to provide focused, continuous intelligence to shape the planning process remains constant. A generic planning model will be used to outline the baseline methodology for providing intelligence support to planning. The components of this generic

model are mission analysis, COA development, COA analysis, and plan/orders development. For a more complete discussion of planning and the planning process, see MCDP 5, Planning, and MCWP 5-1, *Marine Corps Planning Process*. (See figure 2-2.)

Mission Analysis

Mission analysis is conducted to identify the tasks required to accomplish the mission, develop baseline knowledge of the situation, and determine what additional information is required to facilitate the planning process. Intelligence supports mission analysis through providing basic intelligence on the nature of the AO and the threat. Intelligence operations are guided by the results of mission analysis: formulation of initial commander's intent, planning guidance, and PIRs.

Mission Receipt

The receipt of the mission starts the formal planning cycle. However, preliminary planning is normally conducted before the receipt of a mission to anticipate future taskings and potential actions required to accomplish those taskings. Intelligence, in performing its I&W function, will monitor a command's area of interest and identify developing crisis situations and/or potential missions. The commander uses this information to anticipate future missions and to direct the staff to accomplish preliminary planning and intelligence development before the arrival of formal mission tasking. Much of this preliminary

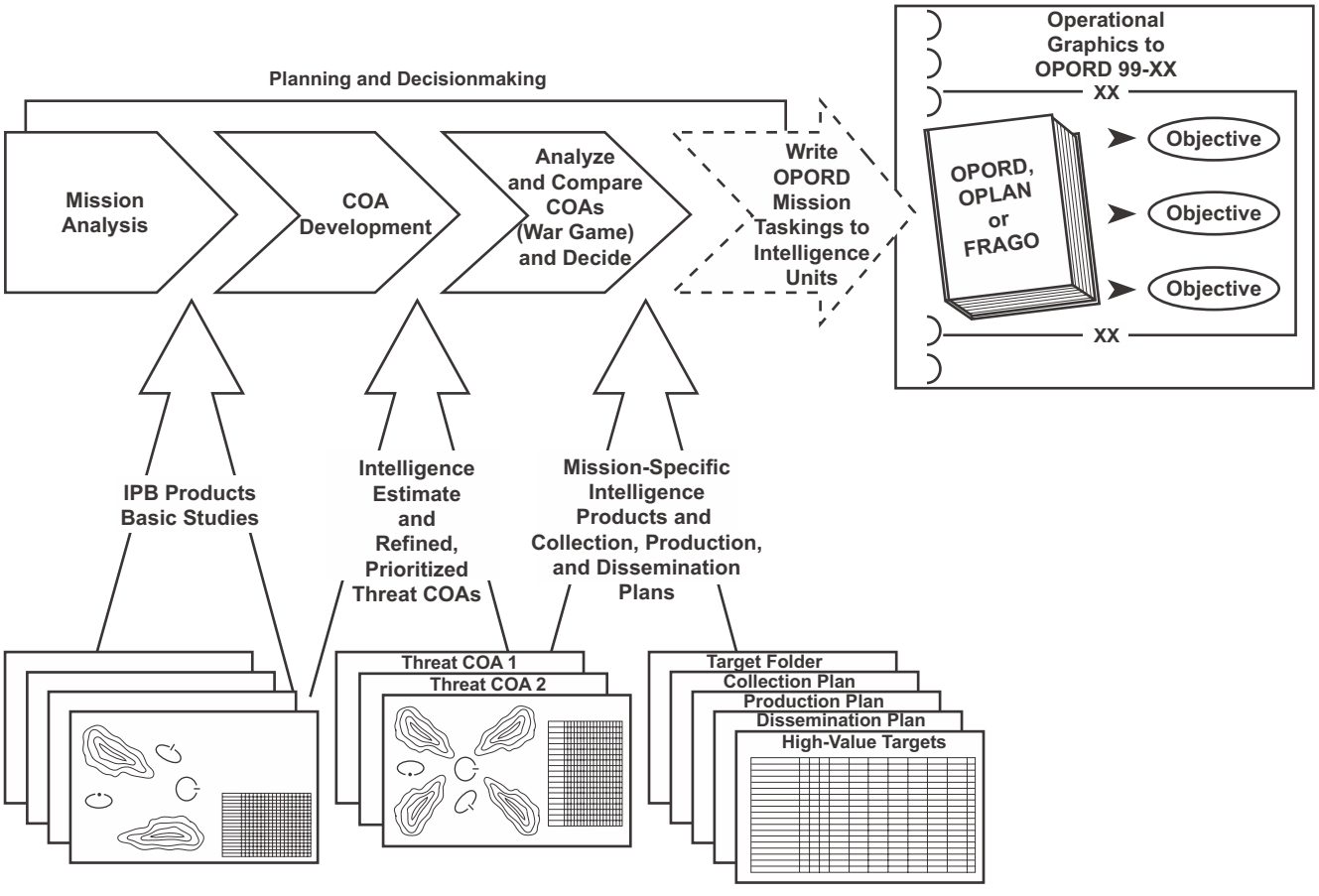


Figure 2-2. Intelligence Support to Planning.

work is carried out by the intelligence section, including collecting basic data on the threat and the environment, IPB analysis, and disseminating intelligence throughout the staff.

Information Requirements and Exchange

The process of identifying IRs and gathering and distributing information within the staff, and throughout the command, begins during preliminary planning and intensifies once the mission is received. Intelligence is provided about threat forces and the AO, focusing on the advantages and limitations presented by the environment and the strengths and critical vulnerabilities of the threat. This intelligence is disseminated through a variety of media: the distribution of basic products (maps, imagery, and threat forces studies); the conduct of orientation briefings, and IPB analysis. The continuous, interactive process of IR development also begins. Products provided by the intelligence section stimulate additional questions from the commander and members of the staff. These questions are translated into new or refined IRs. The new requirements are then used to focus the intelligence development process.

Mission Analysis

The commander makes a critical contribution to the operation during this step, setting the stage for the completion of planning and mission execution. During mission analysis, the commander and the staff draw together all available intelligence and information, focus it on the assigned mission, develop an understanding of the tasks to be accomplished, and formulate a rough concept of how to best accomplish those tasks. The result is an initial statement of commander's intent and commander's planning guidance that focuses the remainder of the planning process.

The intelligence officer is a full participant in mission analysis. During mission analysis, the intelligence officer does the following:

- Orients the commander and the other members of the staff to the battlespace and the nature of the threat.
- Aids in forming the commander's intent by helping to define what is operationally possible and most advantageous. This is accomplished primarily through IPB and the analytical process. These results identify the threat's COG, strengths, and critical vulnerabilities and indicate the potential advantages and limitations imposed by the environment.
- Receives guidance from the commander to help shape the intelligence effort. Guidance can take a variety of forms: a statement of commander's intent, a list of PIRs or direct instructions from the commander about intelligence needs or concerns.

COA Development

Building on the knowledge gained through mission analysis, the commander and staff next develop a concept for carrying out the required tasks that embodies the commander's intent and planning guidance. This concept (or COA) encompasses general schemes for the execution of maneuver, fires, logistics, and other supporting functions necessary for successful implementation of the basic concept.

When time permits, the staff usually develops several COAs on the basis of the commander's intent and planning guidance. Intelligence supports this process by the following:

- Continuously updating the view of the battlespace.
- Defining operational possibilities through the IPB process.
- Identifying intelligence gaps that cannot be filled by organic collection assets.
- Providing the focus on the enemy through identifying the threat's COG, critical vulnerabilities, and potential COAs, emphasizing the most likely and most dangerous of these COAs.
- Ensuring that the commander and staff receive, understand, and use relevant, focused, knowledge-based intelligence that enhances their understanding of the situation, rather than a stream of unfocused information.

The intelligence officer interacts with the staff throughout the COA development process, integrating continuing intelligence development efforts with the potential COAs in an effort to ensure that intelligence will be available to support any COA selected.

When an intuitive approach is used, intelligence helps the commander recognize emerging patterns, identify a workable solution, and rapidly evaluate that solution. Products developed through the IPB process present intelligence in the form of images that permit decisionmakers to quickly visualize the situation, see patterns, and assess potential alternatives.

COA War Game

After COAs are developed, they are analyzed and compared to identify the best COA and the concept of operations to implement that COA. Time permitting, the staff conducts a detailed analysis of each COA; each principal staff officer prepares a formal estimate of supportability. When possible, COAs should be wargamed to predict the action, reaction, and counterreaction dynamics of each COA.

Intelligence assists COA analysis by the following:

- Identifying and refining threat COAs and actions/reactions to friendly COAs under consideration.
- Playing the role of the enemy in the wargaming process.
- Developing an independent evaluation of each friendly COA based on an understanding of the environment and the potential threat response and the ability to provide intelligence support to that COA.
- Helping to focus the staff on the factors of the environment and the enemy, emphasizing the degree of uncertainty and resulting risk associated with each COA.

The intelligence officer's full participation is crucial to successful COA analysis. It is during this step that the full implications of the intelligence estimate are absorbed and applied. To maximize this contribution, the intelligence officer must be able to "think red"—analyze the situation from the enemy's perspective—and "think blue"—understand the intent and construct of friendly plans and operations. Combining these two perspectives enables the intelligence officer to assess the potential effects of threat force actions on the potential COAs.

When time is not available to wargame and conduct a complete COA analysis, the commander makes a rapid mental assessment of available options. The situational awareness that is provided in large part through intelligence guides the commander in evaluating these options and quickly selecting one that offers potential for success.

Orders Development

Based on the COA analysis, the commander selects a COA, refines the intent, and gives further guidance on developing the detailed concept of operations and supporting plans or orders. The emphasis of the intelligence effort, which is focused on the commander's intent, the selected COA, and the identified PIRs, shifts from developing basic and broad-scope intelligence in support of conceptual planning to providing specific intelligence that facilitates functional planning, detailed planning, and mission execution. The intelligence tasks of I&W and supporting the commander's estimate continue, but situation development, support to targeting, and support to force protection now receive increased emphasis.

A concept of intelligence support is prepared to allocate intelligence resources in accordance with the main effort and the concept of operations. COA analysis and wargaming results are used to develop and implement collection, production, and dissemination plans to support the chosen COA. IPB efforts are intensified in an effort to satisfy PIRs and develop the in-depth intelligence required for the detailed planning of specific operational activities. Intelligence sections prepare and disseminate products that embody

the results of the IPB process and intelligence collection activities to provide a shared view of the battlespace at all levels of the force. At the same time, they deliver mission-specific intelligence in response to the extensive and precise functional and detailed planning requirements of units that will execute the operation. CI plans and measures are prepared and implemented to conceal our intentions and protect the force. Results of these intelligence activities shape and develop the overall plan/order and the plan's comprehensive supporting annexes and appendices.

Execution

During execution, the plan is refined, implemented, and adapted in response to changes in the situation and action/reaction of the enemy. C2 is a process that generates swift, appropriate, and decisive action and provides a means of continuously assessing developments that provide the basis for adapting. The commander uses a variety of techniques and measures to supervise, monitor, and modify the execution of the plan, thereby shaping the battle and maintaining unity of effort. The intelligence effort must be responsive to the needs of mission execution and ensure a continuous flow of intelligence throughout the force to maintain a shared picture of the battlespace and satisfy new requirements developed by the operating forces.

Intelligence operations are integrated with the concept of operations to enhance force protection, develop situational awareness, and support combat assessment. The results of these operations are used to modify the plan or exercise tactical options, thereby enabling rapid decisionmaking as well as generating and maintaining tempo. The information developed through these activities is entered into the continuous intelligence development process, which provides the basis for planning future operations.

Intelligence support to execution differs in significant ways from intelligence support to planning. First, while intelligence support to planning requires developing a large volume of basic intelligence and preparing broad-scope estimates to develop and analyze COAs, intelligence support to execution involves the satisfaction of a much larger body of IRs in a significantly greater degree of detail. For example, during COA development, it may be sufficient to tell a MAGTF or ground combat element (GCE) commander that an enemy mechanized force is located in a general area and has an approximate number of tanks and armored personnel carriers of various types. However, the subordinate unit tasked with establishing a blocking position opposite that enemy force will require more detailed information on enemy disposition. In another example, the nature of the intelligence required by a Marine Expeditionary Unit (MEU) commander to decide if a raid or tactical recovery of aircraft and personnel (TRAP) mission is feasible is fundamentally different from the type and detail of intelligence required by the raid or TRAP personnel force commander who will execute that mission.

A second major difference between intelligence support to planning and intelligence support to execution is the time available for developing the intelligence product. Often days, weeks, and sometimes months are available to provide intelligence support to planning, but intelligence support to execution must normally be developed in hours, minutes or even seconds. Success in execution often depends on the ability to provide immediate answers to critical questions concerning threat force dispositions, actions, and intentions.

Finally, the uncertainty and disorder that are inherent in the nature of war manifest themselves primarily during execution. Once execution begins, interaction between the opposing wills of friendly and enemy forces normally causes significant and fundamental changes in

the situation. Discerning environmental conditions and enemy capabilities and intentions becomes increasingly difficult once these forces are set in motion. Yet it is at precisely this time that commanders require detailed and accurate intelligence to help cope with the uncertainty.

The combined factors of the extensive nature of the IRs, the degree of detail required, the limited time available, and the uncertainty inherent during execution make providing intelligence support to execution the most significant intelligence challenge. Intelligence operations must be prepared to meet this challenge and to provide the flexibility and agility required to deliver continuous situational awareness, identify opportunities, and facilitate rapid decisionmaking.

Intelligence support during execution focuses on providing the commander with practical knowledge that gives an exploitable advantage over the enemy. Although eliminating uncertainty during execution is impossible, focused intelligence operations can reduce uncertainty by providing situational awareness and identifying opportunities as they present themselves in the battlespace. Intelligence provides I&W of new or unexpected enemy activities, enhances efforts to engage the enemy through support to targeting, assists in protecting the force through CI measures and operations, and supports the planning of future operations by providing timely and accurate BDA. Three key factors for ensuring effective intelligence support during execution are resource allocation, linkage to operations, and generation of tempo.

Resource Allocation

Since IRs will always exceed available intelligence resources, intelligence operations must focus where they can have the greatest effect. A detailed and well-thought-out concept of intelligence support, developed in accordance with the commander's intent and concept of operations, will provide an appropriate allocation of intelligence capabilities between the main effort and supporting efforts. It is particularly important that Marine Corps forces (MARFOR), MAGTF, and major subordinate commands (MSCs) who control the tasking of intelligence units and capabilities provide access to critical intelligence resources for their subordinate elements. Those intelligence resources best suited to satisfying current, tactical, mission-specific IRs, such as unmanned aerial vehicles (UAVs) or terrain analysts, should be allocated to units responsible for executing the mission.

Linkage to Operations

To provide effective support to execution, intelligence operations must be linked to planned and ongoing operational activity. Intelligence operations are conducted based on the results of the IPB process, wargaming, and the planning process. Collection, production, and dissemination plans are developed to support execution of specific tactical options, engagement of targets, and selecting branches and sequels to the operation plan. Intelligence personnel must have continuous awareness of planned and ongoing operations to monitor potential enemy reactions, identify new opportunities, and assess the effects of actions on the enemy. Close and continuous synchronization of intelligence activities and operations is essential to developing timely, tailored, and relevant intelligence that facilitates rapid decisionmaking and exploitating opportunities in the battlespace.

Generation of Tempo

Intelligence operations during execution must facilitate the generation of tempo. First, intelligence operations generate tempo through prioritization. By focusing intelligence operations on satisfying PIRs and supporting the main effort, intelligence is developed that is directly linked to the commander's intent and C2 effort. Next, intelligence facilitates tempo by supporting the decisionmaking process. Intelligence that provides situational awareness and the ability to recognize emerging patterns enables the commander to employ intuitive decisionmaking to make rapid

decisions that help generate tempo. Finally, intelligence facilitates tempo by providing knowledge—key elements of data and information that have been analyzed, synthesized, and placed in context to help provide situational awareness—not just a mass of unprocessed information or unrelated pieces of data. The critical factor is not the amount of information provided, but key, focused intelligence that is available when needed and in a useful form that improves the commander's knowledge of the hostile situation and his ability to act. Intelligence operations must have the flexibility, agility, and responsiveness to rapidly collect and process relevant information, develop a focused product, and deliver that product to the affected commander in an easily understandable form and in time for the commander to take appropriate action.

CHAPTER 3
DEVELOPING INTELLIGENCE

Intelligence is developed through the use of the intelligence cycle. This process consists of a sequence of related activities that translate requirements for various types of information into intelligence that is furnished to the commander for use in the decisionmaking cycle. During this sequence, intelligence needs are identified; a *plan* is formulated and *directions* are given for satisfying those needs, data is *collected, processed, and exploited* for usable information that is then transformed into a tailored, useful intelligence product that is *disseminated* to and *utilized* by the appropriate commander or unit. This process is called the intelligence cycle. At the same time, a parallel process is used to develop CI plans and measures that deny information to an adversary to protect our forces and help ensure the effectiveness of our operations.

Figure 3-1 shows the six steps of the Marine Corps intelligence cycle. These steps define a sequential and interdependent process for the development of intelligence. Intelligence operations are conducted within the framework of the intelligence cycle; the entire cycle or a specific step within the cycle may be the focus of a particular intelligence activity. Moreover, *all* intelligence, regardless of the scope of the requirement or level of command, is developed by following these steps. (See figures 3-2 and 3-3, page 3-2.)

No single phase of the cycle is more important than the others. All of the phases are interdependent. Without proper direction, the other phases will not focus on the correct objectives. Without effective collection, there may be too much or too little information and what information there is may prove to be irrelevant. Without processing and production, there is a mass of random data instead of the knowledge needed for the planning and execution of operations. Intelligence is meaningless unless it reaches the right people in time to affect the decisionmaking process and in an understandable form.

An understanding of the process used to develop intelligence is critical to the execution of successful intelligence operations. All personnel involved in the *development* and *use* of intelligence must be aware of their role in the process. They must understand the relationship between the steps in the process to ensure that intelligence focuses on the mission and facilitates rapid decisionmaking in

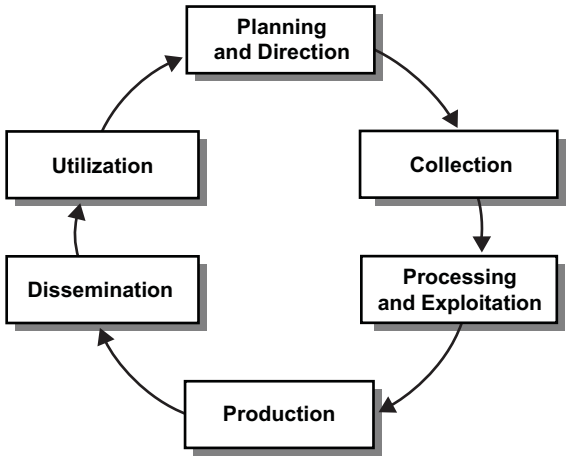


Figure 3-1. The Marine Corps Intelligence Cycle.

the execution of successful combat operations. (See figure 3-4.)

The Intelligence Cycle — Macro View

During a routine review of the situation in the Marine Expeditionary Force's (MEF's) area of interest, the G-2 notes that a recent change in government in one of the countries has created the potential for instability over the next year. The G-2 directs the development of an intelligence estimate to support potential contingency operations in this country. Working with the Marine Corps force G-2 section and the pertinent combatant command's joint intelligence center, the MEF collections section submits requests for imagery intelligence (IMINT), signals intelligence (SIGINT), and HUMINT support. As information is received, the MEF G-2 section's all-source fusion platoon (AFP), with the assistance of the topographic platoon, the imagery intelligence platoon (IIP), and the radio battalion, processes and exploits the information to produce the estimate and supporting studies. The estimate is completed within a month. The G-2 directs that copies be forwarded to all major subordinate commands (MSCs) and staff sections, with priority to the forward-deployed MEU. The G-2 also recommends to the commanding general that the scenario for the MEF's upcoming command post (CP) exercise be based on this estimate to introduce MEF personnel to this contingency area, identify planning requirements, and develop potential COAs. The MEF G-2 has *directed* the development of a comprehensive intelligence product that is focused on an operational requirement. Extensive organic capabilities as well as external resources were integrated to *collect* data, *process* it into information, and *produce* the finished intelligence. The product was then *disseminated* to and *utilized* by the units and staff sections with contingency responsibility for the identified area. The intelligence formulated focuses on the mission and facilitates rapid decisionmaking in the execution of successful combat operations.

Figure 3-2. The Intelligence Cycle—Macro View.

Intelligence Requirements

An intelligence requirement (IR) is a requirement for intelligence to fill a gap in the command's knowledge and understanding of the battlespace or enemy forces. (JP 1-02)

IRs *drive* the intelligence cycle. Properly articulated, mission-oriented requirements focus the intelligence effort and provide the foundation for successful intelligence operations.

The Intelligence Cycle—Micro View

The regiment S-2 section receives a report from one of their reconnaissance teams that an enemy artillery battery has just passed their observation post (OP) and turned off the road. Knowing that enemy artillery is the top targeting priority, the intelligence watch immediately begins developing the target. The S-2 chief checks the map and notes that there are three potential firing positions (identified through the IPB process) close to, but out of visual range of, the reconnaissance OP. The S-2 chief also knows that UAVs are in direct support of the regiment at this time. The S-2 chief alerts the fire support coordination center (FSCC) concerning the potential target and works with the FSCC and air officer to divert an ongoing UAV mission to search the potential firing positions. The UAV quickly locates the enemy artillery in the second firing position. The S-2 chief confirms that the enemy weapons can range friendly positions and, based on their observed activity, are preparing to attack. Using this intelligence, the FSCC coordinates a counterfire mission against the enemy artillery. The S-2 chief successfully executed the intelligence cycle in a matter of minutes. He understood the requirement to develop targeting information, directed the *collection* of information, *processed* the information and *produced* the desired intelligence, that is, a target, and *disseminated* that target to the FSCC, who *utilized* that intelligence to engage the target.

Figure 3-3. The Intelligence Cycle—Micro View.

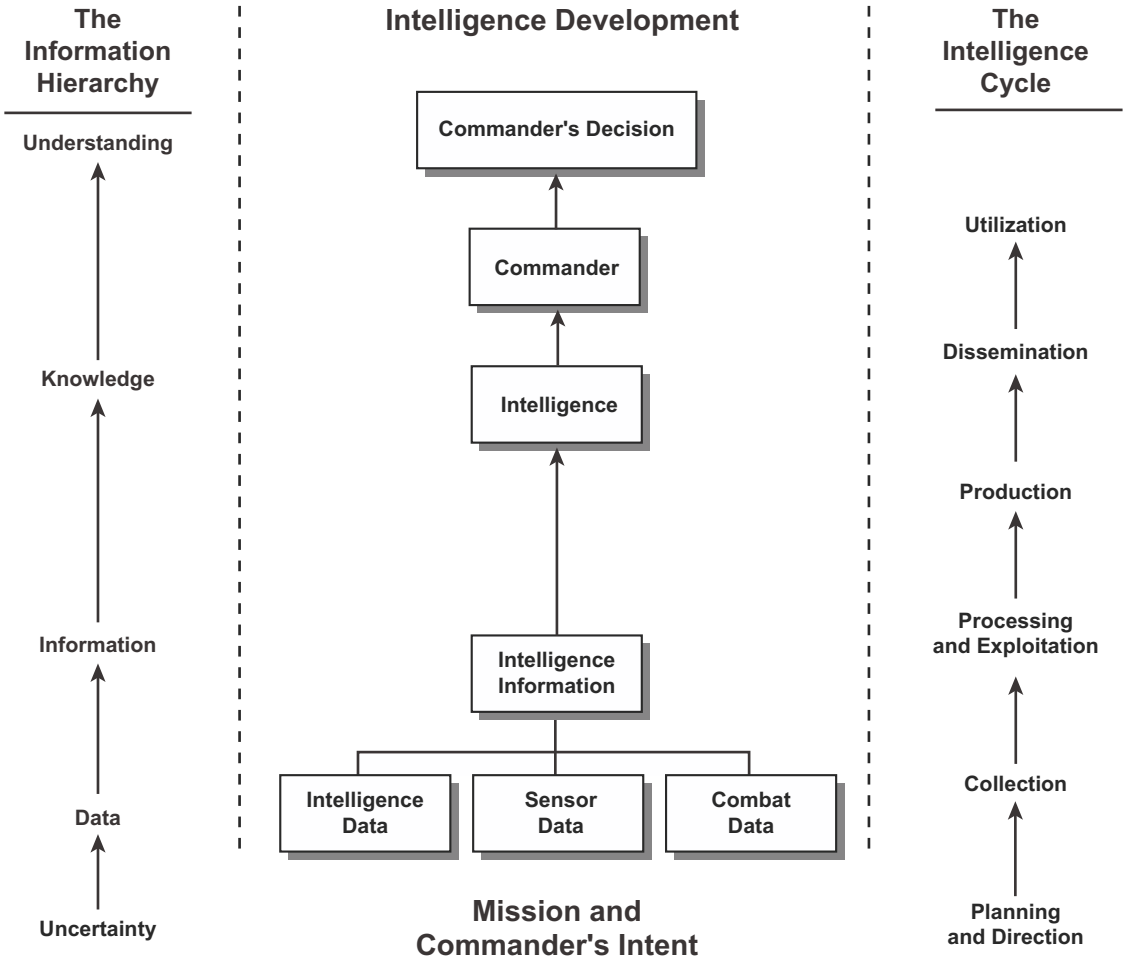


Figure 3-4. Intelligence Development and the Intelligence Cycle.

An IR is a missing piece of information about the enemy or environment that a commander needs to know to make a sound decision. In its simplest form, an IR is a question about the threat or the battlespace, the answer to which is required for the planning and execution of an operation. Examples follow:

- Will the highway bridge support assault amphibious vehicles?
- Will weather conditions interfere with planned air operations?
- Are port facilities and conditions suitable for a maritime prepositioning force pierside offload?
- Can the enemy air defense system threaten low-flying helicopters?
- What is the reaction time of the enemy garrison located south of the amphibious objective area?

Requirements fall into two categories: IRs and PIRs. PIRs and IRs replace the terms essential elements of information and IRs.

Priority Intelligence Requirement

A PIR is an intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. (MCDP 2)

IRs cover the entire spectrum of information that is needed concerning the battlespace and the threat. The scarce intelligence assets and limited time available will rarely permit the satisfaction of all of a command's IRs; thus, it is important to focus the intelligence effort on those requirements that are critical to mission success. These critical IRs are designated as PIRs. PIRs are the subset of the CCIRs that focus on the threat and the environment. CCIRs are intelligence and information requirements the satisfaction of which the commander deems critical to decisionmaking and mission success. PIRs are linked to specific decisions and, in effect, constitute the commander's guidance for intelligence. Notional PIRs follow:

- What size force is defending amphibious force objective B?
- Which bridges over the Sand River are intact?
- Will the enemy use chemical weapons against the beach support area on D-day?

There is no standard list or set rule for determining PIRs. Each tactical situation poses distinct problems and specific gaps in intelligence. However, the commander will often have PIRs that concern the most likely enemy COA, the most dangerous enemy COA, and critical enemy vulnerabilities that can be exploited.

Characteristics

PIRs and IRs have the following characteristics. Each PIR or IR—

- Asks only one question.
- Focuses on specific facts, events or activities concerning the enemy or the battlespace.
- Is tied to mission planning, decisionmaking, and execution.
- Provides a clear, concise statement of what intelligence is required.
- Contains geographic and time elements to limit the scope of the requirement.

Requirements may be simple or complex. It is important to understand that the nature and scope of PIRs and IRs will vary with the mission and the level of command, and on the particular phase in the PDE&A cycle. Requirements will generally become more focused as the intelligence cycle is executed. During execution, the intelligence effort should be directed against a small number of PIRs that are closely linked to the concept of operations.

Planning and Direction

The planning and direction phase of the intelligence cycle consists of those activities that identify pertinent IRs and provide the means for satisfying those requirements. (See figure 3-5.) Intelligence planning and direction is a continuous function and a command responsibility. The commander directs the intelligence effort. The intelligence officer manages this effort for the commander based on the intent, designation of PIRs, and specific guidance provided during the planning process.

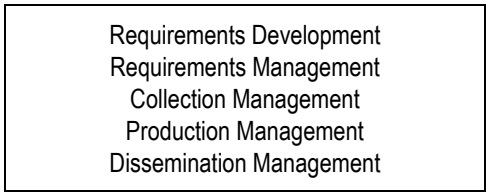


Figure 3-5. Planning and Direction Phase Functions.

Requirements Development

Identification of Requirements

Concise, mission-oriented IRs provide clear direction to the intelligence effort. The entire staff and all subordinate commanders play a role in developing the command's IRs. The intelligence officer formulates most of the initial requirements by using the original mission

tasking together with knowledge of the threat, familiarity with the operating area, and experience derived from participation in the commander's decisionmaking process to anticipate the majority of the basic intelligence needs. As the planning process continues, the commander, other staff officers, and subordinate commands expand on previously identified requirements and develop new ones. Requirements are generally linked to proposed COAs or potential decisions. The intelligence officer records, collates, and refines these requirements as they are identified and maintains a consolidated list of requirements.

Designation of PIRs

The commander makes a critical contribution to the intelligence effort by designating the PIRs. As COAs and supporting information requirements are developed, the satisfaction of certain IRs will be essential to mission success. The identification of these "show stoppers" forms the basis for designating PIRs. The intelligence officer, with input from other members of the staff, draws up a recommended list of PIRs. PIRs will be listed in priority order relative to their importance to mission accomplishment. In forming this list, the G-2/S-2 considers the requirements of his own command, subordinate commands, adjacent commands, and any direction received from higher headquarters. Recommendations are submitted to the commander who reviews, refines, and approves the command's PIRs. In designating PIRs, the commander establishes the following:

- What he wants to know (intelligence required).
- Why he wants it (linked to operational decisionmaking).
- When he needs it (latest time that the information will be of value).
- How he wants it (format, method of delivery).

Once approved and distributed, PIRs constitute the core of the commander's guidance for the intelligence process.

Requirements Management

Management of IRs is a dynamic process that encompasses the continuous evaluation of the following:

- Importance of each requirement to mission success.
- Information and assets needed to satisfy each requirement.
- Resources that are presently committed toward fulfilling that requirement.
- Degree that the requirement has been satisfied by completed intelligence activities.

Processing Requirements

Developing requirements and designating PIRs are not one-time efforts. There is a dynamic flow of new requirements, existing requirements are satisfied or no longer relevant, and the relative importance of each requirement changes as the PDE&A cycle progresses. (See figure 3-6.) As requirements are developed, the intelligence officer validates, refines, and enters them into the management system.

Validation ensures that the requirement is relevant to the mission, has not already been satisfied, and does not duplicate other requirements.

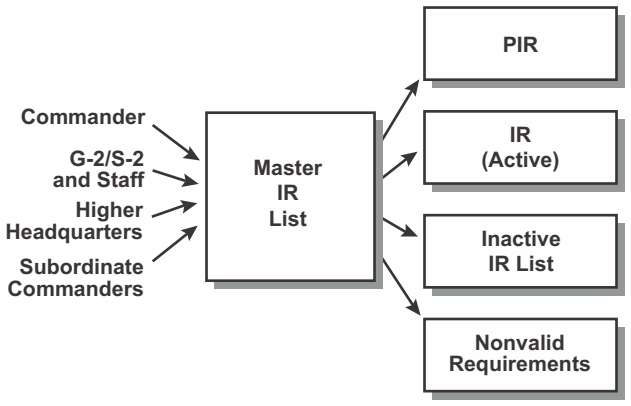


Figure 3-6. Intelligence Requirements Management.

Refining the requirement entails placing it in the proper format, identifying all information components related to the requirement, and adding appropriate qualifiers such as geographic limitations or time constraints. During refinement, similar or related requirements may be combined into a single, comprehensive requirement.

A requirements management system is an essential tool that provides a means to monitor the effort to satisfy each requirement. Each intelligence section must develop a system appropriate to its mission and echelon. Minimal components of any system are a numbering system, identification of who submitted the requirement, designation of collection and production resources committed to satisfying the requirement (or noting when it was submitted to higher headquarters or supporting forces, if organic assets are not available), timeliness requirements, dissemination instructions and information, and a mechanism to ensure user satisfaction.

Determining Priorities

The intelligence officer must continually reassess the emphasis given to each requirement and realign the priorities according to commander's intent and the current phase of the PDE&A cycle. The intelligence officer must also periodically confirm assignment of priorities with the commander to ensure that the intelligence effort is focused in accordance with the commander's desires.

Requirements Satisfaction

Once a requirement has been identified, validated, refined, and prioritized, the intelligence officer must determine how to satisfy the requirement and, if it can be satisfied by organic assets, allocate the appropriate intelligence assets to develop the desired intelligence. If the requirement cannot be satisfied by organic assets, it must be submitted to higher headquarters or supporting forces/agencies for satisfaction. In determining how to satisfy a requirement, the intelligence officer must consider each step in the intelligence cycle to ensure that the plan encompasses the entire process from collection through utilization. The intelligence officer must identify the information needed, where and how to get it, how to package the intelligence into an appropriate product, and how to deliver that product. Normally, an IR will generate a requirement to do the following:

- Collect data or information.
- Process and produce intelligence in the scope and form that answers the question.
- Disseminate the information to a particular user by a specific time. (See figure 3-7.)

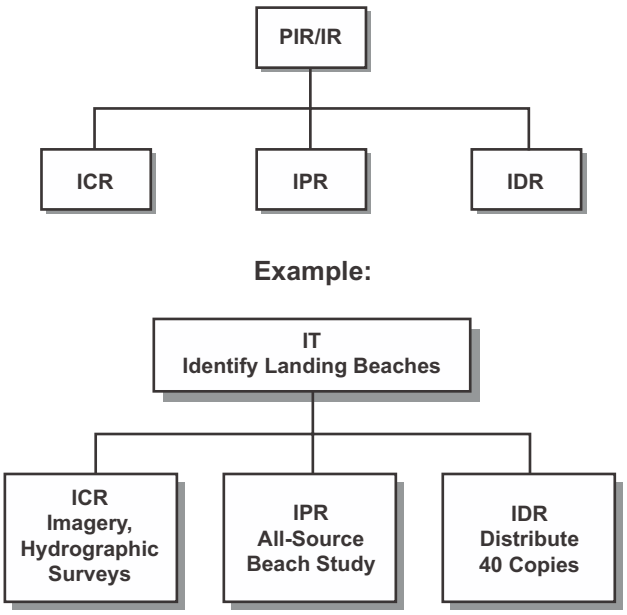


Figure 3-7. Requirements Satisfaction.

Directing the Intelligence Effort

Intelligence direction consists of the requirements development and management process described above combined with the associated functions of collection management, production management, and dissemination management. Because the possible questions about the enemy and the AO are practically infinite but intelligence assets are limited, the intelligence effort must be managed at each step in the process. Management of requirements, collection, production, and dissemination ensures that the effort is focused on the PIRs and delivers knowledge that facilitates sound tactical decisionmaking.

Collection Management

Collection management is the process of converting IRs into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. Its purpose is to conduct an effective effort to collect all necessary data while ensuring the efficient use of limited and valuable collection assets.

Production Management

Production management encompasses determining the scope, content, and format of each product; developing a plan and schedule for the development of each product; assigning priorities among the various intelligence production requirements; allocating processing, exploitation, and production resources; and integrating production efforts with collection and dissemination. As with collection management, the goal is to make effective and efficient use of limited resources and ensure that the production effort is properly focused on established priorities.

Dissemination Management

Dissemination management involves establishing dissemination priorities, selecting dissemination means, and monitoring the flow of intelligence throughout the command. Its objective is to deliver the required intelligence to the appropriate user in the proper form at the right time while ensuring that individual consumers and the dissemination system are not overloaded by attempting to move unneeded or irrelevant information. Dissemination management also provides for use of security controls that do not impede the timely delivery or subsequent use of intelligence while protecting intelligence sources and methods.

Planning the Intelligence Support System

This activity includes designing and establishing the structure that is necessary to provide intelligence support throughout the course of an operation. The intelligence officer looks at the entire body of IRs rather than at individual IRs or PIRs. The intelligence officer anticipates the continuing intelligence needs of the force as it carries out its mission and designs an intelligence support system that has the capability, flexibility, and redundancy to satisfy these needs. After the support system concept is developed, the resources needed to build the system are identified, requested, and acquired. Factors taken into consideration during this effort follow:

- Task organization of intelligence units.
- Identification of personnel and equipment requirements.
- Requirement for liaison teams.
- Connectivity with national, theater, joint, and multinational force intelligence assets.
- Communications and information systems (CIS) requirements.
- Logistic requirements.
- The need for specialized capabilities; e.g., linguists.

Collection

Collection is the gathering of intelligence data and information to satisfy the identified requirements. The collection phase encompasses assembling relevant information from sources that are already on hand or available from other intelligence organizations: intelligence databases, studies, maps, and a workbook or situation map. Collection consists of the activities of organic, attached, and supporting intelligence collection assets to gather new data and deliver it to the appropriate processing or production agency; i.e., the execution of collection operations. Functions carried out during the execution of collection operations follow:

- Mission planning.
- Positioning of assets to locations that are favorable to satisfying collection objectives.

- Data collection.
- Reporting.
- Supervision of individual collection missions.

Intelligence data and information are collected by a variety of intelligence assets, each with unique capabilities and limitations. (See figure 3-8.)

Radio Battalion
Force Reconnaissance Company
Marine Tactical Electronic Warfare Squadron (VMAQ)
Marine UAV Squadron (VMU)
Ground Sensor Platoon (GSP)
Division Reconnaissance Battalion
CI/HUMINT Company
Light Armored Reconnaissance Battalion

Figure 3-8. MAGTF Primary Organic Collection Assets.

The value of a collection source is not necessarily related to the sophistication or cost of that source, but rather to its ability to gather pertinent data from the collection target—the enemy or environmental consideration that is the subject of the particular intelligence collection requirement. Successful intelligence operations require access to data from all types of collection resources: organic, joint, national, and multinational. Collection operations are executed to gather data from all suitable and capable assets, balancing the capabilities of one type of collector against the limitations of another to provide "all-source" data input to the processing and exploitation and production phases. The primary types of intelligence data used to produce tactical intelligence are described in the following paragraphs.

Imagery Intelligence

Imagery intelligence is intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. (JP 1-02)

Principal sources of imagery are national overhead reconnaissance systems; manned aircraft such as the F-14 or F/A-18 with the Advanced Tactical Airborne Reconnaissance System, the U-2 or the Joint Surveillance Target Attack Radar System; and UAVs. IMINT provides concrete, detailed, and precise information on the location and physical characteristics of the environment and the threat. It is the primary source of information concerning key terrain features, installations, and infrastructure used to build detailed intelligence studies and target materials. The main limitation of IMINT is the time required to task, collect, process, and analyze the imagery. Detailed planning and coordination is required to ensure that the results of imagery collection missions are received in time to affect the decisionmaking process. Imagery operations can be hampered by weather, the enemy's air defense capability, and his camouflage, cover, and deception activities.

Signals Intelligence

SIGINT is intelligence information derived from the interception, processing, and analysis of foreign communications, noncommunications electronic emissions, and instrumentation signals. SIGINT is provided by the radio battalion; the Marine tactical electronic warfare squadron; and an integrated network of national, theater, and joint force SIGINT support agencies. SIGINT provides timely and accurate data on enemy forces that may include details on enemy composition, identification, and location. It can also give insight into the enemy's current status and activities and future intentions. SIGINT is one of the primary means for providing I&W of enemy actions. It is also a principal contributor to intelligence support to IO through its analysis and exploitation of the enemy's C2 system. Principal limitations of SIGINT are that the enemy must transmit signals that can be exploited and that

collection assets must be capable of intercepting and positioned to intercept those signals.

Human Intelligence

HUMINT is a category of intelligence derived from information collected and provided by human sources. (JP 1-02)

HUMINT operations cover a wide range of activities, including reconnaissance patrols, aircrew reports and debriefs, debriefing of refugees, and interrogations of enemy prisoners of war. Principal dedicated HUMINT resources are ground reconnaissance units; the CI and interrogator-translator assets of the MEF CI/HUMINT company; and national, theater, and other Service HUMINT elements. All Marines participating in an operation can obtain significant information about the threat and environment. Intelligence operations must aggressively employ Marines as HUMINT sources by teaching them the importance of observing and reporting.

HUMINT can provide insight into intangible factors such as tactics, training, morale, and combat effectiveness that cannot be collected by technical means and offers the best potential source to discern future plans and intentions. HUMINT is particularly important in MOOTW, in which the nature of the mission and of the threat generally provide a lucrative environment for HUMINT operations.

HUMINT has two main limitations as follows:

- HUMINT operations generally require placing humans at risk to gain access to their targets. For that reason, IRs should be satisfied through technical collection means, if possible, before considering the use of human resources.
- HUMINT responsiveness can be limited in certain circumstances because of the time it takes to plan the activities, position the assets, collect the data from what are often hostile or noncooperative sources, and report the information to exploitation and production centers, which are often located a significant distance from the collection site.

Measurement and Signature Intelligence

Measurement and signature intelligence (MASINT) is intelligence information gathered by technical instruments such as radars, passive electro-optical sensors, radiation detectors, and remote ground sensors. Although the primary tactical application of these devices is to collect sensor data, which is generally provided directly to operations centers for immediate decisionmaking, the data collected can also provide significant intelligence information on enemy movements and activities. Key MAGTF MASINT capabilities are remote ground sensors, weapons locating radars, and air surveillance radars. These sensors provide an efficient means to maintain surveillance over large portions of the battlespace. Their limitations include the logistic support required to maintain the equipment, the requirement to place the sensors in proximity to the surveillance area, and the exploitable electronic signatures associated with some of the sensors.

Open-Source Intelligence

Open-source intelligence (OSINT) is information of potential intelligence value that is available to the general public. (JP 1-02)

OSINT sources include books, magazines, newspapers, maps, commercial electronic networks and databases, and radio and television broadcasts. OSINT involves no information that is classified at its origin or acquired through controlled collection. National and theater intelligence production centers have access to a range of OSINT sources. MAGTF intelligence agencies can receive OSINT through these centers in addition to collecting information from open sources that are available in the AO. OSINT can be a valuable source of geographic, political, economic, sociological, and cultural information, particularly in security, humanitarian assistance or peace operations. In multinational operations, OSINT provides intelligence that can be readily shared with members of a multinational force. However, the sources of OSINT should be carefully evaluated to determine the accuracy and reliability of the information provided.

Counterintelligence

CI is the intelligence function concerned with identifying and counteracting the threat posed by foreign intelligence capabilities and by organizations or individuals engaged in espionage, sabotage, subversion or terrorism. The principal objective of CI is to assist with protecting DOD personnel, family members, resources, facilities, and critical infrastructure. CI provides critical intelligence support to command force protection efforts by helping identify potential threats, threat capabilities, and planned intentions to friendly operations while helping deceive the adversary as to friendly capabilities, vulnerabilities, and intentions. CI increases uncertainty for the enemy, thereby making a significant contribution to the success of friendly operations. CI also identifies friendly vulnerabilities, evaluates security measures, and assists with implementing appropriate security plans. The integration of other intelligence disciplines, CI, and operations culminates in a cohesive unit force protection program.

Processing and Exploitation

Processing and exploitation involves the conversion of collected data into information that is suitable for the production of intelligence. Processing is largely a technical function that does not add meaning to the data but that is necessary to convert the data into a form that people can understand. Examples of processing include developing a piece of film, translating a document or communications intercept from a foreign language or converting electronic data into a standardized report that can be analyzed by a system operator. Some types of data require minimal processing. They may be collected in a form that is already suitable for production. Processing may also take place automatically during collection. Other types of data require extensive processing, which can affect the timeliness and accuracy of the resulting information.

Data may be further exploited to gain the fullest possible advantage. For example, an aerial photograph or a frame of UAV video may be exploited by imagery interpreters to identify specific pieces of equipment or measure the dimensions of structures found on that image. When resources are required to accomplish the processing and exploitation phase, it is crucial that processing requirements be prioritized and managed according to the PIRs to ensure that critical information is extracted first.

Production

Production is the activity that converts information into intelligence. It involves the evaluation, interpretation, integration, analysis, and synthesis of all information that is relevant to a particular IR to answer the question that has been asked. Production fuses new information and existing intelligence from all sources to provide meaningful knowledge that can be applied to the decisionmaking process. During the production phase, information is—

- Evaluated to determine pertinence, reliability, and accuracy.
- Analyzed to isolate significant elements.
- Integrated with other relevant information and previously developed intelligence.
- Interpreted to form logical conclusions that bears on the situation and supports the commander's decisionmaking process.
- Applied to estimate possible outcomes.
- Placed into the product format that will be most useful to its eventual user.

Intelligence Preparation of the Battlespace

IPB is the primary analytical methodology used to produce intelligence in support of the decisionmaking process. It furnishes a framework for integrating intelligence and operations throughout the PDE&A cycle. IPB is a systematic, continuous, mission-focused process of analyzing the

environment and the threat in a specific geographic area. (See figure 3-9.)

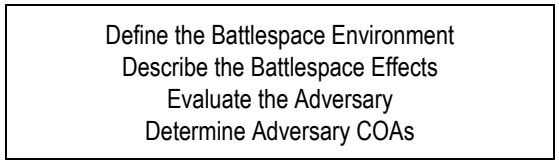


Figure 3-9. Intelligence Preparation of the Battlespace.

IPB provides a means to interpret information and understand the battlespace that can be applied in any operational situation. Through the IPB process, information that has been collected and processed is analyzed, synthesized, and used to estimate possible outcomes that can affect mission accomplishment. The result is knowledge-based intelligence that is incorporated into a variety of intelligence products.

Although IPB is fundamentally an intelligence process, successful application of the process to support planning and execution depends on the participation of the commander and the entire staff. The commander is responsible for intelligence production and IPB. The commander focuses the IPB effort by defining the area and key factors to be studied. The commander's guidance and the complete involvement of the staff are necessary to ensure that the IPB effort encompasses aspects of concern for all warfighting functions and provides detailed and accurate intelligence for COA development and detailed planning. Finally, the commander ensures that the IPB process is fully integrated with mission planning and execution. IPB is an effective tool only when the results are used to develop plans and support decisionmaking during execution.

IPB emphasizes providing intelligence in the form of graphics and images—formats that help the commander to rapidly visualize, assimilate, and apply the intelligence in the decisionmaking process. During planning, products generated from IPB place large volumes of intelligence in context, providing situational awareness for everyone involved in the planning effort. These products form the basis of, or are combined with, the planning tools and decision support aids prepared by other staff sections to provide an integrated planning and execution support product. During execution, the use of graphics display intelligence increases the commander's ability to discern patterns as they are emerging and to conduct intuitive decisionmaking, thereby increasing operational tempo.

Levels of Production

Intelligence production can be extremely simple or incredibly complex. At the MAGTF CE level, particularly during deliberate planning, production normally entails developing detailed, all-source estimates and studies through the combined efforts of several intelligence support elements. During tactical execution, time constraints and the demands of the ongoing battle require rapid processing and production, with an emphasis on developing simple, mission-focused intelligence products such as a hand-annotated image of a helicopter landing zone (HLZ), a target description or an overlay depicting current and future enemy dispositions. An enlisted intelligence specialist on duty in an infantry battalion command post may develop dozens of intelligence products during his watch in the form of answers to questions concerning the enemy situation, targets or terrain to be traversed. Valuable intelligence does not result solely from the investment of time or resources. It is developed by placing relevant information in context, converting it into knowledge through analysis and synthesis, and applying that knowledge to the decisionmaking process.

There is inherent friction between the desire to provide as complete and accurate an intelligence product as possible and the continuous requirement to support the time-sensitive urgency of tactical decisionmaking. In practice, these conflicting demands must be balanced by using

stated direction, such as the commander's intent and PIRs, and knowledge of the operational situation to determine when to finish and disseminate the product. To provide a framework to make these determinations, intelligence production can be viewed as occurring on two levels: deliberate and immediate.

Deliberate production is employed when there is sufficient time to thoroughly evaluate, analyze, and synthesize all available information and produce a formal intelligence product such as a written intelligence estimate, scheduled report or detailed target/objective area study.

Immediate production is conducted to identify, process, and place in context elements of data, information, and intelligence that have a direct effect on ongoing or near-term operations. These elements are subjected to a compressed version of the production process, and the resulting product is rapidly disseminated to those who are affected. Immediate production is normally conducted during execution and results in simple, mission-specific intelligence products: situational assessments or answers to specific, individual IRs. There is no absolute distinction between the two levels. The nature of the situation and pertinent IRs will dictate the amount of time available to complete each production effort. Likewise, IPB methodology should be used during both types of production. However, during immediate production, a rapid mental evaluation and integration of the relevant factors of the threat and environment are used, usually building on a deliberate production effort that has already been completed.

Dissemination

Dissemination is the timely conveyance of intelligence to users in an appropriate form. Many times, intelligence operations focus almost exclusively on the collection and production phases, with the intelligence cycle often breaking down because insufficient attention is given to the dissemination phase. Dissemination must be planned and supervised to the same degree as collection and production or we risk failure of the intelligence support function. Determining the form and selection of the means to deliver the product are key aspects of the dissemination process.

Form

Determining the form to be used in disseminating the intelligence product is a function of several factors: the purpose of the intelligence product, the urgency and relevance of the intelligence to ongoing operations, the type and volume of the intelligence, the user's capability to receive intelligence products, and the dissemination means available. Because decisionmaking is a mental process and human beings think and understand primarily in the form of images, the goal of intelligence dissemination is to convey an accurate image of the battlespace or threat to the decisionmaker in a form that facilitates rapid understanding of that image. For this reason, graphics are the preferred dissemination form. (See figure 3-10 and figure 3-11 on page 3-14.)

Although oral briefings and written reports are the primary dissemination forms used today, the use of automated systems is increasing the capability to develop graphic products. Imagery, overlays, diagrams, and schematics enhanced with appropriate textual data and annotations will be used as the baseline dissemination format whenever possible. However, in time-sensitive situations, the verbal report or short text message may be the most expeditious dissemination form. Whether oral, text or graphic, intelligence products should use standard formats whenever possible. Standard formats facilitate ease of preparation and dissemination, as well as usability of the intelligence product.

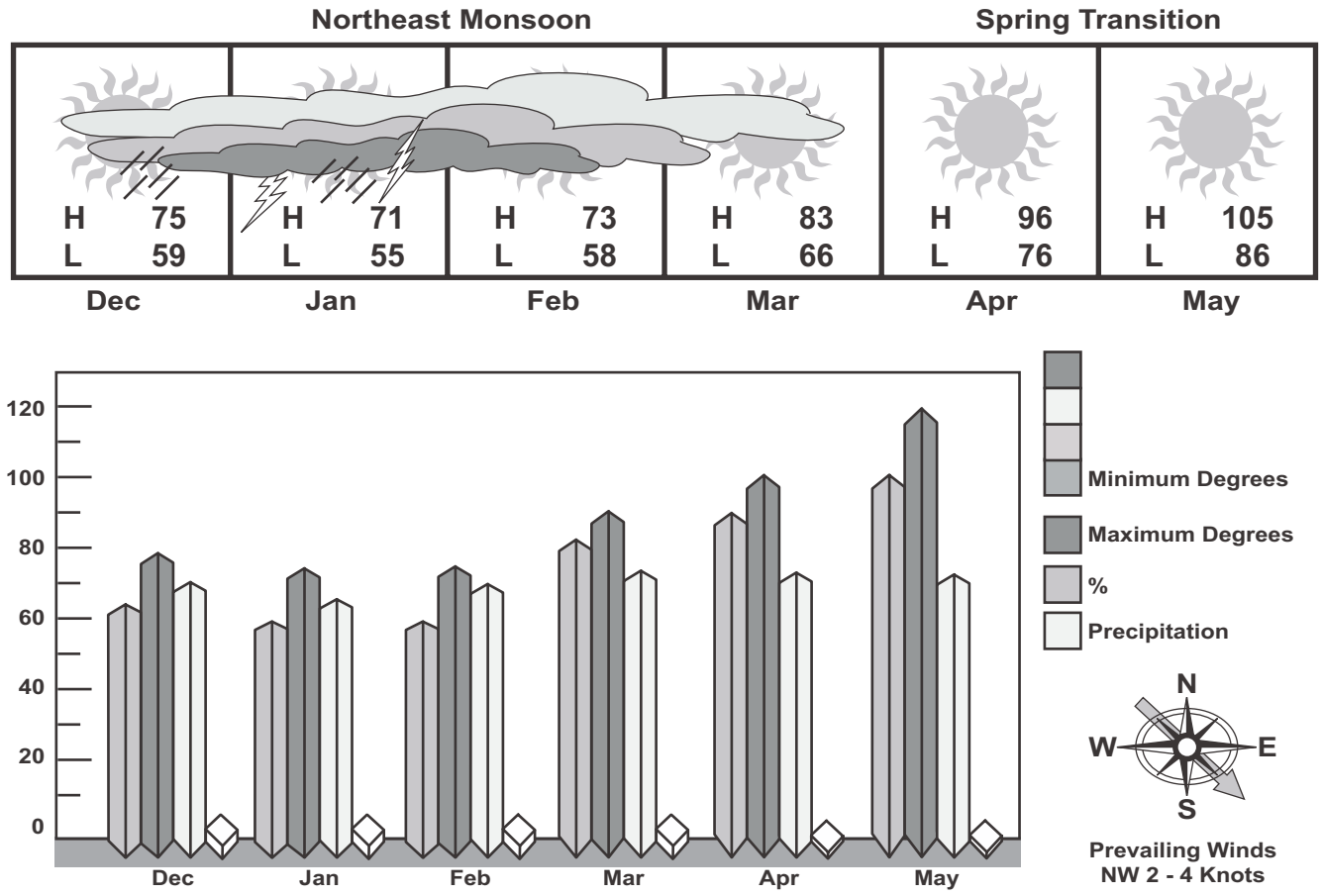


Figure 3-10. Graphic Climatology Study.

Delivery

Delivery of the intelligence product to the right person in a timely manner is directly related to the choice of the means used to disseminate that product. Dissemination is managed by using a combination of methods, channels, and modes to convey the product to the user.

Methods

There are two basic methods used to disseminate intelligence: supply-push and demand-pull. A supply-push system pushes intelligence from the collectors/producers to the users as it becomes available. The main advantage to this method is that users do not have to initiate requests to receive products. However, there is potential for information overload in a supply-push system. To prevent information overload, the dissemination node should tailor what it is passing through the system, not simply dump everything that it has received or developed.

The demand-pull mode provides access to intelligence on an as-needed basis. The user draws the required intelligence from the intelligence support system through a series of searches or inquiries. The use of demand-pull decreases the volume of intelligence being transmitted and diminishes the possibility of overwhelming units with superfluous products. However, demand-pull can also reduce the timeliness of dissemination by developing and providing intelligence only after a request has been received.

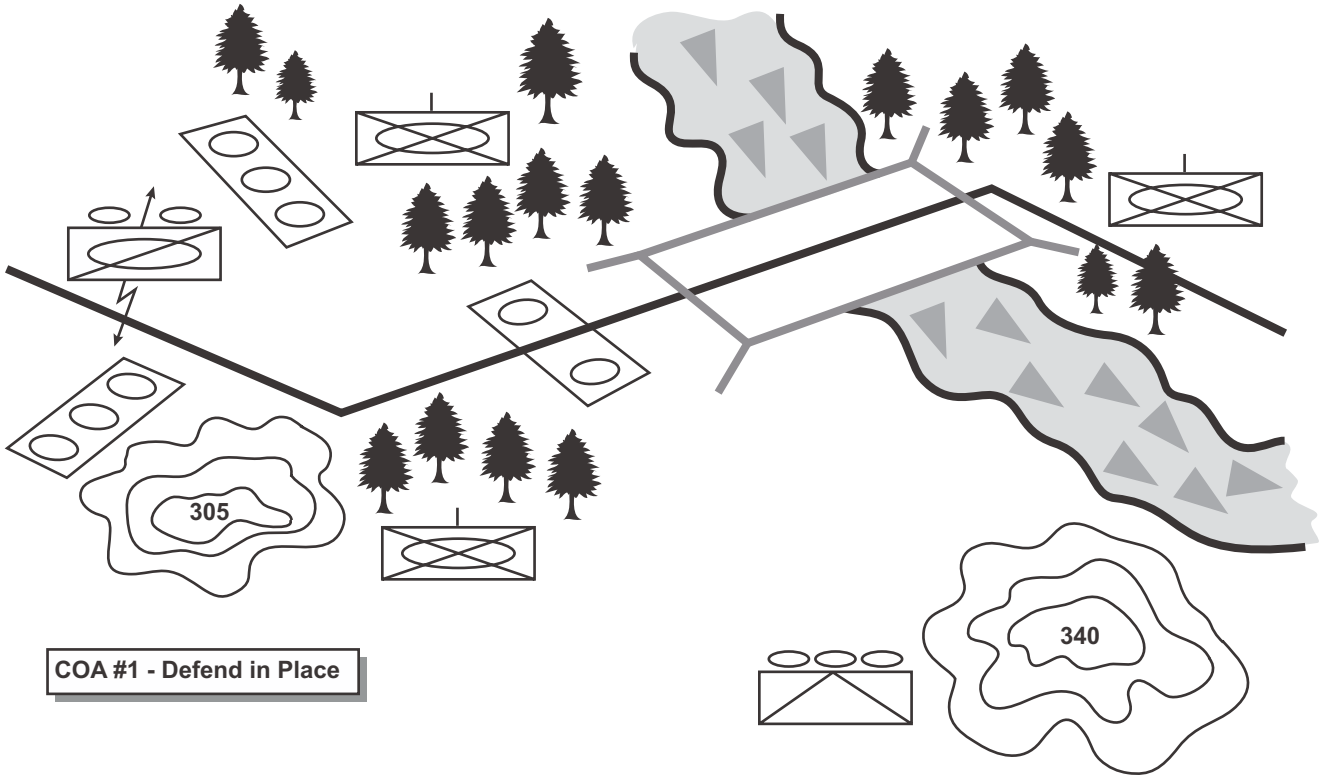


Figure 3-11. Graphic Intelligence Estimate.

The dissemination system must provide the flexibility to use either method, "pushing" important or time-sensitive intelligence directly to the users, while at the same time permitting them to "pull" other relevant intelligence as needed from readily accessible sources such as a database or a watch section at an intelligence center.

Channels

Intelligence is disseminated by using two types of channels: *standard* and *alarm*. Standard dissemination is used for routine intelligence and is transmitted according to a set order and format, usually along established command or staff channels. Examples include the formal staff briefing and standardized reports. The alarm channel is used to disseminate critical, time-sensitive intelligence that can have an immediate effect on the conduct of the operation, such as I&W of hostile activity. I&W alarms must be disseminated rapidly to all units that are affected by that intelligence. Although the standard channel is used to satisfy the majority of dissemination requirements, care must be taken to monitor the flow of what is passing through the pipeline to ensure that the intelligence provided is timely and pertinent to the units receiving it. A particularly important connection that is often neglected in standard dissemination is *lateral dissemination*; intelligence must flow laterally between units as well as up and down the chain of command. The exchange of intelligence between the GCE, aviation combat element (ACE), and combat service support element (CSSE) is an especially important link in ensuring that all commanders have a shared picture of the battlespace.

Modes

Finally, intelligence is disseminated in one of two modes: *broadcast* or *point-to-point*. In broadcast

dissemination, intelligence that affects the majority of units is sent simultaneously to a broad audience. Examples include I&W alarms, intelligence products developed by the MAGTF G-2 section that support the entire MAGTF, and reporting from organic collection assets. Broadcast dissemination may be web-based. Successful use of the broadcast mode depends on several factors, including judicious selection of what intelligence is broadcast, the ability of the appropriate users to monitor the broadcast, and employment of a processing methodology or system to filter and select for detailed examination only those broadcast items that are pertinent to the user's requirements. Undisciplined use of this mode can quickly lead to information overload. In the point-to-point mode, intelligence is sent to a specific user or users, normally in response to a specific request or requirement, and is passed along sequentially as appropriate. Dissemination across the system is slower but is more focused and can provide intelligence that is tailored to the needs of each individual unit. Point-to-point dissemination may be enhanced through the use of classified e-mail systems.

Architectures

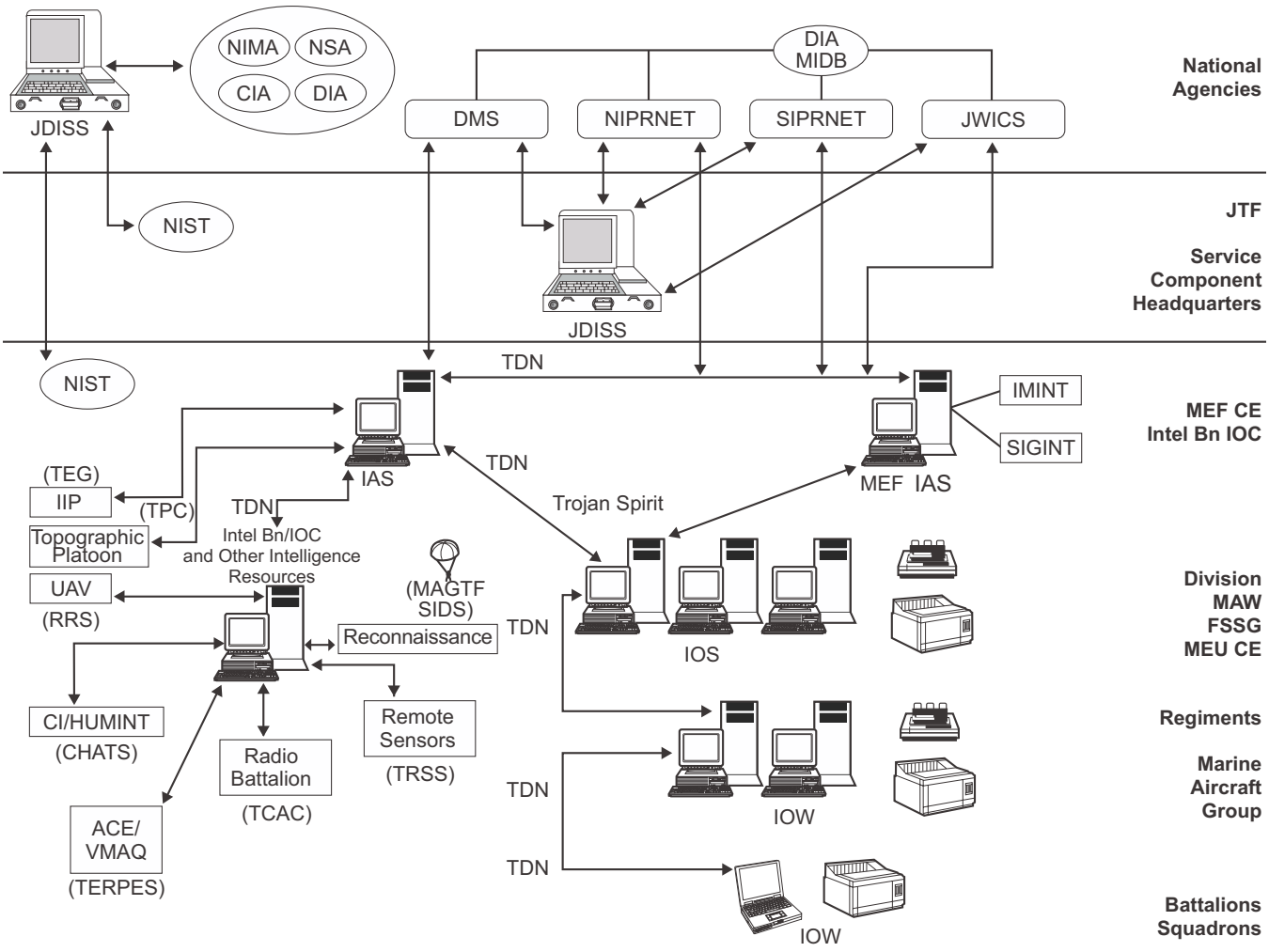
Intelligence architectures provide the means to disseminate intelligence. (See figure 3-12 on page 3-16.) Dissemination planning analyzes and anticipates the dissemination requirements and designs the appropriate architecture to meet those requirements. The architecture should employ all methods, channels, and modes in a flexible, integrated system. The objective is to provide the right intelligence to the appropriate user in a timely manner, while at the same time not overwhelming him with a massive amount of unfocused data.

Architectures will be developed with the objective of facilitating the exchange of *graphic* intelligence throughout the force, down to the lowest tactical echelon. The means will consist of a combination of procedures, CIS, and communications networks, effectively supervised by intelligence specialists to ensure that the dissemination requirements are being satisfied. The intelligence architecture must be interoperable with the overall CIS architecture employed by the MAGTF and the joint force.

Utilization

Intelligence has no inherent value. Its value is realized through its support to operations. Thus, the intelligence cycle is not complete until the intelligence that has been developed is used in decisionmaking during planning and/or execution. The commander is responsible for the effective use of intelligence and for ensuring that decisions are based on the foundation provided by intelligence. The intelligence officer facilitates the effective use of intelligence, supervises the entire intelligence development effort, and assists the commander and the staff in understanding the intelligence product and its application.

The utilization phase also provides the basis for the continuous functioning of the intelligence cycle. On one hand, utilization will determine whether a requirement has been completely satisfied; requirements that have not been met will require additional intelligence development efforts. On the other hand, the satisfaction of one requirement normally generates new or additional requirements, the answers to which are needed to further refine or focus the decisionmaking process. In either case, utilization provides guidance and feedback that are used to initiate the next iteration of the cycle.



CHATS=CI/HUMINT automated tool set	NIMA=National Imagery and Mapping Agency
CIA=Central Intelligence Agency	NIPRNET=Non-Secure Internet Protocol Router Network
CI/HUMINT=counterintelligence/human intelligence	NIST=National Intelligence Support Team
DIA=Defense Intelligence Agency	NSA=National Security Agency
DMS=Defense Message System	RRS=remote receive station
IAS=Intelligence analysis system	SIDS=secondary imagery dissemination system
IIP=imagery intelligence platoon	SIPRNET=Secret Internet Protocol Router Network
intel bn=intelligence battalion	TCAC=Technical Control and Analysis Center
IOS=intelligence operations server	TDN=tactical data network
IOW=intelligence operations workstation	TEG=Technical Exploitation Group
JWICS=Joint Worldwide Intelligence Communication System	TERPES=tactical electronic reconnaissance processing and evaluation system
MAW FSSG=Marine Aircraft Wing Force Serv ice Support Group (USMC)	TPC=topographic production capability
MIDB=modernized integrated database	TRSS=tactical remote sensor system

Figure 3-12. Notional Marine Expeditionary Force Intelligence Architecture.

Application of the Intelligence Cycle

The intelligence cycle is a procedural framework for developing mission-focused intelligence support. It is not an end in itself, nor should it be viewed as a rigid set of procedures that must be carried out in an identical manner on all occasions. The commander and the intelligence officer must consider each IR individually and apply the intelligence cycle in a manner that develops the required intelligence in the most effective way.

Application of the intelligence cycle will vary with the phase of the PDE&A cycle. In theory, a unique iteration of the intelligence cycle is carried out for each individual requirement. In practice, particularly during the planning phase, requirements are grouped together and satisfied through a single, concurrent intelligence development process. During the planning phase, intelligence development is generally carried out through two major iterations of the intelligence cycle.

The first primarily supports decision planning. Completing this iteration of the intelligence cycle results in preparing and using basic intelligence products—an intelligence estimate, supporting studies, and IPB analysis—that describe the battlespace and threat. These products form the basis for developing and selecting COAs.

The second iteration of the intelligence cycle supports execution planning. Decision and execution planning are defined and discussed in MCDP 5. It is an outgrowth of selecting the COA and forming a concept of operations. Implementing the collection plan, refinement of IPB analysis, and generating mission-specific intelligence products are integrated with the concept of operations to support mission execution. During execution, requirements are satisfied on a more individualized basis. New requirements are usually generated in response to a specific operational need. Each requirement is unique and must be satisfied in a timely manner to facilitate rapid decisionmaking and generating or maintaining tempo. (See figure 3-13 on page 3-18.)

The intelligence cycle will also be applied differently depending on the mission and the organizational level of the unit. For example, a MAGTF G-2 section will normally have a separate section that is specifically responsible for each phase of the intelligence cycle—a collections section, processing and exploitation agencies, a production element, and a dissemination section—with an intelligence operations section providing planning and direction for the overall effort. At the MAGTF level, intelligence is normally developed to satisfy multiple requirements concurrently, with simultaneous collection, processing, production, and utilization efforts being carried out by the separate functional sections. In contrast, a battalion or squadron S-2 section must carry out the cycle with a limited number of resources. It will generally focus on a single requirement or a small number of closely related requirements, moving through each phase of the cycle sequentially until that requirement is satisfied.

Counterintelligence

CI is the function of intelligence that is concerned with identifying and counteracting the threat posed by hostile intelligence capabilities and by organizations or individuals engaged in espionage, sabotage, subversion, or terrorism. The objective of CI is to enhance the security of the command by denying an adversary information that might be used to conduct effective operations against friendly forces and to protect the command by identifying and neutralizing espionage, sabotage, subversion, or terrorism efforts. (MCWP 2-14, *Counterintelligence*)

Responsibilities

CI, like all intelligence matters, is a command responsibility. In preparing for operations, all units must develop a CI plan and implement appropriate

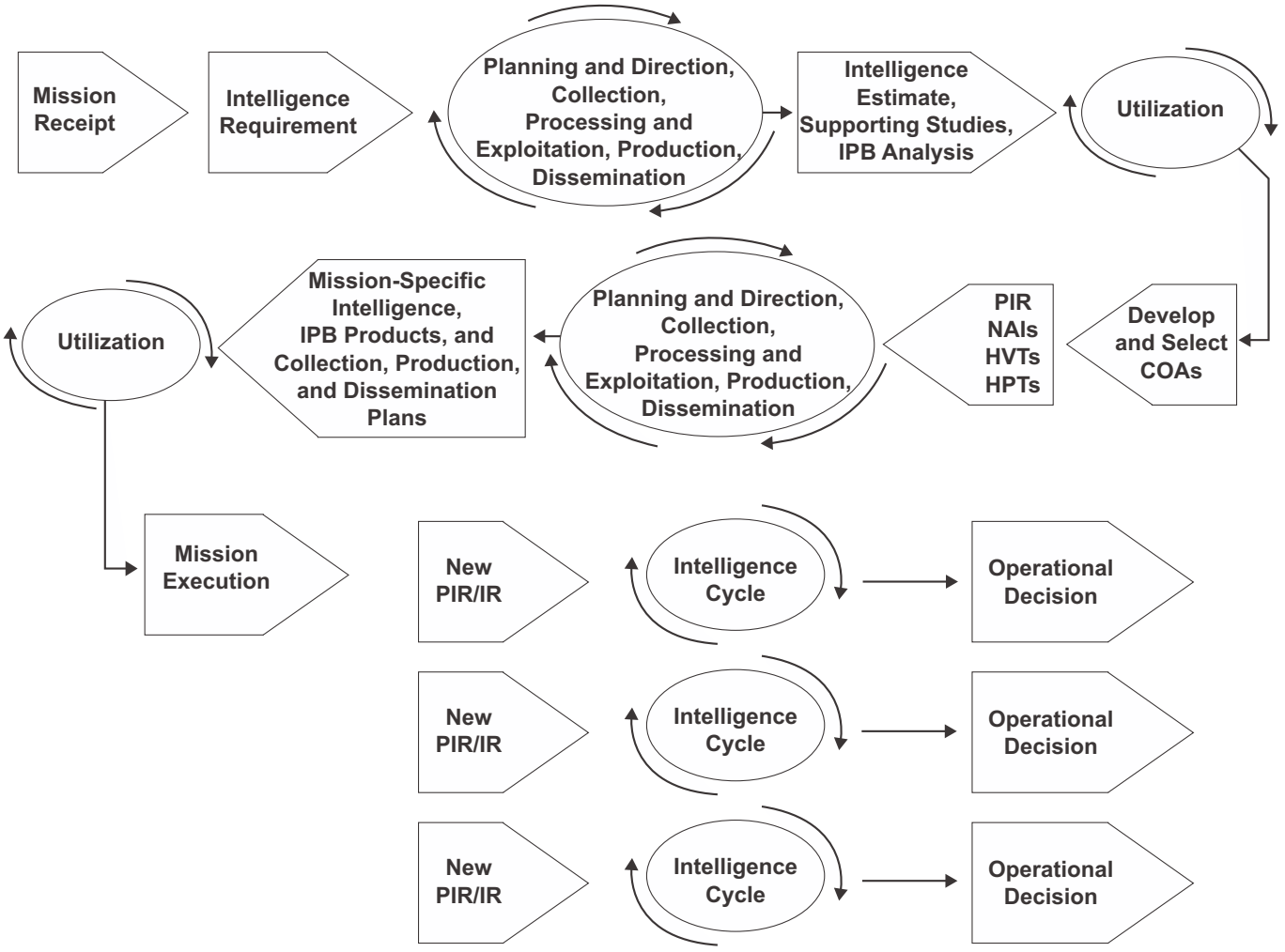


Figure 3-13. Application of the Intelligence Cycle.

CI measures to protect themselves from potential threats. The unit intelligence officer plans, implements, and supervises the CI effort for the commander. The G-2/S-2 may have access to or request support from MAGTF CI units and specialists to assist in developing CI estimates and plans. All members of the command are involved in executing the CI plan and implementing appropriate CI measures. Key participants in this process and their specific responsibilities follow:

- G-3/S-3-overall security and force protection, OPSEC, counterreconnaissance, and deception.
- G-6/S-6-CIS security.
- G-1/S-1-information security.
- Headquarters commandant-physical security of unit CP and echelons.

CI Planning

CI planning at all levels is conducted by using a standard methodology that consists of three steps: developing a CI estimate, conducting a CI survey, and developing the CI plan.

The CI Estimate

The CI estimate details the capabilities and limitations of foreign intelligence, subversive, and terrorist organizations that could carry out actions

against friendly units and facilities or against individuals, groups or locations of concern to our forces, such as the local population or civilian organizations operating in the area. It also provides an estimate of possible and probable COAs that these threat organizations will adopt. Intelligence and CI analysts of the MAGTF CE and CI/HUMINT company will normally prepare a comprehensive CI estimate that addresses threats to the MARFOR or MAGTF by using an IPB methodology that is focused on CI factors and the CI threat. However, each level of command must conduct its own evaluation to determine which of the adversary's capabilities identified in the MAGTF CI estimate represent a threat to their particular unit. The CI estimate must be updated on a regular basis. The revised estimate or appropriate CI warning reports must be disseminated to all units involved in the operation.

The CI Survey

The CI survey assesses a unit's security posture against the threats detailed in the CI estimate. The CI survey should identify vulnerabilities to specific foreign intelligence, espionage, sabotage, subversion or terrorist capabilities and provide recommendations on how to eliminate or minimize these vulnerabilities. The survey should be as detailed as possible. During the planning phase of an operation, it may be possible to do a formal, written survey. CI specialists from the CI/HUMINT company may be available to assist in this effort. In a time-compressed situation, the survey will likely result from a brief discussion between the appropriate intelligence, operations, communications, and security personnel. In either case, it is critical that the survey look forward in space and time to support developing the CI measures necessary to protect the unit as it carries out successive phases of the operation; i.e., the survey makes recommendations to improve the CI posture of the command for now and in the future.

The CI Plan

The CI plan details the activities and operations that the command will use to counter the CI threat. It includes procedures for detecting and monitoring the activities of foreign intelligence and terrorist organizations and directs the implementation of active and passive measures that are intended to protect the force from these activities. The CI plan is based on the threats identified in the CI estimate and the vulnerabilities detected by the CI survey. The MAGTF staff CI officer normally prepares a detailed, comprehensive CI plan that addresses the entire MAGTF. Included in the MAGTF CI plan are details of the employment of dedicated CI capabilities and the conduct of specialized CI operations intended to detect and neutralize or eliminate specific CI threats. Plans of subordinate MAGTF elements closely follow the MAGTF plan, normally adding only security measures that apply to their specific units. As with all plans, CI plans must be continually updated to ensure they are current and support ongoing and future operations.

CI Measures

CI measures encompass a broad range of activities designed to protect against the CI threat. The two general categories of CI measures are active and passive.

Active CI measures are those measures that are designed to neutralize or eliminate the foreign intelligence effort and adversary sabotage, subversion, and terrorism capabilities. Counterreconnaissance operations and deception activities are examples of active measures that are routinely employed by all units. Complex active CI measures such as counterespionage operations, counterterrorism operations, screening and interrogations, and CI force protection source operations are conducted only by CI personnel or other specialized organizations following the direction of the joint force and/or MAGTF commanders.

Passive CI measures are designed to conceal and deny information to foreign intelligence personnel and protect friendly personnel and installations from sabotage, subversion, and terrorism. Camouflage, security of classified material, emission control, information systems security, noise and light discipline, and physical access control are examples of passive CI measures that are employed extensively by all units.

The CI process is summarized in figure 3-14. For further details on CI responsibilities, planning, measures, and operations, see MCWP 2-14.

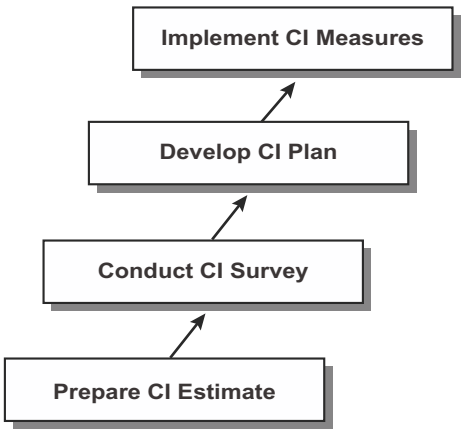


Figure 3-14. The Counterintelligence Process.

CHAPTER 4
CONCEPT OF MAGTF INTELLIGENCE SUPPORT

Marine intelligence operations are conducted primarily to facilitate the planning and execution of MAGTF operations through the development of tactical intelligence. The concept of MAGTF intelligence support ensures that the required intelligence is available to commanders at all levels throughout the force in time to influence their decisionmaking process. Key elements of this concept follow:

- Fully manned and capable organic intelligence sections down to maneuver battalion/squadron level.
- Directing the intelligence effort and maintenance of a robust collection, production, and dissemination capability at the MAGTF level.
- Employing specialized intelligence units to provide dedicated collection, processing, exploitation, and production of all-source intelligence.
- Creating key intelligence nodes at any level to concentrate intelligence support at critical times and locations. (These nodes are created through task organization, split-basing, and the use of intelligence direct support teams [DSTs].) An intelligence DST provides an enhanced intelligence capability to a supported intelligence section. A DST consists of one officer and several enlisted intelligence specialists. DSTs are organic to the MEF and each MSC G-2 sections.
- Full use of the intelligence support available from national, theater, joint, other Service component, and multinational forces to enhance MAGTF intelligence capabilities.
- Augmentation from global sourcing (noncommitted operating forces, the supporting establishment, and the Reserves) to enhance intelligence support to the MAGTF.

This intelligence support concept provides organic intelligence sections to commanders at all levels. These sections develop intelligence to satisfy their units' unique requirements. This intelligence supports their commander's tactical decisionmaking process and generates tailored intelligence products to facilitate mission execution.

Unit intelligence sections are supported by a primary MAGTF intelligence node that can perform all types of intelligence operations. The MAGTF G-2, through its combat intelligence center (CIC), provides centralized direction for the collection, production, and dissemination efforts of organic and supporting intelligence assets and ensures that these efforts remain focused on satisfying the PIRs that are essential to mission success. At the MEF CE level, the intelligence operations center (IOC) is the primary MAGTF intelligence node. Concentration of specialized intelligence capabilities in the radio battalion, the intelligence battalion, and the force reconnaissance company under this centralized direction facilitates unity of effort, effective employment of limited assets, and the collection and production of all-source intelligence.

The concept of intelligence support acknowledges the need to focus intelligence efforts in support of particular MAGTF elements during different phases of an operation. The MAGTF intelligence structure has the flexibility to provide such focused support through task organization. Enhanced support can be provided employing DSTs and integrating MAGTF intelligence assets.

Recognizing that organic intelligence capabilities may be limited in particular environments, the MAGTF can draw on the full range of national, theater, joint, other Service, allied, and multinational intelligence assets. When available, these capabilities will be fully integrated into MAGTF intelligence operations. If a separate Marine component

headquarters is established, it will support the MAGTF by performing those intelligence functions not directly related to warfighting, to include the following:

- Conducting detailed operational-level intelligence planning.
- Providing Marine intelligence liaison to joint task force (JTF) and other component intelligence elements.
- Monitoring the status of MAGTF intelligence collection and production requests for supporting and external support requirements.
- Planning the development and monitoring the adequacy of the JTF/MAGTF's intelligence architectures and the flow of intelligence to the MAGTF.
- Supporting Marine participation in intelligence support to the joint targeting process.

If a separate Marine component headquarters is not established, then the MAGTF CE's CIC will perform these functions. MSCs and other MAGTF elements will be able to access these external capabilities through the MAGTF intelligence architecture to pull available intelligence products on demand. Specialized intelligence units; e.g., the radio battalion or intelligence battalion, will have connectivity with appropriate external agencies to coordinate tasking or support.

Any MAGTF that is committed to an operation can be supported by intelligence assets of nondeployed MAGTFs, the supporting establishment or the Reserves. This support could consist of augmentation to fill shortfalls in manpower, equipment or specialized capabilities and assistance in developing intelligence in response to a Service-unique requirement. Flexibility to draw on assets from across the Marine Corps provides the ability to tailor and enhance particular intelligence capabilities based on the requirements of the committed MAGTF commander.

Role of the Organic Intelligence Section

Most commands from the battalion/squadron level and above in the operating forces have an organic intelligence section. The unit intelligence officer and section occupy the central role in the concept of MAGTF intelligence support. They focus the intelligence effort to develop, disseminate, and ensure effective use of intelligence in support of tactical operations. Intelligence drives operations and remains responsive to mission requirements through close and direct contact with the commander, key staff officers, and subordinate unit leaders.

The Unit Intelligence Officer

The commander directs the intelligence effort. The intelligence officer manages this effort for the commander, acting as the principal advisor on intelligence and implementing activities that carry out the commander's intelligence responsibilities. *The intelligence officer is a full participant in the commander's decisionmaking process, ensuring that intelligence is effectively used throughout the command during all phases of mission planning and execution*. Key responsibilities follow:

- Facilitate understanding and use of intelligence in the planning and execution of operations.
- Support situation development and the commander's estimate of the situation by identifying enemy capabilities, strengths, and critical vulnerabilities and opportunities and limitations presented by the environment.
- Assist the commander in developing PIRs.
- Ensure that the command's IRs are received, understood, and acted on by organic and supporting intelligence assets.
- Develop and disseminate all-source intelligence products that are tailored to the unit's mission and concept of operations.

- Monitor the effective flow of intelligence throughout the command.
- Provide BDA data and analysis to assist the combat assessment process.

The Unit Intelligence Section

The unit intelligence section supports the commander, the intelligence officer, and the entire command through the production and dissemination of mission-oriented intelligence products. Primary functions follow:

- Conduct IPB analysis for the unit's AO and interest.
- Develop and maintain a comprehensive intelligence estimate.
- Tailor intelligence produced at all levels to meet specific unit requirements.
- Form collection plans and support requests to satisfy unit PIRs and IRs.
- Maintain an accurate image of the battlespace and enemy situation.
- Prepare target analysis and target intelligence products.
- Recommend CI and force protection measures.
- Provide linkage to supporting intelligence assets.

Each organic intelligence section performs all six intelligence functions described in chapter 1. However, the priority and level of effort applied to the different functions will vary with the type of unit, level of command, and assigned mission. For example, an infantry battalion S-2 section will normally focus on support of the commander's estimate and situation development, while the S-2 of a combat service support (CSS) unit may concentrate on support of force protection, and the intelligence section of a fixed-wing Marine aircraft group usually places priority on support of targeting and combat assessment (particularly BDA).

Required Capabilities

To carry out these responsibilities, organic intelligence sections must have the following capabilities:

- Sufficient manning to carry out assigned responsibilities.
- Training in all aspects of tactical intelligence development, emphasizing the production of tailored, all-source, mission-specific intelligence products.
- Organic collection, processing, production, and dissemination assets appropriate to its mission and level of command.
- Connectivity to other MAGTF intelligence assets to provide a common picture of the battlespace, receive warning and other critical intelligence, and achieve access for "pulling" pertinent intelligence in response to unit requirements.
- Formation as a base for developing a larger intelligence support node, task-organized to provide expanded intelligence capabilities during particular phases of an operation.

The MAGTF Intelligence Section

The MAGTF intelligence section resident in the MAGTF CE is the focal point for intelligence operations and development in the MAGTF.

MAGTF Intelligence Officer

The MAGTF G-2/S-2, supported by the CIC and its subordinate sections, provides centralized direction for the MAGTF's comprehensive intelligence effort. The G-2/S-2 serves as the intelligence officer for the MAGTF commander. The CIC serves as the primary intelligence node for the entire MAGTF. As such, the CIC must remain responsive to the requirements of all MAGTF elements. The MAGTF intelligence section performs the following tasks:

- Provides centralized direction for MAGTF intelligence operations.

- Plans and implements a concept for intelligence support based on the mission, concept of operations, and commander's intent.
- Consolidates, validates, and prioritizes IRs of the MAGTF.
- Recommends MAGTF PIRs to the MAGTF commander.
- Maintains a consolidated, all-source production center in the MAGTF all-source fusion center (AFC).
- Plans, develops, and directs the MAGTF collection, production, and dissemination plans and operations.
- Directs the employment of MAGTF organic collection assets through the surveillance and reconnaissance cell (SARC) and the operations control and analysis center (OCAC).
- Submits consolidated requests for external intelligence support through the Marine component headquarters to appropriate agencies.
- Links the MAGTF to national, theater, joint, other Service, and multinational intelligence assets and operations.
- Prepares a comprehensive CI plan with recommended force protection measures.
- Supervises the execution of appropriate active and passive CI measures, CI functions, and CI services.

In addition to the responsibilities of all MAGTF intelligence officers, the MEF assistant chief of staff (AC/S) G-2 exercises staff cognizance over several special staff officers and their intelligence units/organizations. (See figure 4-1.)

The AC/S G-2 has staff responsibility for intelligence and intelligence operations. The commander relies on the intelligence officer to provide information on weather, terrain, and enemy capabilities, status, and intentions. Through the intelligence OPLAN and supporting intelligence, CI, and reconnaissance and surveillance (R&S) plans, the G-2 validates and plans information requirements; coordinates intelligence priorities, integrates collection, production, and dissemination activities; allocates resources; assigns specific intelligence and reconnaissance missions to subordinate elements; and supervises the overall intelligence, CI, and reconnaissance efforts. Specific responsibilities follow:

- Develop and answer outstanding MEF and subordinate units' priority information requirements and information requirements by planning, directing, integrating, and supervising organic multidiscipline MEF and supporting intelligence operations.
- Prepare appropriate intelligence, CI, and reconnaissance plans and orders for the MEF and review and coordinate the all-source intelligence CI and reconnaissance plans of JTFs, theaters, and other organizations.
- Submit and coordinate all-source collection, production, and dissemination requirements beyond the capability of the MEF to satisfy to higher headquarters for JTF, theater or national intelligence support.
- Ensure intelligence information is rapidly processed, analyzed, and incorporated where appropriate in all-source intelligence products, and rapidly disseminated to all MEF and external units requiring these.
- Evaluate JTF, theater, and national all-source intelligence support and adjusting stated IRs, if necessary.
- Identify and correct deficiencies in intelligence, CI, and reconnaissance personnel and equipment resources.
- Incorporate intelligence in training exercises to improve MEF individual, collective, and unit readiness.
- Facilitate understanding and use of intelligence in support of the planning and execution of MEF operations.

Special Staff Officers under the Staff Cognizance of G-2 Officer

G-2 Operations Officer

The G-2 operations officer has primary responsibility for intelligence support to the commanding officer and the remainder of the CE in support of

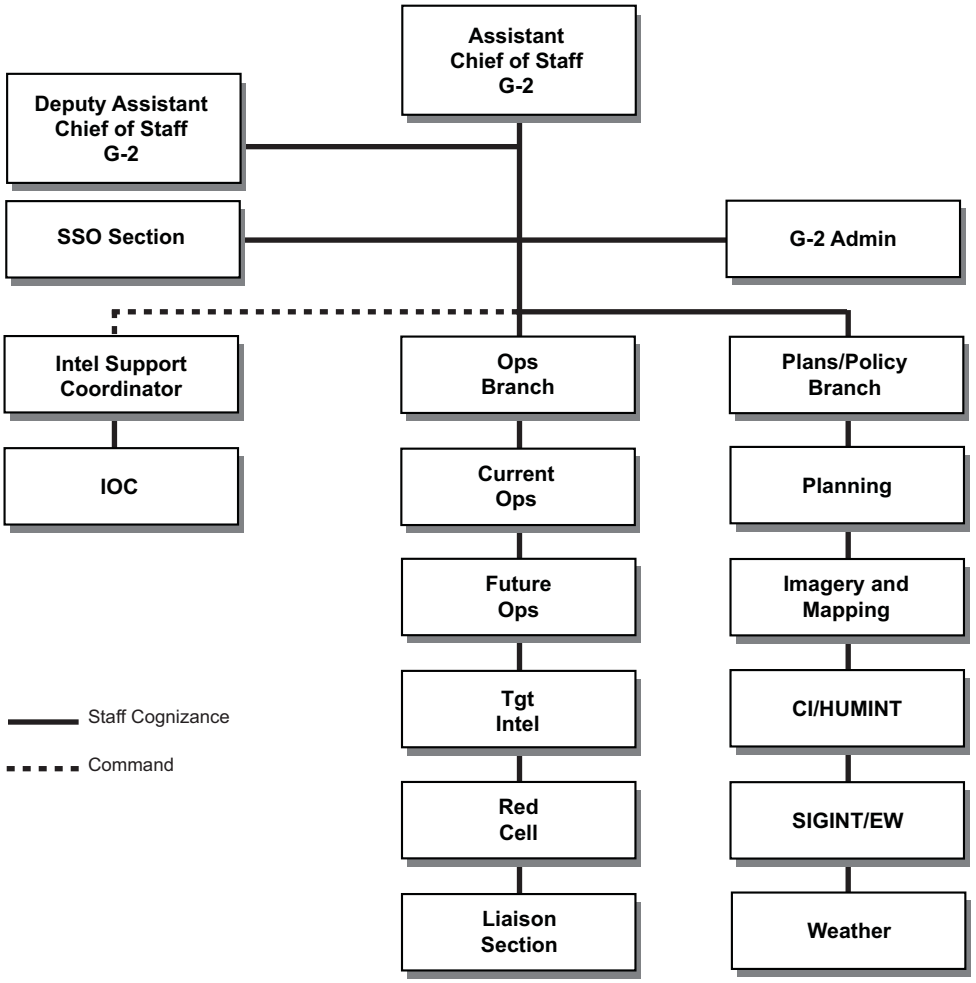


Figure 4-1. Special Staff Officers and Relationships under the Staff Cognizance of the MEF G-2.

current and future operations. Specific responsibilities include the following:

- Coordinate and provide intelligence support to the commander, the G-3 operations section, and the rest of the commander's battle staff.
- Serve as the G-2 representative to the MEF CE crisis action team.
- Coordinate, provide, and supervise intelligence support to the MEF CE current operations center, future operations center, and force fires.
- Plan, direct, and supervise the Red Cell.
- Provide recommendations on PIR and IR validation, prioritization, and taskings to the AC/S G-2 and the intelligence support coordinator (ISC). The intelligence battalion commander is dual-hatted as the ISC.
- Coordinate and supervise the transition of intelligence planning and operations from G-2 plans to G-2 future operations, and from G-2 future operations to G-2 current operations, to effectively support the MEF's "single battle" transition process.
- Plan, direct, and supervise MEF liaison teams to external commands; e.g., the JTF and joint

functional components headquarters, and intelligence organizations.
- Coordinate with the ISC and MEF MSCs' G-2 operations officers to ensure unity of effort of MEF intelligence operations.
- Provide intelligence input and other support to MEF warning and fragmentary orders and to operations related reporting; e.g., periodic situation reports.
- Coordinate intelligence training for the MEF G-2 section and providing G-2 oversight for and integration of the entire MEF intelligence training program.
- Perform other intelligence support and tasks as directed by the AC/S G-2.

G-2 Plans Officer

The G-2 plans officer has primary responsibility for intelligence support to the future plans cell. Specific responsibilities follow:
- Plan the MEF concept of intelligence operations for approval by the AC/S G-2 and subsequent implementation by the integrated staff cell based upon the mission, threat, commander's intent, guidance, and concept of operations.
- Lead, coordinate, and provide intelligence support to MEF G-5 future plans section.
- Plan and coordinate intelligence support requirements for and the deployment of intelligence elements and resources into the AO.
- Provide recommendations on PIR and IR validation, prioritization, and taskings to the AC/S G-2 and the ISC.
- Coordinate, in conjunction with the ISC, G-2 development of Annex B (Intelligence) and Annex M (Geospatial Information and Services) to MEF OPLANs.
- Keep the G-2 section, other CE staff sections, intelligence liaison personnel, augmentees, and others apprised of MEF intelligence planning actions and requirements.
- Identify requirements and provide recommendations to the G-2 operations officer for MEF intelligence liaison teams to external commands; e.g., the JTF or other components' headquarters and intelligence agencies.
- Coordinate and develop policies for MEF intelligence, CI, and reconnaissance operations.
- Plan, direct, and supervise the MEF G-2's imagery and mapping, CI/HUMINT, SIGINT, and weather sections.
- Perform other intelligence support and tasks as directed by the AC/S G-2.

Intelligence Battalion Commander/ Intelligence Support Coordinator

The intelligence battalion commander is responsible for planning, directing, collecting, processing, producing and disseminating intelligence, and providing CI support to the MEF, MEF MSCs, subordinate MAGTFs, and other commands as directed.

Garrison. In garrison the principal task of the intelligence battalion commander is to organize, train, and equip detachments that support MAGTFs or other designated commands to execute integrated collection, intelligence analysis, production, and dissemination of intelligence products.

During Operations. During operations the intelligence battalion commander is dual-hatted as the ISC, serving as such under the direct staff cognizance of the MEF AC/S G-2. The intelligence battalion's S-3 section, along with the operations center element of the MEF G-2, form the core of the ISC support effort, with planning, direction, and C2 conducted within the IOC's support cell. As the ISC, he is responsible to the MEF AC/S G-2 for the overall planning and execution of MEF all-source intelligence operations. Specific responsibilities of the ISC during actual operations follow:
- Implement the concept of intelligence operations developed by the G-2 plans officer and approved by the AC/S G-2.
- Establish and supervise operation of the MEF IOC, which includes the support cell, the

SARC, and the production and analysis (P&A) cell. Generally the IOC will be collocated with the MEF CE's main CP.

- Develop, consolidate, validate, and prioritize recommended PIRs and IRs to support MAGTF planning and operations. The ISC is tasked to perform PIR and IR validation and prioritization *only* during operations when the IOC is activated. During routine peacetime operations, the PIR/IR validation and prioritization tasks are the responsibility of the MEF CE's G-2 operations officer.
- Plan, develop, integrate, and coordinate MEF intelligence collection, production, and dissemination plans, to include the effective organic and external integration and employment and staff cognizance of MEF SIGINT, CI, HUMINT, geographic intelligence, IMINT, ground remote sensors, ground reconnaissance, and tactical air reconnaissance intelligence collections, production, and dissemination operations.
- Develop, in conjunction with the G-2 plans officer and G-2 operations officer, and complete Annex B (Intelligence) and Annex M (Geospatial Information and Services) to MEF operation orders (OPORDs).
- Plan, develop, integrate, and coordinate intelligence and CI support to the commander's estimate, situation development, I&W, force protection, targeting, and combat assessment.
- Manage and fuse the threat (or *red*) common operational picture (COP)/common tactical picture (CTP) inputs from subordinate units and external commands and intelligence agencies into the MEF CE's threat COP/CTP.
- Provide intelligence support to the MEF CE G-2 section and the MSCs.
- Prepare the intelligence and CI estimates to support G-2 plans.
- Plan, develop, and coordinate intelligence CIS architecture, to include its integration with and support of MEF IMINT and other intelligence and reconnaissance requirements.
- Coordinate and integrate all-source intelligence operations with other Service components, JTF joint intelligence support element (JISE), theater joint intelligence center (JIC) or joint analysis center, and national intelligence agencies and operations to include all aspects of intelligence reach back support.
- Assist with the evaluation and improvement of MEF all-source intelligence, CI, and reconnaissance operations.
- Perform other intelligence support and tasks as directed by the AC/S G-2.

Figure 4-2 is a summary of the principal responsibilities of the AC/S G-2's three principal subordinate staff officers.

Intelligence Support Coordinator

- Plan and execute intelligence operations to support all MEF IRs.
- Establish and direct the IOC (P&A cell, SARC, and support cell).
- IR management (collection, production and dissemination) validation, prioritization, and tasking per AC/S G-2 direction.
- Intelligence operations command of intelligence battalion and staff cognizance over SIGINT, CI, HUMINT, MASINT, IMINT, and air/ground reconnaissance (or designated G-2 elements).

G-2 Operations Officer

- Intelligence support to MEF CE battlestaff and current operations center agencies.
- Coordination and support to higher and adjacent headquarters and agencies.
- Recommends IR validation, prioritization, and tasking to AC/S G-2.
- Establish and direct intelligence elements and support to the current operations center, future operations center, target intelligence section, force fires, Red Cell, and MEF intelligence liaison teams.

G-2 Plans Officer

- Intelligence support to the G-5 future planning team for future planning IRs.
- Recommend IR validation, prioritization, and tasking to AC/S G-2.
- Establish and direct the G-2 future planning intelligence element.
- G-2 section's imagery & mapping, CI/HUMINT, SIGINT, and weather sections (less that under the staff cognizance of the ISC).

Figure 4-2. AC/S G-2's Principal Subordinate Staff Officers and their Responsibilities.

Collection Management/Dissemination Officer. The collection management/dissemination officer (CMDO) is sourced from the intelligence battalion's S-3 section and is a key subordinate to the intelligence battalion commander/ISC during operations. The CMDO is

responsible for formulating detailed intelligence collection requirements and intelligence dissemination requirements and tasking and coordinating internal and external operations to satisfy these. The CMDO receives validated PIRs and IRs and direction from the ISC, and then plans and manages the best methods to employ organic and supporting collection and dissemination resources through the intelligence collection and dissemination plans (tabs to Appendix 16, *Intelligence Operations Plan*, to Annex B.) The CMDO is also responsible for validating and forwarding national and theater intelligence collection requests from the MEF and MSCs typically using appropriate intelligence tools and TTP. He also is responsible for coordinating intelligence CIS requirements and maintaining awareness of available CIS connectivity throughout the MAGTF and with key external organizations.

During operations the CMDO works within the support cell. In coordination with the P&A cell officer in charge (OIC), the SARC OIC, G-2 operations officer, intelligence/reconnaissance commanding officers/OICs, and the MEF G-6, the CMDO is responsible to the ISC for the following tasks:

- Determine and coordinate the collection effort of PIRs/IRs that may be collected via intelligence, CI, and reconnaissance resources.
- Determine PIRs/IRs and prepare requests for intelligence that are beyond organic capabilities and prepare submissions to higher headquarters and external agencies for support.
- Recommend dissemination priorities, development of intelligence reporting criteria, and advise on and selecting dissemination means.
- Develop and coordinate all-source intelligence collection plans, coordinate and integrate these with MEF, other components, JTF, theater, and national intelligence production operations.
- Develop and coordinate all-source intelligence dissemination plans and supporting architectures for voice and data networked communications, and coordinate and integrate these with MEF, other components, JTF, theater, and national intelligence CIS and dissemination operations.
- Monitor the flow of intelligence throughout the MEF and ensure that it is delivered to intended recipients in a timely fashion and satisfactorily meet their needs.
- Evaluate the effectiveness of MEF and supporting intelligence collection and dissemination operations.

SARC OIC

The SARC OIC is also an immediate subordinate of the ISC and is responsible for supervising the execution of the integrated organic, attached, and direct support intelligence collection and reconnaissance operations. The SARC OIC is responsible to the ISC for accomplishing the following specific responsibilities:

- Coordinate, monitor, and maintain the status of all ongoing intelligence, CI, and reconnaissance collection operations. This includes—
  - Missions, tasked intelligence collection requirements, and reporting criteria for all collection missions.
  - Locations and times for all pertinent fire support control measures.
  - Primary and alternate CIS plans for routine and time-sensitive requirements for intelligence users (collectors, the SARC, and key MEF, CE, and MSC C2 nodes) to support ongoing C2 of collection operations and dissemination of acquired data and intelligence via the most expeditious means.
- Conduct detailed intelligence collection planning and coordination with the MSCs and intelligence, CI, and reconnaissance organizations' planners, with emphasis on ensuring understanding of the collection plan and specified intelligence reporting criteria.
- Ensure other MAGTF C2 nodes; e.g., the current operations center or force fires are apprised of ongoing intelligence, CI, and reconnaissance operations.

- Receive routine and time-sensitive intelligence reports from deployed collection elements; cross-cueing among intelligence collectors, as appropriate; and the rapid dissemination of intelligence reports to MAGTF C2 nodes and others in accordance with standing PIRs/IRs, intelligence reporting criteria and dissemination plan, and the current tactical situation.

P&A Cell OIC

The P&A cell OIC is the third principal subordinate to the ISC, with primary responsibility for managing and supervising the MEF's all-source intelligence processing and production efforts. Key responsibilities follow:

- Plan, direct, and manage operations of the AFP (to include the fusion, order of battle, IPB, and target intelligence/battle damage assessment teams), the topographic platoon, the IIP, the DSTs, and other P&A elements as directed.
- Coordinate and integrate P&A cell operations, estimates, and products with the MEF G-2 section's G-2 operations branch and its Red Cell operations and estimates.
- Maintain all-source automated intelligence databases, files, workbooks, country studies, and other intelligence studies.
- Plan and maintain imagery, mapping, and topographic resources and other intelligence references.
- Administer, integrate, operate, and maintain intelligence processing and production systems, unclassified general service and senstitive compartmented information systems; e.g., the intelligence analysis system or the image product library.
- Analyze and fuse intelligence and other information into tailored all-source intelligence products to satisfy all supported commanders' stated or anticipated PIRs and IRs.
- Develop and maintain current and future intelligence situational, threat, and environmental assessments and target intelligence based upon all-source analysis, interpretation, and integration.

Manage and fuse the threat COP/CTP inputs from subordinate units and external commands and intelligence agencies into the MEF CE's threat COP/CTP.

MAGTF Intelligence Units

The limited number of specialized intelligence assets, coupled with the requirement to integrate and focus intelligence operations on the satisfaction of the command's PIRs, creates the need for centralized management. Intelligence units whose capabilities support the entire MAGTF are employed in general support of the MAGTF with staff cognizance exercised through the G-2/S-2. Certain intelligence units are capable of performing operational tasks in addition to their primary intelligence functions. For example, a force reconnaissance team may carry out a laser target designation mission or a UAV may be used to assist in maneuver control. Likewise, radio battalion may support maneuver and fires through electronic attack operations. The MAGTF G-2/S-2 provides centralized direction for these assets and facilitates unity of effort, the production of all-source intelligence, and the effective use of limited resources in support of the requirements of the entire force. Direction is provided primarily through MAGTF-level intelligence C2 agencies; e.g., the SARC and the OCAC. Subordinate elements of the MAGTF retain organic intelligence assets and OPCON appropriate to their mission and level of command; e.g., division ground reconnaissance units remain under the OPCON of the division commander.

Organization of MAGTF-Level Intelligence Units

Radio Battalion

The radio battalion provides ground-based SIGINT, electronic warfare (EW), communications security

monitoring, and special intelligence communications capability to support MAGTF operations. In addition to directing the employment of its subordinate elements, the radio battalion is the focal point for MAGTF ground-based SIGINT operations. It plans and coordinates these activities through the OCAC.

Intelligence Battalion

The intelligence battalion plans, directs, collects, produces, and disseminates intelligence and provides CI support to the MEF, MSCs, subordinate MAGTFs and other commands as directed. This support is usually provided by a task-organized detachment sent to the supported command. Within the intelligence battalion is a headquarters company, a P&A company, and a CI/HUMINT company. (See figure 4-3.).

Headquarters Company

The headquarters company consists of a systems support platoon, collections platoon, and the GSP. The systems support platoon maintains the intelligence systems within the battalion in garrison and in the field should the battalion deploy. The collections platoon manages intelligence requirements for the battalion. The GSP is responsible for planning, controlling, and managing the employment of unattended ground remote sensor equipment in support of MAGTF operations or other commands as directed.

P&A Company

The P&A company consists of an AFP, a topographic platoon, and an IIP. The AFP provides fused intelligence to the supported MAGTF and

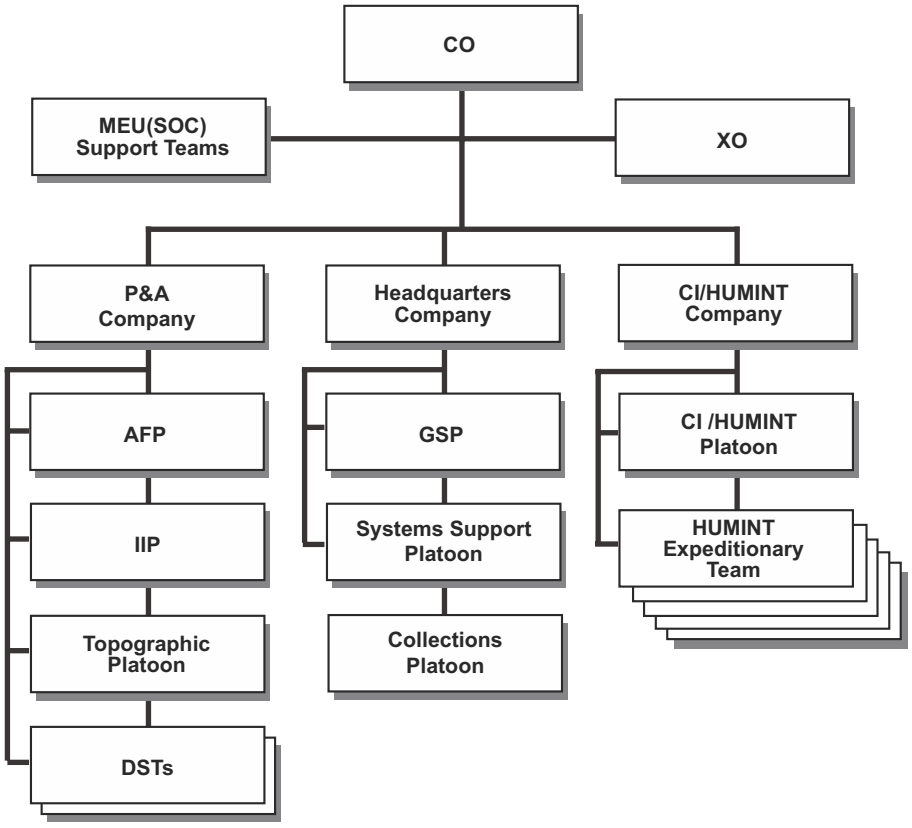


Figure 4-3. Intelligence Battalion.

assists MSC intelligence sections in providing situational awareness to their commanders and staff. The topographic platoon provides geographic intelligence products and services, geodetic and topographic surveys, and hydrographic analysis. The IIP provides imagery analysis support and dissemination to the MAGTF and other commands as directed.

CI/HUMINT Company

The CI/HUMINT company provides CI and HUMINT support to MAGTF operations. This support encompasses the full range of tactical CI and HUMINT operations, including screening operations, interrogation/debriefing of enemy prisoners of war and persons of intelligence interest, conduct of CI force protection source operations, conduct of CI surveys and investigations, preparation of CI estimates and plans, translation of documents, and limited exploitation of captured material. In addition, the CI/HUMINT company maintains a technical surveillance countermeasures team with equipment. CI/HUMINT Marines deploy as a task-organized HUMINT exploitation team (HET) in direct support of MAGTF's and subordinate elements.

Force Reconnaissance Company

The force reconnaissance company conducts preassault and deep postassault R&S in support of MAGTF operations. The company uses specialized insertion, patrolling, reporting, and extraction techniques to carry out amphibious and deep R&S tasks in support of the MAGTF. The company can perform a variety of other operational tasks. When a conflict exists between the requirements for R&S and other missions, the MAGTF commander determines the priority of tasking for the company based on recommendations from the G-2/S-2 and G-3/S-3.

Marine Unmanned Aerial Vehicle Squadron (VMU)

VMUs provide day/night, real-time imagery reconnaissance, surveillance, and target acquisition in support of the MAGTF. The unique capabilities of the UAV can also be used to support target engagement, assisting in the control of fires/supporting arms and maneuver. Squadrons are under the administrative control of the Marine aircraft wing (MAW). However, because of the limited number of assets and the critical capabilities they provide to the entire force, the MAGTF commander retains OPCON of the VMUs.

Employment of MAGTF Intelligence Units

MAGTF intelligence units are employed to meet the requirements of the entire force. The MAGTF G-2/S-2 develops a concept of intelligence support, which employs these units on the basis of the MAGTF mission, PIRs, concept of operations, and commander's intent. This concept must integrate intelligence activities with operations to provide key intelligence to commanders to enable rapid and effective decisionmaking. Based on the results of IPB analysis and the concept of operations, assets are positioned to satisfy PIRs, expose enemy vulnerabilities, monitor key locations, detect and assist in the engagement of targets, and identify opportunities as they arise in the battlespace.

Intelligence units are employed in either general or direct support. Under general support, units are tasked by the MAGTF commander through his G-2/S-2 to satisfy the requirements of the entire force. Because of the limited number of specialized intelligence assets and their ability to develop intelligence that is relevant to current and future operations in all areas of the battlespace (deep, close, and rear), general support is the preferred support relationship. Under direct support, the requirements of a supported commander are given priority. Direct support is used to focus intelligence support for particular phases of an operation or to create enhanced intelligence nodes in support of MAGTF subordinate elements. When MAGTFs smaller than a full MEF are deployed, they will normally be supported by

attached, task-organized detachments from the intelligence battalion, the force reconnaissance company, and the radio battalion.

Focused Intelligence Support

Intelligence must be integrated with the mission, commander's intent, and concept of operations and should normally be weighted to support the main effort. The MAGTF intelligence structure has the flexibility to tailor its capabilities to meet the requirements of various types of expeditionary operations and to adapt to changing operational needs during the execution. For each operation, the MAGTF G-2/S-2 will assess the IRs and develop a concept of intelligence support that positions assets where they can best satisfy those requirements. Intelligence nodes will be used to focus support within the MAGTF. Split-basing will be used to build intelligence nodes within and outside the AO to deliver comprehensive and reliable intelligence support while reducing the size of the deployed force. Intelligence units and DSTs are employed to tailor and enhance the capabilities of organic intelligence sections or to create task-organized intelligence nodes in response to specific requirements.

Intelligence Nodes

The MAGTF can create a series of intelligence nodes, thereby providing focused intelligence support to specific units or areas based on the tactical situation. In the concept of intelligence support, the MAGTF G-2/S-2, in conjunction with the MSC intelligence officers, task-organizes the MAGTF's intelligence units and uses intelligence DSTs to deliver the required intelligence capabilities at key points and times. Although these nodes normally support a specific unit, they can also be used in an area-support mode where an intelligence node is established to support all units operating in a particular sector of the battlespace. For example, during sustained operations ashore, an intelligence node could be built to support units operating in the MAGTF's rear area. Such a node could be built around a DST and specialists from the CI/HUMINT company and topographic platoon. This node might support the rear area operations center, CSSE units operating in the area or any security detachments located within the node's area of responsibility.

Split-basing

Intelligence nodes can also be used to tailor the footprint of the intelligence organization within and outside of a designated AO. Intelligence assets are positioned where they can best carry out their assigned functions. In many cases, it may not be necessary or desirable to forward deploy the entire MAGTF intelligence structure. The concept of operations, C2 support system, physical space limitations, and resource and/or logistical or other constraints may require the split-basing of intelligence assets.

Split-basing is the positioning of critical capabilities within the AO to support the deployed commander and forces, while maintaining in-depth intelligence management, processing, exploitation, analysis, and production elements in rear areas, intermediate support bases, staging areas or garrison locations. Split-basing enables reach back capabilities and can enhance the intelligence effort by providing continued access to sophisticated, nondeployable intelligence capabilities and resources. At the same time, it reduces the footprint of the deployed force, diminishing risk from enemy action and decreasing the administrative and logistic support requirements.

Split-basing is especially useful—

- When operations are conducted in areas with minimal infrastructure and support.
- When there are limitations on the number of personnel who can be deployed within the operating area.

- During the deployment phase when it may not be possible to immediately move all required elements of the intelligence structure to the forward area.

However, the advantages of split-basing must be assessed against its costs, particularly its critical dependence on responsive and reliable communications support.

Task Organization of Intelligence Support Units

Task organization of intelligence support units is one of the principal means for the MAGTF commander to shape the intelligence effort. The collection, exploitation, and unique production capabilities of specialized intelligence units significantly enhance the ability of supported G-2/S-2 sections to develop timely, mission-focused intelligence.

Intelligence battalion, force reconnaissance company, and radio battalion elements are task-organized to provide tailored intelligence capabilities. Specific capabilities provided are based on the threat, the supported unit's anticipated requirements (as determined through IPB), and the concept of operations. Elements from some or all of the intelligence battalion's subordinate companies are combined into intelligence battalion detachments. The CI/HUMINT company provides HETs. The radio battalion forms task-organized SIGINT support units (SSUs), which provide a mix of SIGINT and EW capabilities.

When MAGTFs smaller than a full MEF deploy, an intelligence battalion detachment, a HET, force reconnaissance platoons, and a radio battalion SSU will normally be attached to the MAGTF CE. In MEF operations, when the entire radio battalion, intelligence battalion, and force reconnaissance company are employed, detachments, HETs, SSUs, and platoons may be placed in direct support as required to provide tailored intelligence capabilities or to create an enhanced intelligence node in support of an MSC or other MAGTF element.

Intelligence DSTs

Intelligence DSTs are organic to the intelligence battalion and each of the division, MAW, and force service support group G-2 sections. Teams are made up of one officer and several enlisted personnel who have a mix of intelligence specialty skills. DSTs are used to provide an enhanced analytical and dissemination capability to a unit intelligence section and to link the intelligence structure to the supported units. As assigned by the G-2, they augment the supported unit's intelligence section to carry out the following tasks:

- Perform P&A in support of future operations.
- Tailor AFC and other external source intelligence products to the needs of the supported commander.
- Assist in the management of external intelligence support requirements.
- Facilitate dissemination of intelligence received from external sources.

The MEF and MSC G-2s use their DSTs to tailor and focus intelligence support to units designated as the main effort or to create enhanced intelligence nodes at key times and places in the battlespace.

Intelligence Coordination

Establishing and supervising operation of the MEF IOC, which includes the support cell, the SARC, and the P&A cell, requires a high degree of coordination at all levels. Generally the IOC will be collocated with the MEF CE's main CP. See figure 4-4 on page 4-14 for the basic IOC organization.

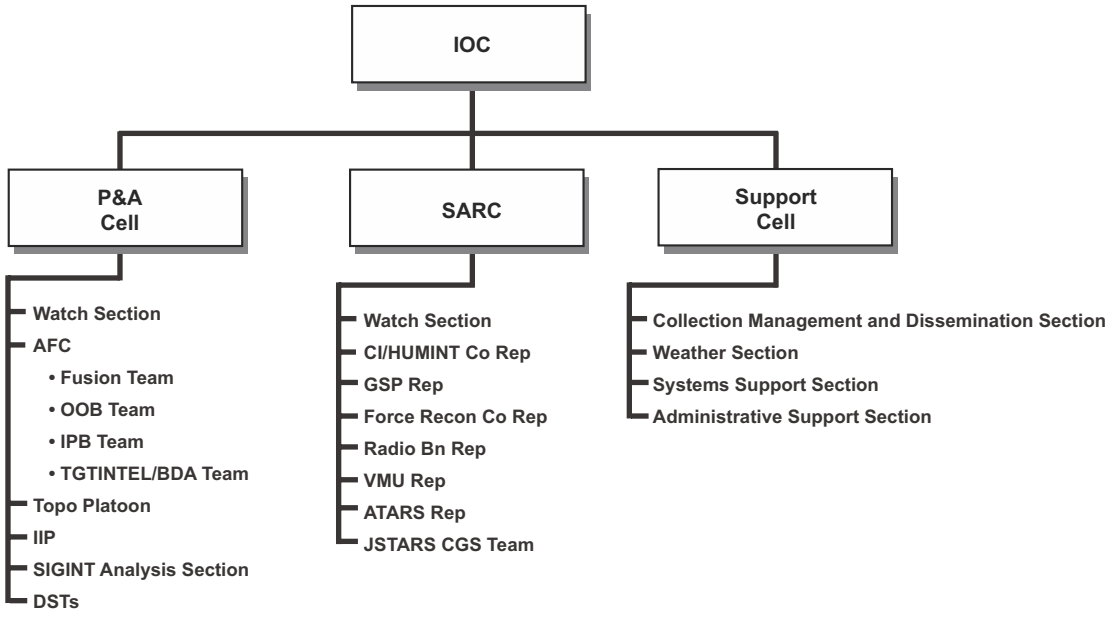


Figure 4-4. Intelligence Operations Center.

External Intelligence Support to the MAGTF

MARFOR Component Intelligence Section

Future military operations will normally be joint operations and may require establishing a MARFOR component headquarters. The Marine component is the level of command that deals directly with the JFC—the theater combatant commander or JTF commander—for MARFORs assigned to combatant command or the JTF. The Marine component functions at the operational level of war to advise and assist the JFC in employing MARFORs while supporting the MAGTF. The Marine component commander coordinates operational actions with the JFC and the other component commanders so that the MAGTF commander can concentrate on warfighting.

Responsibilities

The Marine component intelligence section plays a crucial role in supporting the component commander and staff and in providing intelligence support to the MAGTF. The Marine component supports and enhances the planning and execution of MAGTF intelligence operations through close and continuous coordination with the JFC, joint force headquarters, and other component intelligence organizations. The Marine component G-2 section maintains situational awareness and provides a limited analytical capability to support the component future planning responsibility. It does not normally conduct collection operations or engage in detailed, formal intelligence production. It facilitates, but does not control, the flow of intelligence to the MAGTF. The component relieves the MAGTF commander of intelligence functions that are not directly related to warfighting.

Functions

The size of the Marine component G-2 section will vary with the size of the JTF and the scope of the operation. For major joint operations, the Marine component intelligence section provides the following functions:

- **Planning.** The intelligence section plans and coordinates component and MAGTF connectivity to national, theater, and JTF intelligence architectures. The Marine component develops the architecture to provide the MAGTF with timely, tailored national and theater intelligence. The component G-2 coordinates the provision of additional Service intelligence support (units, personnel, and equipment) to the MAGTF through the Service chain of command.
- **Collection management.** The intelligence section monitors the status of MAGTF collection requests for supporting and external collection resources. The MARFOR leverages joint and national collection resources in support of the MAGTF. It advocates Service component and MAGTF requirements in theater and JTF collection forums and recommends the allocation and tasking of national, JTF, and other component assets to meet MAGTF requirements.
- **P&A.** The intelligence section provides situational awareness to the component commander and staff and limited P&A to support the future planning responsibilities of the component headquarters. This function requires the establishment of a watch section and an analytical element that can tailor operational-level intelligence products to satisfy the needs of component planning cells. The component G-2 monitors the status of and coordinates support for MAGTF production requirements and requests for intelligence that are submitted to joint force or supporting intelligence agencies.
- **Dissemination.** The intelligence section monitors the adequacy of the intelligence architecture and the flow of intelligence to the MAGTF. Intelligence is disseminated directly to the appropriate MAGTF elements, not through the component headquarters unless specifically required. However, the MARFOR facilitates and accelerates the flow of critical intelligence to the MAGTF. The component intelligence section remains aware of current MAGTF requirements and ensures that intelligence that is developed or received by the theater or JTF that can satisfy those requirements is disseminated to the MAGTF.
- **Support of targeting.** The intelligence section supports Marine component participation in the joint targeting process, including representation at various joint target intelligence and/or targeting forums as required. Performing this function ensures that MAGTF target intelligence collection and production requirements as well as collection requirements for support of combat assessment/BDA are adequately supported.

Liaison

The intelligence section provides liaison elements and personnel augmentation to various JTF and other component intelligence organizations. Liaison elements may be provided to the following:

- JISE.
- Other Service or functional component intelligence sections.
- The regional SIGINT operations center.
- The joint force J-2 CI/HUMINT staff element.
- The HUMINT operations cell.
- Task force CI coordinating authority, other joint intelligence organizations such as the joint interrogation and debriefing center or the joint document exploitation center.
- The intelligence elements of various alliance or coalition partners.

Liaison teams or personnel augmentation may be sourced from the Marine component G-2 section, Service augmentation to the component G-2 section, the MAGTF, or some combination of the above.

National, Theater, Joint, and Other Service Intelligence Support

Marine Corps intelligence assets are optimized for the production of tactical intelligence in support of MAGTF operations. National, theater, joint, and other Service intelligence assets provide unique capabilities that are not duplicated in the MAGTF intelligence support structure. (See figure 4-5.) The MAGTF has the ability to use external intelligence assets to enhance its organic capabilities, bringing the full range of these resources to bear on MAGTF requirements. The following are key external capabilities that support MAGTF operations:

- National- and theater-level intelligence analysis and production.
- Geospatial information and services (GI&S). GI&S describes the collection, production, and dissemination of information about the earth, and replaces the term mapping, charting, and geodesy.

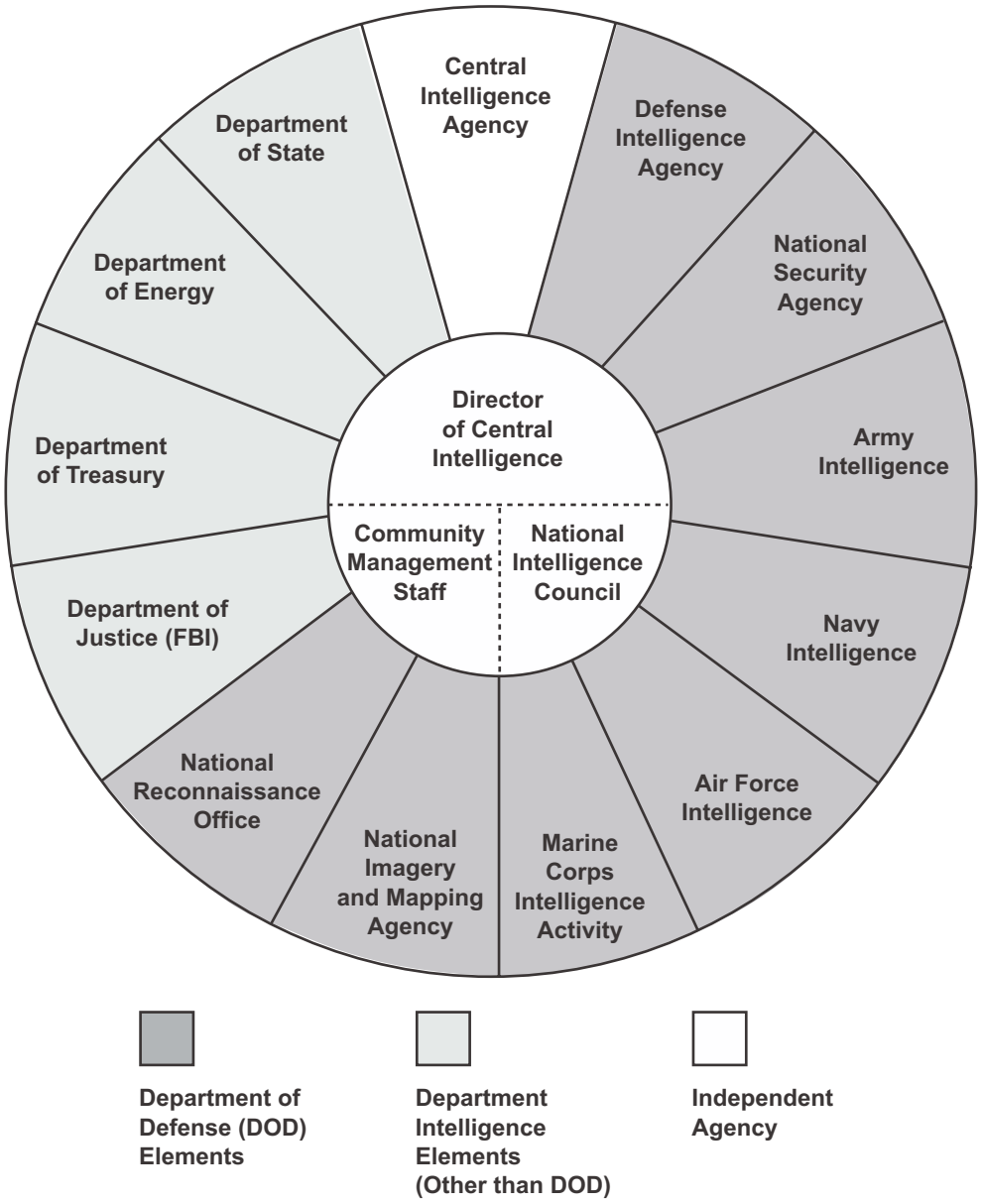


Figure 4-5. The National Intelligence Community.

- Analysis and production of target intelligence and target materials.
- National imagery collection and exploitation.
- SIGINT support from the National Security Agency and the US Cryptologic System.
- National- and theater-level CI and HUMINT collection.
- Liaison elements from national and theater intelligence agencies.

MAGTF Access to External Support. The Marine component headquarters or the MAGTF intelligence section will be the focal point for all external intelligence support to the MAGTF. In major joint operations, a Marine Service component headquarters will be established, and the component G-2 performs this function. When no Service component headquarters is established, the MAGTF acts in this role. Intelligence derived from external sources is used to build a common picture of the battlespace and is incorporated into other intelligence products that are provided to all MAGTF elements. MSCs and other subordinate units will be able to access external intelligence support resources through the MAGTF's intelligence architecture.

Required Capabilities

The following capabilities are required to fully use the resources of external intelligence support assets:

- Personnel trained and experienced in the capabilities, limitations, tasking, and employment procedures of external intelligence support assets.
- Sufficient, reliable CIS connectivity and interoperability with national, theater, and other Service intelligence C2 centers and architectures.
- The ability to receive, process, and disseminate information gathered by national and theater collection assets.
- Integrating Marine intelligence specialists into national, theater, and Service intelligence organizations to articulate Marine Corps capabilities and requirements and to optimize intelligence support to expeditionary forces.
- Establishing liaison between the MARFOR/MAGTF and supporting intelligence agencies through dedicated communications and the exchange of liaison officers.

Augmentation

Like all MAGTF components, intelligence support assets are flexible and respond to a variety of operational missions. They are configured for rapid deployment and can be tailored to meet the requirements of a particular operation. Although each MAGTF is furnished with a baseline intelligence capability to accomplish its anticipated mission, changes in the situation or mission tasking may require augmentation. When a MAGTF is committed to an operation, the intelligence assets of any remaining units in the operating forces can be called on to provide this augmentation. MAGTFs smaller than a MEF will normally be supported by their parent MEF; a fully deployed MEF can be augmented by the assets of any other MEF. Augmentation may consist of providing entire intelligence units, selected equipment or individual personnel with specialized skills. Support may also consist of providing intelligence products that cannot be developed by the deployed MAGTF or its supporting joint intelligence activity.

Supporting Establishment

Marine intelligence personnel and organizations of the supporting establishment enhance and sustain the intelligence activities of the operating forces.

Marine Corps Intelligence Activity

The Marine Corps maintains a Service-level intelligence capability in the Marine Corps Intelligence Activity (MCIA). MCIA focuses on crisis and predeployment support to expeditionary warfare. It complements the efforts of theater, other Service, and national intelligence organizations. It provides

unique threat, technical, and geographic intelligence products that are tailored to Marine Corps operating forces preparing for deployment. It also coordinates Marine Corps Service collection, production, and dissemination requirements by acting as the Service collection, production, and dissemination manager. MCIA is collocated with the National Maritime Intelligence Center, Suitland, MD and at Marine Corps Base, Quantico, VA.

Marine Cryptologic Support Battalion

The Marine cryptologic support battalion provides Marine Corps participation in national and Department of the Navy cryptologic activities worldwide. These Marines perform tasks that are directly related to their military occupational specialty, contributing to the national, theater, and Department of the Navy SIGINT collection, production, and dissemination effort while gaining invaluable skill maintenance and enhancement opportunities. The battalion is collocated with the Naval Security Group, Fort Meade, MD and augments the operating forces with trained SIGINT personnel during crises and exercises.

Navy Marine Corps Intelligence Training Center

The Navy Marine Corps Intelligence Training Center (NMITC), Dam Neck, VA trains Navy and Marine Corps personnel in basic, intermediate, and advanced intelligence methods and applications. During contingency operations, NMITC supports the operating forces through the provision of intelligence training via mobile training teams and/or selective personnel augmentation.

Personnel Augmentation

The supporting establishment is also a source of experienced intelligence personnel who can be called on to fill contingency billets in the intelligence structure of a deploying or committed MAGTF.

Marine Corps Forces Reserve

The mission of Marine Corps Forces Reserve is to provide trained units and/or personnel to augment, reinforce or reconstitute active duty MARFORs during times of war or national emergency. Intelligence capabilities of the Marine Corps Reserve are complementary to those of the active component. This includes individual mobilization augmentee and individual ready reserve personnel and selected Marine Corps Reserve units (including two force reconnaissance companies), a GSP, an imagery interpretation unit, and several interrogator-translator and CI teams, which provide increased depth to limited active component capabilities.

Individual mobilization augmentee members of the Marine Corps Reserve Intelligence Program and the Marine Corps Reserve Cryptologic Program routinely support the training and operational activities of the active component.

CHAPTER 5
OPERATIONAL MANEUVER FROM THE SEA

OMFTS is the maneuver of naval forces at the operational level that projects sea-based power ashore to deal a decisive blow. OMFTS is a bold bid for victory that aims to exploit a significant enemy weakness. It embodies the application of the principles of maneuver warfare to a maritime campaign. Success in OMFTS depends on the ability to seize fleeting opportunities and quickly take advantage of exposed enemy vulnerabilities. See MCDP 1-0, *Marine Corps Operations*.

OMFTS relies on intelligence to drive planning, option selection, and maneuver execution. To support OMFTS, intelligence operations must be conducted across the strategic, operational, and tactical levels of war. Starting with strategic considerations and working down to tactical dispositions, intelligence uncovers the threat's COG, strengths, and weaknesses, thereby exposing critical vulnerabilities to be exploited by naval forces operating from the sea. Intelligence also assesses the potential for maneuver offered by the battlespace, including identifying entry points where the force can establish itself ashore. The term entry point encompasses beaches, boat landing sites, HLZs, and drop zones that can establish elements of the force ashore. Intelligence also provides the foundation for effective force protection and IO efforts. These efforts help surprise, preempt, disrupt, and disorient the enemy during OMFTS execution.

Required Intelligence Capabilitites

- Perform IPB and situation development covering a broad maneuver space.
- Analyze threat forces to determine COG and critical vulnerabilities.
- Conduct detailed terrain and hydrographic analysis to identify suitable entry points.
- Ensure connectivity and interoperability with national, theater, and joint forces' intelligence assets, which provide intelligence support before the arrival of naval forces in the objective area.
- Provide stand-off collection assets that can satisfy force requirements from over-the-horizon.
- Provide organic imagery, SIGINT, HUMINT, CI, remote sensor, GI&S, and ground and aerial reconnaissance assets that can satisfy MAGTF tactical collection requirements as the force transitions ashore.
- Provide responsive processing, exploitation, and production capabilities that can rapidly develop the critical intelligence required to support timely decisionmaking.
- Provide dissemination systems that link widely dispersed forces afloat and ashore.
- Provide flexible intelligence units and organizations that can rapidly transition ashore with minimal degradation of support.
- Provide in-depth support to force protection and information operations activities.

Planning and Direction

There are a number of unique intelligence considerations for OMFTS. (See figure 5-1 on page 5-2.) During the planning phase, the MAGTF intelligence officer provides centralized direction for the intelligence efforts of the entire MAGTF. Navy and Marine intelligence assets operate together from an afloat amphibious force intelligence center, which is normally located on the amphibious force flagship. Initial requirements are broad in scope and are aimed at providing a general description of the battlespace and the threat. As planning progresses, requirements become increasingly focused on uncovering critical vulnerabilities and providing

intelligence that is relevant to the COAs under consideration. The intelligence flow will be predominately from the top down—from national and theater activities—until organic naval intelligence capabilities can be brought to bear. A comprehensive, systematic management effort is required to ensure that the necessary support is requested and received. At the same time, Navy and Marine intelligence officers must also develop detailed plans for the positioning and employment of the organic intelligence assets to support the concept of operations.

Intelligence Cycle	Key Considerations
Planning and direction.	Centralized direction from ATFIC. Transitioning of key capabilities ashore.
Collection.	Initial dependence on national/theater capabilities. Employment of organic assets in advance force/ preassault operations.
Processing, exploitation, and production.	Broad-based effort focusing on entry points and enemy vulnerabilities. Extensive support to CI and IO.
Dissemination.	Widely dispersed units afloat and ashore. Need for rapid intelligence flow to exploit fleeting opportunities.
Utilization.	COA selection shaped by intelligence. Choice of entry points, objectives, and targets driven by intelligence.

Figure 5-1. Intelligence Considerations During OMFTS.

Collection

Collection operations in the planning phase are conducted primarily by national and theater assets. These assets can collect information in denied areas without compromising operational security and/or perform their missions at significant stand-off distances. However, the small number of these systems and inherent limitations on their capabilities normally result in developing an incomplete intelligence picture. Advance force or preassault collection operations by naval assets will often be required to confirm and further develop the situation. An intensive intelligence effort must be provided in support of advance force or preassault operations; this intelligence support is required to select the proper targets for advance force or preassault collection operations, and ensure that these activities do not reveal the intent of the overall operation.

Processing, Exploitation, and Production

Initial production efforts are directed at providing an extensive description of the battlespace and threat. This description is required to focus the planning effort. Under the direction of senior Navy and Marine intelligence officers, the MAGTF, GCE, ACE, CSSE, Navy amphibious staff, and flagship intelligence sections engage in a cooperative effort to develop intelligence products that support the entire force. Individual intelligence sections will normally concentrate on their particular areas of expertise, thereby satisfying their units' requirements while contributing a broad-scope product to the general intelligence production effort. For example, the MAGTF G-2/AFC may focus on describing the battlespace and the enemy's C2, logistics, and reserves, while the GCE studies enemy ground forces, the ACE looks at the air and air defense threats, and the flagship intelligence department concentrates on the naval and coastal defense threat. From this effort, the ATFIC provides a comprehensive IPB analysis, an intelligence estimate, and supporting intelligence studies and products. As the planning phase continues, production efforts concentrate on identifying enemy vulnerabilities to be exploited and providing estimates and other intelligence products to support the specific COAs that are under consideration.

In the final stages of the OMFTS planning process, the production effort shifts to developing mission-specific intelligence products that focus on the selected COAs. These products include

IPB graphics, beach and HLZ studies, and target/objective area studies. An extensive all-source intelligence effort is conducted to support deception, OPSEC, psychological operations (PSYOP), and EW planning in accordance with the MAGTF commander's overall IO strategy. During this stage, the production effort becomes increasingly decentralized as GCE, ACE, and CSSE intelligence sections focus on specific requirements of their units. The MAGTF intelligence section continues to provide products to support the entire force, with efforts concentrated on those MAGTF elements designated as the main effort.

Dissemination

Dissemination in OMFTS presents significant challenges. Naval forces can be widely dispersed and may not assemble until late in the planning phase, if at all. Advances in technology have improved the capability to disseminate information between forces afloat, but there continue to be limitations on the quantity and quality of intelligence that can be exchanged. In particular, dissemination systems will be taxed by the volume of intelligence products, especially critical graphic products that must be distributed during the planning phase. Intelligence officers at all levels, working in coordination with unit operations and CIS officers, must develop plans that provide for dissemination of key intelligence in a timely manner to all elements of the MAGTF. They must be particularly careful to include in these plans units located on ships that are not equipped with the latest C2 or intelligence systems.

Utilization

During the planning phase, intelligence is used to develop and select COAs and prepare detailed plans for implementing the selected COAs. After providing an initial orientation to the battlespace and the threat, the intelligence officer assists the commander and the staff in analyzing the enemy's strengths and weaknesses to identify COG and critical vulnerabilities that can be exploited. COAs are developed that take advantage of identified weaknesses to accomplish the assigned objective. The intelligence effort is refined on the basis of the COAs under consideration, providing answers to IRs generated during COA development. The intelligence developed through this interactive process aids the commander in selecting a favorable COA. Once the COA is chosen, intelligence shapes the concept of operations and supporting plans. Designation of objectives; selecting entry means, points, and times; and identifying targets are all based primarily on intelligence. Particular attention is given to steps that preserve surprise and that preempt, disrupt or disorient the enemy's response to our actions; e.g., force protection measures, and IO (including, but not limited to, physical destruction, military deception, OPSEC, PSYOP, and EW) plans.

Planning and Direction

The ATFIC will continue to act as the central node for the direction of the intelligence effort. As the operation unfolds, intelligence nodes can be established ashore to support units carrying out mission tasking. Depending on the nature and scope of the operation, most of the MAGTF intelligence structure can remain afloat or all of it may transition ashore. Movement of significant portions of the MAGTF intelligence structure ashore must be planned in detail to ensure a rapid transition with minimal degradation of support capability. If it is fully established ashore, the MAGTF intelligence section becomes the central node for intelligence direction. The ATFIC acts in a supporting capacity and continues to provide connectivity and services that cannot be readily established ashore.

IRs that arise during execution are normally time sensitive. Intelligence direction must anticipate these requirements and establish a responsive collection, production, and dissemination structure to satisfy them. Designation of PIRs that are based on the results of IPB analysis, the commander's intent, and the concept of operations is critical. Using these factors to designate PIRs ensures that the intelligence effort remains focused on providing key intelligence to decisionmakers in a timely manner.

Collection

Collection operations transition from depending on national and theater capabilities to relying primarily on organic assets. Collection activities are integrated with the concept of operations. The objective is to develop the intelligence required to make key decisions regarding maneuver, targeting, and future plans. Collection assets are focused on key areas that are associated with the scheme of maneuver, location and development of critical targets, and combat assessment. Reports of units maneuvering through the battlespace and/or in contact with the enemy are a significant source of information. This information must be transmitted to the appropriate intelligence section to help maintain situational awareness and refine the threat assessment. The MAGTF continues to employ national and theater-level collection support against targets located deep in the area of influence, throughout the area of interest, and against less time-sensitive requirements.

Processing, Exploitation, and Production

Rapid processing and production of intelligence are emphasized to support timely decisionmaking. OMFTS depends on decisive action and generating rapid operational tempo to break the enemy's cohesion and ability to resist. Intelligence sections must demonstrate the flexibility, agility, and responsiveness to quickly recognize enemy vulnerabilities and identify opportunities as they develop during the battle. To do this, intelligence sections at all levels must be aware of ongoing tactical activities and potential enemy reactions. They must be able to rapidly integrate all-source intelligence information with sensor data and combat reporting to develop and maintain a coherent picture of enemy dispositions and an assessment of enemy intentions. They must be able to convey this picture and assessment (preferably in graphic form) to commanders in time to exploit identified opportunities. In addition to supporting the ongoing battle, intelligence sections must also be fully engaged in planning for future operations (continuing IPB analysis, delivering combat assessment inputs and BDA results, satisfying new IRs, and participating in the decisionmaking process).

Dissemination

Dissemination is an even greater challenge during OMFTS execution than during planning. Intelligence developed during the processing, exploitation, and production step must be rapidly disseminated to the units that are able to act on that intelligence. These forces may be widely dispersed afloat, airborne, and ashore while engaging in rapid maneuver and contact with the enemy. The dissemination system must be flexible and reliable and focus on the importance and quality of the intelligence distributed rather than on its volume. Dissemination plans must provide alarm channels for warning data and must ensure that pathways remain open for passing critical intelligence that directly affects PIRs or identified decision points. Measures that can help to reduce the volume of intelligence traffic follow:

- Limit routine reporting.
- Set filters to eliminate information that is not pertinent to the tactical situation.
- Establishing minimal reporting thresholds for the generation of intelligence reports.
- Providing alternate means for collection and other intelligence support requests.

Dissemination plans must permit two-way dissemination, providing a means for subordinate

elements to pass along data, information or intelligence that they collect or develop that identifies new enemy vulnerabilities or enhances situation development for the entire force.

Utilization

Utilization of intelligence during the execution of OMFTS is rapid and decentralized. Intelligence identifies enemy vulnerabilities as the battle unfolds.Once developed, this intelligence is quickly disseminated to the MAGTF elements that can act on it, thereby enhancing the ability of individual units to exploit opportunities as they arise. Through integration with operations, assets are positioned to develop new intelligence as the concept of operations is carried out and the enemy responds. Timely collection, analysis, and dissemination of intelligence provides commanders with an accurate picture of the battlespace and the ability to recognize new opportunities as they arise. Commanders use this intelligence to select branches and sequels to the COA, attack targets, protect their own forces, assess the results of their actions, and plan future operations.

CHAPTER 6
SUSTAINED OPERATIONS ASHORE

Sustained operations ashore require broad-based intelligence support that bridges the operational and tactical levels. Tactical plans are based on the results of operational-level intelligence assessments, which identify the enemy's COG and critical vulnerabilities throughout the theater of operations. MAGTF intelligence operations contribute to the operational-level assessments while translating the conclusions from these assessments into relevant tactical intelligence. Considerations for developing intelligence in support of sustained operations ashore are similar to those for OMFTS. Intelligence support during the execution of sustained operations ashore requires the same agility and responsiveness as in OMFTS, with the focus on providing critical intelligence to support timely decisionmaking. However, sustained operations ashore are normally conducted over a greater land area and with a larger force than in OMFTS, creating the requirement for a larger and more widely distributed intelligence support structure. The need for integration with theater, joint, multinational, and other Service intelligence assets is also greater.

Required Intelligence Capabilities

- Field and sustain intelligence structure to support MEF-level operations over extended periods.
- Execute all intelligence functions of a Service component headquarters, including full participation in theater or JTF intelligence activities.
- Ensure sufficient and reliable CIS systems connectivity and interoperability with theater, joint, and other Service intelligence assets participating in the operation.
- Conduct IPB and situation development in support of operational- and tactical-level planning.
- Provide organic imagery, SIGINT, CI, HUMINT, remote sensor, GI&S, and ground and aerial reconnaissance assets that can satisfy MAGTF tactical requirements.
- Provide processing, exploitation, and production capabilities that can supply the extensive products required to support MEF-level planning and execution.
- Provide dissemination systems that link widely dispersed and rapidly maneuvering forces.
- Provide area specialists and linguists with skills that are pertinent to the AO.
- Support force sustainment operations through detailed logistic intelligence.
- Support force protection efforts conducted throughout a large operating area, with emphasis on the security of critical rear area C2 and logistic facilities.

Planning and Direction

Intelligence direction during sustained operations ashore will be centralized during the planning phase and increasingly decentralized during execution. IRs are extensive and cover all aspects of the threat and the battlespace. Comprehensive collection, production, and dissemination efforts will be required to satisfy these requirements. Detailed management is necessary to ensure that these efforts are properly focused and integrated to meet the needs of the entire force. The MAGTF intelligence section will act as the primary intelligence node, developing intelligence to support the MAGTF commander, staff, and subordinate elements. The Marine component headquarters serves as the focal point for connectivity with the theater or JTF intelligence structure. During the planning phase, timeliness of

intelligence production may not be as critical because the planning process for sustained operations ashore normally takes place over an extended period and offers the opportunity to use more time and resources to answer those requirements. (See figure 6-1.)

Intelligence Cycle	Key Considerations
Planning and direction.	MAGTF acting as central mode. Need for broad intelligence structure with extensive liaison requirements.
Collection.	Competition for national, theater, and JTF support. Reliance on organic assets to satisfy many tactical requirements. Support to BDA.
Processing, exploitation, and production	Wide-scope effort that bridges operational and tactical levels. Importance of target and geographic intelligence.
Dissemination.	Extensive CIS infrastructure. Widely dispersed units. Timely support.
Utilization.	Need to integrate operational and tactical levels of intelligence and operations. Support to sustainability functions.

Figure 6-1. Intelligence Considerations During Sustained Operations Ashore.

Once execution begins, the emphasis is on satisfaction of time-sensitive requirements to support operational and tactical decisionmaking. Intelligence nodes will be created at selected times and places to provide tailored intelligence support to units executing specific phases or aspects of the concept of operations. Intelligence direction must balance the support provided among close, deep, and rear operations and the support to current and future operations.

The intelligence structure required to support sustained operations ashore is normally more extensive than that used in other types of MAGTF operations. A detailed planning effort must be undertaken to ensure that the necessary assets are tasked, deployed, and positioned where and when they are required. Sustained operations ashore are frequently based on a theater combatant commander's approved operations plan or other standing contingency plans that include provisions for a baseline intelligence support structure. These plans must be adapted and tailored to the particulars of the current and projected operational situation. Intelligence plans use a building-block approach, phasing in capabilities to keep pace with the buildup of operational forces. Planners must remain aware that intelligence capabilities must be in place to support the earliest steps of the planning phase; therefore, a robust intelligence structure is normally required in the initial stages of the deployment.

Many of the intelligence activities conducted during sustained operations ashore will be joint. Intelligence plans must provide for connectivity with the theater or joint and other component intelligence assets and for participation in theater or JTF intelligence mechanisms. An extensive liaison effort will be required to ensure that MAGTF IRs and operations are fully coordinated with those of joint and other Service intelligence activities. The MARFOR and MAGTF will require significant personnel augmentation to meet the broad scope of intelligence activities in sustained operations ashore and provide liaison teams to the numerous joint and supporting force intelligence agencies. This augmentation can be drawn from residual forces, the supporting establishment or the Reserves.

Collection

Sustained operations ashore will normally be supported by the full range of national- and theater-level collection capabilities and by the organic assets of the participating component forces. Collection priorities for national and theater assets will be determined by the JFC. The bulk of these assets will usually be targeted against overall theater/JTF objectives. Marines must participate in the joint collection management and production processes to ensure that MAGTF PIRs receive

appropriate support from the theater/JTF level. However, even if MAGTF requirements are given priority, the results of national and theater collection operations cannot be relied on to completely satisfy the number of requirements developed during extended sustained operations ashore or to provide the level of detail needed for tactical planning and execution. For this reason, the MAGTF must depend on its organic collection assets to provide the bulk of its tactical intelligence information, particularly during the execution phase. The MAGTF must be prepared to plan and execute imagery, SIGINT, HUMINT, ground reconnaissance, and CI force protection source operations throughout its AO. This includes collection activities in support of deep operations and the planning of future operations. MAGTF collection plans must be coordinated with those of higher, adjacent, and supporting commands to ensure the following:

- All requirements receive adequate coverage.
- Collection assets are employed efficiently with minimal overlaps.
- Collection operations are sufficiently integrated to permit free exchange of collection targeting data and tracking of collection targets as they move through the battlespace.

Processing, Exploitation, and Production

Processing, exploitation, and production efforts in support of sustained operations ashore parallel those for OMFTS. The scope of the initial production is broad, with the focus narrowing as particular COAs are selected and a concept of operations is developed. Geographic intelligence production takes on added importance. Geographic intelligence helps identify opportunities for ground and air maneuver and determine line-of-sight profiles for observation, weapons employment, and the effective use of communications-electronic equipment. Mapping enhancements, lines-of communications studies, and IPB graphics (such as cross-country mobility, weather effects, and combined obstacle overlays) are key intelligence products that support sustained operations ashore.

Threat analysis must be comprehensive and generally deals with large ground and air formations. This analysis covers reserves and committed forces and must consider all factors that affect the enemy's ability to fight at the operational and tactical levels, including leadership, doctrine, training, readiness, and sustainability. An extensive production effort is devoted to supporting CSS operations. The main components of this effort are studies on the local climate, infrastructure, and resources and on the threat to our rear area and lines of communications. Products from national, theater, and JTF intelligence agencies contribute to the production effort, but many of these products will have to be tailored by the AFC and GCE, ACE, and CSSE intelligence sections to satisfy particular MAGTF requirements. During execution, emphasis is placed on rapid processing and production of tactical intelligence to support decisionmaking in the current battle, while at the same time providing detailed intelligence to shape plans for future operations.

Dissemination

The ability to develop and maintain a shared picture of the battlespace among the diverse components of the joint force is essential. MAGTF and Marine component dissemination architectures not only must provide for distributing intelligence within the MAGTF, but also must permit the timely exchange of intelligence with the theater or JTF headquarters, other component commands, and adjacent and supporting units. Marine intelligence architectures must be

fully integrated with the theater or JTF structures. This requires detailed planning and coordination because each theater and JTF has a unique architecture and sometimes separate channels are used for the dissemination of finished intelligence, imagery, SIGINT, HUMINT, and CI information. Dissemination during the early phases is normally simplified by establishing a reliable, redundant communications system between fixed or semi-fixed CPs. However, even a robust communications system will be challenged by the requirement to distribute a large volume of maps, imagery, and other graphic products during the planning stage.

During execution, the dissemination challenges are similar to those of OMFTS; i.e., ensuring the rapid distribution of time sensitive, mission-critical intelligence to widely dispersed units on the move or in contact with the enemy. A number of techniques can be used to prevent the loss of intelligence that is needed for timely decision-making in the stream of intelligence data and information. Some follow:

- Establishing alarm dissemination channels.
- Using broadcast mode for specialized intelligence reporting.
- Employing DSTs or designating a specific element of the intelligence section as a dissemination team.
- Linking dissemination to factors developed in the other phases of intelligence development, such as PIRs, named areas of interest, high-value targets, and high-payoff targets.
- Giving particular attention to the distribution of updated imagery and graphic intelligence products to units that cannot be supported from fixed or semi-fixed intelligence support nodes.

Utilization

The use of intelligence in sustained operations ashore follows the same principles as its use in OMFTS. The difference lies in the scope of the effort required and the need to integrate intelligence and operations simultaneously at multiple levels: theater or JTF, MARFOR, MAGTF, MSC, and tactical units (regiments/groups/battalions/squadrons/detachments).

In sustained operations ashore, intelligence is used to form operational and tactical plans that will accomplish campaign objectives. Broad-based strategic, operational, and tactical intelligence on the enemy and the AO is used by intelligence and operational planners in an interactive process to identify COG and critical vulnerabilities that can be attacked or exploited to achieve campaign objectives. This in turn leads to COA development, selection, and refinement, an effort that must be coordinated and integrated from the theater/JTF down to the tactical level. Intelligence helps determine the main and supporting efforts; designate objectives, times, and locations for these efforts; and identify the support required for each to succeed. During execution, intelligence helps develop the situation, supporting decisions on whether to continue or modify the plan and whether to exploit success or take advantage of new opportunities. At the same time, intelligence facilitates the planning of follow-on operations through support to combat assessment and providing continuing IPB analysis. Intelligence helps plan and conduct critical sustainability functions, contributing key logistic intelligence and force protection recommendations.

CHAPTER 7
MILITARY OPERATIONS OTHER THAN WAR

MOOTW refers to the conduct of Marine and naval expeditionary operations across the range of military operations short of war. MOOTW encompass a wide variety of activities intended to deter war, resolve conflict, promote peace, and support civil authorities. MOOTW encompass a broad range of 16 possible missions and tasks, each of which has its own unique IRs. (See MCDP 1-0.)

Intelligence activities in MOOTW are characterized by the following:

- The initial lack of detailed intelligence databases on the AO.
- An extensive list of nonstandard IRs that must be satisfied to support planning and execution.
- A rapidly changing situation resulting from crisis conditions in the AO.
- A compressed time frame for intelligence development.
- Restrictions on collection operations.

Intelligence shapes operations during MOOTW as it does during other types of expeditionary operations. However, in addition to understanding the physical environment and the threat, the commander must have intelligence on political, economic, and sociological conditions to develop sound military plans that will accomplish the assigned mission.

To support MOOTW, MAGTF intelligence operations and supporting assets must be maintained in a high state of readiness. MAGTF intelligence sections must focus on areas with the greatest potential for executing contingency operations and must be able to respond with minimal warning and preparation. They must also be flexibile to adapt to the wide variety of potential missions, possessing the expertise and specialized capabilities to provide intelligence across the full range of MOOTW.

Required Intelligence Capabilities

- Forward-deployed intelligence sections that are manned, trained, and equipped to respond to a variety of short-notice contingency operations.
- Deployable intelligence assets that can be rapidly "surged" to augment the capabilities of a forward-deployed MAGTF committed to MOOTW.
- Specialized knowledge concerning infrastructure, political, economic, cultural, and sociological conditions in a variety of geographic areas.
- The ability to perform IPB and situation development that focuses on unconventional threat forces, such as security forces, paramilitary groups, insurgents, and terrorists.
- Organic CI and HUMINT capability that is prepared for operation in a variety of MOOTW scenarios.
- SIGINT assets that can collect information from nontraditional targets.
- Dissemination systems that link widely dispersed forces.
- Connectivity to national, theater, joint, and multinational force intelligence assets to provide intelligence support during planning and execution.
- Area specialists and linguists with skills that are pertinent to the AO.
- Expertise in the operations and functioning of non-DOD government agencies, international coalitions, and nongovernmental organizations (NGOs). (An NGO is a transnational organization of private citizens that maintains a consultative status with the United Nations. NGOs may be professional associations, foundations, businesses or groups with a common interest in humanitarian assistance. Examples include the Red Cross and the Cooperative for Assistance and Relief Everywhere.)

Planning and Direction

There are certain unique intelligence considerations during MOOTW. (See figure 7-1.) Direction of the intelligence effort in MOOTW will generally be highly decentralized. During MOOTW, MAGTF elements can be spread across a wide area, each with a different mission and facing a unique situation. While a central node will be needed to direct the efforts of MAGTF intelligence assets and coordinate external support, the bulk of intelligence will be provided by subordinate intelligence sections supporting their individual units. Consideration should be given to directing the intelligence effort on an area-support basis rather than a unit support basis. In an area-support system, intelligence nodes are created to support all units operating in the designated area. IRs will be extensive and diverse. Many will deal with topics and threats that are not normally confronted during conventional operations. Individual intelligence sections and nodes must be provided with expertise or with access to resources that can satisfy these nonstandard requirements.

MOOTW are often generated as a result of fast-moving crisis situations. Intelligence plans must emphasize readiness and flexibility to respond to MOOTW requirements in a timely manner. MAGTF intelligence sections at all levels must maintain an awareness of potential contingency missions and adopt a "lean forward" approach toward anticipating requirements. Forward-deployed MAGTFs must possess all required intelligence capabilities to function in a wide variety of MOOTW missions. The active Marine service components (Marine Forces Atlantic or Pacific) must be prepared to rapidly deploy additional or specialized assets to augment the capabilities of the forward-deployed MAGTF.

In planning the intelligence structure required to support a particular MOOTW, several factors must be considered. The MAGTF intelligence section, whether afloat or ashore, must have connectivity to all supporting external intelligence agencies. It is often necessary to augment subordinate intelligence sections to provide an enhanced capability to support the independent activities of their units. There are normally extensive contacts with organizations outside the US military command structure during MOOTW. Liaison and information exchange with non-DOD agencies and NGOs and multinational and/or host nation military and security forces must be anticipated.

Intelligence Cycle	Key Considerations
Planning and direction.	Decentralized direction. Need for muliple intelligence support nodes with specialized capabilities.
Collection.	Nonstandard requirements. Importance of HUMINT, CI, and nontraditional collection activities.
Processing, exploitation, and production.	Focus on infrastructure, political, economic, and sociological factors. Use of nonstandard production formats.
Dissemination.	Large number of independent units operating throughout the area. Intelligence exchange with joint, multinational, and nonmilitary units.
Utilization.	Need to monitor effectiveness and effect of ongoing operations. Support to force protection, civil affairs, PSYOP, and sustainability.

Figure 7-1. Intelligence Considerations in MOOTW.

Collection

Because MOOTW present nontraditional targets, collection operations must blend the capabilities and limitations of all available assets. Satisfaction of unique MOOTW requirements often requires the use of specialized capabilities or innovative approaches to the employment of standard assets.

During the planning and initial phases of the operation, national and theater assets will be relied on to satisfy basic requirements concerning entry points, infrastructure, and conventional

aspects of the threat. Because supporting intelligence agencies often have limited capabilities in MOOTW situations, organic assets are brought to bear as early as possible, including being employed as part of the advance party or lead element of the force. The nature of the MOOTW environment, threat, and requirements often present a lucrative opportunity for the conduct of HUMINT and CI collections operations. A MAGTF committed to a MOOTW must have a robust CI and HUMINT capability, augmented by appropriate area specialist and linguist support. This capability should be deployed as soon as practical to initiate force protection collection operations and establish necessary liaisons. The MAGTF must also exploit open sources and maintain contact with non-DOD government agencies and NGOs.

Processing, Exploitation, and Production

Intelligence production requirements in MOOTW are normally focused on nontraditional subject areas. For example, detailed knowledge of the host nation's economic, transportation, medical, and public works infrastructure will be required to develop plans for humanitarian assistance operations. Threat studies to support a peacekeeping mission must encompass an extensive treatment of political, cultural, and sociological factors related to various insurgent or paramilitary factions in addition to the threat's military capabilities. Use of area specialists and expertise from external intelligence organizations, non-DOD agencies (State Department, US Agency for International Development, etc.), and NGOs is crucial to satisfying these requirements. Production formats must be adapted to the requirements of a particular situation. Normal IPB analysis must be modified to highlight factors crucial to the specific MOOTW mission. Processing and production in MOOTW must be responsive to the needs of the numerous small elements that may be conducting independent activities throughout the AO. Production in support of these elements must be tailored to specific mission requirements and provide details pertinent to the small-unit level. Intelligence that increases the situational awareness of individual Marines, such as information on local customs, language, and health and sanitation, is an important part of this effort.

Dissemination

Dissemination during MOOTW must provide for the timely distribution of intelligence to a large number of elements that are widely dispersed throughout the AO. Creating intelligence support nodes for a specific area or region will aid the dissemination effort, but only if these nodes are equipped to receive all-source intelligence (in particular imagery and graphic products) from supporting collection and production agencies. Dissemination plans must also include provisions for the exchange of intelligence with other Service and multinational units participating in the operation, non-DOD agencies, and NGOs. Interoperability, sanitation, declassification, and releasability must all be considered and determined before such exchanges can occur.

Utilization

Intelligence shapes the planning and execution of MOOTW just as it does in other types of operations. During planning, intelligence helps determine the nature and scope of the operations and tasks required to accomplish the mission, the size and type of forces required, and the location and duration of the effort required. During execution, intelligence is used to enhance the effectiveness of ongoing operations, assess the results of completed activities, and identify follow-on missions and tasks that will help accomplish the overall objective. Emphasis is also placed on intelligence support of specialized functions that have enhanced importance during MOOTW: logistics, force protection, civil affairs, and PSYOP.

CHAPTER 8
JOINT OPERATIONS AND MULTINATIONAL OPERATIONS

A coordinated intelligence effort makes a critical contribution to the success of joint operations. MAGTFs participate in full partnership with other Services in joint operations. MAGTF intelligence operations are fully integrated with joint intelligence activities to ensure unity of effort, mutual support, and effective employment of limited intelligence resources.

Multinational operations are "military actions conducted by forces of two or more nations, typically organized within the structure of a coalition or alliance." (JP 1-02) MARFORs may participate in a wide variety of multinational operations, ranging from routine bilateral exercises to coalition warfare in major regional contingencies. Instances of unilateral US military operations are becoming less frequent, particularly in MOOTW. Marine units must be prepared to carry out intelligence operations in the context of multinational operations.

Effective intelligence support in joint operations depends on the following:

- Agreement on policies and procedures.
- Mutual intelligence support.
- Shared intelligence capabilities and assets.
- Full interoperability and connectivity among participants.
- Robust liaison.

JFC and Component Commander Responsibilities

JFCs are responsible for all aspects of intelligence support within their commands. They have the responsibility and authority to determine, direct, and coordinate all mission-related collection and analysis activities through centralized or apportioned collection and production management efforts. Component commanders remain responsible for the intelligence function within their commands and use organic intelligence capabilities to support their assigned missions. The JFC makes national, theater, and joint force intelligence assets available to support the efforts of the component commanders. At the same time, component capabilities must be available to assist the joint intelligence effort.

Joint Intelligence Structure

The JFC is assisted in carrying out intelligence responsibilities by the joint force J-2. The J-2 exercises many of the JFC's intelligence functions while acting as the senior intelligence officer in the joint force. Intelligence assets of the joint force headquarters are consolidated in a JISE. The combatant (theater) command is supported by a JIC, which is a standing intelligence element. A JISE is a temporary agency established to provide support to a particular JTF. The JISE provides intelligence support to the JFC and the entire joint force. Marine intelligence specialists will be assigned to the JISE to articulate Marine capabilities and requirements, influence decisions, and optimize intelligence support to the Marine component. Key functions performed by the JISE follow:

- Centralized collection, production, and dissemination management for joint force and supporting intelligence assets.
- All-source intelligence production to satisfy JFC and component requirements.
- Developing and maintaining data bases that support planning, operations, and targeting.

- Producing target studies and materials.
- Providing access to supporting national and theater intelligence assets.

Each theater establishes its own intelligence architecture, providing connectivity between the national- and theater-level intelligence organizations, the JTF, and its component commands. MARFOR and MAGTF intelligence architectures must be able to plug into the architectures of any theater where they might be employed.

Procedures

Joint intelligence activities are governed by joint intelligence doctrine contained in JP 2-0, *Joint Doctrine for Intelligence Support to Operations*, and supporting manuals in the 2-series of JPs. Joint intelligence doctrine is supplemented by combatant commanders' TTP for intelligence developed by each theater command. During joint operations, Marine intelligence activities will adhere to joint doctrine and any published theater TTP pertaining to that operation.

Marine Intelligence Section and Unit Responsibilities

- Operate in accordance with joint intelligence doctrine, theater TTP, and individual JTF procedures.
- Participate in joint intelligence mechanisms to coordinate collection management, intelligence production, HUMINT and SIGINT collection operations, target intelligence support, intelligence architectures, CI activities and collection operations, and other intelligence operations.
- Provide intelligence support to the joint force headquarters or other JTF components as directed.
- Contribute personnel and other assets to augment the J-2 section and JISE if requested.
- Employ joint or other component intelligence assets.
- Enter the JTF intelligence architecture.
- Exchange liaison elements with the J-2, JISE, and/or other JTF components as required.

MARFOR Component Headquarters or MAGTF CE as a JTF Headquarters

A Marine component headquarters or a MAGTF CE may be designated to provide the nucleus of a JTF headquarters.The MARFOR or MAGTF G-2 must be prepared to function as the JTF J-2, with the G-2's intelligence section serving as the base for establishing a JISE. To carry out this function, MARFOR and MEF G-2 sections must prepare plans for operating as a JTF J-2 and conduct the training to be able to execute these plans. Plans should be based on joint doctrine and theater TTP and should include J-2/JISE organization, personnel and equipment requirements (with their augmentation sources), a baseline intelligence architecture, and standing operating procedures. Each MARFOR and MEF G-2 section should establish a standing JTF intelligence planning cell made up of intelligence specialists who are knowledgeable in joint force and other Service intelligence capabilities, limitations, and operating procedures to develop these plans.

Multinational Operations

There is no single intelligence doctrine for multinational operations. Each coalition or alliance must develop its own doctrine. The coalition commander determines standardized procedures for coalition forces. NATO standardization agreements (STANAGs) and quadripartite standing agreements among US, British, Canadian, and Australian forces provide standards and guidance to conduct military operations by forces in these alliances. STANAG 2936, *Intelligence Doctrine*, governs intelligence operations. Joint intelligence doctrine and architectures provide a framework for developing the multinational intelligence support structure. Multinational intelligence operations are based on the following principles:

- Maintain unity of effort. Intelligence operations must be directed at the common threat. A threat to one alliance member should be considered a threat to all.
- Make adjustments. Effective multinational operations require minimizing the differences in national concepts of intelligence support. Commanders and their intelligence officers must be willing to make adjustments to national procedures to share intelligence and integrate intelligence operations. Special arrangements should be considered for developing, communicating, and using intelligence where there are differences in nations' language, culture, doctrine, terminology, organization, and equipment.
- Plan early and concurrently. Multinational forces' IRs and procedures should be identified, planned, coordinated, and exercised before execution.
- Share all necessary intelligence. Each coalition member should share intelligence that supports planning and execution. However, information about intelligence sources and methods should not be shared unless absolutely necessary. The methodology for exchanging intelligence should be developed and exercised before operations begin. Authorization for foreign disclosure should be obtained and procedures for sanitation and declassification should be developed as part of this planning process. During execution, the exchange must be monitored and adapted to ensure that it is meeting the needs of all coalition partners.
- Conduct complementary intelligence operations. Each nation's intelligence assets capitalize on their strengths and offset the weaknesses of other members' assets, providing the coalition with the most effective blend of capabilities.

Many potential allies may not possess the range of US intelligence capabilities; therefore, US intelligence sections must expect to take the lead in developing intelligence during multinational operations. Particular attention must be given to provisions for sanitation, declassification, and releasability of intelligence developed by US forces and agencies to coalition partners. Personnel who are knowledgeable in these techniques and procedures must be included in the MAGTF or Marine component intelligence section. Intelligence plans must provide for connectivity with multinational forces and liaison elements with appropriate linguistic and area specialist skills.

APPENDIX A
GLOSSARY

Section I. Acronyms

ACE . . . . . aviation combat element
AC/S . . . . . .assistant chief of staff
AFC. . . . . all-source fusion center
AFP . . . . . all-source fusion platoon
AIntP. . . . . Allied Intelligence Publication
AO. . . . . .area of operations
ATARS . . . . . advanced tactical airborne reconnaissance system
ATFIC. . . . . amphibious task force intelligence center

BDA . . . . . battle damage assessment

C2 . . . . . .command and control
C2W . . . . . command and control warfare
CCIR. . . . . commander's critical information requirements
CE . . . . . command element
CGS. . . . . common ground station
CHATS . . . . . CI/HUMINT automated tool set
CI . . . . . .counterintelligence
CIA . . . . . Central Intelligence Agency
CIC . . . . . combat intelligence center
CIS . . . . . communications and information systems
CMDO . . . . . collection management/ dissemination officer
Co . . . . . .company
COA . . . . . course of action
COG . . . . . .center of gravity
COP. . . . . common operational picture
CP . . . . . command post
CSS . . . . . combat service support
CSSE. . . . . .combat service support element
CTP. . . . . .common tactical picture
CV. . . . . .critical vulnerability

DIA . . . . . .Defense Intelligence Agency
DMS . . . . . .Defense Message System
DOD . . . . . Department of Defense
DST. . . . . .direct support team

EW . . . . . .electronic warfare
FBI . . . . . .Federal Bureau of Investigation
FRAGO. . . . . .fragmentary order
FSCC. . . . . .fire support coordination center
FSSG. . . . . force service support group

GCE . . . . . ground combat element
GI&S. . . . . .geospatial information and services
GSP. . . . . ground sensor platoon

HET. . . . . .HUMINT exploitation team
HLZ. . . . . helicopter landing zone
HUMINT . . . . . .human intelligence

I&W . . . . . .indications and warning
IAS . . . . . .intelligence analysis system
ICR . . . . . intelligence collection requirement
IDR . . . . . intelligence dissemination requirement
IIP . . . . . imagery intelligence platoon
IMA. . . . . individual mobilization augmentee
IMINT. . . . . .imagery intelligence
intel bn . . . . . intelligence battalion
IO . . . . . .information operations
IOC . . . . . .intelligence operations center
IOS . . . . . .intelligence operations server
IOW . . . . . .intelligence operations workstation
IPB . . . . . .intelligence preparation of the battlespace
IPR . . . . . intelligence production requirement
IR . . . . . .intelligence requirement
ISC . . . . . intelligence support coordinator

JIC. . . . . joint intelligence center
JISE. . . . . joint intelligence support element
JSTARS . . . . . .Joint Surveillance Target Attack Radar System
JTF . . . . . .joint task force
JWICS. . . . . .Joint Worldwide Intelligence Communication System

MAGTF . . . . . Marine air-ground task force

MARFOR . . . . . .Marine Corps forces
MARFORRES . . . . . Marine Forces Reserve
MASINT . . . . . measurement and signature intelligence
MAW . . . . . Marine aircraft wing
MCDP . . . . . Marine Corps doctrinal publication
MCIA . . . . . Marine Corps Intelligence Activity
MCWP . . . . . Marine Corps warfighting publication
MEB . . . . . .Marine Expeditionary Brigade
MEF . . . . . Marine Expeditionary Force
MEU . . . . . Marine Expeditionary Unit
MEU(SOC) . . . . . Marine Expeditionary Unit (Special Operations Capable)
MIDB . . . . . .modernized integrated database
MOOTW . . . . . military operations other than war
MSC . . . . . major subordinate command

NGO . . . . . .nongovernmental organization
NIMA . . National Imagery and Mapping Agency
NMITC . . . . . Navy-Marine Corps Intelligence Training Center
NIPRNET . . . . . Nonsecure Internet Protocol Router Network
NIST . . . . . National Intelligence Support Team
NSA . . . . . National Security Agency

OCAC . . . . operations control and analysis center
OIC . . . . . officer in charge
OMFTS . . . . . operational maneuver from the sea
OODA . . . . . observe, orient, decide, and act
OP . . . . . observation post
OPCON . . . . . operational control
OPLAN . . . . . .operation plan
OPORD . . . . . operational order
OPSEC . . . . . operations security
OSINT . . . . . open-source intelligence

P&A . . . . . production and analysis
PDE&A . . . . . planning, decision, execution, and assessment
PIR . . . . . priority intelligence requirements
PSYOP . . . . . psychological operations

R&S . . . . . reconaissance and surveillance
recon . . . . . reconaissance
rep . . . . . representative
RRS . . . . . .remote receiver station

SARC . . . . . surveillance and reconnaissance cell
SIDS . . secondary imagery dissemination system
SIGINT . . . . . .signals intelligence
SIPRNET . . . . . Secret Internet Protocol Router Network
SSU . . . . . SIGINT support unit
STANAG . . . . . standardization agreement

TCAC . . . Technical Control and Analysis Center
TDN . . . . . tactical data network
TEG . . . . . Technical Exploitation Group
TERPES . . . . . tactical electronic reconnaissance processing and evaluation system
TGTINTEL . . . . . .target intelligence
TRAP . . . . . .tactical recovery of aircraft and personnel
TPC . . . . . topographic production capability
TRSS . . . . . .tactical remote sensor system
TTP . . . . . tactics, techniques, and procedures

UAV . . . . . .unmanned aerial vehicle
VMU . . . . . .Marine unmanned aerial vehicle squadron

Section II. Definitions

all-source intelligence—Intelligence products and/or organizations and activities that incorporate all sources of information, including, most frequently, human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data, in the production of finished intelligence. (JP 1-02)

battle damage assessment—1. The timely and accurate estimate of damage resulting from the application of military force, either lethal or nonlethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage

assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. Also called BDA. (JP 1-02) **2.** The timely and accurate estimate of the damage resulting from the application of military force. BDA estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. (MCWP 2-1)

centers of gravity—1. Those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight. Also called COG. (JP 1-02) **2.** A key source of strength without which an enemy cannot function. (MCDP 1-2)

collection—The gathering of intelligence data and information to satisfy the identified requirements. (MCWP 2-1)

collection management—1. The process of converting intelligence requirements into collection requirements, establishing priorities, and tasking or coordinating with appropriate collection sources or agencies, monitoring results and retasking, as required. (JP 1-02) **2.** Its purpose is to conduct an effective effort to collect all necessary data while ensuring the efficient use of limited and valuable collection assets. (MCWP 2-1)

combat data—Data derived from reporting by operational units. (MCWP 2-1)

command and control—1. The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (JP 1-02) **2.** The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. (MCDP 6) commander's critical information requirements—Information regarding the enemy and friendly activities and the environment identified by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. Also called CCIR. (MCRP 5-12C)

commander's intent—A commander's clear, concise personal articulation of the reason(s) behind one or more tasks assigned to a subordinate. It is one of two components of every mission statement which supports the higher and/or supported commander's intent and guides the exercise of initiative in the absence of instructions. (MCRP 5-12C)

counterintelligence—Within the Marine Corps, CI constitutes active and passive measures intended to deny a threat force valuable information about the friendly situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions. Also called CI. (MCWP 2-1)

critical vulnerability—An aspect of a center of gravity that if exploited will do the most significant damage to an adversary's ability to resist. Also called CV. (MCRP 5-12C)

descriptive intelligence—Class of intelligence which describes existing and previously existing conditions intended to promote situational awareness. Descriptive intelligence has two components: basic intelligence, which is general background knowledge about established and relatively constant conditions; and current intelligence, which is concerned with describing the existing situation. (MCRP 5-12C)

dissemination—Conveyance of intelligence to users in a suitable form. (JP 1-02)

dissemination management—Involves establishing dissemination priorities, selecting dissemination means, and monitoring the flow of intelligence throughout the command. The objective of dissemination management is to deliver the required intelligence to the appropriate user in proper form at the right time while ensuring that individual consumers and the dissemination system are not overloaded by attempting to move unneeded or irrelevant information. Dissemination management also provides for use of security controls that do not impede the timely delivery or subsequent use of intelligence while protecting intelligence sources and methods. (MCWP 2-1)

estimative intelligence—Class of intelligence which attempts to anticipate future possibilities and probabilities based upon descriptive intelligence in the context of planned enemy and friendly operations. (MCRP 5-12C)

human intelligence—1. A category of intelligence derived from information collected and provided by human sources. (JP 1-02) **2.** HUMINT operations cover a wide range of activities encompassing reconnaissance patrols, aircrew reports and debriefs, debriefing of refugees, interrogations of prisoners of war, and the conduct of CI force protection source operations. Also called HUMINT. (MCWP 2-1)

imagery intelligence—Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. Also called IMINT. (JP 1-02)

indications and warning—Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorists' attacks; and other similar events. Also called I&W. (JP 1-02)

intelligence—1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. **2.** Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (JP 1-02) **3.** Knowledge of the enemy and the surrounding environment that is needed to support decisionmaking. (MCDP 2)

intelligence cycle—The steps by which information is converted into intelligence and made available to users. (JP 1-02)

intelligence data—Data derived from assets primarily dedicated to intelligence collection: imagery systems, electronic intercept equipment, human intelligence sources, and so on. (MCWP 2-1)

intelligence discipline—A well-defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. There are five major disciplines: human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence (communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence), and open-source intelligence. (JP 1-02)

intelligence operations—The variety of intelligence tasks that are carried out by various intelligence organizations and activities. (JP 1-02)

intelligence preparation of the battlespace—**1.** An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive data base for each potential area in which a unit may be required to operate. The data base is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB. (JP 1-02) **2.** A systematic, continuous process of analyzing the threat and environment in a specific geographic area. (MCWP 2-1)

intelligence requirement—**1.** Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. Also called IR. (JP 1-02) **2.** Questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. (MCDP 2)

joint force—A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (JP 1-02)

joint intelligence center—The intelligence center of the joint force headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the joint force commander and staff, components, task forces and elements, and the national intelligence community. Also called JIC. (JP 1-02)

joint operations—A general term to describe military actions conducted by joint forces, or by Service forces in relationships (e.g., support, coordinating authority), which, of themselves, do not create joint forces. (JP 1-02)

main effort—The designated subordinate unit whose mission at a given point in time is most critical to the overall mission success. (MCRP 5-12C)

maneuver warfare—A warfighting philosophy that seeks to shatter the enemy's cohesion through a variety of rapid, focused, and unexpected actions which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope. (MCDP 1)

measurement and signature intelligence—**1.** Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the target. The detected feature may be either reflected or emitted. Also called MASINT. (JP 1-02) **2.** Intelligence information gathered by technical instruments such as radars, passive electrooptical sensors, radiation detectors, and remote ground sensors. (MCWP 2-1)

open-source intelligence—**1.** Information of potential intelligence value that is available to the general public. Also called OSINT. (JP 1-02) **2.** OSINT sources include books, magazines, newspapers, maps, commercial electronic networks and databases, and radio and television broadcasts. OSINT involves no information that is classified at its origin or acquired through controlled collection. (MCWP 2-1)

priority intelligence requirements—**1.** Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. Also called PIR. (JP 1-02) **2.** An intelligence requirement MCWP 2-1 Intelligence Operations A-5 associated with a

decision that will critically affect the overall success of the command's mission. (MCDP 2)

production management—Encompasses determining the scope, content, and format of each product; developing a plan and schedule for the development of each product; assigning priorities among the various IPRs; allocating processing, exploitation, and production resources; and integrating production efforts with collection and dissemination. (MCWP 2-1)

sensor data—Data derived from sensors whose primary mission is surveillance or target acquisition: air surveillance radars, counterbattery radars, and remote ground sensors. (MCWP 2-1)

signals intelligence—1. A category of intelligence comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. **2.** Intelligence derived from communications, electronics, and foreign instrumentation signals. Also called SIGINT (JP 1-02)

situational awareness—Knowledge and understanding of the current situation which provides timely, relevant and accurate assessment of friendly, enemy and other operations within the battlespace. Also called SA. (MCRP 5-12C)

tactical intelligence—1. Intelligence that is required for planning and conducting tactical operations. (JP 1-02) **2.** Tactical intelligence concerns itself primarily with the location, capabilities, and possible intentions of enemy units on the battlefield and with the tactical aspects of terrain and weather. (MCDP 2)

warfighting functions—The six mutually supporting military activities integrated in the conduct of all military operations: command and control, intelligence, maneuver, fires, logistics, and force protection. (MCRP 5-12C)

APPENDIX B
REFERENCES

Standardization Agreement (STANAG)

2936	Intelligence Doctrine - AIntP-1(A)

Joint Publication (JP)

2-0	Joint Doctrine for Intelligence Support to Operations

Marine Corps Doctrinal Publications (MCDPs)

1	Warfighting
1-0	Marine Corps Operations
2	Intelligence
5	Planning

Marine Corps Warfighting Publications (MCWPs)

2-14	Counterintelligence
5-1	Marine Corps Planning Process

This Page Is Intentionally Left Blank

FM 3-55

Information Collection

April 2012

DISTRIBUTION RESTRICTION. Approved for public release; distribution is unlimited.

Headquarters, Department of the Army

This publication is available at
Army Knowledge Online (www.us.army.mil) and
General Dennis J. Reimer Training and Doctrine
Digital Library at (www.train.army.mil).

Field Manual
No. 3-55

Headquarters
Department of the Army
Washington, DC, 23 April 2012

Information Collection

Contents

Page

PREFACE ..... **iii**

INTRODUCTION ..... **iv**

Chapter 1 FOUNDATIONS OF INFORMATION COLLECTION **1-1**
Definition 1-1
Purpose 1-2
Information Collection Process 1-3
Primary Information Collection Tasks and Missions 1-5

Chapter 2 COMMANDER AND STAFF RESPONSIBILITIES **2-1**
The Role of the Commander 2-1
Commander's Needs 2-2
Commander's Guidance 2-2
Role of the Staff 2-4
Working Group Input to Information Collection 2-5

Chapter 3 PLANNING REQUIREMENTS FOR AND ASSESSING INFORMATION COLLECTION **3-1**
The Operations Process and Information Collection 3-1
Information Collection Planning Considerations 3-1
Support to Personnel Recovery 3-2
The MDMP and Information Collection Planning 3-2
Assess Information Collection Activities 3-8

Chapter 4 TASKING AND DIRECTING INFORMATION COLLECTION **4-1**
Task and Direct Information Collection 4-1
Finalize the Information Collection Plan 4-1
Develop the Information Collection Overlay 4-4
Develop the Information Collection Scheme of Support 4-4
Re-task Assets 4-8

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

Appendix A INFORMATION COLLECTION ASSETS A-1
Appendix B THE INFORMATION COLLECTION ANNEX TO THE OPERATION ORDER .. B-1
Appendix C JOINT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE..... C-1
GLOSSARY Glossary-1
REFERENCES..... References-1
INDEX Index-1

Figures

Figure 1-1. Information collection activities 1-2
Figure 2-1. Example of the operations and intelligence working group 2-7
Figure 4-1. Sample information collection matrix 4-3
Figure 4-2. Example of an information collection overlay 4-5
Figure B-1. Example Annex L (Information Collection) annotated format B-1
Figure B-2. Sample information collection plan B-6

Tables

Table 4-1. Scheme of support 4-6
Table A-1. Sample information collection assets A-1
Table A-2. Battlefield surveillance brigade information collection assets A-5
Table A-3. Infantry brigade combat team information collection assets A-7
Table A-4. Heavy brigade combat team information collection assets A-8
Table A-5. Stryker brigade combat team information collection assets A-9

Preface

Although this is the first edition of field manual (FM) 3-55, the concepts are not new. Many who read this FM will recognize that it is a culmination of decades of refinement. In this manual, the term *information collection* is introduced as the Army's replacement for *intelligence, surveillance, and reconnaissance* (also known as ISR). ISR is a joint term, for which the Army revised to meet Army needs. The manual describes the following activities: planning requirements, assessing collection, tasking and direct information collection assets. Also it contains the actions taken by the commanders and staffs in planning, preparing, executing, and assessing information collection activities. As the Army fields new formations and equipment with inherent and organic information collection capabilities, it needs a doctrinal foundation to ensure their proper integration and use to maximize their capabilities.

PURPOSE

This FM provides essential and enduring doctrine for Army forces conducting information collection activities. This FM aligns information collection with current Army doctrine. The modular force structure with the brigade combat team as the centerpiece of the deployed force also moves many information collection assets to lower echelons. The latter is a major shift from previous ways of operating.

SCOPE

This manual covers the principles and fundamental considerations for information collection planning and execution in operations. Although it recognizes and discusses the impact of systems that support information collection activities, this manual emphasizes fundamentals and concepts rather than equipment or systems. The doctrine contained herein is intended to be broad enough to apply to all operational themes—from a peacetime military engagement to a major combat operation—and applicable at battalion through corps echelons deployed in an area of operations, although each organization employs tactics, techniques, and procedures appropriate to its level.

AUDIENCE

This manual is designed for officers and Soldiers assigned to units that direct or conduct information collection activities as well as commanders and staffs of corps, division, brigade combat teams, support brigades, and battalions. It applies to the Active Army, the Army National Guard, Army National Guard of the United States, and the United States Army Reserve unless otherwise stated; and U.S. Army Training and Doctrine Command institutions and components. This FM forms the foundation for instruction on information collection activities within the Army's educational system.

ADMINISTRATIVE INFORMATION

The information presented is descriptive, not prescriptive or restrictive. This manual complies with ADP 3-0, FM 2-0, FM 5-0, FM 6-0, and FM 7-15.

This publication applies to the Active Army, the Army National Guard (ARNG)/Army National Guard of the United States (ARNGUS), and the United States Army Reserve (USAR) unless otherwise stated.

The proponent of this publication is the United States Army Training and Doctrine Command (TRADOC). The preparing agency is the Combined Arms Doctrine Directorate, U.S. Army Combined Arms Center. Send written comments and recommendations on a DA Form 2028 (Recommended Changes to Publications and Blank Forms) to Commander, U.S. Army Combined Arms Center and Fort Leavenworth, ATTN: ATZL-MCK-D (FM 3-55), 300 McPherson Avenue, Fort Leavenworth, KS 66027-2337 or by e-mail to usarmy.leavenworth.mccoe.mbx.cadd-org-mailbox@mail.mil.

Introduction

A nuanced understanding of the situation is everything. Analyze the intelligence that is gathered, share it, and fight for more. Every patrol should have tasks designed to augment understanding of the area of operations and the enemy. Operate on a "need to share" rather than a "need to know" basis. Disseminate intelligence as soon as possible to all who can benefit from it.

General David H. Petraeus, U.S. Army
Military Review

The Army currently has no unified methodology or overall plan to define or establish how it performs or supports information collection activities at all echelons. This publication clarifies how the Army plans, prepares, and executes information collection activities within or between echelons.

This manual emphasizes three themes. First, foundations of information collection that demonstrate information collection activities are a synergistic whole, with emphasis on synchronization and integration of all components and systems. Second, commanders and staff have vital responsibilities in information collection planning and execution, with emphasis on the importance of the commander's role. Finally, the planning requirements and assessing success of information collection is measured by its contributions to the commander's understanding, visualization, and decisionmaking abilities.

With the exception of cyberspace, all operations will be conducted among the people and outcomes will be measured in terms of effects on populations. This increases the complexity of information collection planning, execution, and assessment, requiring a deeper level of situational understanding from commanders. It demands full staff integration into information collection activities as well as the engagement of every Soldier in collecting and reporting information. This field manual cannot provide all the answers, but its purpose is to prompt the user to ask the right questions.

Chapter 1 provides the Army definition of information collection.

Chapter 2 examines the roles and actions of the commander and staff in information collection planning and execution. This chapter also discusses the working group for information collection.

Chapter 3 describes planning requirements and assessing collection of information collection activities.

Chapter 4 discusses the tasking and directing of collection assets. The operations staff integrates collection assets through a deliberate and coordinated effort across all warfighting functions. Tasking and directing is vital to control limited collection assets. During task and direct, the staff recommends redundancy, mix, and cue, as appropriate.

Appendix A provides an overview of the information collection assets and capabilities available to Army commanders.

Appendix B provides instructions for preparing Annex L (Information Collection) in Army plans and orders.

Appendix C examines joint intelligence, surveillance, and reconnaissance activities.

Commanders drive information collection activities through their choice of critical information requirements and through mission command in driving the operations process. Commanders visualize, describe, direct, lead, and assess throughout the operations process with understanding as the start point. Intelligence preparation of the battlefield assists them in developing an in-depth understanding of the enemy and the operational environment. They then visualize the desired end state and a broad concept of how to shape the current conditions into the end state. Commanders describe their visualization through the commander's intent, planning guidance, and concept of operations in order to bring clarity to an uncertain situation. They also express gaps in relevant information as commander's critical information requirements. The challenge is for information collection activities to answer those requirements with timely, relevant, and accurate intelligence that enables commanders to make sound decisions.

Chapter 1

Foundations of Information Collection

This chapter presents the basics of information collection. It begins with the definition and purpose of information collection. It then discusses the information collection processes. Lastly, the chapter discusses primary information collection tasks and missions.

DEFINITION

1-1. Knowledge is the precursor to effective action, whether in the informational or physical domain. Knowledge about an operational environment requires aggressive and continuous operations to acquire information. Information collected from multiple sources and analyzed becomes intelligence that provides answers to commander's critical information requirements.

1-2. Commanders have used to provide intelligence to reduce the inherent uncertainty of war. Achieving success in today's conflicts demands extraordinary commitment to reducing this uncertainty. The Army describes information collection as an activity implies a function, mission, or action, as well as the organization that performs it. Information collection activities are a synergistic whole, with emphasis on synchronization and integration of all those components and systems.

1-3. Information collection is an activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination of systems in direct support of current and future operations. This activity implies a function, mission, or action as well as the organization that performs it. Information collection activities are a synergistic whole with emphasis on synchronization and integration of all those components and systems. Information collection integrates the intelligence and operations staffs functions focused on answering the commander's critical information requirements. For joint operations, refer to appendix C.

1-4. At the tactical level, reconnaissance, surveillance, security, and intelligence missions or operations are the primary means by which a commander plans, organizes, and executes shaping operations that answer the commander's critical information requirements and support the decisive operation. Figure 1-1 on page 1-2 displays information collection activities.

1-5. The intelligence and operations staffs work together to collect, process, and analyze the information the commander requires concerning the enemy, other adversaries, climate, weather, terrain, population, and other civil considerations that affect operations. Intelligence relies on reconnaissance, security, intelligence operations, and surveillance for its data and information. Conversely, without intelligence, commanders and staffs do not know where or when to conduct reconnaissance, security, intelligence operations, or surveillance. The usefulness of the data collected depends upon the processing and exploitation common to these activities.

1-6. Commanders integrate information collection to form an information collection plan that capitalizes on different capabilities. Information collection assets provide data and information. *Intelligence* is the product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity (JP 2-0). Intelligence informs commanders and staffs where and when to look. Reconnaissance, security, intelligence operations, and surveillance are the **ways**—with the **means** ranging from national and joint collection capabilities to individual Soldier observations and reports. The **end** is intelligence that supports commander's decisionmaking. The result—successful execution and assessment of operations—depends upon the effective synchronization and integration of the information collection effort.

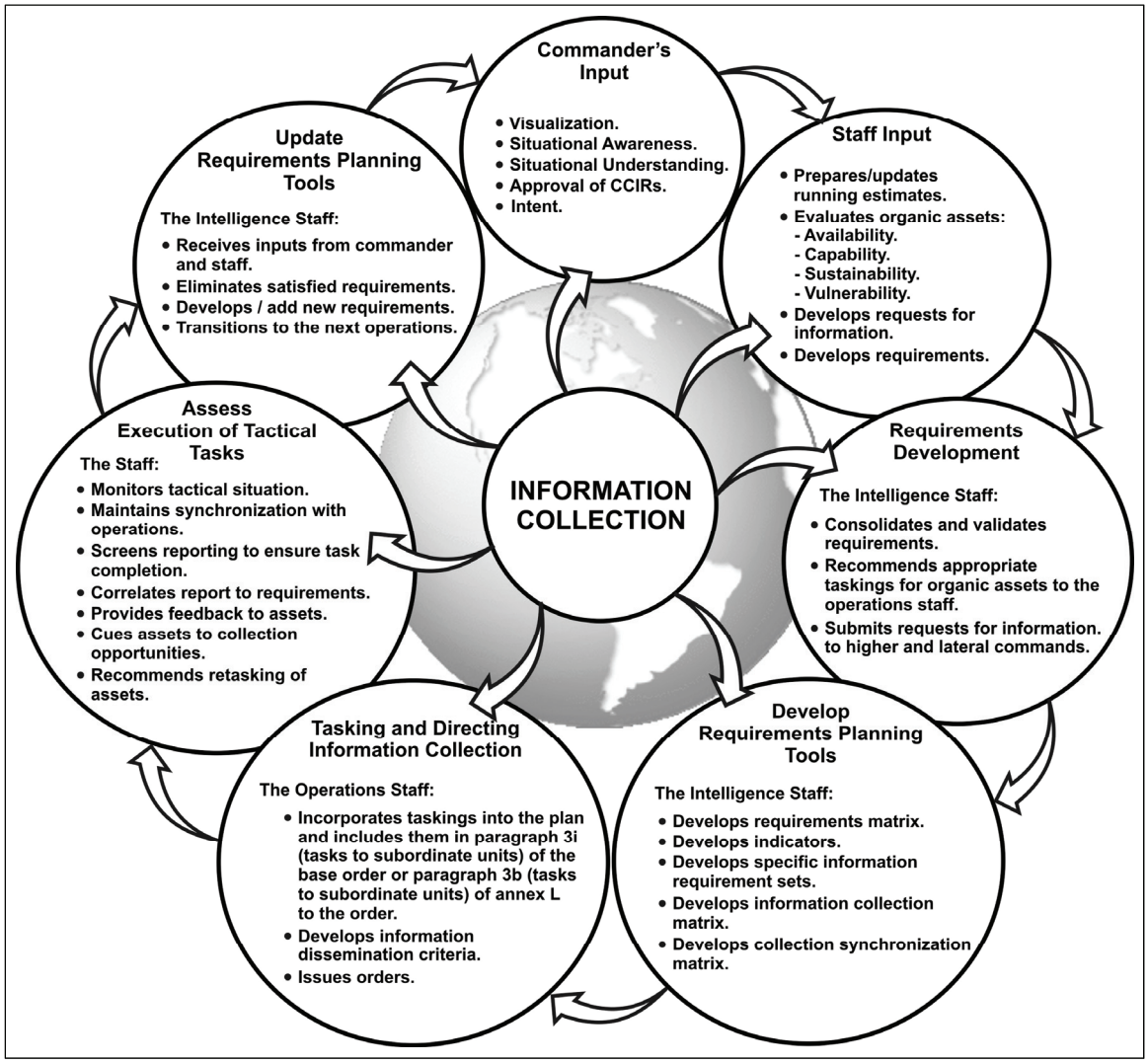


Figure 1-1. Information collection activities

1-7. These activities of information collection support the commander's understanding and visualization of the operation by identifying gaps in information, aligning assets and resources against them, and assessing the collected information and intelligence to inform the commander's decisions. They also support the staff's integrating processes during planning and execution. The direct result of the information collection effort is a coordinated plan that supports the operation. As staff assesses information and intelligence, they refine the plan and issue fragmentary orders to the plan to re-task or re-mission assets and units.

PURPOSE

1-8. Information collection activities provide commanders with detailed, timely, and accurate intelligence, enabling them to visualize threat capabilities and vulnerabilities, and to gain situational understanding. Information collected from multiple sources and analyzed becomes intelligence that provides answers to commander's critical information requirements as part of an evolving understanding to the area of operations. These activities contribute to the achievement of a timely and accurate common operational picture (COP). By answering the commander's critical information requirements (CCIRs), information collection activities enable commanders to make informed decisions.

1-9. Effective information collection activities—

- Provide relevant information and intelligence products to commanders and staffs.
- Provide combat information to commanders.
- Contribute to situational awareness and facilitates continuous situational understanding.
- Generate a significant portion of the COP vertically and horizontally among organizations, commanders, and staffs.
- Support the commander's visualization, permitting more effective mission command.
- Answer the CCIRs.
- Facilitate and are facilitated by the intelligence preparation of the battlefield (IPB).
- Support effective, efficient, and accurate targeting.
- Decrease risk for the unit.

1-10. Commanders and staffs continuously plan, task, and employ collection assets and forces to collect information. They request information and resources through higher echelons as needed. This information and intelligence enable commanders to make informed decisions that are translated into action.

1-11. Information collection planning is crucial to mission success. The four fundamentals in effectively planning, synchronizing, and integrating information collection activities are—

- The commander drives the information collection effort.
- Effective information collection synchronization and integration requires full staff participation.
- Conducting information collection requires a collection capability, either organic or augmented by nonorganic resources.
- Conducting information collection requires an analytical capability to analyze and produce actionable intelligence.

1-12. Commanders must be involved in the information collection planning process by quickly and clearly articulating their CCIRs to the staff. This enables the staff to facilitate the commander's visualization and decisionmaking by focusing on the CCIRs.

1-13. Effective information collection requires the entire staff's involvement and input. This enables the intelligence staff to identify and assess information requirements and the operations staff to task and direct the effort.

1-14. Conducting information collection activities requires an organic collection capability, either organic or augmented by nonorganic resources. Acquiring the required information to answer the requirements encompasses the efforts of reconnaissance, security, surveillance, intelligence operations, and the skills of Soldiers. All the activities that contribute to developing continuous knowledge about the area of operations are considered information collection activities. Planners must understand all collection assets and resources available to them and the procedures to request or task collection from those assets, resources, and organizations. Refer to appendix A for additional information.

1-15. Conducting these activities requires an analytical capability to interpret information and produce actionable intelligence. The analyst's ability to employ critical thinking and use multiple sources during intelligence analysis reduces uncertainty and helps solve problems that could not be resolved via a single source of information. This requires staff sections to understand the capabilities and limitations of assets to collect and report. The staff must also establish reporting guidelines to the collection assets.

INFORMATION COLLECTION PROCESS

1-16. Information collection is the acquisition of information and the provision of this information to processing elements. This process performs the following tasks:

- Plan requirements and assess collection.
- Task and direct collection.
- Execute collection.

PLAN REQUIREMENTS AND ASSESS COLLECTION

1-17. The intelligence staff (in collaboration with the operations officer and the entire staff) receives and validates requirements for collection, prepares the requirements planning tools, recommends collection assets and capabilities to the operations staff, and maintains synchronization as operations progress. (Chapter 3 of this manual discusses plan and assess in detail.)

TASK AND DIRECT COLLECTION

1-18. The operations officer (based on recommendations from the staff) tasks, directs, and when necessary re-tasks the information collection assets. (Chapter 4 of this manual discusses tasking and directing of collection.)

EXECUTE COLLECTION

1-19. Executing collection focuses on requirements tied to the execution of tactical missions (such as reconnaissance, surveillance, security, and intelligence operations) based on the CCIRs. Collection activities acquire information about the adversary and the area of operations and provide that information to intelligence processing and exploitation elements. Typically collection activities begin soon after receipt of mission and continue throughout preparation and execution of the operation. They do not cease at conclusion of the mission but continue as required. This allows the commander to focus combat power, execute current operations, and prepare for future operations simultaneously.

1-20. The subtasks are—

- Establish technical channels and provide guidance.
- Collect and report information.
- Establish a mission intelligence briefing and debriefing program.

Establish Technical Channels and Provide Guidance

1-21. This subtask includes providing and conducting technical channels to refine and focus the intelligence disciplines' information collection tasks. It coordinates the disciplines' assets when operating in another unit's area of operations. (FM 2-0 contains additional information for this task and its two subtasks: "*Establish and maintain technical channels*" and "*Conduct deconfliction and coordination*.")

1-22. Due to the unique characteristics of intelligence operations, technical channels ensure adherence to applicable laws and policies, ensure proper use of doctrinal techniques, and provide technical support and guidance to intelligence operations and discipline assets. Applicable laws and policies include all relevant U.S. laws, the law of war, international laws, directives, Department of Defense instructions, and orders. Commanders direct operations but often rely on technical control to conduct portions of the collection effort.

1-23. Technical channels refer to supervision of intelligence operations and disciplines. Technical channels do not interfere with the ability to task organic intelligence operations assets. It ensures adherence to existing policies or regulations by providing technical guidance for intelligence operations tasks contained within the information collection plan. While not a formal command or support relationship, technical channels is a critical function that ensures the collection asset has the required technical data to perform mission-related tasks.

1-24. Technical channels also involve translating tasks into the specific parameters used to focus the highly technical intelligence operations collection or the legally sensitive aspects of signals intelligence collection as well as human intelligence military source operations and counterintelligence tasks. Technical channels provide the means to meets the overall commander's intent for intelligence operations. Technical channels include but are not limited to defining, managing, or guiding the use of specific intelligence assets or identifying critical technical collection criteria (such as technical indicators and recommending collection techniques or procedures).

Note: In specific cases, regulatory authority is granted to specific national and Department of Defense intelligence agencies for specific intelligence discipline collection and is passed through technical control channels.

Collect and Report Information

1-25. This task involves collecting and reporting information in response to collection tasks. Collection assets collect information and data about the threat, terrain and weather, and civil considerations for a particular area of operations (AO) and area of interest. A successful information collection effort results in the timely collection and reporting of relevant and accurate information, which supports the production of intelligence or combat information.

Collect

1-26. As part of the collection plan, elements of all units obtain information and data concerning the threat, terrain and weather, and civil considerations within the AO. Well-developed procedures and carefully planned flexibility to support emerging targets, changing requirements, and the need to support combat assessment is critical. Once staffs collect the information, they process it into a form that enables analysts to extract essential information and produce intelligence and targeting data. Once Solders collect the information, it is processed into a form that enables analysis. Collected and processed information is provided to the appropriate units, organizations, or agencies for analysis or action. This analyzed information forms the foundation of running estimates, targeting data, intelligence databases, and intelligence.

Report

1-27. Collection assets must follow standard operating procedures (SOPs) to ensure staffs tag reports with the numbers of the tasks they satisfy. Simultaneously, SOPs ensure assets understand and have a means of reporting important but unanticipated information. Collection assets reporting may convey that collection occurred, but the unit did not observe any activity satisfying the information collection task, which may be a significant indicator. As a part of reporting, the staff tracks which specific collection task originates from which intelligence requirement Such tracking ensures the staff provides the collected information to the original requester and to all who need the information. Correlating reporting to the original requirement and evaluating reports is key to effective information collection. The staff tracks the progress of each requirement and cross-references incoming reports to outstanding requirements.

Establish a Mission Intelligence Briefing and Debriefing Program

1-28. The commander establishes, supports, and allocates appropriate resources for a mission briefing and debriefing program. The battle updates and after action reviews are separate tasks from the mission briefing and debriefing program. The G-2 (S-2) develops a mission intelligence briefing program and complementary debriefing program to support the commander's program.

PRIMARY INFORMATION COLLECTION TASKS AND MISSIONS

1-29. Information collection encompasses all activities and operations intended to gather data and information that, in turn, are used to create knowledge and support the commander's requirements, situational understanding, and visualization. Commanders maximally achieve information collection when they care carefully employ all the collection tasks and missions together in an operation. This appropriate mix of collection tasks and missions helps satisfy as many different requirements as possible. It also ensures that the operations and intelligence working group does not favor or become too reliant on one particular unit, discipline, or system. The Army has four tasks or missions it primarily conducts as a part of the information collection plan:

- Reconnaissance.
- Surveillance.

- Security operations.
- Intelligence operations.

RECONNAISSANCE

1-30. *Reconnaissance* is those operations undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographical or geographical characteristics and the indigenous population of a particular area (FM 3-90). Reconnaissance primarily relies on the human dynamic rather than technical means. Reconnaissance is a focused collection effort. A combined arms operation, reconnaissance is normally tailored to actively collect information against specific targets for a specified time based on mission objectives.

1-31. Units perform reconnaissance using three methods: dismounted, mounted, and aerial (each can be augmented by sensors). Successful and effective units combine these methods. To gain information on the enemy or a particular area, units can use passive surveillance, technical means, and human interaction, or they can fight for information.

1-32. Reconnaissance produces information concerning the AO. Staffs perform reconnaissance before, during, and after other operations to provide information used in the IPB process. Commanders perform reconnaissance to formulate, confirm, or modify a course of action (COA). Reconnaissance provides information that commanders use to make informed decisions to confirm or modify the concept of operations. This information may concern the enemy, the local population, or any other aspect of the AO. Commanders at all echelons incorporate reconnaissance into their operations.

1-33. Reconnaissance identifies terrain characteristics, enemy and friendly obstacles to movement, and the disposition of enemy forces and civilians so that commanders can maneuver forces freely with reduced risk. Reconnaissance prior to unit movements and occupation of assembly areas is critical to protecting the force and preserving combat power. It also keeps U.S. forces free from contact as long as possible so that they can concentrate on the decisive operation.

Reconnaissance Objective

1-34. Commanders orient their reconnaissance by identifying a reconnaissance objective within the AO. The reconnaissance objective is a terrain feature, geographic area, enemy force, or specific civil considerations about which the commander wants to obtain additional information. The reconnaissance objective clarifies the intent of the reconnaissance by specifying the most important result to obtain from the reconnaissance mission. Every reconnaissance mission specifies a reconnaissance objective. Commanders assign reconnaissance objectives based on commander's critical information requirements, reconnaissance asset capabilities, and reconnaissance asset limitations. The reconnaissance objective can be information about a specific geographical location (such as the cross-country trafficability of a specific area), a specific enemy activity to be confirmed or denied, a specific enemy element to be located or tracked, or specific civil considerations (such as critical infrastructure). When the unit lacks time to complete all the tasks associated with a specific form of reconnaissance, it uses the reconnaissance objective to guide it in setting priorities.

1-35. Commanders may need to provide additional detailed instructions beyond the reconnaissance objective (such as specific tasks to be performed or the priority of tasks). They do this by issuing additional guidance to their reconnaissance units or by specifying these instructions in the tasks to subordinate units in the operation order. For example, if a unit S-2 concludes that the enemy is not in an area and the terrain appears to be trafficable without obstacles, the commander may direct the reconnaissance squadron to conduct a zone reconnaissance mission with guidance to move rapidly and report by exception any terrain obstacles that will significantly slow the movement of subordinate maneuver echelons. Alternatively, when the objective is to locate an enemy force, the reconnaissance objective would be that force, and additional guidance could be to conduct only that terrain reconnaissance necessary to find the enemy and develop the situation.

Reconnaissance Fundamentals

1-36. The seven fundamentals of reconnaissance are—

- Ensure continuous reconnaissance.
- Do not keep reconnaissance assets in reserve.
- Orient on the reconnaissance objective.
- Report information rapidly and accurately.
- Retain freedom of maneuver.
- Gain and maintain enemy contact.
- Develop the situation rapidly.

Ensure Continuous Reconnaissance

1-37. The commander conducts reconnaissance before, during, and after all operations. Before an operation, reconnaissance focuses on filling gaps in information about the enemy, specific civil considerations, and the terrain. During an operation, reconnaissance focuses on providing the commander with updated information that verifies the enemy's composition, dispositions, and intentions as the battle progresses. This allows commanders to verify which COA the enemy is actually adopting and to determine if the plan is still valid based on actual events in the AO. After an operation, reconnaissance focuses on maintaining contact with the enemy forces to determine their next move and collecting information necessary for planning subsequent operations. In stability and defense support of civil authorities operations, reconnaissance focuses on specific civil considerations.

Do Not Keep Reconnaissance Assets in Reserve

1-38. Reconnaissance assets, like artillery assets, are never kept in reserve. When committed, reconnaissance assets use all their resources to accomplish the mission. This does not mean that all assets are committed all the time. Commanders use reconnaissance assets based on their capabilities and the mission variables—mission, enemy, terrain and weather, troops and support available-time available and civil considerations—to achieve the maximum coverage needed to answer the CCIRs. At times, this requires commanders to withhold or position reconnaissance assets to ensure they are available at critical times and places. Commanders sustain and rest reconnaissance assets as necessary, but they are not placed in reserve. All reconnaissance assets should be treated as committed assets with specific missions assigned to them at all times. This fundamental does not apply to units with multiple roles that can conduct reconnaissance, security, and other combat missions in an economy of force role. Commanders may elect to place them in reserve as needed.

Orient on the Reconnaissance Objective

1-39. The commander uses the reconnaissance objective to focus the unit's reconnaissance efforts. Commanders of subordinate reconnaissance elements remain focused on achieving this objective, regardless of what their forces encounter during the mission. When time, limitations of unit capabilities, or enemy actions prevent a unit from performing all the tasks normally associated with a particular form of reconnaissance, the unit uses the reconnaissance objective to focus the reconnaissance effort.

Report Information Rapidly and Accurately

1-40. Reconnaissance assets acquire and report accurate and timely information on the enemy, civil considerations, and the terrain over which operations are to be conducted. Information may quickly lose its value. Reconnaissance units report exactly what they see and, if appropriate, what they do not see. Seemingly unimportant information may be extremely important when combined with other information. Negative reports are as important as reports of enemy activity. Reconnaissance assets must report all information, including a lack of enemy activity; failure to report tells the commander nothing. The unit communications plan ensures that unit reconnaissance assets have the proper communication equipment to support the integrated information collection plan.

Retain Freedom of Maneuver

1-41. Reconnaissance assets must retain battlefield mobility to successfully accomplish their missions. If these assets are decisively engaged, reconnaissance stops and a battle for survival begin. Reconnaissance assets must have clear engagement criteria that support the maneuver commander's intent. Initiative and knowledge of both the terrain and the enemy reduce the likelihood of decisive engagement and help maintain freedom of movement. Prior to initial contact, the reconnaissance unit adopts a combat formation designed to gain contact with the smallest possible friendly element. This provides the unit with the maximum opportunity for maneuver and enables it to avoid decisively engaging the entire unit. The IPB process can identify anticipated areas of likely contact to the commander. Using indirect fires to provide suppression and obscuration as well as destroy point targets is a method reconnaissance assets use to retain their freedom of maneuver.

Gain and Maintain Enemy Contact

1-42. Once a unit conducting reconnaissance gains contact with the enemy, it maintains that contact unless the commander directing the reconnaissance orders otherwise or the survival of the unit is at risk. This does not mean that individual scout and reconnaissance teams cannot break contact with the enemy. The commander of the unit conducting reconnaissance is responsible for maintaining contact using all available resources. The methods of maintaining contact can range from surveillance to close combat. Surveillance, combined with stealth, is often sufficient to maintain contact and is the preferred method. Units conducting reconnaissance avoid combat unless it is necessary to gain essential information, in which case the units use maneuver (fire and movement) to maintain contact while avoiding decisive engagement.

Develop the Situation Rapidly

1-43. When a reconnaissance asset encounters an enemy force or an obstacle, it must quickly determine the threat it faces. For an enemy force, it must determine the enemy's composition, dispositions, activities, and movements, and assess the implications of that information. For an obstacle, the reconnaissance asset must determine the type and extent of the obstacle and whether it is covered by fire. Obstacles can provide information concerning the location of enemy forces, weapons capabilities, and organization of fires. In most cases, the reconnaissance unit developing the situation uses actions on contact.

Reconnaissance Forms

1-44. The four forms of reconnaissance are—

- Route reconnaissance.
- Zone reconnaissance.
- Area reconnaissance.
- Reconnaissance in force.

Route Reconnaissance

1-45. Route reconnaissance focuses along a specific line of communications (such as a road, railway, or cross-country mobility corridor). It provides new or updated information on route conditions (such as obstacles and bridge classifications, and enemy and civilian activity along the route). A route reconnaissance includes not only the route itself, but also all terrain along the route from which the enemy could influence the friendly force's movement. The commander normally assigns this mission to use a specific route for friendly movement.

Zone Reconnaissance

1-46. Zone reconnaissance involves a directed effort to obtain detailed information on all routes, obstacles, terrain, enemy forces, or specific civil considerations within a zone defined by boundaries. Obstacles include both existing and reinforcing, as well as areas with chemical, biological, radiological, and nuclear (CBRN) contamination. Commanders assign zone reconnaissance missions when they need additional information on a zone before committing other forces in the zone. Zone reconnaissance missions are appropriate when the enemy situation is vague, existing knowledge of the terrain is limited, or combat operations have altered the terrain. A zone reconnaissance may include several route or area reconnaissance missions assigned to subordinate units.

Area Reconnaissance

1-47. Area reconnaissance focuses on obtaining detailed information about the enemy activity, terrain, or specific civil considerations within a prescribed area. This area may include a town, a neighborhood, a ridgeline, woods, an airhead, or any other feature critical to operations. The area may consist of a single point (such as a bridge or an installation). Areas are normally smaller than zones and not usually contiguous to other friendly areas targeted for reconnaissance. Because the area is smaller, units conduct an area reconnaissance more quickly than a zone reconnaissance.

Reconnaissance in Force

1-48. A reconnaissance in force is an aggressive reconnaissance conducted as an offensive operation with clearly stated reconnaissance objectives. A reconnaissance in force is a deliberate combat operation designed to discover or test the enemy's strength, dispositions, reactions, or to obtain other information. Battalion-sized task forces or larger organizations usually conduct a reconnaissance in force. A commander assigns a reconnaissance in force when the enemy is known to be operating within an area and the commander cannot obtain adequate intelligence by any other means. A unit may also conduct a reconnaissance in force in restrictive-type terrain where the enemy is likely to ambush smaller reconnaissance forces. The overall goal of reconnaissance in force is to determine enemy weaknesses that can be exploited. It differs from other reconnaissance because it is normally conducted only to gain information about the enemy and not the terrain.

Reconnaissance Focus, Reconnaissance Tempo, and Engagement Criteria

1-49. Commanders decide what guidance they will provide to shape the reconnaissance and surveillance effort. In terms of guidance, reconnaissance tempo and engagement criteria most closely apply organic reconnaissance elements. Reconnaissance focus can also be generally applied to surveillance assets, but in the specific sense of focusing a reconnaissance mission, it more closely applies to reconnaissance. The information below describes them in terms of reconnaissance.

Reconnaissance Focus

1-50. Reconnaissance focus, combined with one or more reconnaissance objectives, helps to concentrate the efforts of the reconnaissance assets. The commander's focus for reconnaissance usually falls in three general areas: CCIRs, targeting, and voids in information. The commander's focus enables reconnaissance units to prioritize taskings and narrow their scope of operations. An operation may have a terrain focus where the status of routes, bridges, and obstacles are more important than the enemy. Conversely, the operation may focus on the enemy in which friendly forces must locate the enemy's security zone, main body, and reserves. Additionally, commanders may express their focus in terms of reconnaissance pull and push. (FM 3-90 and FM 3-20.96 provide more detailed information on reconnaissance focus.)

1-51. Commanders use a reconnaissance pull when they do not know the enemy situation well or the situation changes rapidly. Reconnaissance pull fosters planning and decisionmaking based on changing assumptions into confirmed information. The unit uses initial assumptions and CCIRs to deploy reconnaissance assets as early as possible to collect information for developing COAs. The commander uses reconnaissance assets to confirm or deny initial CCIRs prior to deciding on a COA or maneuver option, thus pulling the unit to the decisive point on the battlefield. Success of the reconnaissance pull requires an integrated information collection plan that can be executed prior to the commander having to make a COA decision. (FM 3-90 and FM 3-20.96 provide more detailed information on reconnaissance pull.)

1-52. Commanders use a reconnaissance push once committed to a COA or maneuver option. The commander pushes reconnaissance assets forward, as necessary, to gain greater visibility on specific named area of interest (NAI) to confirm or deny the assumptions on which the COA is based. Staffs use the information gathered during reconnaissance push to finalize the unit's plan.

Reconnaissance Tempo

1-53. Tempo is the relative speed and rhythm of military operations over time with respect to the enemy. In terms of reconnaissance, tempo not only defines the pace of the operation, but also influences the depth of detail the reconnaissance can yield. Commanders establish time requirements for the reconnaissance force and express those requirements in a statement that describes the degree of completeness, covertness, and potential for engagement they are willing to accept. Commanders use their guidance on reconnaissance tempo to control the momentum of reconnaissance. Reconnaissance tempo is expressed as *rapid* or *deliberate* and *forceful* or *stealthy*.

1-54. Rapid operations and deliberate operations provide a description of the degree of completeness required by the commander. Rapid operations are fast paced, are focused on key pieces of information, and entail a small number of tasks. They describe reconnaissance that personnel must perform in a time-constrained environment. Deliberate operations are slow, detailed, and broad-based. They require the accomplishment of numerous tasks. The commander must allocate a significant amount of time to conduct a deliberate reconnaissance.

1-55. Forceful and stealthy operations provide a description of the level of covertness that the commander requires. Units conduct forceful operations without significant concern about being observed. Mounted units or combat units serving in a reconnaissance role often conduct forceful operations. In addition, forceful operations are appropriate in stability operations where the threat is not significant in relation to the requirement for information. Units conduct stealthy operations to minimize chance contact and prevent the reconnaissance force from being detected. They often are conducted dismounted and require increased allocation of time for success.

Engagement Criteria

1-56. Engagement criteria establish minimum thresholds for engagement (lethal and nonlethal). They clearly specify which targets the reconnaissance element is expected to engage and which it will hand off to other units or assets. For example, nonlethal contact identifies engagement criteria for tactical questioning of civilians and factional leaders. This criterion allows unit commanders to anticipate bypass criteria and to develop a plan to maintain visual contact with bypassed threats.

SURVEILLANCE

1-57. *Surveillance* is the systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means (JP 3-0). Surveillance involves observing an area to collect information.

1-58. In the observation of a given area, the focus and tempo of the collection effort primarily comes from the commander's intent and guidance. Surveillance involves observing the threat and local populace in a NAI or targeted area of interest (TAI). Surveillance may be conducted as a stand-alone mission, or as part of a reconnaissance mission (particularly area reconnaissance). Elements conducting surveillance must maximize assets, maintain continuous surveillance on all NAIs and TAIs, and report all information rapidly and accurately.

1-59. Surveillance tasks can be performed by a variety of assets (ground, air, sea, and space), means (Soldier and systems), and mediums (throughout the electromagnetic spectrum).

1-60. Generally, surveillance is considered a "task" when performed as part of a reconnaissance mission. However, many Army, joint, and national systems are designed specifically to conduct only surveillance. These are surveillance missions. Army military intelligence organizations typically conduct surveillance missions. Reconnaissance units can conduct surveillance tasks as part of reconnaissance, security, or other missions. The commonality of reconnaissance and surveillance is observation and reporting.

1-61. Surveillance is distinct from reconnaissance. Surveillance is tiered and layered technical assets collecting information. Often surveillance is passive and may be continuous. Reconnaissance is active in the collection of information (such as maneuver) and usually includes human participation. Additionally, reconnaissance may involve fighting for information. Sometimes these operations are deliberate, as in a reconnaissance in force; however, the purpose of reconnaissance is to collect information, not initiate

combat. Reconnaissance involves many tactics, techniques, and procedures throughout the course of a mission. An extended period of surveillance may be one of these. Commanders complement surveillance with frequent reconnaissance. Surveillance, in turn, increases the efficiency of reconnaissance by focusing those missions while reducing the risk to Soldiers.

1-62. Both reconnaissance and surveillance involve detection, location, tracking, and identification of entities in an assigned area and gaining environmental data, but they are not executed in the same way. During reconnaissance, collection assets are given the mission to find specific information by systematically checking different locations within the area. During surveillance, collection assets watch the same area, waiting for information to emerge when an entity or its signature appears.

1-63. Reconnaissance and surveillance complement each other by cueing the commitment of collection assets against specific locations or specially targeted enemy units. An airborne surveillance asset may discover indicators of enemy activity that cues a reconnaissance mission. In some cases, surveillance assets may also be tasked to answer specific questions.

Surveillance Characteristics

1-64. Effective surveillance—

- Maintains continuous observations of all assigned NAIs and TAIs.
- Provides early warning.
- Identifies, tracks, and assesses key targets.
- Provides mixed, redundant, and overlapping coverage.

Maintains Continuous Surveillance of All Assigned Named Areas of Interest and Targeted Areas of Interest

1-65. Once the surveillance of a NAI or TAI commences, units maintain it until they complete the mission or the higher commander terminates the mission. Commanders designate the receiver of the information and the means of communication. Continuous surveillance requires multiple collection assets, a purpose (requirement), a location (NAI or TAI) for each asset, and an information collection task. Effective commanders avoid designating too many NAIs and TAIs. Information collection suffers as a result of excessive requirements. During the plan and assess phase, the staff selects collection assets that can best answer the specific information requirements generated from the CCIRs. During tasking and direct phases, the operations officer tasks specific assets to perform these tasks to ensure continuous coverage.

Provides Early Warning

1-66. Surveillance aims to provide early warning of an enemy or threat action. Together with IPB, commanders use information collection to ascertain the enemy or threat course of action and timing. They then orient assets to observe these locations for indicators of threat actions. Reporting must be timely and complete.

Detects, Tracks, and Assesses Key Targets

1-67. Surveillance support for targeting includes detecting, tracking, and assessing those key targets. Surveillance support to targeting includes detecting and tracking desired targets in a timely, accurate manner. Clear and concise tasks must be given so the surveillance systems can detect a given target. Target tracking is inherent to detection. Mobile targets must be tracked to maintain a current target location. Once a target is detected, targeting planning cells must also consider the need to *track* targets. Tracking targets—such as moving, elusive, low contrast targets (to include individuals)—requires a heavy commitment of limited information collection assets and resources. Assessing key targets pertains to the results of attacks on targets. This helps commanders and staffs determine if their targeting objectives were met.

Provides Mixed, Redundant, and Overlapping Coverage

1-68. Commanders integrate the capabilities of limited assets to provide mixed, redundant, and overlapping coverage of critical locations identified during planning. The intelligence and operations staff work

together to achieve balance. Commanders and staff continuously assess surveillance results to determine any changes in critical locations requiring this level of coverage.

Surveillance Types

1-69. The types of surveillance are zone, area, point, and network.

Note: *Forms* of reconnaissance, as opposed to *types* of surveillance, are associated with maneuver units and missions.

Zone Surveillance

1-70. Zone surveillance is the temporary or continuous observation of an extended geographic zone defined by boundaries. It can be associated with but is not limited to a TAI or a NAI. Zone surveillance covers the widest geographical area of any type of surveillance. Multiple assets, including airborne surveillance assets and radar with wide coverage capabilities, are typically employed in zone surveillance.

Area Surveillance

1-71. Area surveillance is the temporary or continuous observation of a specific prescribed geographic area. It can be associated with, but is not limited to, a TAI or NAI. This area may include a town, a neighborhood, ridgeline, wood line, border crossing, farm, plantation, cluster or group of buildings, or other manmade or geographic feature. Unlike area reconnaissance, it does not include individual structures (such as a bridge or single building). Ground-mounted surveillance systems are particularly useful in area surveillance.

Point Surveillance

1-72. Point surveillance is the temporary or continuous observation of a place (such as a structure), person, or object. This can be associated with, but is not limited to, a TAI or a NAI. It is the most limited in geographic scope of all forms of surveillance. Point surveillance may involve tracking people. When surveillance involves tracking people, the "point" is that person or persons, regardless of movement and location. Tracking people normally requires a heavier commitment of assets and close coordination for handoff to ensure continuous observation.

Network Surveillance

1-73. Network surveillance is the observation of organizational, social, communications, cyberspace, or infrastructure connections and relationships. Network surveillance can also seek detailed information on connections and relationships among individuals, groups, and organizations, and the role and importance of aspects of physical or virtual infrastructure (such as bridges, marketplaces, and roads) in people's lives. It can be associated with but is not limited to a TAI or a NAI.

SECURITY OPERATIONS

1-74. Security operations are shaping operations that can take place during all operations. Reconnaissance is a part of every security operation. Other collection assets provide the commander with early warning and information on the strength and disposition of enemy forces. The availability of information collection assets enables greater flexibility in the employment of the security force.

1-75. Security operations aim to protect the force from surprise and reduce the unknowns in any situation. A commander undertakes these operations to provide early and accurate warning of enemy operations, to provide the force being protected with time and maneuver space to react to the enemy, and to develop the situation to allow the commander to effectively use the protected force. Commanders may conduct security operations to the front, flanks, and rear of their forces. The main difference between security operations and reconnaissance is that security operations orient on the force or facility being protected, while reconnaissance is enemy, populace, and terrain oriented.

1-76. The five forms of security operations commanders may employ are screen, guard, cover, area security, and local security. (Refer to FM 3-90 for more information on the five forms of security operations and their tactical employment.)

1-77. Successful security operations depends upon properly applying the following five fundamentals:

- Provide early and accurate warning.
- Provide reaction time and maneuver space.
- Orient on the force or facility to be secured.
- Perform continuous reconnaissance.
- Maintain enemy contact.

1-78. To properly apply the fundamental of "perform continuous reconnaissance," the security force aggressively and continuously seeks the enemy, interacts with the populace, and reconnoiters key terrain. It conducts active area or zone reconnaissance to detect enemy movement or enemy preparations for action and to learn as much as possible about the terrain. The ultimate goal is to detect the enemy's COA and assist the main body in countering it. Terrain information focuses on its possible use by the enemy or friendly force, either for offensive or defensive operations. Stationary security forces use combinations of observation posts, aviation, intelligence collection assets, and battle positions to perform reconnaissance. Moving security forces perform zone, area, or route reconnaissance along with using observation posts and battlefield positions, to apply this fundamental.

INTELLIGENCE OPERATIONS

1-79. Intelligence operations align intelligence assets and resources against requirements to the collect information and intelligence to inform the commander's decisions. Conducting intelligence operations requires an organic collection and analysis capability. Those units without resources must rely on augmentation from within the intelligence enterprise for intelligence. Although the focus is normally on tactical intelligence, the Army draws on both strategic and operational intelligence resources. Each intelligence discipline provides the commander specific technical capabilities and sensors. Because of the unique capabilities and characteristics of intelligence operations, these capabilities and sensors require specific guidance through technical channels. The Army's intelligence disciplines that contribute to intelligence operations are—

- Counterintelligence.
- Human intelligence.
- Geospatial intelligence.
- Measurement and signature intelligence.
- Signals intelligence.
- Technical intelligence.

Counterintelligence

1-80. Counterintelligence counters or neutralizes intelligence collection efforts by foreign intelligence and security services and international terrorist organizations. It does this through collection, counterintelligence investigations, operations, analysis, production, and functional and technical services. Counterintelligence includes all actions taken to detect, identify, track, exploit, and neutralize the multidiscipline intelligence activities of friends, competitors, opponents, adversaries, and enemies. It is the key intelligence community contributor to protect U.S. interests and equities. Counterintelligence helps identify essential elements of friendly information (EEFI) by identifying vulnerabilities to threat collection and actions taken to counter collection and operations against U.S. forces.

Human Intelligence

1-81. *Human intelligence* is a category of intelligence derived from information collected and provided by human sources (JP 2-0). This information is collected by a trained human intelligence collector, from people and their associated documents and media sources. Units use the collected information to identify threat elements, intentions, composition, strength, dispositions, tactics, equipment, personnel, and capabilities.

Geospatial Intelligence

1-82. Title 10, U.S. Code establishes geospatial intelligence. *Geospatial intelligence* is the exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information (JP 2-03). No longer is an intelligence discipline, imagery intelligence is a subset of geospatial intelligence. Imagery intelligence is derived from the exploitation of imagery collected by visual photography, infrared sensors, lasers, multispectral sensors, and radar. These sensors produce images of objects optically, electronically, or digitally on film, electronic display devices, or other media.

Measurement and Signature Intelligence

1-83. Measurement and signature intelligence is technically derived intelligence that detects, locates, tracks, identifies, or describes the specific characteristics of fixed and dynamic target objects and sources. It also includes the additional advanced processing and exploitation of data derived from imagery intelligence and signals intelligence collection. Measurement and signature intelligence collection systems include but are not limited to radar, spectro-radiometric, electro-optical, acoustic, radio frequency, nuclear detection, and seismic sensors. Measurement and signature intelligence collection also includes techniques for collecting CBRN and other materiel samples.

Signals Intelligence

1-84. Signals intelligence is produced by exploiting foreign communications systems and noncommunications emitters. Signals intelligence provides unique intelligence and analysis information in a timely manner. The discipline comprises communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence.

Technical Intelligence

1-85. Technical intelligence is intelligence derived from the collection and analysis of threat and foreign military equipment and associated materiel. Units use this collected intelligence for the purposes of preventing technological surprise, assessing foreign scientific and technical capabilities, and developing countermeasures designed to neutralize an adversary's technological advantages.

Chapter 2

Commander and Staff Responsibilities

This chapter examines the roles, knowledge, and guidance of the commander in information collection activities. The commander's involvement facilitates an effective information collection plan that is synchronized and integrated within the overall operation. This chapter then discusses the role of the staff. Lastly, this chapter discusses contributions from working groups.

THE ROLE OF THE COMMANDER

2-1. Commanders understand, visualize, describe, direct, lead, and assess operations. Understanding is fundamental to the commander's ability to establish the situation's context. Understanding involves analyzing and understanding the operational or mission variables in a given operational environment. It is derived from applying judgment to the common operational picture through the filter of the commander's knowledge and experience.

2-2. Numerous factors determine the commander's depth of understanding. Information from information collection and the resulting intelligence products prove indispensable in assisting the commander in understanding the area of operations (AO). Formulating commander's critical information requirements (CCIRs) and keeping them current also contribute to this understanding. Maintaining understanding is a dynamic ability; a commander's situational understanding changes as an operation progresses.

2-3. The commander must be involved in information collection planning. The commander directs information collection activities by—

- Asking the right questions to focus the efforts of the staff.
- Knowing the enemy. Personal involvement and knowledge have no substitutes.
- Stating the commander's intent clearly and decisively designating CCIRs.
- Understanding the information collection assets and resources to exploit their full effectiveness.

2-4. Commanders prioritize collection activities primarily through providing their guidance and commander's intent early in the planning process. Commanders must—

- Personally identify and update CCIRs.
- Ensure CCIRs are tied directly to the scheme of maneuver and decision points.
- Limit CCIRs to only their most critical needs (because of limited collection assets).
- Aggressively seek higher echelons' collection of, and answers to, the information requirements.
- Ensure CCIRs include the latest time information is of value (LTIOV) or the event by which the information is required.

2-5. The commander may also identify essential elements of friendly information (EEFI). The EEFI are not part of the CCIRs; rather they establish friendly information to protect, not enemy information to obtain. However, the commander may need to determine if the enemy has learned specific EEFI. In this case, finding this out can become a CCIR. (FM 6-0 provides detailed information on EEFI.)

2-6. Commanders ensure that both intelligence preparation of the battlefield (IPB) and information collection planning are integrated staff efforts. Every staff member plays an important role in both tasks. The chief of staff or executive officer ensures all staff members participate in and provide their functional expertise into the IPB process and information collection planning, preparation, execution, and assessment. Full staff engagement in these activities supports planning and helps facilitate the commander's visualization and understanding.

2-7. Information collection planning and assessment must be continuous. Commanders ensure they properly assign information collection tasks based on the unit's abilities to collect. Therefore, commanders match their information requirements as to not exceed the information collection and analytical ability of their unit. When not using organic assets, commanders use habitual relationships to optimize effective operations as a combined arms team, when possible.

2-8. Commanders assess operations. Commanders ensure collection activities provide the information needed. Timely reporting to the right analytical element at the right echelon is critical to information collection activities. Commanders continuously assess operations throughout the planning, preparation, and execution phases. The commander's involvement and interaction enable the operations and intelligence officers to more effectively assess and update collection activities. The commander's own assessment of the current situation and progress of the operation provides insight on what new information is needed and what is no longer required. The commander communicates this to the staff to assist them in updating CCIRs. Commanders should use regularly scheduled staff assessments (for example, end of phase assessments) to update information collection guidance as well as to increase their own understanding of the situation. Every echelon works together and tailors the intelligence enterprise making it seamless as possible by removing information sharing barriers.

COMMANDER'S NEEDS

2-9. Staffs synchronize and integrate information collection activities with the warfighting functions based on the higher commander's guidance and decisions. Commanders' knowledge of collection activities enables them to focus the staff and subordinate commanders in planning, preparing, executing, and assessing information collection activities for the operation.

2-10. Commanders must understand the overall concept of operations from higher headquarters to determine specified and implied tasks and information requirements. There are a finite number of assets and resources for information collection activities. Commanders communicate this as guidance for planners and the staff. Commanders must visualize how multiple collection components work together and understand how their unit's activities fit into and contribute to those of higher, adjacent, and lower echelons.

2-11. Extended areas of operations, the necessity to conduct missions and develop information and intelligence over large areas, and extended time spans can surpass the organic capabilities of a unit. Commanders must be able to deal effectively with many agencies and organizations in the area of operations to help enable the unit to perform information collection activities. One of the essential aspects to this is terminology. When dealing with non-U.S. Army personnel and organizations, commanders ensure those involved understand the terms used and provide or request clarification as needed. Commanders should gain a working knowledge of joint and multinational vocabulary and ways of operating. They should also know as much as possible about the roles and contributions of other organizations to better communicate and leverage resources.

COMMANDER'S GUIDANCE

2-12. Commanders play a central role in planning primarily by providing guidance. This should include specific guidance for collection assets and required information. Commanders consider risks and provide guidance to the staff on an acceptable level of risk for information collection planning. The commander issues formal guidance at three specific points in the process:

- *Initial guidance* following receipt of mission.
- *Commander's planning guidance* following mission analysis to guide course of action (COA) development.
- *Final planning guidance* after the COA decision but before the final warning order (WARNO).

INITIAL GUIDANCE

2-13. After a unit receives a mission, the commander issues initial guidance. (FM 5-0 provides detailed information on the initial guidance.) The initial guidance accomplishes several things. It—

- Begins the visualization process by identifying the tactical problem (the first step to problem solving).
- Defines the area of operations. This presents a common operational picture for the commander and staff in seeing the terrain, including the populace.
- Develops the initial commander's intent, specifically key tasks (including tasks for reconnaissance), decisive point, and end state.
- Lists challenges and initial CCIRs. Challenges include any guidance for specific staff sections.
- Results in the WARNO.

2-14. For information collection planning, the initial guidance includes—

- Initial timeline for information collection planning.
- Initial information collection focus.
- Initial information requirements.
- Authorized movement.
- Collection and product development timeline.

2-15. The initial WARNO can alert information collection assets to begin collection activities to begin at this time. If this is the case, the initial WARNO includes—

- Named areas of interest (NAIs) to be covered.
- Collection tasks and specific information requirements to be collected.
- Precise guidance on infiltration method, reporting criteria and timelines, fire support and casualty evacuation plan.

COMMANDER'S PLANNING GUIDANCE

2-16. The commander issues the commander's planning guidance during the mission analysis step of the MDMP, following the approval of the restated mission and mission analysis brief. Part of the commander's planning guidance is directly related to collection activities—the initial CCIRs and information collection guidance. The guidance for planning should contain sufficient information for the operations officer to complete a draft information collection plan. As a minimum, the commander's planning guidance includes—

- Current CCIRs.
- Focus and tempo.
- Engagement criteria.
- Acceptable risk to assets.

2-17. The commander issues the initial commander's intent with the commander's planning guidance. The staff verifies the draft information collection plan is synchronized with the commander's intent assesses any ongoing information collection activities, and recommends changes to support the commander's intent, CCIRs, and concept of operations.

FINAL PLANNING GUIDANCE

2-18. After the decision briefing, the commander determines a COA the unit follows and issues final planning guidance. Final planning guidance includes—

- Any new CCIRs, including the LTIOV.
- Rehearsals.

ROLE OF THE STAFF

2-19. The staff must function as a single, cohesive unit—a professional team. Effective staff members know their respective responsibilities and duties. They are also familiar with the responsibilities and duties of other staff members. (ATTP 5-0.1 details staff duties and responsibilities.) The information collection responsibilities of other coordinating staff members include assisting in the development of the information collection plan and annexes.

2-20. The chief of staff or executive officer directs the efforts of coordinating and special staff officers, integrates and synchronizes plans and orders, and supervises management of the CCIRs.

2-21. The G-2 (S-2) must work in concert with the entire staff to identify collection requirements and implement the information collection plan. The intelligence staff determines collection requirements, (based upon inputs from the commander and other staff sections) develops the information collection matrix with input from the staff representatives, and continues to work with the staff planners to develop the information collection plan. The G-2 (S-2) also identifies those intelligence assets and resources—human intelligence, geospatial intelligence, measurement and signature intelligence, or signals intelligence—which can provide answers to the CCIRs.

2-22. The G-2X (S-2X) (hereafter referred to as the 2X) is the doctrinal term used to refer to the counterintelligence and human intelligence operations manager who works directly for the G-2 (S-2). The term also refers to the staff section led by the 2X. The 2X manages counterintelligence and human intelligence operations in support of the overall unit operation. The 2X section works with the G-2 (S-2) in information collection planning and assessing, taking developed counterintelligence and human intelligence requirements and identifying the proper assets to answer the requirements. This information is used to develop requirement planning tools and the overall collection plan.

2-23. The G-3 (S-3) is the primary information collection tasking and directing staff officer within the unit, tasking the organic and assigned assets for execution. The G-3 (S-3) collaboratively develops the information collection plan and ensures its synchronization with the operation plan.

2-24. The other members of the staff support the operations process. Through the conduct of the planning process, staffs develop requirements that are considered for inclusion as CCIRs and into the information collection plan. Staffs also monitor the situation and progress of the operation towards the commander's desired goal. Staffs also prepare running estimates. A *running estimate* is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable (FM 5-0). Staffs continuously assess how new information might impact conducting operations. They update running estimates and determine if adjustments to the operation are required. Through this process, the staffs ensure that the information collection plan remains updated as the situation changes and requirements are answered or new requirements developed.

2-25. Staff members consider the following when supporting the information collection planning and execution:

- **Nature of the mission**. Offensive, defensive, and stability or defense support of civil authorities (DSCA) operations have different requirements, time frames, rules of engagement, and other differences. These differences influence information staffs require to provide recommendations or decisions. Unit movements before an operation begins may require a route reconnaissance.
- **Terrain and weather**. Specific environments (urban, mountain, jungle, and desert), the size of the operational area, trafficability, and severe weather conditions affect when and how assets are deployed and may degrade sensor capabilities. Additionally terrain management for asset locations is a staff responsibility in the creation of the information collection plan.
- **Higher commander's intent and guidance**. The commander's intent and guidance may specify the initiation of collection activities or they may leave wide leeway for subordinate commanders and staffs. Staffs determine how information collection activities support the commander's visualization expressed in the commander's intent.
- **What is known and not known about the enemy and the environment**. The commander determines the criticality of the information identified through CCIRs, which include the

LTIOV. When the information is required drives the collection timeframe. The staff recommends requirements as part of the CCIR development process, ensuring that requirements remain current with the situation and on-going operations.

- **Risk to collection assets**. Using the composite risk management process, commanders include acceptable risk to collection assets in their guidance. This may preclude the use or early use of some types of assets. For example, a long-range surveillance company may be available, but the nature of the terrain and the enemy may dictate the use of a less vulnerable asset.
- **Rules of engagement that affect information collection activities**. These may include limitations on where or when aircraft may fly, the use of tracked vehicles in urban areas, protection measures, surveillance of U.S. citizens (in DSCA), and other restrictions that affect information collection activities.
- **Need for operations security**. Staffs balance the need for information with the need to avoid revealing intentions by conducting information collection activities. This may dictate selection of assets, such as an airborne asset instead of ground reconnaissance asset, or the use of deception.
- **Support for friendly deception operations**. Information collection activities can support friendly deception operations by causing the enemy to wrongly predict friendly intentions based upon the reconnaissance and surveillance efforts they observe.
- **Available assets.** The availability, capabilities, and limitations of assets impact decisions on when and how to deploy them.
- **Enemy counterreconnaissance**. Staffs need to be cognizant of the nature of the enemy's counterreconnaissance intentions and capabilities, and plan to defeat or avoid them.

WORKING GROUP INPUT TO INFORMATION COLLECTION

2-26. *Battle rhythm* is a deliberate daily cycle of command, staff, and unit activities intended to synchronize current and future operations (JP 3-33). A headquarters' battle rhythm consists of a series of meetings, briefings, and other activities synchronized by time and purpose. The chief of staff or executive officer oversees the battle rhythm. Each meeting, to include working groups and boards, should be logically sequenced so that one meeting's outputs are available as another meeting's inputs (to include higher headquarters meetings).

2-27. A working group is a grouping of predetermined staff representatives who meet to provide analysis, coordinate, and provide recommendations for a particular purpose or function. Working groups are cross functional by design to synchronize the contributions of multiple command posts cells and staff sections.

2-28. A board is a grouping of predetermined staff representatives with delegated decision authority for a particular purpose or function. Boards are similar to working groups. However, commanders appoint boards with the purpose to arrive at a decision. When the process or activity being synchronized requires command approval, a board is the appropriate forum.

OPERATIONS AND INTELLIGENCE WORKING GROUP

2-29. At division and higher echelons, there are dedicated cells responsible for information collection planning. At battalion and brigade, there are no designated cells for information collection planning, this function is provided by the operations and intelligence staffs. Depending on the availability of personnel, the commander may choose to designate an ad hoc group referred to as an operations and intelligence working group. Because the primary staff officers' responsibilities cannot be delegated, the staff—chief of staff or executive officer—should direct and manage the efforts of this working group to achieve a fully synchronized and integrated information collection plan.

2-30. Unit standard operating procedures and battle rhythms determine how frequently an operations and intelligence working group meets. This working group should be closely aligned with both the current operations and future operations (or plans) cells to ensure requirements planning tools are properly integrated into the overall operation plan. These planning tools should also be nested in the concepts for plans.

2-31. The operations and intelligence working group is a temporary grouping of designated staff representatives who coordinate and integrate information collection activity and provide recommendations to the commander. This group ensures maximum efficiency in information collection by carefully employing all the collection tasks or missions together in the information collection plan. This helps satisfy as many different requirements as possible while ensuring that the operations and intelligence work group does not favor or become too reliant on one particular unit, discipline, or system. The working group usually includes, at a minimum, the following representatives:

- Chief of staff or executive officer.
- G-3 (S-3) (alternate chair) or representative.
- Engineer coordinator representative.
- Air defense airspace management or brigade aviation element representative.
- G-2 (S-2) or representative.
- G-2X (S-2X) or representative.
- Military intelligence company commander or representative.
- Reconnaissance squadron S-3, S-2, the S-3 and S-2, or a representative.
- G-2X (S-2X) or representative.
- Fire support officer or representative.
- G-7 (S-7) or representative.
- Signal officer or representative.
- Electronic warfare officer.
- G-9 (S-9) or representative.
- Chemical, biological, radiological, and nuclear officer.
- Sustainment cell representative.
- Subordinate unit representatives (if available).
- Special operations forces representative (if available).
- Legal representative (if available).

2-32. The working group aims to bring together the staff sections to validate requirements and deconflict the missions and taskings of organic and attached collection assets. Input is required from each member of the working group. The output of the working group is validation of outputs. This includes the following:

- An understanding of how the enemy is going to fight.
- A refined list of requirements.
- Confirmation of the final disposition of all collection assets.
- Review of friendly force information requirements, priority intelligence requirements (PIRs), and EEFI.
- Validation of outputs of other working groups (for example, fusion and targeting working groups).
- Review and establish critical NAIs and targeted areas of interest (TAIs).

2-33. The working group meeting is a critical event. Staffs must integrate it effectively into the unit battle rhythm to ensure the collection effort provides focus to operations rather than disrupting them. Preparation and focus are essential to a successful working group. All representatives, at a minimum, must come to the meeting prepared to discuss available assets, capabilities, limitations, and requirements related to their functions. Planning the working group's battle rhythm is paramount to conducting effective information collection operations. Staffs schedule the working group cycle to complement the higher headquarters' battle rhythm and its subsequent requirements and timelines.

2-34. The G-3 (S-3) (or representative) comes prepared to provide the following:

- The current friendly situation.
- Current CCIRs.
- The availability of collection assets.
- Requirements from higher headquarters (including recent fragmentary orders or taskings).
- Changes to the commander's intent.

- Changes to the task organization.
- Planned operations.

2-35. The G-2 (S-2) (or representative) comes prepared to provide the following:

- The current enemy situation.
- The current information collection priorities and strategies.
- Current requirements planning tools.
- The situational template tailored to the time discussed.
- Support from resources the G-2 (S-2) must request from higher headquarters.
- Weather and effects of weather on intelligence collection, reconnaissance, and surveillance.

2-36. Figure 2-1 describes a method for the operations and intelligence working group.

Purpose: To synchronize information collection with operations, determine current requirements, and make full use of all available assets to meet the commander's intent and requirements. **Frequency:** Twice weekly. **Duration:** 30 to 45 minutes. **Location:** To be determined.	**Staff Proponent:** G-2 (S-2) **Chair:** Deputy commander **Attendees:** Primary staff sections, fires officer, G-2X (S-2X), brigade or battalion liaison officers, Air Force liaison officer.
Inputs: • Command group guidance. • Area of operations update. • CCIRs update. • Future operations requirements. • Subordinate unit requirements • Targeting requirements. • Air tasking order nomination. **Outputs:** • Priorities and recommendations for latest information collection plan. • Latest scrub of the CCIRs. • FRAGO input.	**Agenda:** • Command group guidance review. • Area of operations review. • Past information collection plan review. • Weather. • Future operations requirements. • Subordinate unit requirements. • Targeting requirements. • Allocation of collection resources and assets availability. • Review issues. • Summary. • Closing comments.
CCIR commander's critical information requirement	FRAGO fragmentary order

Figure 2-1. Example of the operations and intelligence working group

FUSION WORKING GROUP

2-37. Typically, brigade and above form a fusion working group. This working group aims to refine and fuse the intelligence between the command and its subordinate units. The output of this working group provides the intelligence staff with refinements to the situation template and the event template. The working group also refines existing PIRs and recommends new PIRs to the operations and intelligence working group. Additionally the working group reviews requirements to ensure currency.

TARGETING WORKING GROUP

2-38. The purpose of the targeting working group is to synchronize the unit's targeting assets and priorities. For the staff, supporting the planning for the decide, detect, and assess (known as D3A) activities of the targeting process requires continuous updating of IPB products (such as situation templates and COA matrixes). The targeting working group considers targeting related collection and exploitation requirements. It also recommends additional requirements to the operations and intelligence working group. Staffs articulate these requirements as early in the targeting process as possible to support target development and other assessments.

2-39. Information collection support to target development takes the decide, detect, deliver, and assess methodology and applies this to the development of targets. Units using other targeting techniques—like find, fix, finish, exploit, assess, disseminate (known as F3EAD) or find, fix, track, target, engage, and assess (known as F2T2EA)—require no adaptation to the information collection support to targeting process. Nominations for request to current and future tasking orders as well as refinements to the high-value target lists are outputs of this working group.

2-40. The results of these working groups form the basis of the requests for information collection as well as products used by the intelligence staff in the creation of requirements planning tools. The operations staff integrates these tools in the creation of the information collection plan.

Chapter 3

Planning Requirements for and Assessing Information Collection

This chapter describes planning requirements for and assessing information collection for information collection activities. It discusses considerations for commanders for information collection planning. Then it discusses the support information collections provides to personnel recovery. It then covers the military decisionmaking process and information collection planning. Lastly, this chapter discusses assessing information collection activities.

THE OPERATIONS PROCESS AND INFORMATION COLLECTION

3-1. Commanders direct information collection activities by approving commander's critical information requirements (CCIRs) and through driving the operations process. The success of information collection is measured by its contribution to the commander's understanding, visualization, and decisionmaking. The operations process and information collection activities are mutually dependent. Commanders provide the guidance and focus that drive both by issuing their commander's intent and approving CCIRs. The activities of information collection occur during all parts of the operation providing continuous information to the operations process.

3-2. Throughout the operations process, commanders and staffs use integrating processes to synchronize the warfighting functions to accomplish missions. Information collection activities, as well as intelligence preparation of the battlefield (IPB) are among these integrating processes. *Synchronization* is the arrangement of action in time, space, and purpose to produce maximum relative combat power at a decisive place and time (JP 1-02). This collaborative effort by the staff, with the commander's involvement, is essential for synchronizing information collection with the overall operation. Planning, preparing, executing, and assessing information collection activities is a continuous cycle whose time frame depends on the echelon, assets engaged, and the type of operation. For example, offensive operations have a significantly shorter time frame for gathering information and expecting to see changes in the situation than stability operations.

3-3. Conducting information collection activities consists of various staff functions; planning, collection, processing and exploitation; analysis and production; dissemination and integration; and evaluation and feedback. It should focus on the commander's requirements. The purpose of these staff functions is to place all collection assets and resources into a single plan in order to capitalize on the different capabilities. The plan synchronizes and coordinates collection activities within the overall scheme of maneuver. A good information collection plan (refer to example in appendix B) fits into and supports the overall operations plan or order. It positions and tasks collection assets so they can collect the right information, sustain or reconstitute for branches or sequels, or shift priorities as the situation develops. Effective information collection focuses on answering the commander's requirements through collection tasks translated into orders.

INFORMATION COLLECTION PLANNING CONSIDERATIONS

3-4. The information collection plan synchronizes activities of the information collection assets to provide intelligence to the commander required to confirm course of action selection and targeting requirements. The intelligence staff, in coordination with the operations staff, ensures all available collection assets provide the required information. They also recommend adjustments to asset locations, if required.

3-5. To be effective, the information collection plan must be based on the initial threat assessment and modified as the intelligence running estimate changes. Other staff sections' running estimates may contain requirements for inclusion into the information collection plan. Additionally, the plan must be synchronized with the scheme of maneuver and updated as that scheme of maneuver changes. Properly synchronized information collection planning begins with the development and updating of IPB (threat characteristics, enemy templates, enemy course of action statements, and, most importantly, an enemy event template or matrix). Properly synchronized information collection planning ends with well-defined CCIRs and collection strategies based on the situation and commander's intent.

SUPPORT TO PERSONNEL RECOVERY

3-6. Support to personnel recovery consists of the staff activities and unit capabilities focused on collecting information to recover and return own personnel—whether Soldier, Army civilian, selected Department of Defense contractors, or other personnel as determined by the Secretary of Defense—who are isolated, missing, detained, or captured in an area of operations. This support also includes developing detailed analysis, detailed products, and estimates to support operations undertaken to recover isolated, missing, detained, or captured personnel.

THE MDMP AND INFORMATION COLLECTION PLANNING

3-7. Information collection planning is embedded in the military decisionmaking process (MDMP) and depends extensively on all staff members thoroughly completing the IPB process. Information collection planning starts with receipt of the mission (which could be a warning order). Information collection directly supports the development of intelligence and operations products used throughout the decision-making process. At each step in the MDMP, the staff must prepare certain products used in the plan and prepare phases of the operations process as described below.

3-8. Information collection activities are continuous, collaborative, and interactive. Several of the outputs from the various MDMP steps require the collaboration of the staff, especially the intelligence and operations staffs. The information collection plan cannot be developed without constant coordination among the entire staff. At every step in the MDMP, the intelligence staff must rely on input from the entire staff and cooperation with the operations staff to develop information collection products that support the commander's intent and maximize collection efficiency for each course of action under consideration. Paragraphs 3-9 through 3-59 highlight information collection planning inputs and outputs during the MDMP. Additional information on the conduct of the MDMP is contained in ATTP 5-0.1.

RECEIPT OF MISSION

3-9. Before receipt of the mission, the intelligence staff generates intelligence knowledge in anticipation of the mission. In addition to the knowledge already available, the intelligence staff uses intelligence reach and requests for additional information to higher headquarters to fill in the information gaps in the initial intelligence estimate. The intelligence staff should identify and tap into any ongoing or existing information collection activities or joint intelligence, surveillance, and reconnaissance (ISR) collection that may offer relevant information to fill gaps.

3-10. When a mission is received, the commander and staff shift their efforts to describing the operational environment using mission variables and begin preparations for the MDMP. Commanders provide their initial guidance to the staff. The staff uses it to generate the initial information collection tasks to units and transmits it as part of the first warning order. In their guidance, commanders state the critical information required for the area of operations. Expressed in later steps of the MDMP, these requirements identify the critical pieces of information that the commander must know to successfully plan, prepare, execute, and assess operations.

3-11. During the receipt of mission step, the staff gathers tools needed for the MDMP, begins the intelligence estimate, updates running estimates, and performs an initial assessment of the time available to subordinate units for planning, preparation, and execution. Since information collection assets are required early, the staff needs sufficient preparation time to begin sending information that the commander needs.

3-12. The information collection outputs from this step are—

- The commander's initial information collection guidance.
- Intelligence reach tasks.
- Requests for information to higher headquarters.
- Directions for accessing on-going or existing information collection activities or joint ISR.
- The first warning order (WARNO) with initial information collection tasks.

MISSION ANALYSIS

3-13. When mission analysis begins, the staff should have the higher headquarters plan or order and all available products. The staff adds their updated running estimates to the process. The initial information collection tasks issued with the first WARNO may yield information to be analyzed and evaluated for relevance to mission analysis. The commander provides initial guidance that the staff uses to capture the commander's intent and develop the restated mission.

Analyze the Higher Headquarters Order

3-14. During mission analysis, the staff analyzes the higher headquarters order to extract information collection tasks and constraints such as limits of reconnaissance. The order also contains details on the availability of information collection assets from higher echelons and any allocation of those assets to the unit.

Perform Intelligence Preparation of the Battlefield

3-15. IPB is one of the most important prerequisites to information collection planning. During IPB, staffs develop several key products that aid information collection planning. Those products include—

- Threat characteristics.
- Terrain overlays.
- The weather effects matrix.
- Enemy situational templates and course of action statements.
- The enemy event template and matrix.
- The high-payoff target list.
- An updated intelligence estimate including identified information gaps.

3-16. These products aid the staff in identifying—

- Information gaps that can be answered by existing collection activities, intelligence reach, and requests for information to higher echelons. The remaining information gaps are used to develop requirements for information collection.
- Threat considerations that may affect planning.
- Terrain effects that may benefit, constrain, or limit the capabilities of collection assets.
- Weather effects that may benefit, constrain, or negatively influence the capabilities of collection assets.
- Civil considerations that might affect information collection planning.

Note: When considering terrain effects, planners can use the geospatial information team to develop line-of-sight products.

3-17. The most useful product for information collection planning for the intelligence officer is the threat event template. Once developed, the threat event template is a key product in the development of the information collection plan. Likely threat locations, avenues of approach, infiltration routes, support areas, and areas of activity become named areas of interest (NAIs) or targeted areas of interest (TAIs) on which collection assets focus their collection efforts. Indicators, coupled with specific information requirements and essential elements of information (EEFI), provide collection assets with the required information on which units identify and report. FM 2-01.3 contains additional information on the IPB process and products.

3-18. As the staff completes mission analysis, the intelligence staff completes development of initial collection requirements. These collection requirements form the basis of the initial information collection plan, requests for collection support, and requests for information to higher and lateral units. When the mission analysis is complete, staffs have identified intelligence gaps, and planners have an initial plan on how to fill those gaps. Additionally, the operations officer and the remainder of the staff thoroughly understand the unit missions, tasks, and purposes.

Determine Specified, Implied, and Essential Tasks

3-19. The staff also identifies specified, implied, and essential information collection tasks. Specified tasks are directed toward subordinate units, systems, sensors, and Soldiers. Implied tasks determine how a system or sensor is initialized for collection. Essential information collection tasks are derived from specified and implied tasks. They are the focus of the information collection effort.

Review Available Assets

3-20. The staff must review all available collection assets, effectively creating an inventory of capabilities to be applied against collection requirements. Building the inventory of assets and resources begins with annex A of the higher headquarters order. The staff takes those assets attached or under operational control of the unit and adds those resources available from higher echelons and those belonging to adjacent units that might be of assistance. The higher headquarters order should specify temporary or permanent operating locations and the air tasking order details for aerial assets.

3-21. While reviewing the available collection assets, the staff evaluates the collection assets according to their capability and availability. First, the staff measures the capabilities of the collection assets. They must know and address the practical capabilities and limitations of all unit organic assets. Capability includes—

- Range.
- Day and night effectiveness.
- Technical characteristics.
- Reporting timeliness.
- Geolocation accuracy.
- Durability.
- Threat activity.
- Sustainability.
- Vulnerability.
- Performance history.

3-22. Range deals with the collector's ability to provide target coverage. It is important to not only consider mission range (duration and distance), but also how close the collection asset must be to the target. In addition, intelligence staffs consider the communications requirements from the asset to the controlling headquarters. What is the asset's effective range to observe target activity? What is the asset's ability to move and maneuver including travel and support times? If the best asset is an unmanned aircraft system, what it the range of the aircraft? What is the flight time duration? How far is the preplanned coverage area from the aircraft launch locations?

3-23. Day and night effectiveness discusses the collector's ability to collect information in varying degrees of light. Some collection sensors were exclusively designed for nighttime or limited visibility conditions, while some sensors cannot operate at night or with limited visibility. Is the asset capable of conducting collection during the hours of darkness and low visibility? How does thermal crossover effect the asset's capabilities?

3-24. Technical characteristics address the capabilities and limitations of the collector's resources. Urban environments degrade some capabilities of collection sensors. Weather effects on sensors must be considered. Collectors take into account the time factors each asset requires for task performance. Can the sensor see through fog or smoke? What are the effects of the environment (including such factors as urban

or rural terrain and soil composition) on the collection asset? Can it continue despite hostile electronic attack? Can the aircraft launch in high winds or limited visibility? Can the prime mover cross-restricted terrain?

3-25. Reporting timeliness deals with the collector's promptness for reporting. Some collection assets require additional processing time to convert data into a useable format. What are the established reporting criteria for each collection asset? How long does it take a collector to disseminate collected information to the requestor?

3-26. Geolocation accuracy discusses the collector's ability to identify exact locations. Targeting requirements and rules of engagement may require greater geolocational accuracy. Accuracy implies reliability and precision. How accurate is the locational data provided by the asset? Is the asset capable of providing locational accuracy required for precision guided munitions?

3-27. Durability addresses the stability and endurance of the materials used by collectors. Can the aircraft launch in high winds or limited visibility? Can the prime mover cross-restricted terrain?

3-28. Threat activity deals with amount of enemy activity the collector can identify. Is the threat conducting activities that can be obtained and reported by the collection system?

3-29. Sustainability addresses the length of time a collector can use an asset without additional resources. Each collection asset has unique sustainment requirements; therefore, the staff must consider the collection asset's sustainability for long duration operations. The longer the collection period, the harder it will be to find assets for continuous activity. Weather can significantly affect sustainability of certain collection assets.

3-30. Vulnerability discusses the collector's vulnerability to threat forces, not only in the target area but also along the entire route of travel. Collectors evaluate their vulnerability to threat forces. Collectors consider the threat's ability to locate, identify, and destroy the collectors anywhere their collection mission might take them. What is the threat's ability to locate, identify, and destroy the collection asset? Is the collection asset or sensor vulnerable to threat denial and deception?

3-31. Performance history covers the known reliability of collection assets. Experienced staffs know which collection assets they can rely on to meet the commander's requirements. Readiness rates, responsiveness, and accuracy over time may raise one collector's reliability factor. Certain sensors require confirmation, especially if targeting is an issue.

3-32. The second criteria staffs evaluate is the availability of collection assets. Staffs must know the collectors and processors available at their own echelon and at echelons above and below it. They also know how to access those assets and resources. Theater and joint echelons apportion joint ISR assets to subordinate echelons. Corps and divisions allocate support from the apportioned amount they receive to brigade combat teams and below. Staffs understand the system of apportionment and allocation so they can determine what is available and what they can request by analyzing the higher headquarters order and reviewing the various scheduling or tracking mechanisms.

Note: Military source operations take time to establish and cultivate. Human intelligence collection availability and responsiveness is linked to geographic access, support relationships, protection restrictions, and workload. For more information on military source and human intelligence, refer to FM 2-22.3 and TC 2-22.303.

Signals intelligence assets are also valuable collection assets in stability operations when properly focused and supported through all-source intelligence analysis. Staffs employ signals intelligence collection with another collection asset. This mix of coverage allows signals intelligence collectors to cue and be cued by other collection assets.

3-33. Certain capabilities require confirmation, especially if targeting is an issue. For example, target selection standards may require the staff to rely on systems capable of providing targeting accuracy. If experience shows that a particular system is often unavailable because of local weather patterns, the staff considers this in evaluating the system's performance history perhaps leading to the selection of an alternate system.

Determine Constraints

3-34. When determining constraints, the staff considers legal, political, operational, and rules of engagement constraints that might constrain reconnaissance, security, intelligence operations, and surveillance. The staff must consider planning constraints such as limits of reconnaissance, earliest time information is of value, and not earlier than times. In some cases, the commander may impose constraints on the use of certain collection assets. In other cases, system specific constraints—such as the weather, crew rest, or maintenance cycle limitations—may impose limits the staff must consider.

Identify Critical Facts and Assumptions

3-35. When staffs identify critical facts and assumptions, they identify critical facts and assumptions pertinent to information collection planning that they will use later in course of action (COA) development. For example, a critical fact might be that imagery requests may take 72 to 96 hours to fulfill or that the human intelligence effort requires significant time before a good source network is fully developed.

3-36. Developing assumptions for planning include the availability and responsiveness of organic assets and resources from higher echelons. For example, the staff might use a certain percentage (representing hours) of unmanned aircraft system support available on a daily basis, weather and maintenance permitting.

Perform Risk Assessment

3-37. When performing a risk assessment, the staff considers the asset's effectiveness versus the protection requirements and risk to the asset. For example, placing a sensor forward enough on the battlefield that it can return valuable data and information may put the asset at high risk of being compromised, captured, or destroyed. The calculus of payoff versus loss will always be determined by mission variables and the commander's decision.

3-38. In some cases, friendly forces may reveal a collection capability by taking certain actions. If it is important to keep a collection capability concealed, then the staff carefully considers every lethal or nonlethal action based on current intelligence.

Determine Initial CCIRs and EEFI

3-39. Determining initial CCIRs and EEFI is the most important prerequisite for information collection planning. The staff refines the list of requirements they derive from the initial analysis of information available and from intelligence gaps identified during IPB. They base this list on higher headquarters tasks, commander's guidance, staff assessments, and subordinate and adjacent unit requests for information.

3-40. The staff then nominates these requirements to the commander to be CCIRs and EEFI. Commanders alone decide what information is critical based on their experience, the mission, the higher commander's intent, and input from the staff. The CCIRs are the primary focus for information collection activities.

Develop the Initial Information Collection Plan

3-41. The initial information plan is crucial to begin or adjust the collection effort to help answer requirements necessary in developing effective plans. The initial information collection plan sets information collection in motion. Staffs may issue it as part of a WARNO, a fragmentary order, or an operation order. As more information becomes available, staffs incorporate it into a complete information plan to the operation order.

3-42. At this point in the MDMP, the initial information plan has to be generic because the staffs have yet to develop friendly COAs. The basis for the plan is the commander's initial information collection guidance, the primary information gaps identified by the staff during mission analysis, and the enemy situational template developed during IPB. (Chapter 4 contains additional information on tasking and directing collection assets.)

3-43. The intelligence staff creates the requirements management tools for the information collection plan. The operations staff is responsible for the information collection plan. During this step, the operations and intelligence staff work closely to ensure they fully synchronize and integrate information collection activities into the overall plan.

3-44. The operations officer considers several factors when developing the initial information collection plan, including—

- Requirements for collection assets in follow-on missions.
- The time available to develop and refine the initial information collection plan.
- The risk the commander is willing to accept if information collection missions are begun before the information collection plan is fully integrated into the scheme of maneuver.
- Insertion and extraction methods for reconnaissance, security, surveillance, and intelligence units.
- Contingencies for inclement weather to ensure coverage of key NAIs or TAIs.
- The communications plan for transmission of reports from assets to tactical operations centers.
- The inclusion of collection asset locations and movements into the fire support plan.
- The reconnaissance handover with higher or subordinate echelons.
- The sustainment support.
- Legal support requirements.

Develop Requests for Information and Requests for Collection or Support

3-45. Submitting a request for information to the next higher or lateral echelon is a method for obtaining information not available with organic information collection assets. Units enter requests for information into a request for information management system where all units can see them. Hence, analysts several echelons above the actual requester become aware of the request and may be able to answer it.

3-46. When the unit cannot satisfy a collection requirement with its own assets, the intelligence staff composes and submits a request for information to the next higher echelon (or lateral units) for integration within its own information collection plan. At each echelon, the requirement is validated and a determination made as to whether or not that echelon can satisfy the requirement. If that echelon cannot satisfy the requirement, it is passed to the next higher echelon.

Note: This process continues until the requirement is satisfied, the information or intelligence is no longer needed, or it is determined that the requirement cannot be satisfied.

3-47. Throughout the request for information process, units must apprise the submitting organization of the status of their request for information as either accepted for action, passed to another organization for action, returned without action (invalid or impracticable request), or closed (satisfied). For PIR, the intelligence staff tracks all production requirements, particularly those transmitted to higher echelons. When a requirement is satisfied or determined to be overcome by events, intelligence officers must notify the higher headquarters that the requirement is closed.

Develop and Synchronize Production Requirements

3-48. Intelligence staffs develop and synchronize production requirements to provide timely and relevant intelligence analysis and products to commanders, staff, and subordinate forces. Staffs use the unit's battle rhythm as a basis for determining the daily, weekly, and monthly analytical products. The intelligence staff then designs an analytical and production effort to answer the CCIRs and meet the commander's need for situational understanding and the staff's need for situational awareness.

3-49. Intelligence production includes analyzing information and intelligence. It also includes presenting intelligence products, assessments, conclusions, or projections regarding the area of operations and threat forces in a format that aids the commander in achieving situational understanding. Staffs devote the remainder of the analytical effort to processing, analyzing, and disseminating data and information.

3-50. Commanders and staffs measure the success of the analytical and production effort by the products provided and their ability to answer or satisfy the CCIRs, intelligence requirements, and information requirements. For the purposes of the intelligence warfighting function an intelligence requirement is a type of information requirement developed by subordinate commanders and staff (including subordinate staffs) that requires dedicated collection.

COURSE OF ACTION DEVELOPMENT

3-51. Using the continually updated IPB products and the enemy situation template, the intelligence staff must integrate information collection considerations to develop friendly COAs. In many cases, the information collection considerations for each COA are similar depending on the characteristics of the friendly COA.

3-52. The operations and intelligence staffs must collaborate on information collection considerations to support each COA developed. The staff works to integrate its available resources into an integrated plan. Intelligence and operations staffs focus on the relationship of collection assets to other friendly forces, the terrain and weather, and the enemy.

3-53. The development of NAIs and TAIs based upon suspected enemy locations drive the employment of collection assets. The staff considers how to use asset mix, asset redundancy, and asset cueing to offset the capabilities of the various collection assets.

3-54. During COA development, the staff refines and tailors the initial CCIRs for each COA. Technically, these are initial requirements for each course of action. Later in the MDMP, once a COA is approved, the commander approves the final CCIR, and the staff publishes it.

COURSE OF ACTION ANALYSIS (WAR-GAMING)

3-55. The intelligence staff records the results of COA analysis and uses that information to develop the requirements planning tools. The entire staff uses the action-reaction-counteraction process to move logically through the war-gaming process. These events have a bearing on the assets recommended for tasking to the operations staff.

ORDERS PRODUCTION

3-56. Orders production is putting the plan into effect and directing units to conduct specific information collection tasks. The staff prepares the order by turning the selected COA into a clear, concise concept of operations and supporting information. The order provides all the information subordinate commands need to plan and execute their operations. However, this is not the first time subordinate commanders and their staffs have seen this data. Within the parallel and collaborative planning process, planners at all echelons have been involved in the orders process.

ASSESS INFORMATION COLLECTION ACTIVITIES

3-57. Assessment guides every operations process activity. Assessment is the continuous monitoring and evaluation of the current situation, particularly the enemy, and progress of an operation. Assessing information collection activities enables the operations and intelligence staffs to monitor and evaluate the current situation and progress of the operation. The desired result is to ensure all collection tasks are completely satisfied in a timely manner.

3-58. Staffs begin assessing information collection task execution with monitoring and reporting by collection assets as they execute their missions. Staffs track reporting to determine how well the information collection assets satisfy their collection tasks. The desired result is relevant information delivered to the commander before the latest time information is of value.

3-59. The running estimate informs the staff of the status of collection on all requirements. A running estimate is even more effective when staffs compare previous ones that refer to the same time. This comparison grades accuracy and relevancy of the prediction to what actually occurred enabling the staff to develop COAs that avoid repeating mistakes.

3-60. After each phase of the operation, staffs conduct an assessment. They examine the audit trail to determine which requirements were answered and which ones were not answered. Then the operation and intelligence staffs assess the accuracy and effectiveness of the collection assets and analytic elements. (Refer to FM 5-0, chapter 6, for further information on assessment.)

This page intentionally left blank.

Chapter 4

Tasking and Directing Information Collection

Commanders direct information collection activities by approving requirements and through mission command in driving the operations process. This chapter describes the tasking and directing of information collection assets. It discusses how the staff finalizes the information collection plan and develops the information collection overlay. It then discusses the development of the information collection scheme of support. Lastly it discusses re-tasking assets.

TASK AND DIRECT INFORMATION COLLECTION

4-1. The operations staff integrates collection assets through a deliberate and coordinated effort across all warfighting functions. Tasking and directing information collection is vital to control limited collection assets. During task and direct information collection, the staff recommends redundancy, mix, and cue, as appropriate. The process of planning information collection activities begins once requirements are established, validated, and prioritized. Staffs accomplish tasking information collection by issuing warning orders, fragmentary orders, and operation orders. They accomplish directing information collection assets by continuously monitoring the operation. Staffs conduct re-tasking to refine, update, or create new requirements.

FINALIZE THE INFORMATION COLLECTION PLAN

4-2. To finalize the information collection plan, the staff must complete several important activities and review several considerations to achieve a fully synchronized, efficient, and effective plan. The information collection plan also applies to the rapid decisionmaking and synchronization process. Updating information collection activities during the execution and assessment phases of the operations process is crucial to the successful execution and subsequent adjustments of the information collection plan. The information collection plan is implemented through execution of asset tasking. The tasking process provides the selected collection assets with specific, prioritized requirements. When collection tasks or requests are passed to units, the staff provides specific details that clearly define the collection requirements. These requirements identify—

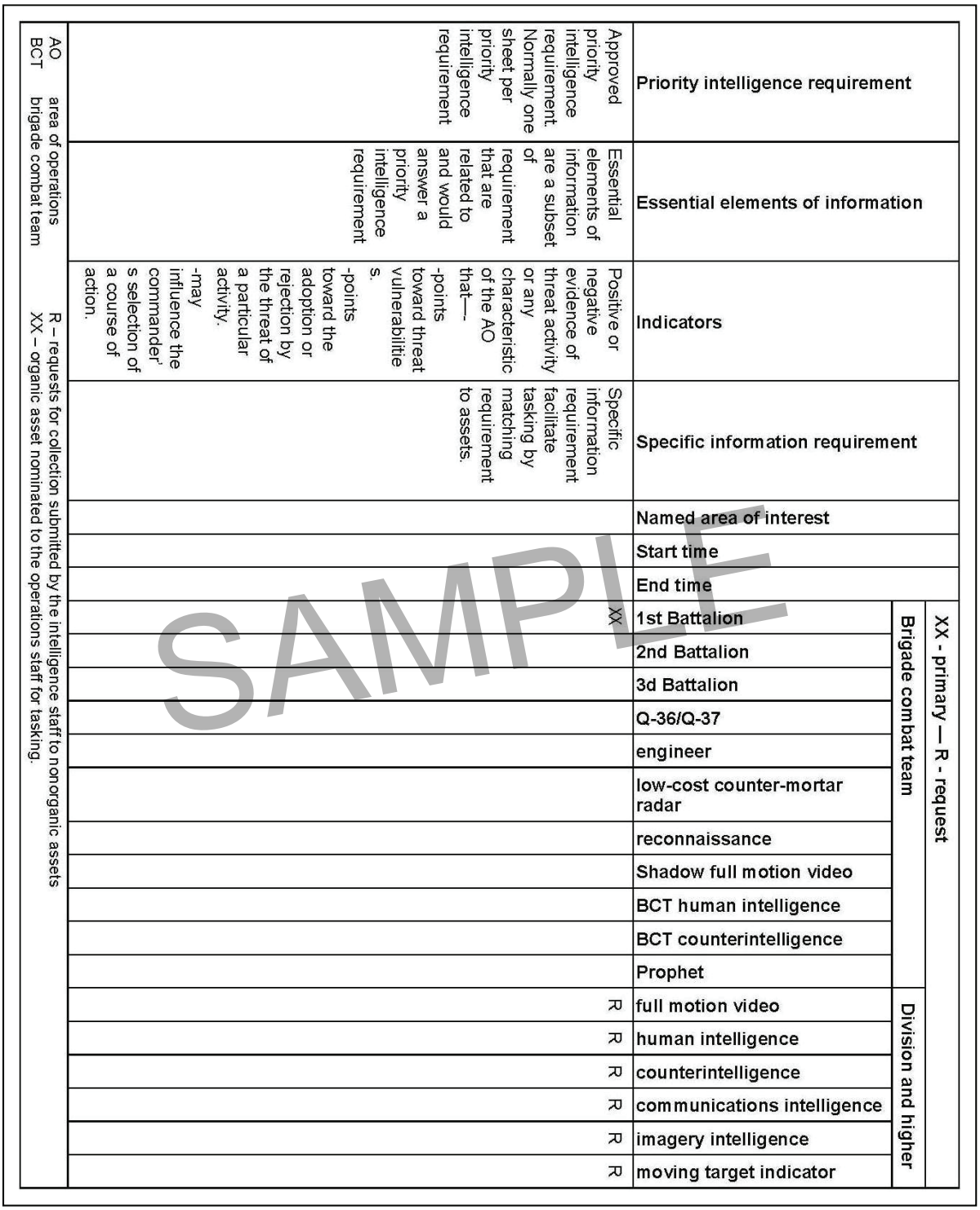
- What to collect—specific information requirements and essential elements of information.
- Where to collect it—named areas of interest and targeted areas of interest.
- When and how long to collect.
- Why to collect—answer commander's critical information requirements.

4-3. The information collection plan is an execution order and should be published in the five-paragraph operation order (OPORD) format as a warning order (WARNO), an OPORD, or a fragmentary order (FRAGO). Staffs use the information collection plan for tasking, directing, and managing of collection assets (both assigned and attached assets) to collect against the requirements. The operations officer tasks and directs information collection activities. The intelligence staff assists the staff in the development of the information collection plan by providing the requirement planning tools. (Refer to TC 2-01 and ATTP 2-01 on how the requirement planning tools are developed.) Staffs—

- Integrate the information collection plan into the scheme of maneuver.
- Publish annex L (information collection) to the OPORD that tasks assets to begin the collection effort.

- Ensure that the information collection plan addresses all of the commander's requirements, that assigned and attached assets have been evaluated and recommended for information collection tasks within their capabilities, and that collection tasks outside the capabilities of assigned and attached assets have been prepared as requests for information to appropriate higher or lateral headquarters.
- Publish any FRAGOs and WARNOs associated with information collection.

4-4. Appendix B contains examples of the annex L and an information collection WARNO. Figure 4-1 is a sample information collection matrix format which can be used as an appendix to annex L. ATTP 2-01 contains additional information and techniques on completing the information collection matrix.



Priority intelligence requirement	Essential elements of information	Indicators	Specific information requirement	Named area of interest	Start time	End time	XX - primary — R - request	
							Brigade combat team	Division and higher
Approved priority intelligence requirement. Normally one sheet per priority intelligence requirement	Essential elements of information are a subset of requirement that are related to and would answer a priority intelligence requirement	Positive or negative evidence of threat activity or any characteristic of the AO that— -points toward threat vulnerabilities. -points toward the adoption or rejection by the threat of a particular activity. -may influence the commander's selection of a course of action.	Specific information requirement tasking by matching requirement to assets.				1st Battalion	XX
							2nd Battalion	
							3d Battalion	
							Q-36/Q-37	
							engineer	
							low-cost counter-mortar radar	
							reconnaissance	
							Shadow full motion video	
							BCT human intelligence	
							BCT counterintelligence	
							Prophet	
							full motion video	R
							human intelligence	R
							counterintelligence	R
							communications intelligence	R
							imagery intelligence	R
							moving target indicator	R

AO area of operations
BCT brigade combat team

R – requests for collection submitted by the intelligence staff to nonorganic assets
XX – organic asset nominated to the operations staff for tasking.

SAMPLE

Figure 4-1. Sample information collection matrix

4-5. The primary means of tasking assets is through an information collection plan. Staffs can issue this plan as part of the completed OPORD; however, the tactical situation may impose a limited time constraint. In such cases, staffs can issue the information collection plan as early as the initial WARNO. This gives collection assets time to prepare for information collection activities. Staffs use FRAGOs to re-task assets that are already conducting operations and to adjust execution as requirements and priorities change.

DEVELOP THE INFORMATION COLLECTION OVERLAY

4-6. The staff may issue an information collection overlay depicting the information collection plan in graphic form as an appendix or annex L to the OPORD. Typical items on the overlay include the following:

- Friendly boundaries and phase lines.
- Reconnaissance handover lines.
- Named areas of interest and targeted areas of interest.
- Limits of advance and limits of reconnaissance. Limits of reconnaissance are constraints derived from higher headquarters orders that may designate a limit of advance impacting reconnaissance units.
- Counterreconnaissance areas.
- Fire support control measures.
- Graphics depicting zone, area, or route reconnaissance.
- Routes start points, release points, infiltration lanes, and checkpoints.
- Primary and alternate observation post locations.
- Ambulance exchange points and logistics release points.
- Planned or existing obstacles.
- Scan sectors for sensors.
- Unmanned aircraft system flight paths.
- Retransmission locations.

4-7. Figure 4-2 on page 4-4 displays an example of an information collection overlay.

DEVELOP THE INFORMATION COLLECTION SCHEME OF SUPPORT

4-8. The information collection scheme of support includes the planning and execution of operations and resources to support the Soldiers and units who perform information collection. This support includes fires, movement, protection, and sustainment (logistics, personnel services, health services support, and other sustainment related functions). The staff prepares the initial scheme of support. The operations officer approves the plan and tasks units.

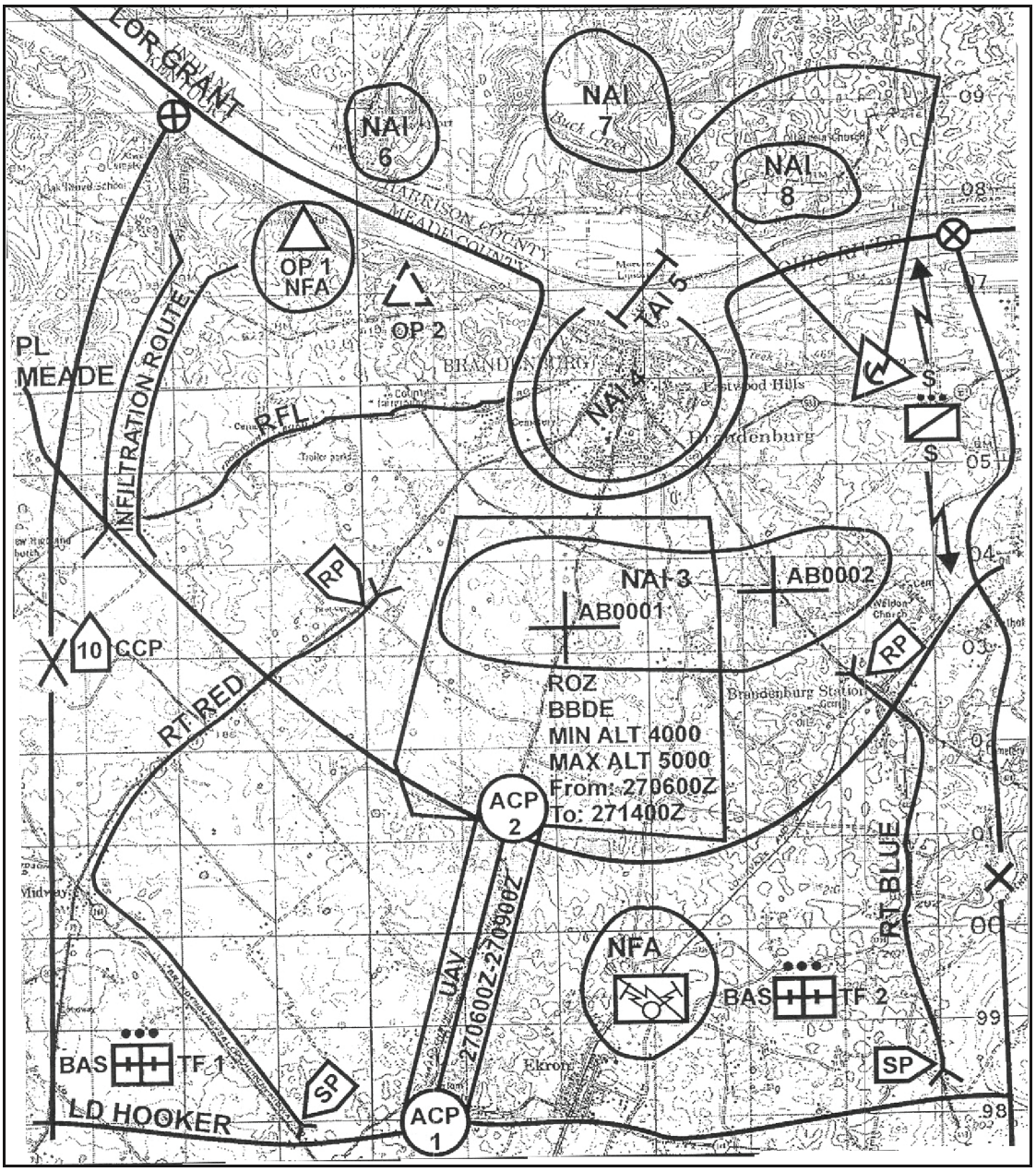


Figure 4-2. Example of an information collection overlay

4-9. The staff publishes the scheme of support in annex L. It addresses as a minimum those items shown in table 4-1.

Table 4-1. Scheme of support

Warfighting Functions	*Items Addressed*
Movement and maneuver	• Provide asset movement routes to and from mission execution location.
Fires	• Call for fire. • Request immediate attack helicopter support. • Request immediate close air support.
Protection	• Air defense.
Sustainment	• Medical evacuation request. • Casualty evacuation request. • Landing zone and pickup zone procedures for rotary-wing aircraft to perform air-ground integration, casualty evacuation, or aerial resupply. • Casualty reporting. • Reconstitution. • Postal and administrative support. • Religious support. • Resupply of classes I, III, and V. • Field maintenance support, recovery, and evacuation of unserviceable equipment including vehicles, collection platforms, and systems.

PROVIDE SUPPORT TO SITE EXPLOITATION

4-10. *Site exploitation* is systematically searching for and collecting information, material, and persons from a designated location and analyzing them to answer information requirements, facilitate subsequent operations, or support criminal prosecution (ATTP 3-90.15). Refer to ATTP 3-90.15 for additional information on site exploitation.

4-11. Site exploitation consists of a related series of activities to exploit personnel, documents, electronic data, and material captured, while neutralizing any threat posed by the items or contents. Units conduct site exploitation using one of two techniques: hasty and deliberate. Commanders chose the technique based on time available and the unit's collection capabilities.

MONITOR OPERATIONS

4-12. Staffs track the progress of the operation against the requirements and the information collection plan. The operation seldom progresses on the timelines assumed during planning and staff war-gaming. The staff watches for changes in tempo that require changes in reporting times, such as latest time information is of value (LTIOV). The intelligence and operations staffs coordinate any changes with all parties concerned, including commanders and appropriate staff sections. Sometimes the staff's assumptions about enemy courses of action (COAs) will not prove entirely correct. Usually this results in a change in requirements as well as adjustments to the timelines. Staffs may initiate abbreviated versions of the intelligence preparation of the battlefield (IPB) and decisionmaking processes to accommodate changes in their assumptions.

CORRELATE REPORTS TO REQUIREMENTS

4-13. Correlating information reporting to the original requirement and evaluating reports is key to effective requirements management. This quality control effort helps the staff ensure timely satisfaction of requirements. Requirements management includes dissemination of reporting and related information to original requesters and other users.

4-14. To correlate reports, the staff tracks which specific collection task originates from which requirement to ensure the original requester and all who need the collected information actually receive it. For

efficiency and timeliness, the staff ensures production tasks are linked to requirements. This allows the staff to determine which requirements have been satisfied and which require additional collection.

4-15. The staff address the following potential challenges:

- Large volumes of information that could inundate the intelligence analysis section. The intelligence staff may have trouble finding the time to correlate each report to a requirement.
- Reports that partially satisfy a number of collection tasks. Other reports may have nothing to do with the collection task.
- Reported information that fails to refer to the original task that drove collection.
- Circular reporting and spam or unnecessary message traffic that causes consternation and wastes valuable time.

SCREEN REPORTS

4-16. The staff screens reports to determine whether the collection task has been satisfied. In addition, the staff screens each report for the following criteria:

- **Relevance.** Does the information actually address the tasked collection task? If not, can the staff use this information to satisfy other requirements?
- **Completeness.** Is essential information missing? (Refer to the original collection task.)
- **Timeliness.** Was the asset reported by the LTIOV established in the original task?
- **Opportunities for cueing.** Can this asset or another asset take advantage of new information to increase the effectiveness and efficiency of the overall information collection effort? If the report suggests an opportunity to cue other assets, intelligence and operations staffs immediately cue them and record any new requirements in the information collection plan.

4-17. Information collection assets do not submit reports that simply state *nothing significant to report*. These reports may convey that collection occurred, but no activity satisfying the information collection task was observed, which may be a significant indicator. *Nothing significant to report* is by no means a reliable indicator of the absence of activity.

PROVIDE FEEDBACK

4-18. The staff provides feedback to all collection assets on their mission effectiveness and to analytic sections on their production. Normally the mission command element of that unit provides this feedback. Feedback reinforces whether collection or production satisfies the original task or request and provides guidance if it does not. Feedback is essential to maintaining information collection effectiveness and alerting leaders of deficiencies to be corrected.

4-19. As the operation continues, the intelligence and operations staffs track the status of each collection task, analyze reporting, and ultimately satisfy requirements. They pay particular attention to assets not producing required results, which may trigger adjustments to the information collection plan. During execution, the staff assesses the value of the information from collection assets as well as develops and refines requirements to satisfy information gaps.

4-20. When reporting satisfies a requirement, the staff relieves the collection assets of further responsibility to collect against information collection tasks related to the satisfied requirement. The operations officer, in coordination with the intelligence staff, provides additional tasks to satisfy emerging requirements. The operations staff notifies—

- Collection assets and their leadership of partially satisfied requirements to continue collection against, of those collection tasks that remain outstanding, and what remains to be done.
- Collection assets of new tasks designed to exploit cueing and other opportunities.

4-21. By monitoring operations, correlating reports to requirements, screening reports, and providing feedback, the staff ensures the most effective employment of collection assets.

UPDATE THE INFORMATION COLLECTION PLAN

4-22. Evaluation of reporting, production, and dissemination identifies updates for the information collection plan. As the current tactical situation changes, staffs adjust the overall information collection plan to synchronize collection tasks, optimizing collection and exploitation capabilities. They constantly update requirements to ensure that information gathering efforts are synchronized with current operations while also supporting future operations planning. As collected information answers requirements, the staff updates the information collection plan.

4-23. The steps in updating the information collection plan are—

- Maintain information collection activities synchronized to operations.
- Cue assets to other collection requirements.
- Eliminate satisfied requirements.
- Develop and add new requirements.
- Re-task assets.
- Transition to the next operation.

4-24. The steps in updating information collection taskings are collaborative efforts by the intelligence and operations staff. Some steps predominately engage the intelligence staff, others the operations staff. Some steps may require coordination with other staff sections, and others may engage the entire operations and intelligence working group.

Maintain Information Collection Activities Synchronized to Operations

4-25. As execution of the commander's plan progresses, the staff refines decision point timeline estimates used when the information is required. The staff stays alert to the need for recommending changes in the information collection plan because of these refinements. As the need for changes arises, the intelligence staff coordinates with the appropriate staff sections to update products required to refine the information collection plan. This may be as simple as updating timelines, or it may require that these products be completely redone.

Cue Assets to Other Collection Requirements

4-26. The intelligence and operations staffs track the status of collection assets, cueing and teaming assets together as appropriate to minimize the chance of casualties. For example, if a Soldier reports the absence of normal activity in a normally active market area, the staff could recommend redirecting an unmanned aircraft system or other surveillance means to monitor the area for a potential threat.

Eliminate Satisfied Requirements

4-27. During its evaluation of the information collection plan, the staff identifies requirements that were satisfied. The staff eliminates satisfied requirements and requirements that are no longer relevant, even if unsatisfied. When a requirement is satisfied or no longer relevant, the intelligence staff eliminates it from the information collection plan and updates any other logs or records.

RE-TASK ASSETS

4-28. The staff may issue orders to re-task assets. This is normally in consultation with the intelligence officer and other staff sections. Re-tasking is assigning an information collection asset with a new task and purpose. It occurs—

- Upon completion of the staff's initial requirement.
- On order, after the LTIOV and having not satisfied the original requirement. (Adjusting the LTIOV may be required.)
- As planned to support a branch or sequel.
- In response to a variance.

DEVELOP AND ADD NEW REQUIREMENTS

4-29. As the operation progresses and the situation develop, commanders generate new requirements. Intelligence staff begins updating the requirements planning tools. The intelligence staff prioritizes new requirements against remaining requirements. The intelligence staff consolidates the new requirements with the existing requirements, reprioritizes the requirements, evaluates resources based upon the consolidated listing and priorities, and makes appropriate recommendations to the commander and operations officer.

TRANSITIONS

4-30. A transition occurs when the commander decides to change focus from one type of military operation to another. Updating information collection tasking may result in a change of focus for several collection assets. As with any other unit, collection assets may require rest and refit—or lead time for employment—to transition from one mission or operation to another effectively.

This page intentionally left blank.

Appendix A

Information Collection Assets

This appendix discusses information collection assets available to Army commanders for the planning and execution of collection activities. This appendix discusses those assets by level, phase, and echelon. Lastly, this chapter discusses the network-enabled information collection.

BACKGROUND

A-1. An information collection capability is any human or automated sensor, asset, or processing, exploitation, and dissemination system that can be directed to collect information that enables better decisionmaking, expands understanding of the operational environment, and supports warfighting functions in decisive action. Factors—a unit's primary mission, typical size area of operations (AO), number of personnel, and communications and network limitations—significantly impact what sensors, platforms, and systems are fielded.

A-2. When a unit requires more robust collection assets to meet its mission, it may request resources and products from higher echelons and adjacent units. During prolonged conflict or joint and multinational operations, the conduct of routine or protracted reconnaissance, security, surveillance, and intelligence operations also impact joint intelligence, surveillance, and reconnaissance (ISR) resource allocation and formalized information collection tasking and requesting procedures.

MONITOR THE TACTICAL PLAN

A-3. Staffs ensure the collection activities remain focused on the commander's critical information requirements (CCIRs). They continuously update staff products and incorporate those products into the running estimates and common operational picture (COP). Lastly, they quickly identify and report threats and decisive points in the AO.

A-4. Paragraphs A-5 through A-8 illustrate collection activities at different levels during different phases of an operation. Strategic, operational, and tactical levels have different tasks to perform during the phases of an operation, but all levels work together to provide commanders the intelligence they need to successfully complete each phase of an operation. Table A-1 provides some examples of information collection assets.

Table A-1. Sample information collection assets

Levels	*Examples of information collection assets*
Strategic	• Defense Human Intelligence Service agents. • Central Intelligence Agency. • Federal Bureau of Investigation. • Defense Intelligence Agency. • National Security Agency.
Operational	• Regionally focused joint information centers. • Theater army's military intelligence brigades. • Army aerial exploitation battalions. • Joint aerial assets.

Table A-1. Sample information collection assets (continued)

Levels	*Examples of information collection assets*
Tactical	• A battlefield surveillance brigade. • Target acquisition radars. • Reconnaissance and cavalry squadrons and troops. • Attack reconnaissance aviation units. • Unmanned aircraft system. • Any Soldier with information to report.

STRATEGIC

A-5. National and theater-level collection assets provide tactical forces updates before and during deployment. Theater-level shaping operations require actionable intelligence including adversary centers of gravity and decision points, as well as the prediction of adversary anti-access measures. Space-based resources are key to supporting situational awareness during deployment and entry phases because they—

- Monitor protection indicators.
- Provide warning of ballistic missile launches threatening aerial and sea ports of debarkation and other threats to arriving forces.
- Provide the communications links to forces en route.
- Provide meteorological information that could affect operations.

OPERATIONAL

A-6. The intelligence staff requests collection support with theater, joint, and national assets. Respective collection managers employ organic means to cover the seams and gaps between units. These means provide the deploying tactical force the most complete portrayal possible of the enemy and potential adversaries, the populace, and the environmental situation upon entry. The operational-level intelligence assets operate from a regional focus center. This regional focus center (located in the crisis area) assumes primary analytical overwatch for the alerted tactical maneuver elements. The theater army's military intelligence brigade (MIB) provides overwatch and functions as both a command post and a research node. The MIB intelligence staff must completely understand the deploying tactical force commanders' intent. The MIB must understand the deploying forces' situation and current mission statuses. In additrion, the MIB requires access to all relevant data and knowledge about what is being planned at higher headquarters and national levels.

TACTICAL

A-7. The entire information collection and analysis effort shifts to provide tailored support to deploying forces in response to their CCIRs. Priority within the brigade combat team (BCT) shifts to planning to deploy and conduct offensive operations to secure a lodgment in the objective areas. The BCT prepares to conduct combat operations upon arrival. The BCT commander understands the situation sufficiently to employ the combat power of the BCT effectively. The BCT's intelligence element collaborates with higher echelons to satisfy CCIRs and provide the context and focus to the information gathered.

A-8. As the unit prepares to fight upon arrival, it synchronizes its information collection activities with division and higher echelon headquarters. Operational-, theater-, and national-level intelligence collection reports are used to develop and continually update the COP.

INFORMATION COLLECTION ASSETS BY PHASE

A-9. Paragraphs A-10 through A-17 illustrate collection activities at different phases of an operation. Units perform different tasks during deployment, entry, and transition. Commanders require certain information assets to complete each phase of an operation successfully.

DEPLOYMENT

A-10. Prior to issuing the execution order, higher tactical echelons and joint, interagency, intergovernmental, and multinational information collection assets support situation development and shaping operations in the objective area. Upon receipt of the execution order and approval of the course of action, the geographic combatant command expands the size and scope of information collection activities. The geographic combatant command is in the area of responsibility with significant collection assets to detect, identify, and track adversary decision points and centers of gravity. Information collected by the geographic combatant command is immediately available to the tactical echelon, through the network, to continuously update the COP and intelligence running estimate. Combat assessments of lethal and nonlethal effects drive decisions regarding the deployment timing, locations, and actions on arrival.

ENTRY

A-11. During the entry phase, deploying units are particularly vulnerable to enemy actions. Effective intelligence reduces that vulnerability. Tactical forces use the information that their higher headquarters, and theater- and national-level assets provide to maintain situational awareness and refine plans. The intelligence running estimate provides the commander predictive intelligence to anticipate adversary actions. Updates en route provide continuing information about the situation, the threat, and the environment. They allow the commander to adjust the plan prior to arrival in response to changes in the AO or threat actions.

A-12. Forces conduct tactical assault upon arrival as necessary. They conduct continuous reconnaissance, intelligence, and security operations. As the buildup of forces continues, the tactical forces strives to reduce dependence on higher echelon resources while becoming more reliant upon organic assets. As organic and supporting assets arrive into the theater, commanders immediately employ them to support tactical-level situational awareness. In addition, operational and strategic resources still contribute to the COP. Arriving units and staffs establish liaisons with units already in the AO.

A-13. As the BCT enters the AO, it continues to rely primarily on national-, theater-, and higher-tactical echelon information collectors until its organic assets become fully available. The intelligence overwatch support section provides context and focus to information gathered by theater and national collectors. Appropriate to echelon, the S-2 and military intelligence elements focus and put into context the information collected, analyzed, and disseminated by higher echelons. The different echelons integrate raw and analyzed information to answer their commander's priority intelligence requirements and tailor reports to specific mission requirements. In the early phases of entry operations, focused, detailed collection and analysis of the BCT's operational environment remains a primary responsibility of its higher headquarters. The BCT becomes responsible for providing its own situational awareness of the operational environment when assigned its operational area.

A-14. Once on the ground, the BCT immediately begins to deploy its information collection reconnaissance units, sensors, and collection systems. The tactical echelon expands its sensing and collecting capabilities until the entire force is on the ground and achieves maximum situational awareness. During entry operations, echelons above brigade continue to provide collection support and serve to complement the BCT's organic reconnaissance units and assets. Once the BCT deploys, strategic and operational echelons continue to complement the BCT's organic assets and focus on those areas outside the sensing range and capability of the maneuver elements. Sensors covering the noncontiguous AO provide early warning and cueing of the BCT's reconnaissance squadron and sensors.

TRANSITION

A-15. Information collection requirements during the transition phase shift from one operation to another. regardless, the combatant commander remains aware that major combat operations and stability operations may occur simultaneously.

A-16. Commanders may reprioritize strategic and operational echelon information collection assets. The BCT's collection assets become a resource for division headquarters and higher echelon units for their information needs. The AO generally involves other nations. Often, multinational information collection focus increases along with the involvement of nongovernmental organizations. There may be multinational collection entities operating in each brigade's AO with no formal command relationship. Commanders

must effectively integrate these capabilities into collection plans and processes to prevent unnecessary redundancy and maximize information sharing.

A-17. During this phase, the combatant commander and all subordinate echelons redefine adversary centers of gravity and focus information collection activities on political, social, economic, information, and criminal activities that pose a threat to friendly forces and the stability of the AO. Collaboration and interaction with all friendly elements in the AO is essential. Predictive assessments for the remaining threat forces or illicit factions contribute to future operational planning and force disposition.

INFORMATION COLLECTION ASSETS BY ECHELON

A-18. Paragraphs A-19 through A-41 illustrate collection activities in different echelons of an operation. Different units perform different tasks at each echelon. Commanders at different echolons require certain information assets to complete each phase of an operation successfully.

SPECIAL OPERATIONS FORCES

A-19. Special operations forces may possess a high degree of cultural awareness due to their extensive training, experience, and regional orientation. Some members of every unit will communicate in the local language. Civil affairs units are also sources of useful information; however, commanders recognize that the legitimacy of civil affairs activities often hinges on whether the local population perceives those forces are collecting information. Civil affairs personnel may be tasked to collect information en route to or returning from a meeting with host-nation personnel but may not be tasked to collect information during the meeting. Some special operations forces make ideal collection assets during stability operations because they can interact with the local population.

A-20. Historically, special operations forces have operated independently from conventional forces, although both plan and execute operations within a synchronized framework to support the joint force commander's overall plan. Recent operations have produced situations in which conventional forces and special operations forces operated in the same operational area simultaneously, requiring close coordination. Conventional forces and special operations forces can complement one another in a number of areas, including information collection activities. Special operations forces can provide conventional forces with special reconnaissance capabilities, positive identification of specific targets, target marking and terminal guidance, battle damage assessment, information on indigenous forces, and combat weather support. Conventional forces can provide special operations forces with robust fire support, multiple attack resource options, lethal and nonlethal fires, and other resources available to heavier forces.

A-21. Key lessons for successfully integrating conventional forces with special operations forces include the following:

- Establish personal relationships (rapport).
- Train integrated forces early and often, before conducting tactical operations.
- Clearly define and articulate command relationships.
- Fully integrate planning and intelligence efforts to alleviate misunderstandings.
- Understand the strengths and limitations of each force, and use this knowledge to advantage.

MILITARY INTELLIGENCE BRIGADE

A-22. The theater army's MIB provides intelligence support, including support for information collection activities. The MIB supports the theater army, other Army operational-level commands in the area of responsibility, and combatant, joint, or multinational commands.

A-23. The MIB consists of the—

- Operations battalion.
- Forward collection battalion (counterintelligence and human intelligence).
- Forward collection battalion (signals intelligence).
- Strategic signals intelligence battalion.
- Theater support battalion.

A-24. The MIB performs intelligence operations, all-source intelligence analysis, intelligence production, intelligence collection management, and intelligence dissemination in support of the theater army. It provides dedicated long-term, continuous support to the geographic combatant commander or subunified commander for that commander's theater security cooperation plan and small-scale contingencies. It also provides in-theater intelligence support during major combat operations.

A-25. The MIB provides the theater army commander with dedicated intelligence capabilities for all intelligence disciplines. It has robust counterintelligence and human intelligence capabilities with interrogation and exploitation potential. Each MIB also has dedicated imagery intelligence analysts, and most have imagery intelligence collection capabilities. The MIB also has measurement and signature intelligence capabilities.

BATTLEFIELD SURVEILLANCE BRIGADE

A-26. The battlefield surveillance brigade (BFSB) conducts reconnaissance and security to collect information to support operations at echelons-above-brigade level. It helps develop the COP, and it enhances commanders' decisionmaking. Table A-2 identifies BFSB collection assets. The BFSB fills two roles in division-level and higher operations. It augments BCTs and supporting brigades to enhance their abilities to accomplish their missions. It also executes their portion of the information collection plan—

- In that portion of the AO not assigned to a subordinate unit (unassigned area).
- In an AO assigned to it by the supported unit.
- In an area that has characteristics of both types (unassigned area and assigned AO).

Table A-2. Battlefield surveillance brigade information collection assets

Warfighting Function	*Organization*	*Capability*
Movement and Maneuver	Reconnaissance Squadron	Conduct area, zone, or route reconnaissance.
Intelligence	Military Intelligence Battalion Intelligence Operations	Provide signals intercept and signal emitter location data that use 12–person multifunction teams that combine signals intelligence, human intelligence, and counterintelligence capabilities and supporting operational management teams.
		Provide counterintelligence and human intelligence teams and supporting operational management teams that provide general support to division or corps collection requirements.
		Provide counterintelligence and human intelligence teams that provide general support to augment capabilities of a maneuver brigade.
		Provide counterintelligence or human intelligence capability to a functional brigade.
		Provide aerial reconnaissance and surveillance capability. Provide battle damage assessment capability.
	Headquarters and Headquarters Company	Support development of brigade common operational picture, targeting, intelligence preparation of the battlefield, and analysis of reporting across all the warfighting functions and development of intelligence products.
		Provide geospatial intelligence.
		Receive, process, and display near-real time information from nonorganic airborne sensors, including Joint Surveillance Target Attack Radar System.
		Provide additional information collected during conduct of primary missions.

Table A-2. Battlefield surveillance brigade information collection assets (continued)

Warfighting Function	*Organization*	*Capability*
Sustainment	Brigade Support Company	Provide information and intelligence developed and disseminated through mission command systems (such as command post of the future).
Mission Command	Brigade Headquarters and Headquarters Company	Provide additional information collected during conduct of primary missions.
		Provide signal retransmission teams that can provide additional observation posts.

A-27. Although assets above division level can fulfill many intelligence requirements, they may not answer all of them. Often, higher-level operational needs take precedence and cause assets at these levels to focus on the next higher echelon's CCIRs. In some cases, higher-level assets may not provide the level of detail or timeliness the BFSB's supported command requires. The BFSB bridges the gap between the tactical reconnaissance and security executed at brigade level and the operational and strategic reconnaissance executed at levels above the division.

A-28. In its other role, the BFSB augments other brigades by providing counterintelligence, human intelligence, signals intelligence, and unmanned aircraft system. In some situations, augmentation includes elements of the reconnaissance squadron. The BFSB provides a means for the supported commander to weight the decisive operation or the main effort and to provide other brigades with assets, capabilities, or the increased capacity required for a specific mission or operation. Refer to FM 3-55.1 for additional information on BFSB operations.

COMBAT AVIATION BRIGADE

A-29. The combat aviation brigade (CAB) accomplishes reconnaissance and surveillance with its attack reconnaissance battalions and (when fielded) one unmanned aircraft system company. The heavy, medium, light, and expeditionary CABs have similar organization, varying only in the type and number of attack reconnaissance battalions. Heavy and medium CABS have more robust firepower capabilities than light and expeditionary CABs.

A-30. The CAB commander is the higher commander's senior advisor for employment of aviation assets. The CAB commander and staff are the primary integrators of manned aircraft and unmanned aircraft system operations.

A-31. The unmanned aircraft system company of the CAB, when fully fielded, deploys a one system ground control station (known as OSGCS) to the BFSB and fires brigade as required for mission planning and execution. Based on higher echelon requirements, the BFSB and fires brigade control the unmanned aircraft for reconnaissance and surveillance operations. Typically, the CAB launches the aircraft and turns control over to the one system ground control station operators. The one system ground control station locates where it can best control the aircraft and allows for the dissemination of collected information.

FIRES BRIGADE

A-32. Normally fires brigades are assigned, attached, or placed under the operational control of a division headquarters. However, they may be attached or placed operational control to a corps headquarters, a joint forces land component command, a joint task force (JTF), or another Service or functional component. Fire brigades are task organized to accomplish missions.

A-33. Fires brigades have the ability to reconnoiter, detect, and attack targets and confirm the effectiveness of fires. Fire brigades have robust communications and control systems that facilitate the efficient application of fires. They have the necessary fire support and targeting structure to effectively execute the entire decide, detect, deliver, and assess targeting process for their assigned tasks.

A-34. The fires brigade and each of its subordinate organizations can be augmented (task-organized) as required. For instance, executing a strike may require placing additional collection assets capabilities under operational control of the fires brigade headquarters. Alternatively, the BFSB can retain control of its organic assets and provide the information and desired effects to the fires brigade.

BRIGADE COMBAT TEAM

A-35. The BCT is the Army's largest defined combined arms organization and the Army's primary close combat force. For combat operations, the combatant commander builds the ground component of a JTF around the BCT. The BCT includes units and capabilities from every warfighting function; it is task-organized to meet specific mission requirements. Some capabilities, such as unmanned aircraft system platoons, are assets whose sole purpose is support to information collection activities. However, commanders consider some information collection assets that are not immediately obvious when planning reconnaissance and surveillance tasks and missions to answer CCIRs fully. Tables A-3, A-4, and A-5 show each BCT's information collection assets.

Table A-3. Infantry brigade combat team information collection assets

Warfighting Function	*Organization*	*Capability*
Movement and Maneuver	Reconnaissance Squadron	Conduct Soldier sensor missions, as needed, to satisfy requirements.
		Conduct security operations and surveillance tasks as required.
		Conduct area, zone, or route reconnaissance.
	Infantry Battalion	Conduct Soldier sensor missions, as needed, to satisfy requirements, including tactical questioning.
		Provide scout platoon capability for real-time detection, recognition, and identification of distant target locations.
Intelligence	Brigade Special Troops Battalion Military Intelligence Company	Conduct intelligence operations military source operations, document exploitation, interrogation and debriefing, and counterintelligence operations (such as preliminary investigations).
		Support development of brigade common operational picture, targeting, intelligence preparation of the battlefield, analysis, reconnaissance and surveillance reporting across all the warfighting functions, and intelligence products.
		Provide organic aerial reconnaissance and surveillance and battle damage assessment capability.
Fires	Fires Battalion	Conduct Soldier sensor missions, as needed, to satisfy information requirements.
		Detect artillery and mortar fires, establish long-duration observation posts.
Sustainment	Brigade Support Battalion	Provide additional information collected during conduct of primary missions.
		Provide information on types of wounds or injuries, diseases, and health and welfare of population that refines understanding of operational environment or enemy capabilities.

Table A-3. Infantry brigade combat team information collection assets (continued)

Warfighting Function	*Organization*	*Capability*
Protection	Brigade Special Troops Battalion	Provide information collected during internment and resettlement, area security, and maneuver mobility support operations.
	Engineer Company	Conduct Soldier sensor missions, as needed, to satisfy information requirements.
		Provide terrain teams and reconnaissance teams that identify key terrain, obstacle intelligence, and infrastructure information.
Mission Command	Brigade Special Troops Battalion	Provide information and intelligence developed and disseminated through mission command systems.
		Conduct route, area, and zone CBRN reconnaissance to detect, identify, mark, report, and sample for presence of CBRN hazards.

CBRN chemical, biological, radiological, and nuclear

Table A-4. Heavy brigade combat team information collection assets

Warfighting function	*Organization*	*Capability*
Movement and Maneuver	Reconnaissance Squadron	Conduct security operations and surveillance tasks to include Soldier sensor missions, as needed, to satisfy information requirements.
		Conduct area, zone, or route reconnaissance.
	Combined Arms Battalion	Conduct Soldier sensor missions, as needed, to satisfy information requirements, including tactical questioning.
		Provide scout platoon capability for real-time detection, recognition, and identification of distant target locations.
Intelligence	Brigade Special Troops Battalion Military Intelligence Company	Conduct intelligence operations source operations, document exploitation, interrogation and debriefing, and counterintelligence operations (such as preliminary investigations).
		Provide organic aerial reconnaissance and surveillance, and battle damage assessment capability.
		Receive, process, and display near real-time information from non-organic airborne sensors.
Fires	Fires Battalion	Conduct Soldier sensor missions, as needed, to satisfy information requirements.
		Detect artillery and mortar fires.
		Establish long-duration observation posts.

Table A-4. Heavy brigade combat team information collection assets (continued)

Warfighting function	*Organization*	*Capability*
Sustainment	Brigade Support Battalion	Provide additional information collected during conduct of primary missions.
		Provide information on types of wounds or injuries, diseases, and health and welfare of population that refines understanding of operational environment or enemy capabilities.
		Provide additional information collected during conduct of primary missions.
Protection	Brigade Special Troops Battalion	Provide information collected during internment and resettlement, area security, and maneuver mobility support operations.
		Conduct Soldier sensor missions, as needed, to satisfy information requirements.
		Provide terrain teams and reconnaissance teams identify key terrain, obstacle intelligence, and infrastructure information.
		Conduct route, area, and zone CBRN reconnaissance to detect, identify, mark, report, and sample for presence of CBRN hazards.
Mission Command	Brigade Special Troops Battalion	Provide additional information collected during conduct of primary missions.
		Provide signal retransmission teams that can provide additional observation post capability.

CBRN chemical, biological, radiological, and nuclear

Table A-5. Stryker brigade combat team information collection assets

Warfighting function	*Organization*	*Capability*
Movement and Maneuver	Reconnaissance Squadron	Conduct security operations, surveillance tasks, and tactical questioning to include Soldier sensor missions, as needed, to satisfy information requirements.
		Conduct area, zone, or route reconnaissance.
		Provide organic unmanned aircraft system platoon to conduct aerial reconnaissance and surveillance and battle damage assessment.
		Provide Prophet Signal Intercept System to provide signals intercept and signal emitter location data.
		Provide CBRN platoon to conduct route, area, and zone CBRN reconnaissance to detect, identify, mark, report, and sample for presence of CBRN hazards.
		Provide unattended ground sensors platoon for increased unmanned monitoring of terrain.
	Stryker Battalions	Conduct Soldier sensor missions, as needed, to satisfy information requirements, including tactical questioning.

Table A-5. Stryker brigade combat team information collection assets (continued)

Warfighting function	*Organization*	*Capability*
Intelligence	Military Intelligence Company	Conduct intelligence operations military source operations, document exploitation, interrogation and debriefing, and counterintelligence operations (such as preliminary investigations).
		Support development of brigade common operational picture, targeting, IPB, analysis of reporting across all the warfighting functions and development of intelligence products.
		Receive, process, display near real time information from non-organic airborne sensors.
Fires	Fires Battalion	Conduct Soldier sensor missions, as needed, to satisfy information collection requirements.
		Detect artillery and mortar fires, establish long duration observation posts.
Sustainment	Brigade Support Battalion	Provide additional information collected during conduct of primary missions.
		Provide information on types of wounds or injuries, diseases, health and welfare of population that refines understanding of operational environment or enemy capabilities.
Protection	Military Police Platoon	Provide information collected during internment and resettlement, area security, and maneuver mobility support operations
		Conduct route, area, and zone CBRN reconnaissance to detect, identify, mark, report, and sample for presence of CBRN hazards.
	Engineer Company	Conduct Soldier sensor missions, as needed, to satisfy information requirements.
		Provide terrain teams and reconnaissance teams identify key terrain, obstacle Intelligence, and infrastructure information.
Mission Command	Brigade Support Battalion	Provide combat information and intelligence developed and disseminated through mission command systems (such as command post of the future).
		Provide additional information collected during conduct of primary missions.
		Provide signal retransmission teams that can provide additional observation post capabilities.

CBRN chemical, biological, radiological, and nuclear

A-36. The BCT conducts reconnaissance, security, and intelligence operations. The BCT commander gains situational understanding by conducting integrated reconnaissance and security operations that answer the CCIRs. Typically the BCT assigns short-term reconnaissance, intelligence, and security tasks to its reconnaissance squadron; sustained missions usually require participation from the entire BCT. When the BCT assigns reconnaissance or security tasks to a subordinate element, the BCT task-organizes the subordinate element and allocates to it the resources necessary to meet its mission requirements. The BCT may allocate tank and mechanized infantry units, reconnaissance units, engineer elements, attack helicopter units, close air support priority, and intelligence systems to perform reconnaissance or security tasks. (Refer to FM 3-90.6, for additional information.)

A-37. The BCT operations section—

- Is responsible for development of the information collection plan.
- Tasks subordinate units.
- Ensures the information collection plan supports the overall scheme of maneuver.

A-38. The BCT intelligence section—

- Assesses information received to derive intelligence.
- Performs requirements planning and assessment of information collection.

BRIGADE COMBAT TEAM RECONNAISSANCE SQUADRON

A-39. The reconnaissance squadrons of the heavy brigade combat team, infantry brigade combat team, and Stryker brigade combat team are organized to accomplish reconnaissance and security missions throughout the BCT's AO. By leveraging information technology with air and ground reconnaissance capabilities in complex terrain, the reconnaissance squadron helps develop the situation by focusing on all categories of threats in a designated AO. This allows the BCT commander to maintain battlefield mobility and agility while choosing the time, place, and method to confront the enemy. The squadron commander has various tools to conduct reconnaissance and security missions across the spectrum of conflict. The squadron commander can task-organize to optimize complementary effects while maximizing support throughout the BCT's AO. (Refer to FM 3-20.96, for additional information.)

A-40. Most Army information collection assets have been assigned at the brigade level to ensure intelligence and information is readily available to commanders in increasingly decentralized AOs. Corps, division, and BCTs often require information from the same assets. The requirement for layering information collection capabilities—some with theater-level applications—and the often long or personnel-intensive logistics, processing, exploitation, and dissemination of those assets require management at echelons above brigade.

A-41. Information collection capabilities are rapidly evolving to meet new challenges of the current and future area of operations and provide the flexibility required to provide information across the spectrum of operations. To act decisively, commanders and staffs identify, understand, and integrate (sometimes creatively) the multitude of information collection capabilities found at every echelon across the warfighting functions.

NETWORK-ENABLED INFORMATION COLLECTION

A-42. The networking of all joint force elements creates capabilities for unparalleled information sharing and collaboration and a greater unity of effort via synchronization and integration of force elements at the lowest echelons. Distributed Common Ground System (Army) (DCGS-A) provides a network-centric, enterprise intelligence, weather, geospatial engineering, and space operations capabilities to maneuver, maneuver support, and sustainment organizations at all echelons from battalion to joint task forces. The DCGS-A is being implemented to integrate intelligence tasking, collection, processing, and dissemination capabilities across the Army and joint community. The purpose of DCGS-A is to unite the different systems across the global information network. DCGS-A is the Army's primary system for—

- Receipt of and processing select information collection asset data.
- Control of select Army sensor systems.
- Fusion of sensor data and information
- Direction and distribution of relevant threat, terrain, weather, and civil considerations products and information.
- Facilitation of friendly information and reporting.

This page intentionally left blank.

Appendix B

The Information Collection Annex to the Operation Order

This appendix provides instructions for preparing Annex L (Information Collection) in Army plans and orders. It provides a format for the annex that can be modified to meet the requirements of the base order and operations, and an example information collection plan. Refer to ATTP 5-0.1 for additional guidance on formatting and procedures.

ANNEX L (INFORMATION COLLECTION)

B-1. The information collection annex clearly describes how information collection activities support the offensive, defensive, and stability or defense support of civil authorities operations throughout the conduct of the operations described in the base order. See figure B-1. It synchronizes activities in time, space, and purpose to achieve objectives and accomplish the commander's intent for reconnaissance, surveillance, and intelligence operations (including military intelligence disciplines).

[CLASSIFICATION]

Place the classification at the top and bottom of every page of the Information Collection Annex. Place the classification marking (TS), (S), I, or (U) at the front of each paragraph and subparagraph in parentheses. Refer to AR 380-5 for classification and release marking instructions.

ANNEX L (Information Collection) TO OPERATION ORDER # [number] [(code name)]—[issuing headquarters] [(classification of title)]

1. (U) Situation.

a. (U) Area of Interest. *No change to Annex B (Intelligence) or appendix 1 to annex C (Operations).*

b. (U) Area of Operations. *No change to Appendix 2 (Operation Overlay) to Annex C (Operations).*

(1) (U) Terrain. *Describe the aspects of terrain that impact operations. Refer to Annex B (Intelligence) as required.*

(2) (U) Weather. *Describe the aspects of weather that impact operations. Refer to Annex B (Intelligence) as required.*

c. (U) Enemy Forces. *No change to Annex B (Intelligence).*

d. (U) Friendly Forces. *No change to base order, Annex A (Task Organization) and Annex C (Operations).*

[page number]

[CLASSIFICATION]

Figure B-1. Example Annex L (Information Collection) annotated format

[CLASSIFICATION]

ANNEX L (INFORMATION COLLECTION) TO OPERATION ORDER # [number] [(code name)]—[issuing headquarters] [(classification of title)]

e. (U) Interagency, Intergovernmental, and Nongovernmental Organizations. *Identify and describe other organizations in the area of operations that may impact the conduct of operations or implementation of information collection-specific equipment and tactics. Refer to Annex V (Interagency Coordination) as required.*

f. (U) Civil Considerations. *Describe the critical aspects of the civil situation that impact information collection activities. Refer to Appendix 1 (Intelligence Estimate) to Annex B (Intelligence) and Annex K (Civil Affairs Operations) as required.*

g. (U) Attachments and Detachments. *If pertinent, list units or assets attached to or detached from the issuing headquarters. State when each attachment or detachment is effective (for example, on order, on commitment of the reserve) if different from the effective time of the base order. Do not repeat information already listed in Annex A (Task Organization).*

h. (U) Assumptions. *List any information collection-specific assumptions that support the annex development.*

2. (U) Mission. *State the mission in support of the operation—a short description of the who, what (task), when, where, and why (purpose) that clearly indicates the action to be taken and the reason for doing so.*

3. (U) Execution.

a. (U) Concept of Operations. *This is a statement of the overall information collection objective. Describe how the tasks or missions of reconnaissance, surveillance, security, intelligence operations, and so forth support the commander's intent and the maneuver plan. Direct the manner in which each element of the force cooperates to accomplish the key information collection tasks and ties that to support of the operation with task and purpose statement. Must describe, at minimum, the overall scheme of maneuver and concept of fires. It should refer to Appendix 1 (Information Collection Plan) to Annex L (Information Collection).The following subparagraphs are examples. Omit what is unnecessary for brevity.*

(1) (U) Movement and Maneuver. *Provide the scheme of movement and maneuver for collection assets and any other unit given a key information collection task, in accordance with the concept of operations in the base order (paragraph 3b) and Annex C (Operations). Describe the employment of information collection assets in relation to the rest of the force and state the method forces will enter the area of operations (AO).*

(2) (U) Intelligence. *Describe the intelligence concept for supporting information collection. Refer to Annex B (Intelligence) as required.*

(3) (U) Fires. *Describe the concept of fires in support of information collection. Identify which information collection assets have priority of fires and the coordinating purpose of, priorities for, allocation of, and restrictions on fire support and fire support coordinating measures. Refer to Annex D (Fires) as required.*

(4) (U) Protection. *Describe protection support to information collection. Refer to Annex F (Protection) as required.*

[page number]

[CLASSIFICATION]

Figure B-1. Example Annex L (Information Collection) annotated format (continued)

[CLASSIFICATION]

ANNEX L (INFORMATION COLLECTION) TO OPERATION ORDER # [number] [(code name)]—[issuing headquarters] [(classification of title)]

(5) (U) Engineer. *Describe engineer support, if applicable, to information collection. Identify priority of mobility and survivability assets. Refer to Annex G (Engineer) as required.*

(6) (U) Sustainment. *Describe sustainment support to information collection as required. Refer to Annex F (Sustainment).*

(7) (U) Signal. *Describe signal support to information collection as required. Refer to Annex H (Signal).*

(8) (U) Inform and influence. *State overall concept for synchronizing information collection with inform and influence operations. Refer to Annex J (Inform and Influence Activities).*

(9) (U) Assessment. *If required, describe the priorities for assessment for the information collection plan and identify the measures of effectiveness used to assess end state conditions and objectives. Refer to Annex M (Assessment) as required.*

b. (U) Tasks to Subordinate Units. *State the information collection task assigned to each unit not identified in the base order. (Refer to Appendix 1 (Information Collection Plan) to Annex L (Information Collection) as needed.)*

(1) (U) Information Collection Support Tasks for Maneuver Units.

(a) (U) Tasks to Maneuver Unit 1.

(b) (U) Tasks to Maneuver Unit 2.

(c) (U) Tasks to Maneuver Unit 3.

(2) (U) Information Collection Support Tasks for Support Units. *Direct units to observe and report in accordance with Appendix 1 (Information Collection Plan) to Annex L (Information Collection). Consider all options such as Naval gunfire support.*

(a) (U) Military Intelligence. *Refer to Annex B (Intelligence).*

(b) (U) Engineer. *Refer to Annex G (Engineer).*

(c) (U) Fires. *Refer to Annex D (Fires).*

(d) (U) Signal. *Refer to Annex H (Signal).*

(e) (U) Sustainment. *Refer to Annex F (Sustainment).*

(f) (U) Protection. *Refer to Annex E (Protection).*

[page number]

[CLASSIFICATION]

Figure B-1. Example Annex L (Information Collection) annotated format (continued)

[CLASSIFICATION]

ANNEX L (INFORMATION COLLECTION) TO OPERATION ORDER # [number] [(code name)]—[issuing headquarters] [(classification of title)]

(g) (U) Public Affairs. *Refer to Appendix 1 (Public Affairs) to Annex J (Inform and Influence Activities).*

(h) (U) Civil Affairs. *Refer to Annex K (Civil Affairs Activities).*

c. (U) Coordinating Instructions. *List only instructions applicable or not covered in unit standard operating procedures (SOPs).*

(1) (U) Time or Condition When the Plan Becomes Effective.

(2) (U) Priority Intelligence Requirements. *List priority intelligence requirements (PIRs) here, the information collection tasks associated with them, and the latest time information is of value for each PIR.*

(3) (U) Essential Elements of Friendly Information. *List essential elements of friendly information (EEFI) here.*

(4) (U) Fire Support Coordinating Measures. *List fire support coordinating or control measures. Establish no fire areas.*

(5) (U) Intelligence Handover Lines with Adjacent Units. *Identify handover guidance and parameters; refer to necessary graphics or attachments as required.*

(6) (U) Limits of Advance, Limits of Reconnaissance, and Quick Reaction Force Response Instructions. *Identify as required, referencing graphical depictions in attachments or instructions as needed.*

(7) (U) Airspace Coordinating Measures. *List airspace control measures.*

(8) (U) Intelligence Coordination Measures. *List information such as restrictions on international borders or other limitations and the coordination or special instructions that apply. Identify what unit is responsible for coordinating information collection activities in relation to the AO.*

(9) (U) Rules of Engagement. *Refer to Appendix 11 (Rules of Engagement) to Annex C (Operations) as required.*

(10) (U) Risk Reduction Control Measures. *State any reconnaissance, surveillance, and security-specific guidance such as fratricide prevention measures not included in SOPs, referring to annex F (Protection) as required.*

(11) (U) Environmental Considerations. *Refer to Appendix 5 (Environmental Considerations) to Annex G (Engineer) as required.*

(12) (U) Other Coordinating Instructions. *List only instructions applicable to two or more subordinate units not covered in the base plan or order.*

4. (U) Sustainment. *Describe any sustainment requirements, subparagraphs may include:*

a. (U) Logistics. *Refer to Appendix 1 (Logistics) to Annex F (Sustainment) as required.*

b. (U) Personnel. *Refer to Appendix 2 (Personnel Services Support) to Annex F (Sustainment) as required.*

[page number]

[CLASSIFICATION]

Figure B-1. Example Annex L (Information Collection) annotated format (continued)

[CLASSIFICATION]

ANNEX L (INFORMATION COLLECTION) TO OPERATION ORDER # [number] [(code name)]—[issuing headquarters] [(classification of title)]

c. (U) Health Services Support. *Refer to Appendix 3 (Army Health System Support) to Annex F (Sustainment) as required. This includes Medical Evacuation*.

5. (U) Command and Control.

a. (U) Command. No change.

b. (U) Control. No change.

c. (U) Signal.

ACKNOWLEDGE: *Include instructions for the acknowledgement of the OPLAN or OPORD by addressees. The word "acknowledge" may suffice. Refer to the message reference number if necessary. Acknowledgement of a plan or order means that it has been received and understood.*

[Authenticator's name]
[Authenticator's position]

ATTACHMENTS: *List lower-level attachment (appendixes, tabs, and exhibits).*

Appendix 1 – Information Collection Plan

Appendix 2 – Information Collection Overlay

DISTRIBUTION: (if distributed separately from the base order).

[page number]

[CLASSIFICATION]

Figure B-1. Example Annex L (Information Collection) annotated format (continued)

THE INFORMATION COLLECTION PLAN

B-2. Figure B-2 (page B-6) is an example of an ~~i~~nformation collection plan. This plan can also be accompanied by a graphical depiction of the plan, called the ~~i~~nformation collection overlay. Units may develop and adjust the format of their information collection plan to meet the requirements of the mission and clearly depict information collection in terms of time and space for execution. The information collection plan must contain—

- Information about the area of operations for the collection assets.
- Reporting guidance.
- Identified named area of interest or targeted area of interest.
- The task for each asset.
- The time the asset is to collect or that information is relevant.
- References to any passage of lines or fire support and airspace control measures that are not standard operating procedures.

Unit: **INFORMATION COLLECTION PLAN** Period Covered From: To:

PIR / IR	Indicators (Analysis of Intelligence Requirements)	Avenue of Approach Coordinates: From_____ To_____ Mobility Corridor No From_____ To_____ NAI	Time NET	Time NLT	Specific Information Or Requests	Assets To Be Employed: AN/PPS-5D	1st BN Scouts	2nd BN Scouts	3rd BN Scouts	Prophet	Shadow	CI				Hour and Destination of Reports	Remarks
1.		1														AS PER SOP	
		2														AS PER SOP	
2.		3														AS PER SOP	

SAMPLE

Figure B-2. Sample information collection plan

Appendix C

Joint Intelligence, Surveillance, and Reconnaissance

The Army conducts operations as part of a joint force. This appendix examines joint intelligence, surveillance, and reconnaissance activities as part of unified action. It discusses the joint intelligence, surveillance, and reconnaissance doctrine, resources, planning systems, considerations, and organizations.

UNIFIED ACTION

C-1. *Unified action* is the synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort (JP 1). It involves the application of all instruments of national power, including actions of other government agencies and multinational military and nonmilitary organizations. Combatant as well as subordinate commanders use unified action to integrate and synchronize their operations directly with the activities and operations of other military forces and nonmilitary organizations in their area of operations.

C-2. Army forces operating in an operational area are exposed to many non-U.S. Army participants. Multinational formations, host-nation forces, other government agencies, contractors, and nongovernmental organizations are all found in the operational area. Each participant has distinct characteristics, vocabulary, and culture, and all can contribute to situational understanding. Commanders, Soldiers, and all who seek to gather information have much to gain by being able to work with and leverage the capabilities of these entities. The Army expands the joint intelligence, surveillance, and reconnaissance (ISR) doctrine (contained in JP 2-01) by defining information collection as an activity that focuses on answering the commander's critical information requirements (see paragraph 1-3).

CONCEPTS OF JOINT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE

C-3. Joint ISR is an intelligence function, and its collections systems are intelligence assets and resources under the control of the J-2. This is different from Army information collection. Joint ISR does not include reconnaissance and surveillance units. Joint usage of reconnaissance and surveillance refers to the missions conducted by predominately airborne assets. Two key concepts impact how Army conducts joint ISR in the joint operations area: integration and interdependence.

INTEGRATION

C-4. The Army uses integration to extend the principle of combined arms to operations conducted by two or more Service components. The combination of diverse joint force capabilities generates combat power more potent than the sum of its parts. This integration does not require joint command at all echelons; however, it does require joint interoperability at all echelons.

INTERDEPENDENCE

C-5. The Army uses interdependence to govern joint operations and impact joint ISR activities. This interdependence is the purposeful reliance by one Service's forces on another Service's capabilities to maximize the complementary and reinforcing effects of both. Army forces operate as part of an interdependent joint force. Areas of interdependence that directly enhance Army information collection activities include—

- **Joint command and control**. Integrated capabilities that—
  - Gain information superiority through improved, fully synchronized, integrated ISR, knowledge management, and information management.
  - Share a common operational picture.
  - Improve the ability of joint force and Service component commanders to conduct operations.
- **Joint intelligence**. Integrated processes that—
  - Reduce unnecessary redundancies in collection asset tasking through integrated ISR.
  - Increase processing and analytic capability.
  - Facilitate collaborative analysis.
  - Provide global intelligence production and dissemination.
  - Provide intelligence products that enhance situational understanding by describing and assessing the operational environment.

C-6. Other Services also rely on Army forces to complement their capabilities, including intelligence support, detainee and prisoner of war operations, and others.

JOINT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE DOCTRINE

C-7. JP 2-01 governs joint ISR doctrine. The joint force headquarters in the theater of operations govern operational policies and procedures specific to that theater. Army personnel serving in joint commands must be knowledgeable of joint doctrine for ISR. Army personnel involved in joint operations must understand the joint operation planning process. The joint operation planning process focuses on the interaction between an organization's commander and staff and the commanders and staffs of the next higher and lower commands. The joint operation planning process continues throughout an operation.

C-8. Army and joint doctrine share many of the same terms and definitions; however, commanders and staffs must understand their use and differences. Examples include joint use of ISR and the Army's use of information collection, joint operations area instead of area of operations, and the joint operation planning process instead of the military decisionmaking process.

JOINT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE RESOURCES

C-9. When organic collection assets or other Army resources are not sufficient, the intelligence officer and operations officer need to understand how to access joint resources. The exact procedures vary in each operational theater. The joint force collection manager reviews all requests for joint ISR resources based on validated needs as established by the command's formal intelligence requirements.

C-10. One type of resource is a request for information. Subordinate Army commanders submit their requests for information through echelon channels. If the intermediate echelons cannot answer them, they are passed to the joint task force's (JTF's) request for information section for research and response. Once a request for information is returned without an answer, subordinate commanders can submit a request for joint ISR support to the joint intelligence operations center. The joint intelligence operations center apportions its assets or other resources from higher echelons against the requests it receives, in order of priority, as defined by the JTF commander. Requests that cannot be satisfied by assets controlled or apportioned by the JTF are translated into the national intelligence system for collection.

C-11. Another resource is air support. At echelons below Army Service component command, requests for joint ISR air support go through an air support operations center or similar organization. Units requesting joint ISR support must accurately write air support requests, and they must request the desired capability or effect, not the specific airframe. Air Force air liaison officers at that headquarters may assist in training Army personnel how to prepare air support requests; however, their primary duty is to advise the commander and staff.

C-12. Some resources are outside the theater. The mission may require joint ISR resources not organic to the theater or to the components of the subordinate joint force. Joint ISR resources are typically in high demand and requirements usually exceed platform capabilities or inventory. The joint force collection manager must ensure that all requests for additional joint ISR resources are based on validated needs as established by the command's formal intelligence requirements.

JOINT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE PLANNING SYSTEMS

C-13. Two joint ISR planning systems— the collection management mission application and the Planning Tool for Resource, Integration, Synchronization, and Management (PRISM)—help facilitate access to joint resources. In joint collection management operations, the collection manager, in coordination with the operations directorate, forwards collection requirements to the component commander exercising tactical control over the theater reconnaissance and surveillance assets. A mission tasking order goes to the unit selected to be responsible for the collection operation. At the selected unit, the mission manager makes the final choice of specific platforms, equipment, and personnel required for the collection operations based on operational considerations such as maintenance, schedules, training, and experience. The collection management mission application is used by the Air Force. It is a web-centric information systems architecture that incorporates existing programs sponsored by several commands, Services, and agencies. It also provides tools for recording, gathering, organizing, and tracking intelligence collection requirements for all disciplines. PRISM, a subsystem of collection management mission application, is a Web-based management and synchronization tool used to maximize the efficiency and effectiveness of theater operations. PRISM creates a collaborative environment for resource managers, collection managers, exploitation managers, and customers.

JOINT AIR PLANNING PROCESS

C-14. Any joint ISR plan involving airborne assets or resources must consider the joint air planning process. The combatant commander's air component's air and space operations center controls the airspace in the area of responsibility and all air activity above the coordinating altitude determined by that commander. The air and space operations center must be informed of everything that is going to fly above the coordinating altitude. The air and space operations center also prioritizes joint ISR requirements for the assets that the Air Force component command controls and apportions. In a multinational headquarters, the air and space operations center is the combined air and space operations center.

C-15. Recent operations have demonstrated the value of having joint ISR liaison officers at Army organizational headquarters to help tactical commanders integrate theater ISR assets into their operations. These officers come from the air and space operations center, combined air and space operations center, or the Combined Forces Air Component Command. These liaison elements provide joint expertise and direct liaison with the combined air and space operations center. They also provide insight to the combined air and space operations center and related organizations into the operations they support.

JOINT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE CONCEPT OF OPERATIONS

C-16. The counterpart to the joint ISR plan is the joint ISR concept of operations, which is developed in conjunction with operational planning. The joint ISR concept of operations is based on the collection strategy and ISR execution planning, and is developed jointly by the joint force J-2 and J-3. The joint ISR concept of operations addresses how all available ISR assets and associated tasking, processing, exploitation, and dissemination infrastructure, to include multinational or coalition and commercial assets, are used to answer the joint force's intelligence requirements. It identifies asset shortfalls relative to the joint force's validated priority intelligence requirements (PIRs). It requires periodic evaluation of the capabilities and contributions of all available ISR assets in order to maximize their efficient utilization, and to ensure the timely release of allocated ISR resources when no longer needed by the joint force. JP 2-01 chapter 2 discusses the concept of operations in detail.

NATIONAL INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE RESOURCES AND GUIDELINES

C-17. Within the context of the National Intelligence Priorities Framework, the concept of ISR operations may be used to justifying requests for additional national ISR resources. National collection resources are leveraged against national priorities. Intelligence officers must remember that these assets are scarce and have a multitude of high-priority requirements.

NATIONAL INTELLIGENCE SUPPORT TEAMS

C-18. National intelligence support teams (NISTs) are formed at the request of a deployed joint or combined task force commander. NISTs are comprised of intelligence and communications experts from Defense Intelligence Agency, Central Intelligence Agency, National Geospatial-Intelligence Agency, National Security Agency, and other agencies as required to support the specific needs of the joint force commander. Defense Intelligence Agency is the executive agent for all NIST operations. Once on station, the NIST supplies a steady stream of agency intelligence on local conditions and potential threats. The needs of the mission dictate size and composition of NISTs.

C-19. Depending on the situation, NIST personnel are most often sent to support corps- or division-level organizations. However, during recent operations in Operation Iraqi Freedom and Operation Enduring Freedom, national agencies placed personnel at the brigade combat team level in some cases.

PLANNING AND REQUESTS FOR INFORMATION SYSTEMS

C-20. Several national databases and Intelink Web sites contain information applicable to the intelligence preparation to the battlefield process and national ISR planning. Commanders and their staff should review and evaluate those sites to determine the availability of current data, information, and intelligence products that might answer intelligence or information requirements.

- **Modernized integrated database** (known as MIDB) is accessible via Intelink and contains current, worldwide order-of-battle data organized by country, unit, facility, and equipment.
- **National Geospatial-Intelligence Agency's National Exploitation System** (known as NES) is accessible via Intelink. This site permits users to research the availability of imagery coverage over targets of interest and to access historical national imagery archives and imagery intelligence reports.
- **Country knowledge bases** and **crisis home pages** are maintained by many combatant command and joint force commands as Intelink Web sites containing the best and most up-to-date intelligence products available from the intelligence community.
- **Signals Intelligence On-Line Information System** (known as SOLIS) database contains current and historical finished signals intelligence products.
- **Secure analyst file environment** (known as SAFE) structured data files provide access to the following databases:
  - **Intelligence Report Index Summary File** (known as IRISA) contains index records and the full text of current and historical intelligence information reports.
  - **All-Source Document Index** (known as ASDIA) contains index records and abstracts for hardcopy all-source intelligence documents produced by Defense Intelligence Agency.
- **Human intelligence collection requirements** is a registry of all validated human intelligence requirements and tasking.
- **Modernized Defense Intelligence Threat Data System** (known as MDITDS) is a collection of analytic tools that support the retrieval and analysis of information and intelligence related to counterintelligence, indications and warning, and counterterrorism.
- **Community on-line intelligence system for end users and managers** (known as COLISEUM) is a database application which allows the user to identify and track the status of all validated crisis and noncrisis intelligence production requirements.

REQUIREMENTS MANAGEMENT SYSTEM

C-21. The requirements management system provides the national and Department of Defense imagery communities with a uniform automated collection management system. The requirements management system manages intelligence requirements for the national and Department of Defense user community in support of the United States' imagery and geospatial information system. This system—managed by National Geospatial-Intelligence Agency—provides end-to-end management of national and strategic imagery collection, exploitation, and dissemination. It enables creation, review, and approval of imagery requests. It tasks requirements for collection, production, and exploitation of imagery to appropriate locations. The requirements management system determines satisfaction of imagery requests, can modify imagery requests based on input from other sources of intelligence, and provides analytical tools for users to exploit.

C-22. The generated messages of the requirements management system are dispatched for approval and subsequent collection and exploitation tasking. The system is central to current and future integrated imagery and geospatial information management architectures supporting national, military, and civil customers.

C-23. Nominations management services provide the coordination necessary to accept user requirements for new information. These services aggregate, assign, and prioritize these user requirements. Nominations management services also track requirement satisfaction from the users.

NATIONAL SIGNALS INTELLIGENCE REQUIREMENTS PROCESS

C-24. The national signals intelligence requirements process (NSRP) is an integrated and responsive system of the policies, procedures, and technology used by the intelligence community to manage requests for national-level signals intelligence products and services. The NSRP replaced the previous system called the national signals intelligence requirement system.

C-25. The NSRP establishes an end-to-end crypto-logic mission management tracking system using information needs. Collectors of signals intelligence satisfy tactical through national-level consumer information needs based on NSRP guidance. The NSRP improves the consumer's ability to communicate with the collector by adding focus and creating a mechanism for accountability and feedback.

C-26. Information needs are used in NSRP to relay the collection requirements to signals intelligence collectors and systems. Users prioritize and classify information needs according to standardized time categories. Priorities for research information needs involve limited efforts and only exist for a set time using existing data (no new collection is required). Limited duration information needs require collection and production over a period of up to 90 days. Standing information needs require sustained collection over periods exceeding 90 days and up to 2 years.

C-27. Information needs are further prioritized based on how quickly the signals intelligence community must react to the request for collection by identifying—

- Routine information needs that require action in 30 or more days.
- Time sensitive information needs that require actions within 4 to 29 days after submission.
- Time critical information needs that require actions within the first three days after submission.

C-28. Requests for national signals intelligence collection must be sponsored at the national level, validated by the intelligence community, and prioritized among all the other competing requirements.

GUIDELINES FOR ACCESSING NATIONAL RESOURCES FOR INFORMATION

C-29. Depending upon local procedures and systems available, the Army intelligence officer may use various means to submit a request for information. The guidelines below assist in accessing national-level resources to answer the request for information—

- Know the PIRs and identify gaps that exist in the intelligence database and products.
- Know what collection assets are available from supporting and supported forces.
- Understand the timeline for preplanned and dynamic collection requests for particular assets.

- Identify collection assets and dissemination systems that may help answer the commander's PIRs.
- Ensure liaison and coordination elements are aware of PIRs and timelines for satisfaction. Ensure PIRs are tied to specific operational decisions.
- During planning, identify collection requirements and any trained analyst augmentation required to support post-strike battle damage assessment or other analysis requirements.
- Plan for cueing to exploit collection platforms.

JOINT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE CONSIDERATIONS

C-30. Communication and cooperation with other agencies and organizations in the joint operations area can enhance ISR collection efforts, creating sources of information with insights not otherwise available. Commanders must understand the respective roles and capabilities of the civilian organizations in the joint operations area to coordinate most effectively. Civilian organizations have different organizational cultures and norms. Some organizations may work willingly with Army forces while others may not. Some organizations are particularly sensitive about being perceived as involved in intelligence operations with the military. Some considerations in obtaining the valuable information these organizations may have access to are—

- **Building a relationship**—this takes time, effort, and a willingness to schedule time to meet with individuals.
- **Patience**—it is best not to expect results quickly and to avoid the appearance of tasking other agencies to provide information.
- **Reciprocity**—U.S. forces often can provide assistance or support that facilitate cooperation.
- **Mutual interests**—other organizations may have the same interests as U.S. forces (such as increased security).
- **Trust**—it should be mutual. At a minimum, organizations trust U.S. forces will not abuse the relationship and that the information is provided in good faith.

C-31. Commanders cannot task civilian organizations to collect information. However, U.S. government intelligence or law enforcement agencies normally collect or have access to information as part of their operations. These organizations may benefit by mutual sharing of information, and can be an excellent resource. Provincial reconstruction teams, for example, work in cooperation with military efforts and can provide information that is important to the commander's lines of effort such as infrastructure, governance, economic development, and health care.

JOINT INTELLIGENCE, SURVEILLANCE, AND RECONNAISSANCE ORGANIZATION

C-32. The JTF is the primary organization for joint operations. If other nations are included, it is a combined JTF. The JTF is designed to perform missions of short duration with specific, limited objectives. The JTF draws units from theater components and may receive augmentation—units, intelligence capabilities, and communications—from outside the theater.

C-33. When Army forces operate under a JTF or combined JTF for unified action, several organizations in the joint intelligence architecture can assist lower echelons with their joint ISR and information collection plans. The J-2 headquarters of a typical JTF has a joint intelligence operations center. Within this center, the collection management and the request for information sections are useful to Army intelligence officers as they plan joint ISR operations. In some cases, the collection management and dissemination sections are combined by the J-2 into one section: collection management and dissemination. Chapter 2 of JP 3-33 discusses the organization of the typical joint task force staff.

C-34. Key joint organizations for joint ISR include—

- Joint intelligence support element.
- Air and space operations center or combined air and space operations center.

- Intergovernmental and nongovernmental organizations.
- Multinational operations.

JOINT INTELLIGENCE SUPPORT ELEMENT

C-35. The joint intelligence support element may also be created to augment the J-2 element of the JTF. The collection management operations branch section within the joint intelligence support element is the interface where subordinate Army commanders receive support from the JTF. The collection management operations branch oversees the JTF's ISR activities. Dynamic re-tasking of joint resources must be coordinated with the joint intelligence support element collection management operations branch.

AIR AND SPACE OPERATIONS CENTER OR COMBINED AIR AND SPACE OPERATIONS CENTER

C-36. Joint air planning products produced by the air and space operations center include the air tasking order, airspace control order, and special instructions. The air tasking order, airspace control order, and special instructions provide operational and tactical direction at the appropriate levels of detail. For aerial assets, these products are important for intelligence staffs as well as mission managers and operators (for example, unmanned aircraft system operators and aircraft pilots).

C-37. Army intelligence staffs coordinate with the air and space operations center through an Army unit called a battlefield coordination detachment. The battlefield coordination detachment is the Army Service component command's liaison at the air and space operations center. This detachment communicates the land component commander's issues to the air component commander. Aerial collection requests flow through the battlefield coordination detachment to the air and space operations center for consideration. (See ATTP 3-09.13 for more information on battlefield coordination detachment duties and responsibilities.)

C-38. The air and space operations center sends a liaison element to the air component command element to communicate the air component commander's issues to the land component commander.

INTERGOVERNMENTAL AND NONGOVERNMENTAL ORGANIZATIONS

C-39. In addition to working with U.S. government agencies, unified action involves synchronizing joint or multinational military operations with activities of other government agencies, intergovernmental organizations, nongovernmental organizations, and contractors. These organizations may have significant access, specialized knowledge, or insight and understanding of the local situation because of the nature of what they do. These organizations vary widely in their purposes, interests, and ability or willingness to cooperate with the information-gathering activities of U.S. forces. It is often preferable to simply cultivate a relationship that enables the exchange of information without revealing specific requirements.

MULTINATIONAL OPERATIONS

C-40. The Army uses the joint definition of *multinational operations*—a collective term to describe military actions conducted by forces of two or more nations, usually undertaken within the structure of a coalition or alliance (JP 3-16). Intensive coordination, training, and extensive liaison are important to effective multinational ISR operations.

C-41. In multinational operations, the JTF must share intelligence, as necessary, for mission accomplishment with foreign military forces and coordinate the exchange of intelligence liaisons with those forces. Command and control of ISR resources may remain essentially national or may be integrated into a combined command and control structure. There is no single intelligence doctrine for multinational operations. Each coalition or alliance must develop its own unique procedures. Refer to JP 2-01 for more information on the intelligence considerations for multinational operations.

C-42. Multinational force commanders establish a system that optimizes each nation's contributions. Managing assets from multinational partners requires close coordination and at times, maintenance support. U.S. forces often also provide technical assistance to share information and intelligence.

C-43. Early, concurrent planning is critical to the success of joint and multinational operations. Multinational ISR planning activities include, but are not limited to—

- **Developing requirements**—information regarding the threat and the environment that needs to be collected and processed to meet the intelligence requirements of the commander.
- **Developing indicators**—activity or lack of activity that confirms or denies the action or event specified in an intelligence requirement. Intelligence analysts develop indicators.
- **Developing the ISR plan**—which involves coordination between the collection manager and operations directorate.

C-44. U.S. personnel assigned to a multinational organization should be aware of, and remain sensitive to, cultural and religious differences among its members. In some instances, these differences may result in periods of increased vulnerability for the joint force or require scheduling changes for meetings or briefings.

C-45. In most multinational operations, U.S. forces share intelligence with foreign military forces and receive intelligence from those forces. Unique intelligence policy and criteria are tailored to each multinational operation. In some multinational operations or campaigns, existing international standardization agreements may provide a basis for establishing rules and policies for conducting joint intelligence operations. Since each multinational operation is unique, such agreements may have to be modified or amended based on the situation. Policy and procedures are tailored based on theater guidance and national policy as contained in DODD 5230.11. Staffs never disclose classified information automatically. Any disclosure must be consistent with U.S. national policy and U.S. military objectives, be done with security assurances in place, present a clearly defined U.S. advantage, and be limited to only necessary information.

Glossary

The glossary lists acronyms and terms with Army, multi-Service, or joint definitions, and other selected terms. Where Army and joint definitions are different, (Army) follows the term. Terms for which FM 3-55 is the proponent (authority) manual are marked with an asterisk (*). The proponent manual for other terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

AO	area of operations
ATTP	Army tactics, techniques, and procedures
BCT	brigade combat team
BFSB	battlefield surveillance brigade
CAB	combat aviation brigade
CBRN	chemical, biological, radiological, and nuclear
CCIR	commander's critical information requirement
COA	course of action
COP	common operational picture
DA	Department of the Army
DCGS-A	Distributed Common Ground System (Army)
DODD	Department of Defense directive
DSCA	defense support of civil authorities
EEFI	essential elements of friendly information
FM	field manual
FRAGO	fragmentary order
G-2	assistant chief of staff, intelligence
G-2X	assistant chief of staff, counterintelligence and human intelligence
G-3	assistant chief of staff, operations
G-7	assistant chief of staff, information operations
G-9	assistant chief of staff, civil affairs operations
IPB	intelligence preparation of the battlefield
ISR	intelligence, surveillance, and reconnaissance
J-2	intelligence directorate of a joint staff
JP	joint publication
JTF	joint task force
LTIOV	latest time information is of value
MDMP	military decisionmaking process
MIB	military intelligence brigade
NAI	named area of interest
NIST	national intelligence support team
NSRP	national signals intelligence requirements process
OPORD	operation order

PIO	public information officer
PIR	priority intelligence requirement
PRISM	Planning Tool for Resource, Integration, Synchronization, and Management
S-2	intelligence staff officer
S-2X	intelligence staff executive officer
S-3	operations staff officer
S-7	information operations staff officer
S-9	civil affairs operations staff officer
SOP	standard operating procedure
TAI	target area of interest
TC	training circular
U.S.	United States
UAS	unmanned aircraft system
WARNO	warning order

SECTION II – TERMS

battle rhythm

A deliberate daily cycle of command, staff, and unit activities intended to synchronize current and future operations. (JP 3-33)

geospatial intelligence

The exploitation and analysis of imagery and geospatial information to describe, assess, and visually depict physical features and geographically referenced activities on the Earth. Geospatial intelligence consists of imagery, imagery intelligence, and geospatial information. (JP 2-03)

human intelligence

A category of intelligence derived from information collected and provided by human sources. (JP 2-0)

***information collection**

An activity that synchronizes and integrates the planning and employment of sensors and assets as well as the processing, exploitation, and dissemination of systems in direct support of current and future operations.

intelligence

The product resulting from the collection, processing, integration, evaluation, analysis, and interpretation of available information concerning foreign nations, hostile or potentially hostile forces or elements, or areas of actual or potential operations. The term is also applied to the activity which results in the product and to the organizations engaged in such activity. (JP 2-0)

multinational operations

A collective term to describe military actions conducted by forces of two or more nations, usually undertaken within the structure of a coalition or alliance. (JP 3-16)

reconnaissance

Those operations undertaken to obtain, by visual observation or other detection methods, information about the activities and resources of an enemy or adversary, or to secure data concerning the meteorological, hydrographical or geographical characteristics and the indigenous population of a particular area. (FM 3-90)

running estimate

The continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if planned future operations are supportable. (FM 5-0)

site exploitation

Systematically searching for and collecting information, material, and persons from a designated location and analyzing them to answer information requirements, facilitate subsequent operations, or support criminal prosecution. (ATTP 3-90.15)

surveillance

The systematic observation of aerospace, surface, or subsurface areas, places, persons, or things, by visual, aural, electronic, photographic, or other means. (JP 3-0)

synchronization

The arrangement of action in time, space, and purpose to produce maximum relative combat power at a decisive place and time. (JP 1-02)

unified action

The synchronization, coordination, and/or integration of the activities of governmental and nongovernmental entities with military operations to achieve unity of effort. (JP 1)

This page intentionally left blank.

References

Field manuals and selected joint publications are listed by new number followed by old number.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

FM 1-02 (FM 101-5-1). *Operational Terms and Graphics*. 21 September 2004.

JP 1-02. *Department of Defense Dictionary of Military and Associated Terms*. 15 November 2011.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

ARMY PUBLICATIONS

Army doctrinal publications are available online: <http://www.apd.army.mil/>.

ADP 3-0. *Unified Land Operations*. 10 October 2011.

AR 380-5. *Department of the Army Information Security Program*. 29 September 2000.

ATTP 2-01. *Planning Requirements and Assessing Collection*. 23 April 2012.

ATTP 3-09.13. *The Battlefield Coordination Detachment*. 21 July 2010.

ATTP 3-90.15. *Site Exploitation Operations*. 8 July 2010.

ATTP 5-0.1. *Commander and Staff Officer Guide*. 14 September 2011.

FM 2-0. *Intelligence*. 23 March 2010.

FM 2-01.3. *Intelligence Preparation of the Battlefield/Battlespace*. 15 October 2009.

FM 2-22.3. *Human Intelligence Collector Operations*. 6 September 2006.

FM 3-20.96. *Reconnaissance and Cavalry Squadron*. 12 March 2010.

FM 3-55.1. *Battlefield Surveillance Brigade*. 14 June 2010.

FM 3-90. *Tactics*. 4 July 2001.

FM 3-90.6. *Brigade Combat Team*. 14 September 2010.

FM 5-0. *The Operations Process*. 26 March 2010.

FM 6-0. *Mission Command.* 13 September 2011.

FM 7-15. *The Army Universal Task List*. 27 February 2009.

TC 2-01. *Intelligence, Surveillance, and Reconnaissance Synchronization*. 22 September 2010.

TC 2-22.303. *The 2X Handbook*. 31 July 2006.

JOINT PUBLICATIONS

Joint publications are available online: <http://www.dtic.mil/doctrine/new_pubs/jointpub.htm.>

DODD 5230.11, *Disclosure of Classified Military Information to Foreign Governments and International Organizations*, 16 June 1992.
<http://www.dtic.mil/dtic/pdf/customer/STINFOdata/DoDD_523011.pdf>

JP 1. *Doctrine for the Armed Forces of the United States*. 2 May 2007.

JP 2-0. *Joint Intelligence*. 22 June 2007.

JP 2-01. *Joint and National Intelligence Support to Military Operations*. 7 October 2004.

JP 2-03. *Geospatial Intelligence Support to Joint Operations*. 22 March 2007.

JP 3-0. *Joint Operations*, 11 August 2011.

JP 3-16. *Multinational Operations*. 7 March 2007.

JP 3-33. *Joint Task Force Headquarters*. 16 February 2007.

OTHER PUBLICATIONS

Petraeus, David H. "Multi-National Force-Iraq Commander's Counterinsurgency Guidance." *Military Review*. September-October 2008. 210–212.

Title 10 United States Code, Armed Forces.

PRESCRIBED FORMS

None

REFERENCED FORMS

DA forms are available on the APD web site (www.apd.army.mil).

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

Index

Entries are by paragraph number.

A

action, knowledge and, 1-1

air and space operations center, C-36–C-38

air support, C-11

annex, information collection, B-1–B-2

area, 1-47

area surveillance, 1-71

assess, 2-8
  information collection, 1-17
  information collection activities, 3-57–3-60

assessment, 3-57,3-60
  information collection planning, 2-7

assets, availability of, 3-32
  capabilities of, 3-21–3-22
  collection requirements, 4-26
  information collection, A-1–A-42
  multinational operations, C-43
  reconnaissance, 1-38, 1-41
  requirements, A-2
  re-tasking, 4-28–4-30
  review, 3-20–3-33
  tasking, 4-5

assumptions, identify, 3-35–3-36

B

battle rhythm, defined, 2-26
  operations and intelligence working group, 2-30

battlefield coordination detachment, air and space operations center, C-37

battlefield surveillance brigade, A-26–A-28
  augmentation, A-28
  support from, A-26

board, 2-28

briefing, 1-28

brigade combat team, A-35–A-39
  intelligence, A-38
  operations, A-37
  reconnaissance squadron, A-39

C

capabilities, assets, 3-21–3-22, 3-33

CCIR, 3-50
  COA development, 3-54
  information collection activities, A-3
  information collection planning, 3-39–3-40

COA, information collection plan, 3-42
  reconnaissance, 1-32

COA analysis, wargaming, 3-55

COA development, 3-51–3-54
  CCIR, 3-54
  collection considerations, 3-51
  integrated plan, 3-52

collect, information and data, 1-26

collection assets, 4-20

collection management system, C-21

collection requirements, assets, 4-26

combat aviation brigade, A-29–31

combined air and space operations center, C-36–C-38

commander guidance, central role, 2-12
  collection activities, 2-15
  collection planning, 2-14
  information collection plan, 2-16
  initial commander's intent, 2-17
  planning, 2-16–2-17

commander's critical information requirements, *See* CCIR

commanders, assess, 2-8
  EEFI, 2-5
  guidance by, 2-4, 2-12–2-18
  information collection, 2-3
  initial guidance, 2-13–2-15
  needs, 2-9–2-11
  restrictions, C-31
  role, 2-1–2-8
  staff efforts, 2-6
  understanding, 2-1, 2-10, 2-11

concept of operations, joint ISR, C-16

constraints, determine, 3-34

counterintelligence, 1-80

course of action, *See* COA

culture, multinational operations, C-44

D

deployment, information collection assets, A-10

durability, 3-27

E

EEFI, 2-5
  information collection planning, 3-39–3-40

engagement criteria, 1-56

entry, information collection assets, A-11–A-14
  reconnaissance, A-12
  vulnerability, A-11

essential elements of friendly information, *See* EEFI

execute, information collection, 1-19–1-28

F

facts, identify, 3-35–3-36

feedback, provide, 4-18–4-21
  requirements, 4-20, 4-27

fires brigade, A-32–A-34
  capabilities, A-33
  task-organized, A-34

focus, reconnaissance, 1-50–1-52

fusion working group, refine and fuse intelligence, 2-37

G

geolocation, accuracy, 3-26

geospatial intelligence, defined, 1-82

guidance, commander, 2-12–2-18
  technical channels, 1-21–1-24

H

higher headquarters order, mission analysis, 3-14

human intelligence, defined, 1-81

I

information, 1-5
  collectors, A-13
  correlate, 4-13–4-15
  reconnaissance, 1-32, 1-40
  sharing, C-31
  transition, A-16

information collection, activities, 1-8, 3-1, 3-3, 3-8, 3-57–3-60, 4-25, A-4–A8

Entries are by paragraph number.

information collection (continued)
analytical capability, 1-15
annex, B-1
assess, 1-17
capabilities, A-1, A-41
CCIR, 1-12, 3-5, A-3
COA selection, 3-4
collect and report, 1-25–1-27
decisions, 1-10
definition, 1-1–1-7
direct, 4-1
effective, 1-9
elements, 1-16
execute, 1-19–1-28
foundations, 1-1–1-85
integration of, 1-6, 4-1
missions, 1-29–1-85
network-enabled, A-42
operations process, 3-1–3-60
outputs, 3-12
process, 1-16–1-28
purpose, 1-8–1-15
resources, 1-14
scheme of support, 4-8–4-27
staff, 1-13
support from, 1-7
support personnel recovery, 3-6
task, 1-18, 1-29–1-85, 3-58, 4-1
technical channels, 1-21–1-24

information collection assets, A-1–A-42
by echelon, A-18–A-41
by level, A-4–A-8
by phase, A-9–A-17
deployment, A-10
entry, A-11–A-14
transition, A-15–A-17

information collection overlay, 4-6–4-7

information collection plan, 1-29, 3-41–3-44, 4-2–4-5, B-2
collection requirements, 4-2
considerations, 3-44
format, 4-3
information collection matrix, 4-4
information collection overlay, 4-6
tasking, 4-5
tools, 3-43
update, 4-22–4-24

information collection planning, 1-11, 2-3, 3-4–3-5
assessment, 2-7
CCIR, 3-39–3-40
EEFI, 3-39–3-40
IPB, 2-6
IPB, 3-7
MDMP, 3-7–3-56
operations and intelligence working group, 2-29

initial guidance, 2-13–2-15

integration, joint ISR and, C-4

intelligence, coordination, C-37
defined, 1-6
disciplines, 1-79
multinational operations, C-41
production of, 3-49
reconnaissance and surveillance, 1-2
staff, 3-18

intelligence estimate, tools, 3-11

intelligence operations, 1-79–1-85
technical channels, 1-23

intelligence preparation of the battlefield, See IPB,

intelligence, surveillance, and reconnaissance, *See* ISR

interdependence, joint ISR and, C-5–C-6

intergovernmental organizations, C-39

IPB, 3-15–3-18
information collection planning, 2-6, 3-7
products, 3-15–3-16
reconnaissance, 1-31

J

joint air planning, products, C-36

joint air planning process, joint ISR plan, C-14–C-15
liaison, C-15

joint intelligence, organizations, C-33

joint intelligence operations center, C-33

joint intelligence support element, C-35

joint ISR, C-1–C-45
concept of operations, C-16
concepts of, C-3–C-6
considerations, C-30–C-31
doctrine, C-7–C-8
information sharing, C-31
organization, C-32–C-45
planning systems, C-13–C-16
resources, C-9–C-12

joint task force, C-32–C-33

K–L

knowledge, action and, 1-1

laws, technical channels, 1-22

liaison, air and space operations center, C-38
joint air planning process, C-15

light, effects of, 3-23

M

MDMP, 3-9–3-56
information collection planning, 3-7–3-56

measure and signature intelligence, 1-83

military decisionmaking process, *See* MDMP

military intelligence brigade, A-22–A-25
support from, A-24
theater army and, A-25

mission, anticipation of, 3-9
information collection, 1-29–1-85

mission analysis, 3-13–3-50
higher headquarters order, 3-14
initial collection requirements, 3-18
initial guidance, 3-13
IPB, 3-15
tasks, 3-19

mission intelligence, briefing and debriefing, 1-28

multinational operations, C-40–C-45
contributions, C-42
defined, C-40
intelligence, C-41
planning activities, C-43, C-44
standardized agreements, C-45

N

national intelligence support teams, C-18–C-19

national ISR, guidelines, C-17
planning, C-20
requests for information systems, C-20
resources, C-17

national signals intelligence requirements process, *See* NSRP

network surveillance, 1-73

Entries are by paragraph number.

nongovernmental organizations, C-39
NSRP, C-24–C-28
  information needs, C-26
  prioritized, C-27
  tracking, C-25

O

objectives, reconnaissance, 1-34–1-35, 1-39
operational area, participants, C-2
operational environment, describing, 3-10
operations, monitor, 4-12
  shaping, 1-4
operations and intelligence working group, battle rhythm, 2-33
  information collection planning, 2-29
  method, 2-36
  output, 2-32
  representatives, 2-31
  responsibilities of, 2-31
operations process, information collection, 3-1–3-60
orders, production, 3-56

P

performance, history, 3-31
personnel recovery, support to, 3-6
phases, information collection assets, A-9–A-17
plan, information collection, 1-17, 1-29, B-2
  tactical, A-3–A-8
planning, 2-12
  assumptions, 3-36
  information collection, 1-11, 2-3
  national ISR, C-20
planning activities, multinational operations, C-44
planning considerations, information collection, 3-4–3-5
planning guidance, 2-16–2-17
  final, 2-18
planning systems, joint ISR, C-13–C-16
point surveillance, 1-72
production, requirements of, 3-48–3-50
products, IPB, 3-16
protection, reconnaissance, 1-33
pull, reconnaissance, 1-51
push, reconnaissance, 1-52

R

range, capability, 3-21–3-22
receipt of mission, 3-9–3-12
reconnaissance, 1-30–1-56
  accurate and timely information, 1-40
  assets, 1-38
  continuous, 1-37
  course of action, 1-32
  criteria, 1-49–1-56
  defined, 1-30
  deployment of, A-14
  develop, 1-43
  effort, 1-39
  enemy contact, 1-42
  forceful and stealthy, 1-55
  forms, 1-44–1-48
  freedom of maneuver, 1-41
  fundamentals, 1-36–1-43
  instructions, 1-35
  IPB, 1-31
  methods, 1-31
  objectives, 1-34
  protection, 1-33
  rapid and deliberate, 1-54
  tempo, 1-53–1-55
  versus surveillance, 1-61–1-63
reconnaissance and surveillance, intelligence and, 1-2
reconnaissance in force, 1-48
religions, multinational operations, C-44
reports, correlate to requirements, 4-13–4-15
  information and data, 1-27
  information collection, A-8
  screen, 4-17
requests for collection or support, 3-45–3-47
requests for information, 3-45–3-47, C-10
  national ISR, C-20
requirements, correlate to reports, 4-13–4-15
  develop, 4-29
requirements management system, C-21–C-23
resources, characteristics, 3-24
  guidelines, C-29
  information collection, 1-14
  joint ISR, C-9–C-12
  outside the theater, C-12
re-tasking, assets, 4-28–4-30
risk, assessment, 3-37–3-38
route, 1-45
running estimate, 3-59
  defined, 2-24

S

scheme of support, information collection, 4-8–4-27
screen reports, 4-16–4-17
security operations, 1-74–1-78
  forms, 1-76
  fundamentals, 1-77
  protect the force, 1-75
  shaping operations, 1-74
shaping operations, security operations, 1-74
signals intelligence, 1-84
site exploitation, defined, 4-10
  support to, 4-10–4-11
special operations forces, capabilities, A-20
  conventional forces and, A-21
  information collection assets, A-19–A-21
staff, considerations, 2-25, 3-44
  efforts, 2-6
  feedback, 4-18
  functions, 3-3
  input, 1-13
  intelligence, 3-18
  professional team, 2-19
  responsibilities, 1-5, 2-9, 2-34–2-35, 4-2–4-3, 4-19
  role, 2-19–2-25
  running estimate, 2-24
  support from, 2-24
strategic, information collection assets, A-5
surveillance, 1-57–1-73
  area, 1-71
  characteristics, 1-64–1-67
  continuous, 1-65
  defined, 1-57
  early warning, 1-66
  key targets, 1-67
  network, 1-73
  observing, 1-58
  overlapping coverage, 1-68
  performing, 1-59
  point, 1-72
  task, 1-60
  types, 1-69–1-73

Entries are by paragraph number.

surveillance (continued)
versus reconnaissance, 1-61–1-63
watch, 1-62
zone, 1-70
sustainability, 3-29
synchronization, defined, 3-2

T

tactical, information collection assets, A-7–A-8
tactical plan, monitor, A-3–A-8
targeting working group, 2-38–2-40
information collection support, 2-39
purpose, 2-38
results, 2-40
tasks, information collection, 1-29–1-85, 3-19
reconnaissance, 1-30
technical channels, 1-24
technical channels, applicable laws and policies, 1-22
establish, 1-21–1-24
subtasks, 1-20–1-28
supervision of intelligence assets, 1-23
tasks, 1-21
translate tasks, 1-24
technical characteristics, resources, 3-24
technical intelligence, 1-85
tempo, defined, 1-53
reconnaissance, 1-53–1-55
threat activity, 3-28
threat event template, 3-17
timelines, reporting, 3-25
tools, information collection plan, 3-43
intelligence estimate, 3-11
transition, 4-30
information collection assets, A-15–A-17

U–V

understanding, commander, 2-1, 2-10
factors of, 2-2
unified action, C-1–C-2
defined, C-1
vulnerability, 3-30

W

wargaming, COA analysis, 3-55
working group, description, 2-27
fusion, 2-37
input from, 2-26–2-40
operations and intelligence working group, 2-29–2-36
targeting, 2-38–2-40

Z

zone, 1-46
zone surveillance, 1-70

FM 3-55
23 April 2012

By order of the Secretary of the Army:

RAYMOND T. ODIERNO
General, United States Army
Chief of Staff

Official:

JOYCE E. MORROW
Administrative Assistant to the
Secretary of the Army
1135303

DISTRIBUTION:

Active Army, Army National Guard, and United States Army Reserve: Not to be distributed. Electronic media only.

PIN: 102534-000

This Page Is Intentionally Left Blank

ATP 2-33.4

Intelligence Analysis

JANUARY 2020

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

This publication supersedes ATP 2-33.4, dated 18 August 2014.

Headquarters, Department of the Army

This publication is available at Army Knowledge Online (https://armypubs.army.mil), and the Central Army Registry site (https://atiam.train.army.mil/catalog/dashboard).

*ATP 2-33.4

Army Techniques Publication
No. 2-33.4

Headquarters
Department of the Army
Washington, DC, 10 January 2020

Intelligence Analysis

Contents

Page

PREFACE ..... **vii**

INTRODUCTION ..... **xi**

PART ONE FUNDAMENTALS

Chapter 1 UNDERSTANDING INTELLIGENCE ANALYSIS **1-1**
Intelligence Analysis Overview 1-1
Conducting Intelligence Analysis 1-5
Intelligence Analysis and Collection Management 1-8
The All-Source Intelligence Architecture and Analysis Across the Echelons 1-9
Intelligence Analysis During Large-Scale Ground Combat Operations 1-11
Intelligence Analysis During the Army's Other Strategic Roles 1-13

Chapter 2 THE INTELLIGENCE ANALYSIS PROCESS **2-1**
Overview 2-1
The Phases of the Intelligence Analysis Process 2-1

Chapter 3 ALL-SOURCE ANALYTICAL TASKS **3-1**
Overview 3-1
Generate Intelligence Knowledge (ART 2.1.4) 3-2
Perform Intelligence Preparation of the Battlefield (ART 2.2.1) 3-3
Provide Warnings (ART 2.1.1.1) 3-3
Perform Situation Development (ART 2.2.2) 3-4
Provide Intelligence Support to Targeting and Information Operations (ART 2.4) 3-4

PART TWO TASK TECHNIQUES

Chapter 4 ANALYTIC TECHNIQUES **4-1**
Overview 4-1
Applying Structured Analytic Techniques 4-1

Chapter 5 BASIC AND DIAGNOSTIC STRUCTURED ANALYTIC TECHNIQUES **5-1**
Section I – Basic Structured Analytic Techniques **5-1**
Sorting 5-1
Chronologies 5-4

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

*This publication supersedes ATP 2-33.4, dated 18 August 2014.

Matrices 5-6
Weighted Ranking 5-7
Link Analysis 5-8
Event Tree 5-12
Event Mapping 5-13
Section II – Diagnostic Structured Analytic Techniques 5-15
Key Assumptions Check 5-15
Quality of Information Check 5-16
Indicators/Signposts of Change 5-18

Chapter 6 ADVANCED STRUCTURED ANALYTIC TECHNIQUES 6-1
Section I – Contrarian Structured Analytic Techniques 6-1
Analysis of Competing Hypotheses 6-1
Devil's Advocacy 6-3
Team A/Team B 6-4
High-Impact/Low-Probability Analysis 6-5
"What If?" Analysis 6-6
Section II – Imaginative Structured Analytic Techniques 6-7
Brainstorming 6-8
Functional Analysis Using Critical Factors Analysis 6-9
Outside-In Thinking 6-10
Red Hat/Team Analysis 6-11

PART THREE INTELLIGENCE ANALYSIS CONSIDERATIONS

Chapter 7 ANALYTIC SUPPORT TO ARMY FORCES AND OPERATIONS 7-1
Overview 7-1
Analysis Across the Echelons 7-1
Support to Functional Elements 7-3
Analysis Across the Army's Strategic Roles 7-6

Chapter 8 ANALYSIS AND LARGE-SCALE GROUND COMBAT OPERATIONS 8-1
Overview 8-1
Tactical to Operational Situation: An Enemy Attack 8-1

Chapter 9 MANAGING LONG-TERM ANALYTICAL ASSESSMENTS 9-1
Overview 9-1
The Basics of Analytic Design 9-1
Collaboration During Analytic Design 9-6
Transitioning from the Analytic Design Process to Presenting the Results 9-6
Crosswalking Analytic Design with Tactical Intelligence Analysis 9-7

Appendix A AUTOMATION SUPPORT TO INTELLIGENCE ANALYSIS A-1
Appendix B COGNITIVE CONSIDERATIONS FOR INTELLIGENCE ANALYSTS B-1
Appendix C ANALYTIC STANDARDS AND ANALYSIS VALIDATION C-1
Appendix D THREAT CONSIDERATIONS DURING LARGE-SCALE GROUND COMBAT OPERATIONS D-1
Appendix E INTELLIGENCE PRODUCTION E-1
Appendix F INTELLIGENCE SUPPORT TO TARGETING F-1

GLOSSARY **Glossary-1**
REFERENCES **References-1**
INDEX **Index-1**

Figures

Introductory figure. Intelligence analysis at a glance xii
Figure 1-1. Achieving situational awareness and understanding 1-1
Figure 1-2. Intelligence analysis within doctrinal constructs 1-3
Figure 1-3. Information and intelligence reporting example 1-4
Figure 1-4. Analytic standards 1-8
Figure 1-5. All-source analysis across the echelons 1-10
Figure 1-6. Key aspects of the operational framework 1-12
Figure 2-1. The intelligence analysis process 2-2
Figure 3-1. The all-source analytical tasks 3-1
Figure 4-1. Applying analytic techniques to understand the operational environment 4-2
Figure 4-2. Structured analytic techniques summarized 4-3
Figure 5-1. Sorting data using a pattern analysis plot sheet example 5-3
Figure 5-2. Timeline example 5-5
Figure 5-3. Time event chart example 5-5
Figure 5-4. Threat intentions matrix example 5-7
Figure 5-5. Weighted ranking (steps 1–5) to determine the threat's most likely COA 5-8
Figure 5-6. Weighted ranking (step 6) to determine the threat's most likely COA 5-8
Figure 5-7. Link diagram example 5-10
Figure 5-8. Association matrix example 5-11
Figure 5-9. Activities matrix example 5-11
Figure 5-10. Event tree example 5-13
Figure 5-11. Event mapping example 5-14
Figure 6-1. Analysis of competing hypotheses used during step 4 of the IPB process 6-3
Figure 6-2. Team A/Team B used during step 4 of the IPB process 6-5
Figure 6-3. Functional analysis using critical factors analysis 6-10
Figure 6-4. Outside-in thinking used during step 2 of the IPB process 6-11
Figure 8-1. Brigade combat team situation example 8-2
Figure 8-2. Division situation example 8-4
Figure 8-3. Tactical/Operational (corps) situation example 8-6
Figure 9-1. Analytic design steps 9-2
Figure 9-2. Frame the question/issue 9-3
Figure 9-3. Review and assess knowledge 9-3
Figure 9-4. Review resources 9-4
Figure 9-5. Select the analytic approach/methodology and plan project 9-4
Figure 9-6. Develop knowledge 9-5

Figure 9-7. Perform analysis 9-5
Figure 9-8. Evaluate analysis 9-6
Figure A-1. Intelligence analysis enabled by DCGS-A A-3
Figure B-1. Types of reasoning examples B-3
Figure C-1. Estimative language: expressions of likelihood C-2
Figure E-1. Annex B (Intelligence) to the operation order example E-2
Figure E-2. Appendix 1 (Intelligence Estimate) example E-4
Figure E-3. Intelligence running estimate example E-5
Figure E-4. Intelligence summary example E-6
Figure E-5. Graphic intelligence summary example E-8
Figure E-6. Intelligence report example E-8
Figure E-7. Periodic intelligence report example E-9
Figure F-1. High-payoff target list example F-4
Figure F-2. Example target selection standard matrix F-5
Figure F-3. Battle damage assessment chart (based on threat organization) F-10
Figure F-4. Battle damage assessment chart (based on location) F-10

Tables

Table 1-1. Intelligence analysis during large-scale ground combat operations 1-11
Table 1-2. Intelligence analysis during the other Army strategic roles 1-14
Table 2-1. Evaluation ratings for source reliability and information accuracy 2-5
Table 5-1. Sorting technique 5-2
Table 5-2. Chronologies technique 5-4
Table 5-3. Matrices technique 5-6
Table 5-4. Weighted ranking technique 5-7
Table 5-5. Link analysis technique 5-9
Table 5-6. Event tree technique 5-12
Table 5-7. Event mapping technique 5-14
Table 5-8. Key assumptions check technique 5-15
Table 5-9. Quality of information check technique 5-16
Table 5-10. Questioning guideline for checking information quality 5-17
Table 5-11. Indicators/Signposts of change technique 5-18
Table 6-1. Analysis of competing hypotheses technique 6-2
Table 6-2. Devil's advocacy technique 6-3
Table 6-3. Team A/Team B technique 6-4
Table 6-4. High-impact/Low-probability analysis technique 6-6
Table 6-5. "What if?" analysis technique 6-7
Table 6-6. Brainstorming structured technique 6-8
Table 6-7. Functional analysis technique using critical factors analysis 6-9
Table 6-8. Outside-in thinking technique 6-10

Table 6-9. Red hat/team analysis technique 6-12
Table 7-1. Intelligence analysis support to functional elements 7-3
Table 7-2. Intelligence requirements associated with operations to shape 7-6
Table 7-3. Intelligence requirements associated with operations to prevent 7-7
Table 7-4. Intelligence requirements associated with large-scale ground combat operations 7-7
Table 7-5. Intelligence requirements associated with the offense 7-9
Table 7-6. Intelligence requirements associated with the defense 7-10
Table 7-7. Intelligence requirements associated with operations to consolidate gains 7-11
Table 8-1. Intelligence analysis (brigade combat team) example 8-2
Table 8-2. Intelligence analysis (division) example 8-5
Table 8-3. Intelligence analysis (tactical/operational [corps]) example 8-7
Table 9-1. Analytic design to tactical intelligence analysis crosswalk 9-7
Table B-1. Checklist for reasoning B-5
Table C-1. Analytical actions and levels of rigor C-5
Table D-1. Threat analysis by warfighting function example D-2
Table D-2. Analyst considerations based on threat equipment capabilities D-4
Table E-1. Support to orders and briefings E-11
Table F-1. Battle damage assessment components F-9

This page intentionally left blank.

Preface

ATP 2-33.4 provides fundamental information to a broad audience, including commanders, staffs, and leaders, on how intelligence personnel conduct analysis to support Army operations. It describes the intelligence analysis process and specific analytic techniques and information on the conduct of intelligence analysis performed by intelligence personnel, especially all-source analysts, across all intelligence disciplines. Additionally, ATP 2-33.4 describes how intelligence analysis facilitates the commander's decision making and understanding of complex environments.

The principal audience for ATP 2-33.4 is junior to midgrade intelligence analysts conducting intelligence analysis. This publication provides basic information on intelligence analysis for commanders, staffs, and other senior military members.

ATP 2-33.4 readers must have an understanding of the following:

- Intelligence doctrine described in ADP 2-0 and FM 2-0.
- Collection management described in ATP 2-01.
- Intelligence preparation of the battlefield (IPB) described in ATP 2-01.3.
- Operational doctrine described in ADP 3-0 and FM 3-0.
- Joint targeting described in JP 3-60.

Commanders, staffs, and subordinates ensure their decisions and actions comply with applicable United States (U.S.), international, and, in some cases, host-nation laws and regulations. Commanders at all levels ensure their Soldiers operate in accordance with the law of war and the rules of engagement. (See FM 6-27.)

This publication contains copyrighted material.

ATP 2-33.4 uses joint terms where applicable. Selected joint and Army terms and definitions appear in both the glossary and the text. For definitions shown in the text, the term is italicized, and the number of the proponent publication follows the definition. This publication is not the proponent for any Army terms.

ATP 2-33.4 applies to the Active Army, Army National Guard/Army National Guard of the United States, and U.S. Army Reserve unless otherwise stated.

The proponent of ATP 2-33.4 is the U.S. Army Intelligence Center of Excellence. The preparing agency is the Directorate of Doctrine and Intelligence Systems Training, U.S. Army Intelligence Center of Excellence, Fort Huachuca, AZ. Send comments and recommendations on a DA Form 2028 (*Recommended Changes to Publications and Blank Forms*) to Commander, U.S. Army Intelligence Center of Excellence, ATTN: ATZS-DST-D (ATP 2-33.4), 550 Cibeque Street, Fort Huachuca, AZ 85613-7017; by email to usarmy.huachuca.icoe.mbx.doctrine@mail.mil; or submit an electronic DA Form 2028.

This page intentionally left blank.

Acknowledgement

The critical thinking material in appendix B has been used with permission from the Foundation for Critical Thinking, http://www.criticalthinking.org/: *The Thinker's Guide to Analytic Thinking*, 2017, and *The Miniature Guide to Critical Thinking: Concepts and Tools*, 2014, by Dr. Linda Elder and Dr. Richard Paul. The copyright owners have granted permission to reproduce material from their works. With their permission, some of the text has been paraphrased and adapted for military purposes.

This page intentionally left blank.

Introduction

ATP 2-33.4 discusses doctrinal techniques—descriptive methods for performing missions, functions, or tasks as they apply to intelligence analysis. ATP 2-33.4—

- Describes the intelligence analysis process.
- Discusses structured analytic techniques and the methods for implementing them.
- Describes unique considerations related to intelligence analysis.

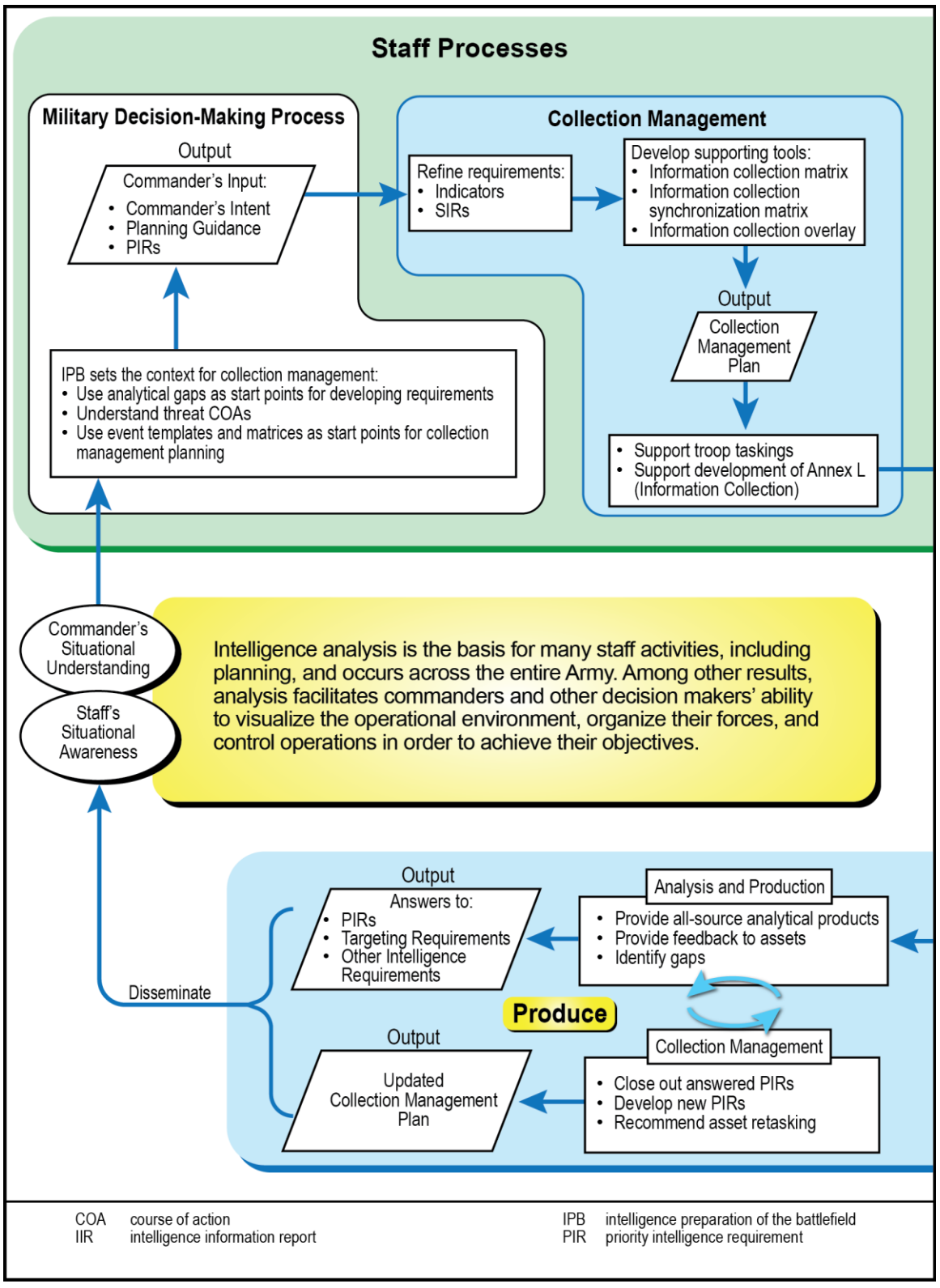
ATP 2-33.4 does not discuss—

- The Army's intelligence fundamentals and the intelligence warfighting function. See ADP 2-0 and FM 2-0 for the fundamentals.
- Techniques used to perform IPB and collection management. See ATP 2-01.3 and ATP 2-01, respectively.
- Information on how individual intelligence disciplines conduct specific tasks. See the appropriate intelligence discipline Army techniques publications.
- Specific organizational structures and manning information and specific techniques at echelons above corps, corps and divisions, and/or brigade combat teams. See classified ATP 2-19.1, ATP 2-19.3, and/or ATP 2-19.4, respectively.

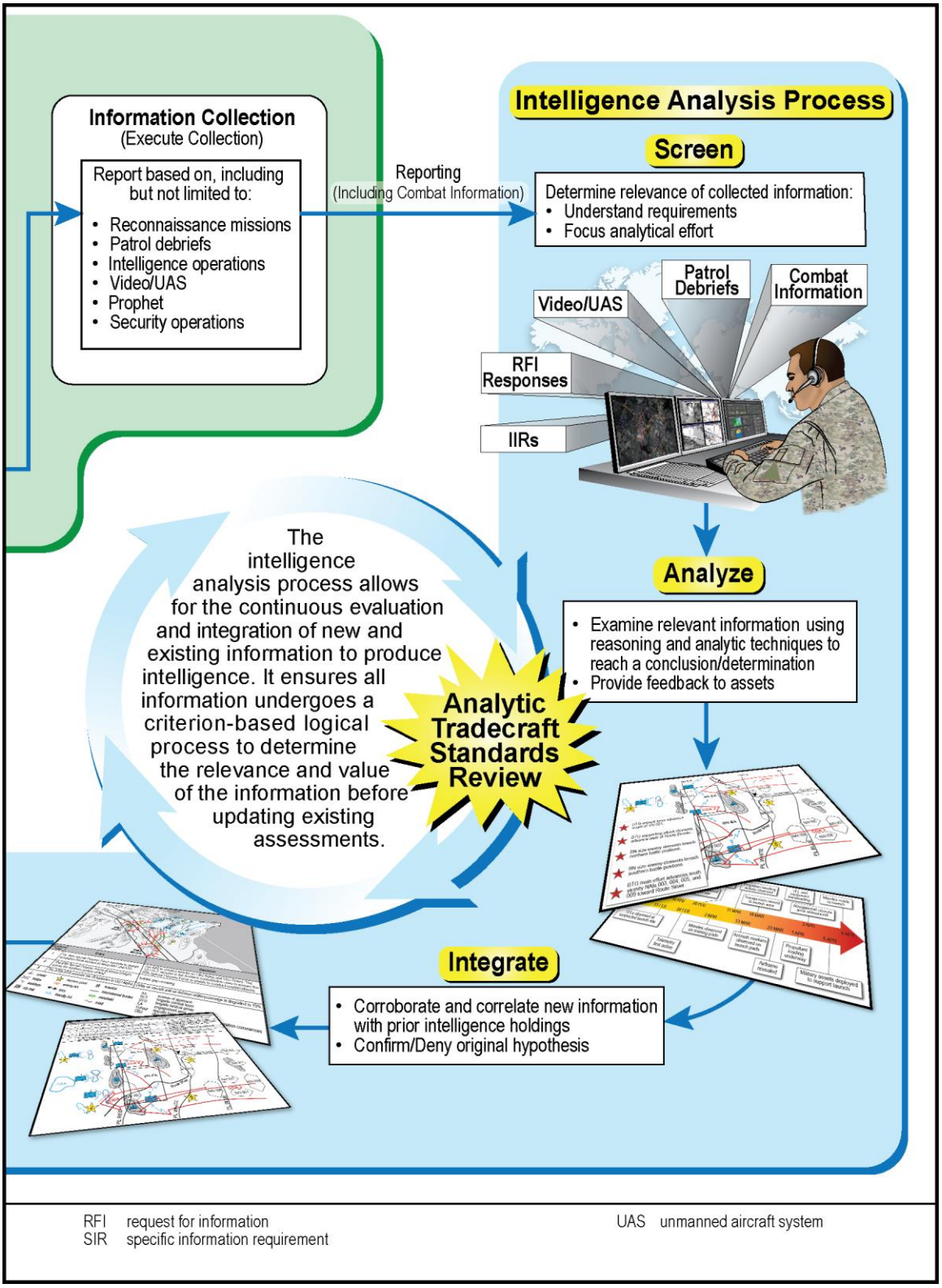
Intelligence analysis is central to intelligence. It is the basis for many staff activities, including planning, and occurs across the entire Army. Among other results, analysis facilitates commanders and other decision makers' ability to visualize the operational environment (OE), organize their forces, and control operations to achieve their objectives. To understand the role of intelligence analysis, intelligence professionals must understand how intelligence analysis corresponds with other staff processes, especially the military decision-making process and information collection (including collection management).

The introductory figure on pages xii and xiii displays the intelligence analysis process and shows how intelligence analysis fits with the other staff processes to facilitate the commander's understanding:

- The commander's initial intent, planning guidance, and priority intelligence requirements (PIRs) drive the collection management plan.
- The entire staff, led by the intelligence and operations staffs, develops the information collection plan that results in reporting.
- All-source intelligence is based on information from all intelligence disciplines, complementary intelligence capabilities, and other available sources, such as reconnaissance missions, patrol debriefs, and security operations.
- Information collected from multiple sources moves through the intelligence analysis process, resulting in intelligence.
- The intelligence staff conducts all-source analysis and produces timely, accurate, relevant, predictive, and tailored intelligence that satisfies the commander's requirements and facilitates the commander's situational understanding and the staff's situational awareness.



Introductory figure. Intelligence analysis at a glance



Introductory figure. Intelligence analysis at a glance (*continued*)

ATP 2-33.4 updates and describes the fundamentals of intelligence analysis. ATP 2-33.4 has nine chapters and six appendixes:

- **Chapter 1** provides an overview of intelligence analysis based on the Army's mission, providing intelligence professionals with the fundamentals they must understand to conduct intelligence analysis. The overview also includes the role of intelligence analysis in the Army's mission to fight for intelligence as peer threats counter information collection efforts and during large-scale ground combat operations.
- **Chapter 2** describes the intelligence analysis process (screen, analyze, integrate, and produce) and how it will be executed to answer the commander's PIRs.
- **Chapter 3** identifies and defines the all-source analytical tasks and how their application facilitates commanders and other decision makers' visualization.
- **Chapter 4** discusses intelligence analysts' use of analytic techniques and tools to solve intelligence problems and to limit analytical errors. This chapter introduces those structured analytic techniques discussed further in chapters 5 and 6.
- **Chapter 5** describes the basic and diagnostic structured analytic techniques, which improve the assessment and presentation of a finished intelligence product.
- **Chapter 6** describes those advanced structured analytic techniques required by analytic teams to prove or disapprove current or sometimes opposing analytical assessments. These techniques allow for greater absorption of alternative perspectives through cognitive processes.
- **Chapter 7** discusses how the tasks performed by intelligence analysts differ significantly based on the echelon, the supported functional element, the Army's strategic roles, and the specific mission.
- **Chapter 8** presents three tactical to operational examples that illustrate the situation a unit might encounter along the forward edge of the battle area with friendly and threat forces poised to engage in large-scale ground combat.
- **Chapter 9** discusses managing long-term analytical assessments, also referred to as analytic design, to ensure the analytical effort is properly focused and carefully planned and executed, and analytical results are communicated effectively to the requestor.
- **Appendix A** briefly describes the role of automation in enabling intelligence analysis to facilitate real-time collaboration, detailed operational planning, and support to collection management.
- **Appendix B** provides cognitive considerations for intelligence analysts, detailing basic thinking abilities, critical and creative thinking, and how to avoid analytical pitfalls—all of which when applied ensure accurate, timely, and reliable intelligence to the commander. These considerations are essential for anyone conducting analysis, but not necessarily through the intelligence analysis process.
- **Appendix C** details the Intelligence Community Analytic Standards established by Intelligence Community Directive 203, as well as the integration of the standards into Army intelligence analysis in action.
- **Appendix D** describes the threat and provides threat considerations based on threat doctrine, capabilities, and equipment that may assist intelligence analysts during large-scale ground combat operations in identifying likely threat requirements.
- **Appendix E** discusses intelligence production, specifically those reports and presentations required to support operations.
- **Appendix F** discusses how intelligence analysts support the overall targeting effort.

This publication—

- Introduces acronyms at their first use in the front matter of this publication (preface and introduction), and again in the body of the publication (chapters and appendixes).
- Uses *U.S.* as a modifier (for example, *U.S. forces*) and *United States* as a noun (for example, the *United States, a country in North America*).
- Uses *G-2/S-2* and *G-3/S-3* to denote the *division or corps/battalion or brigade intelligence staff officer* and *division or corps/battalion or brigade operations staff officer*, respectively.
- Uses the term *threat*, which includes all enemies and adversaries that are part of the OE.

PART ONE

Fundamentals

Chapter 1

Understanding Intelligence Analysis

INTELLIGENCE ANALYSIS OVERVIEW

1-1. *Analysis* is the compilation, filtering, and detailed evaluation of information to focus and understand that information better and to develop knowledge or conclusions. In accordance with ADP 6-0, *information* is, in the context of decision making, data that has been organized and processed in order to provide context for further analysis (ADP 6-0). Information generally provides some of the answers to the *who*, *what*, *where*, *when*, *why*, and *how* questions. *Knowledge* is, in the context of decision making, information that has been analyzed and evaluated for operational implications (ADP 6-0). Knowledge assists in ascribing meaning and value to the conditions or events within an operation. Analysis performed by intelligence personnel assists in building the commander's knowledge and understanding. ADP 6-0 provides an in-depth discussion on how commanders and staffs process data to progressively develop their knowledge to build and maintain their situational awareness and understanding. (See figure 1-1.)

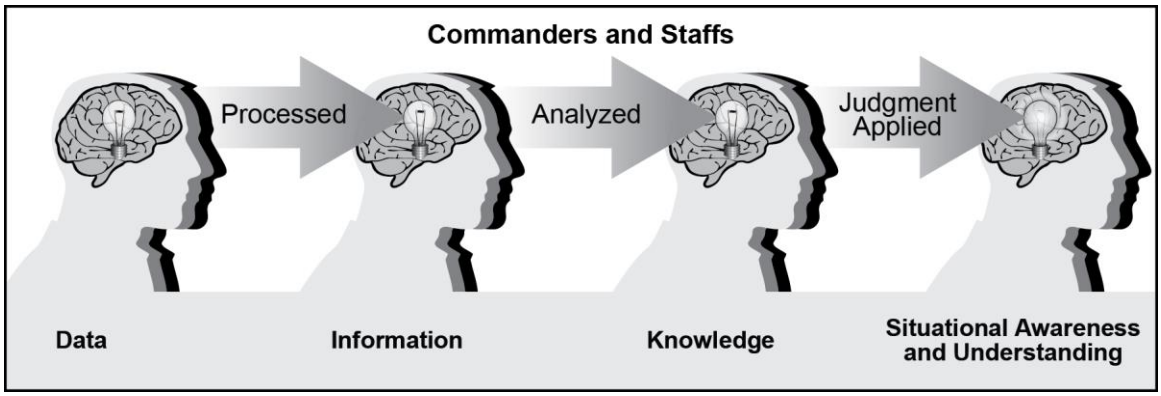


Figure 1-1. Achieving situational awareness and understanding

1-2. Analysis is the basis for many staff activities, including planning, and occurs across the entire Army. Among other results, analysis facilitates commanders and other decision makers' ability to visualize the operational environment (OE), organize their forces, and control operations in order to achieve their objectives.

1-3. Intelligence analysis is a form of analysis specific to the intelligence warfighting function. It is continuous and occurs throughout the intelligence and operations processes. *Intelligence analysis* is the process by which collected information is evaluated and integrated with existing information to facilitate intelligence production (ADP 2-0). Analysts conduct intelligence analysis to produce timely, accurate, relevant, and predictive intelligence for dissemination to the commander and staff. The purpose of intelligence analysis is to describe past, current, and attempt to predict future threat capabilities, activities, and tactics; terrain and weather conditions; and civil considerations.

1-4. Army forces compete with an adaptive enemy; therefore, perfect information collection, intelligence planning, intelligence production, and staff planning seldom occur. Information collection is not easy, and a single collection capability is not persistent and accurate enough to provide all of the answers. Intelligence analysts will be challenged to identify erroneous information and enemy deception, and commanders and staffs will sometimes have to accept the risk associated with incomplete analysis based on time and information collection constraints.

1-5. Some unique aspects of intelligence analysis include—

- The significant demand on analysts to compile and filter vast amounts of information in order to identify information relevant to the operation.
- The need for analysts to clearly separate confirmed facts from analytical determinations and assessments.
- Insight into how the physical environment (terrain, weather, and civil considerations) may affect operations.
- The ability to assess complex situations across all domains and the information environment.

1-6. Although ATP 2-33.4 is the primary publication for the intelligence analyst, it is designed to be used with ADP 2-0, *Intelligence*, and FM 2-0, *Intelligence*. ADP 2-0 discusses various aspects of intelligence analysis within a few different doctrinal constructs (see figure 1-2):

- As one of the four intelligence core competencies in chapter 2.
- As an inherent part of the steps and continuous activities of the intelligence process in chapter 3.
- As a part of or closely related to all-source intelligence, single-source intelligence capabilities, and intelligence processing, exploitation, and dissemination capabilities in chapter 4.

1-7. Intelligence analysis comprises single-source analysis and all-source analysis. ADP 2-0 discusses both single-source and all-source intelligence capabilities. As shown in figure 1-2, single-source intelligence capabilities comprise the intelligence disciplines, complementary intelligence capabilities, and multifunction intelligence units. Single-source and all-source intelligence capabilities include but are not limited to—

- Single-source analytical elements:
  - Brigade combat team (BCT) human intelligence (HUMINT) analysis cell.
  - Division signals intelligence cell.
  - Corps counterintelligence analysis cell.
  - Brigade through corps geospatial intelligence cells.
- All-source analytical elements:
  - Battalion intelligence cell.
  - Brigade intelligence support element (also known as BISE).
  - Division analysis and control element (ACE).
  - Corps ACE.
  - Theater army ACE.
  - National Ground Intelligence Center (NGIC).

Note. In this publication, all-source analytical elements include the intelligence staff for each unit as well as its supporting analytical element when applicable.

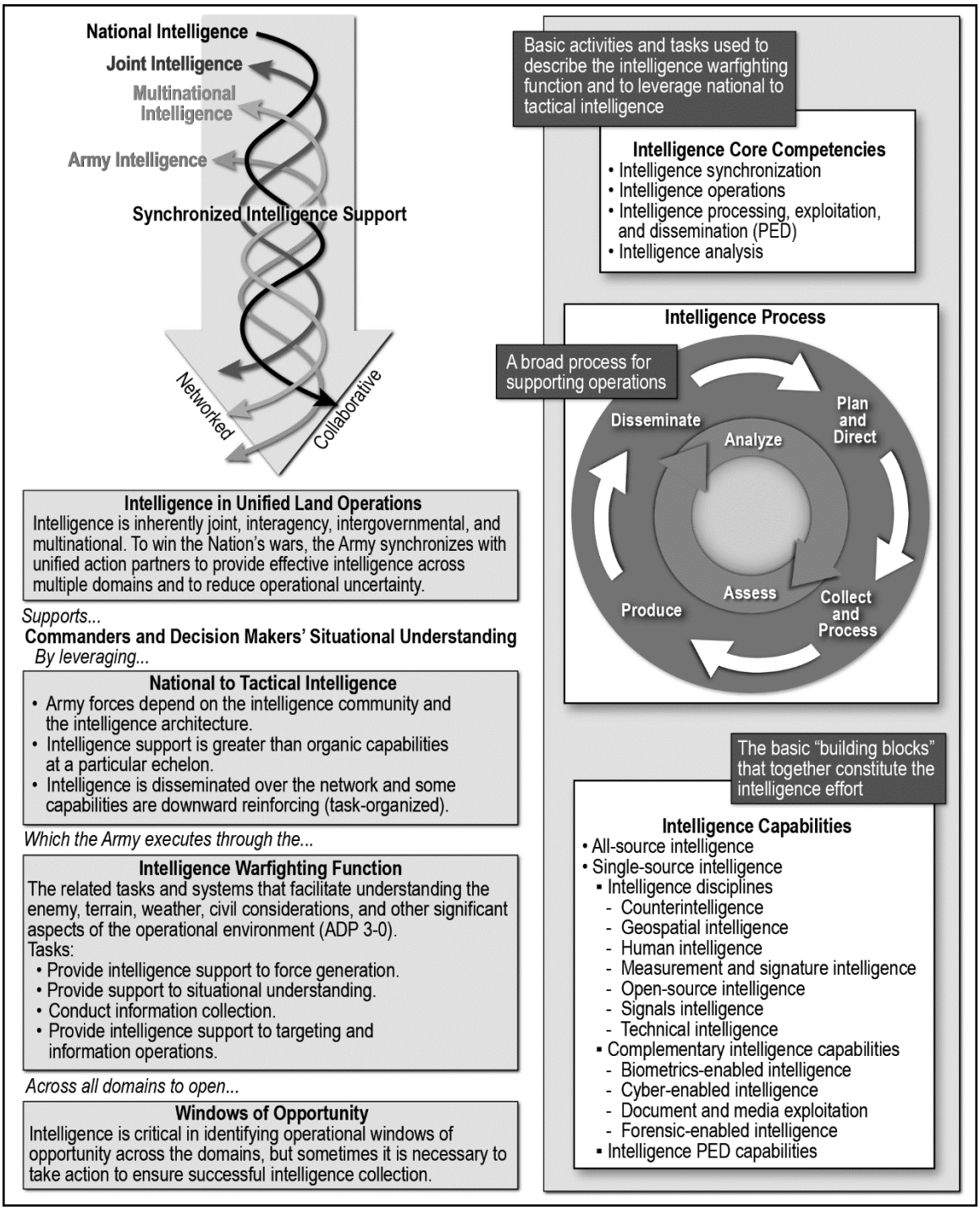


Figure 1-2. Intelligence analysis within doctrinal constructs

SINGLE-SOURCE ANALYSIS

1-8. Single-source collection is reported to single-source analytical elements. Single-source analytical elements conduct continuous analysis of the information provided by single-source operations. Following single-source analysis, analytical results are disseminated to all-source analytical elements for corroboration, to update the common operational picture, and to refine all-source intelligence products. A continuous analytical feedback loop occurs between all-source analytical elements, single-source analytical elements, and collectors to ensure effective intelligence analysis. Figure 1-3 provides a simplified example of this single-source to all-source information flow for HUMINT reporting and analysis at the BCT level.

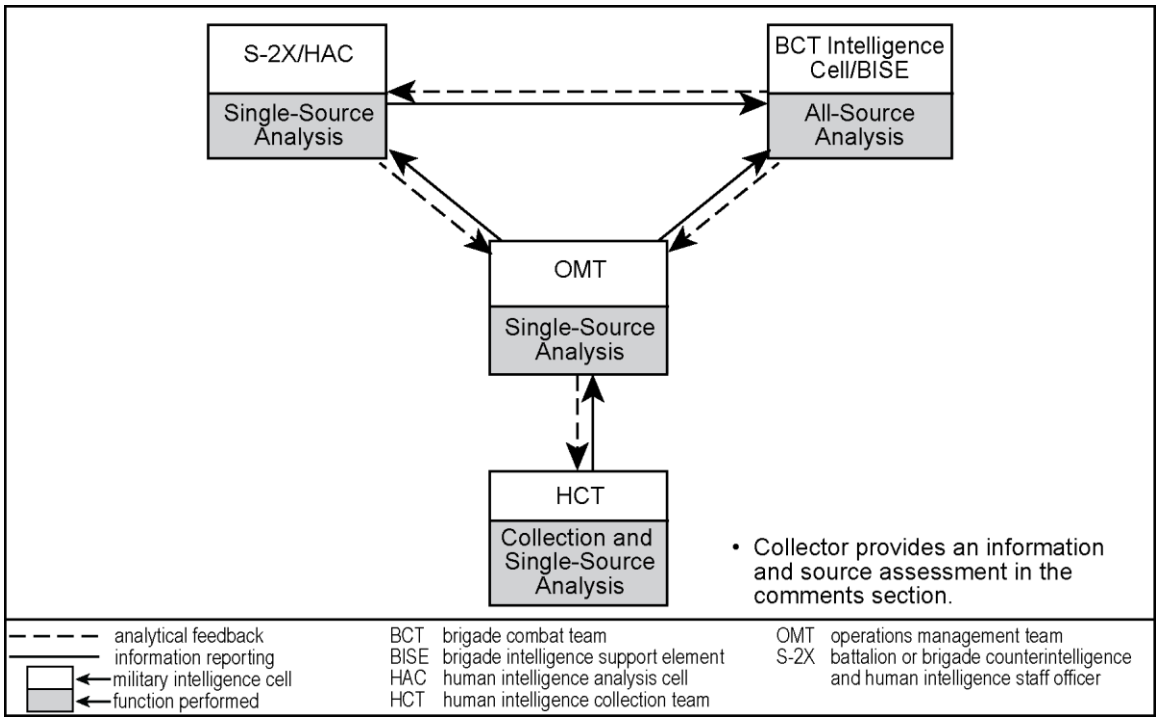


Figure 1-3. Information and intelligence reporting example

1-9. Several portions of this publication apply to single-source analysis, especially the intelligence analysis process in chapter 2 and the analytic techniques in chapters 4 through 6. Specific doctrine on single-source analysis is contained in the following publications:

- Intelligence disciplines:
  - For counterintelligence analysis, see ATP 2-22.2-1, *Counterintelligence Volume I: Investigations, Analysis and Production, and Technical Services and Support Activities*, chapter 4.
  - For HUMINT analysis, see FM 2-22.3, *Human Intelligence Collector Operations*, chapter 12.
  - For open-source intelligence analysis, see ATP 2-22.9, *Open-Source Intelligence*, chapters 1, 2, and 3.
  - For signals intelligence analysis, see ATP 2-22.6-2, *Signals Intelligence Volume II: Reference Guide*, appendix G.
- Complementary intelligence capabilities:
  - For biometrics-enabled intelligence analysis (the foundation of identity intelligence), see ATP 2-22.82, *Biometrics-Enabled Intelligence*, chapter 7.
  - For document and media exploitation (DOMEX) analysis, see ATP 2-91.8, *Techniques for Document and Media Exploitation*, chapter 9.

ALL-SOURCE ANALYSIS AND PRODUCTION

1-10. Various all-source analytical elements integrate intelligence and information from all relevant sources (both single-source and other information collection sources) to provide the most timely, accurate, relevant, and comprehensive intelligence possible and to overcome threat camouflage, counterreconnaissance, and deception. All-source analytical elements, such as the brigade intelligence support element or ACE, are functionally aligned to support the commander and the intelligence staff. The intelligence staff is integrated with the rest of the staff to ensure they have a thorough understanding of the overall operation, the current situation, and future operations. Additionally, all-source analytical elements often corroborate their analytical determinations and intelligence products through access to and collaboration with higher, lower, and adjacent all-source analytical elements.

1-11. All-source intelligence analysts use an array of automation and other systems to perform their mission. (See appendix A.) From a technical perspective, all-source analysis is accomplished through the fusion of single-source information with existing intelligence in order to produce intelligence. For Army purposes, *fusion* is consolidating, combining, and correlating information together (ADP 2-0). Fusion occurs as an iterative activity to refine information as an integral part of all-source analysis and production.

1-12. With the vast amounts of information and broad array of all-source intelligence capabilities, the G-2/S-2 provides the commander and staff with all-source intelligence. All-source intelligence products inform the commander and staff by facilitating situational understanding, supporting the development of plans and orders, and answering priority intelligence requirements (PIRs), high-payoff targets (HPTs), and other information requirements.

1-13. The G-2/S-2 can use single-source intelligence to support the commander and staff. In those instances, it is best to first send that single-source intelligence to the all-source analytical element to attempt to quickly corroborate the information. Corroboration reduces the risk associated with using that single-source intelligence by comparing it to other information reporting and existing intelligence products. Following corroboration and dissemination of the intelligence to the commander and staff, the all-source analytical element incorporates the single-source intelligence into the various all-source intelligence products and the threat portion of the common operational picture.

1-14. In certain situations and specific organizations, especially at echelons above corps, a single-source analytical element can produce single-source intelligence products for dissemination to the commander and staff without all-source corroboration. However, there is significant risk in using uncorroborated single-source intelligence at the tactical level. For example, a BCT commander may choose to make decisions based on a single HUMINT report. This is similar to the commander using combat information to make decisions during an operation. In those situations, the commander and G-2/S-2 should be aware of and try to mitigate the risk associated with using uncorroborated single-source reporting and intelligence.

Note. *Combat information* is unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements (JP 2-01).

CONDUCTING INTELLIGENCE ANALYSIS

1-15. The goal of intelligence analysis is to provide timely and relevant intelligence to commanders and leaders to support their decision making. Intelligence analysis requires the continuous examination of information and intelligence about the threat and significant aspects of the OE. To be effective, an intelligence analyst must—

- Understand and keep abreast of intelligence doctrine.
- Maintain complete familiarity on all aspects of the threat, including threat capabilities, doctrine, and operations.

- Have knowledge on how to account for the effects of the mission variables (mission, enemy, terrain and weather, troops and support available, time available, and civil considerations [METT-TC]) and operational variables (political, military, economic, social, information, infrastructure, physical environment, and time [PMESII-PT]) on operations.
- Thoroughly understand operational doctrine (especially FM 3-0, *Operations*), operational and targeting terminology, and operational symbology.

1-16. Analysts conduct intelligence analysis to ultimately develop effective intelligence. They do this by applying the basic thinking abilities (information ordering, pattern recognition, and reasoning) and critical and creative thinking, all described in appendix B. FM 2-0 describes the characteristics of effective intelligence as accurate, timely, usable, complete, precise, reliable, relevant, predictive, and tailored. Beyond those characteristics, intelligence analysts must also understand the six aspects of effective analysis:

- Embracing ambiguity.
- Understanding intelligence analysis is imperfect.
- Meeting analytical deadlines with the best intelligence possible.
- Thinking critically.
- Striving to collaborate closely with other analysts.
- Adhering to analytic standards as much as possible.

EMBRACING AMBIGUITY

1-17. Intelligence personnel must accept and embrace ambiguity in conducting analysis as they will never have all the information necessary to make certain analytical determinations. Intelligence analysts will be challenged due to the constantly changing nature of the OE and the threat and to the fog of war—all imposed during large-scale ground combat operations, creating complex, chaotic, and uncertain conditions. Intelligence analysts must understand the OE is complex; embrace ambiguity; and recognize and mitigate their own or others' biases, challenge their assumptions, and continually learn while conducting analysis across the breadth of operations.

1-18. Analysts operate within a time-constrained environment and with limited information. Therefore, they may sometimes produce intelligence that is not as accurate and detailed as they would prefer. Having both an adequate amount of information and extensive subject matter expertise does not guarantee the development of logical or accurate determinations. To be effective, analysts must have—

- A detailed awareness of their commander's requirements and priorities.
- An understanding of the limitations in information collection and intelligence analysis.
- A thorough knowledge of the OE and all aspects of the threat.
- Expertise in applying the intelligence analysis process and analytic techniques.

1-19. The effective combination of the aforementioned bullets provides intelligence analysts with the best chance to produce accurate and predictive intelligence and also to detect threat denial and deception efforts. To adequately account for complexity and ambiguity, intelligence analysts should continually identify gaps in their understanding of the OE and the threat, and factor in those gaps when conducting intelligence analysis.

ANALYTICAL IMPERFECTION

1-20. Given the ambiguity, fog of war, and time-constraints, intelligence analysts must accept imperfection. As much as possible, analysts should attempt to use validated facts, advanced analytic techniques, and objective analytical means. However, using them and providing completely objective and detailed analytical determinations may be challenging, especially during tactical operations. Analysts should also consider that logical determinations are not necessarily facts.

1-21. When presenting analytical determinations to the commander and staff, intelligence personnel must ensure they can answer the *so what* question from the commander's perspective. Additionally, they should clearly differentiate between what is relatively certain, what are reasonable assumptions, and what is unknown, and then provide the degree of confidence they have in their determination as well as any significant issues associated with their analysis. This confidence level is normally subjective and based on—

- The collection asset's capability (reliability and accuracy).
- Evaluation criteria.
- The confidence in the collected data.
- The analyst's expertise and experience.
- Intelligence gaps.
- The possibility of threat deception.

1-22. Intelligence analysts should be prepared to explain and justify their conclusions to the commander and staff. Over time, the all-source analytical element should learn the most effective way to present analytical determinations to the commander and staff. A deliberate and honest statement of what is relatively certain and what is unknown assists the commander and staff in weighing some of the risks inherent in the operation and in creating mitigation measures.

MEETING ANALYTICAL DEADLINES

1-23. Analysts must gear their efforts to the time available and provide the best possible intelligence within the deadline. Operational planning and execution deadlines often impose challenging time constraints that analysts must meet. Analysts must often produce intelligence without all of the information that would result in a more thorough or certain analytical determination. Analysts must meet the deadline because a quick analytical assessment in time to affect staff planning and friendly courses of action (COAs) is far better than a perfect analytical assessment that is received too late to affect staff planning.

CRITICAL THINKING

1-24. Intelligence analysts must know how to arrive at logical, well-reasoned, and unbiased conclusions as a part of their analysis. Analysts strive to reach determinations based on facts and reasonable assumptions. Therefore, critical thinking is essential to analysis. Using critical thinking, which is disciplined and self-reflective, provides more holistic, logical, ethical, and unbiased analyses and determinations. Applying critical thinking assists analysts in fully accounting for the elements of thought, the intellectual standards, and the traits of a critical thinker. (See appendix B for information on critical and creative thinking.)

COLLABORATION

1-25. Commanders, intelligence and other staffs, and intelligence analysts must collaborate. They should actively share and question information, perceptions, and ideas to better understand situations and produce intelligence. Collaboration is essential to analysis; it ensures analysts work together to achieve a common goal effectively and efficiently. Analysts can leverage national to tactical intelligence, using Department of Defense (DOD) intelligence capabilities, to enable analytical collaboration and assist them in producing intelligence.

1-26. Through collaboration, analysts develop and enhance professional relationships, access each other's expertise, enhance their understanding of the issues, and expand their perspectives on critical analytical issues. Collaboration is another means, besides critical thinking, by which intelligence analysts avoid potential pitfalls, such as mindsets and biases, and detect threat denial and deception efforts. (For information on analytical pitfalls, see appendix B.)

ADHERING TO ANALYTIC STANDARDS

1-27. As much as possible, the conclusions reached during intelligence analysis should adhere to analytic standards, such as those established by the Director of National Intelligence in Intelligence Community Directive (ICD) 203, to determine the relevance and value of the information before updating existing assessments. (See figure 1-4 on page 1-8.) These standards govern the production and evaluation of national intelligence analysis to meet the highest standards of integrity and rigorous analytic thinking. Although created for national-level intelligence agencies, these analytic standards are also valid at the operational and tactical levels. (See appendix C for a detailed discussion of the analytic standards.)

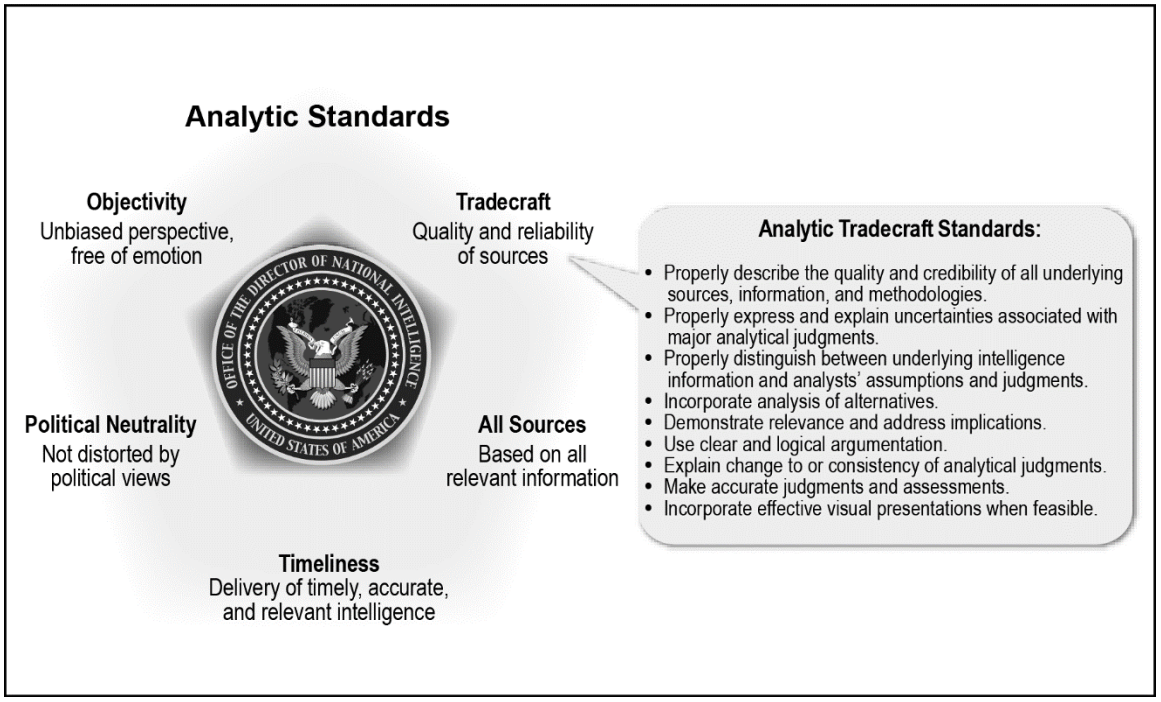


Figure 1-4. Analytic standards

INTELLIGENCE ANALYSIS AND COLLECTION MANAGEMENT

1-28. While collection management is not part of intelligence analysis, it is closely related. Analysis occurs inherently throughout collection management, and intelligence analysts must understand the information collection plan.

1-29. Collection management is a part of the larger information collection effort. Information collection is an integrated intelligence and operations function. ATP 2-01 discusses collection management in detail. The intelligence staff performs the collection management process in collaboration with the operations staff. The collection management process comprises the following tasks:

- Develop requirements.
- Develop the collection management plan.
- Support tasking and directing.
- Assess collection.
- Update the collection management plan.

Note. *Plan requirements and assess collection*, as an information collection task, has been replaced with the term *collection management*.

1-30. The intelligence warfighting function focuses on answering commander and staff requirements, especially PIRs, which are part of the commander's critical information requirements. Intelligence analysis for a particular mission begins with information collected based on commander and staff requirements (which are part of collection management); those requirements are usually developed within the context of existing intelligence analysis. Together, these two activities form a continuous cycle—intelligence analysis supports collection management and collection management supports intelligence analysis. The G-2/S-2 must synchronize these two activities, and analysts and personnel within both activities must cooperate and collaborate closely to enable effective intelligence support.

1-31. Intelligence analysis and collection management overlap or intersect in several areas. While not all inclusive, the following includes some of these areas:

- The all-source intelligence architecture and analysis across the echelons are important aspects of planning effective information collection. To answer the PIR and present the commander and staff with a tailored intelligence product, there must be adequate time. Collection management personnel must understand the all-source intelligence architecture and analysis across the echelons and consider those timelines.
- Collection management personnel depend on the intelligence analysis of threats, terrain and weather, and civil considerations in order to perform the collection management process. Intelligence preparation of the battlefield (IPB) often sets the context for collection management:
  - Intelligence analytical gaps are the start points for developing requirements.
  - All-source analysts and collection management personnel must understand the threat COAs and how to execute those COAs as reflected in the situation templates.
  - Event templates and event matrices are the start points for developing subsequent collection management tools.
- All-source analysts and collection management personnel—
  - Use and refine threat indicators during the course of an operation.
  - Mutually support and track threat activities relative to the *decide*, *detect*, *deliver*, and *assess* (also called D3A) functions of the targeting methodology.
  - Must confer before answering and closing a PIR.
- The effectiveness of intelligence analysis is an integral part of assessing the effectiveness of the information collection plan during collection management.

1-32. A disconnect between intelligence analysis and collection management can cause significant issues, including a degradation in the overall effectiveness of intelligence support to the commander and staff. Therefore, intelligence analysts and collection management personnel must collaborate closely to ensure they understand PIRs, targeting and information operations requirements (when not expressed as PIRs), threat COAs and other IPB outputs, the current situation, and the context/determinations surrounding current threat activities.

THE ALL-SOURCE INTELLIGENCE ARCHITECTURE AND ANALYSIS ACROSS THE ECHELONS

1-33. All-source analysis, collaboration, and intelligence production occur both within and between echelons. Intelligence analysts not only integrate the broad array of information collected and intelligence produced at their echelon, but they also collaborate across the various echelons and the intelligence community to benefit from the different knowledge, judgments, experience, expertise, and perceptions—all invaluable to the analytical effort. Intelligence analysis is facilitated by an all-source push (deliberately sending) and pull (accessing from a different unit) of information and intelligence. Figure 1-5 on page 1-10 depicts single-source collection and analysis as a layer of the all-source intelligence architecture across the echelons. Chapter 7 details intelligence analysis across the echelons.

1-34. At the different echelons, based on a number of factors, the intelligence staff and supporting all-source analytical element are divided into teams to support the various command posts and to perform the various all-source analytical tasks. There is no standard template on how best to structure the all-source analytical effort. The G-2/S-2 decides on an all-source structure that is optimized to support command and control and is requirements-driven based on ongoing operations.

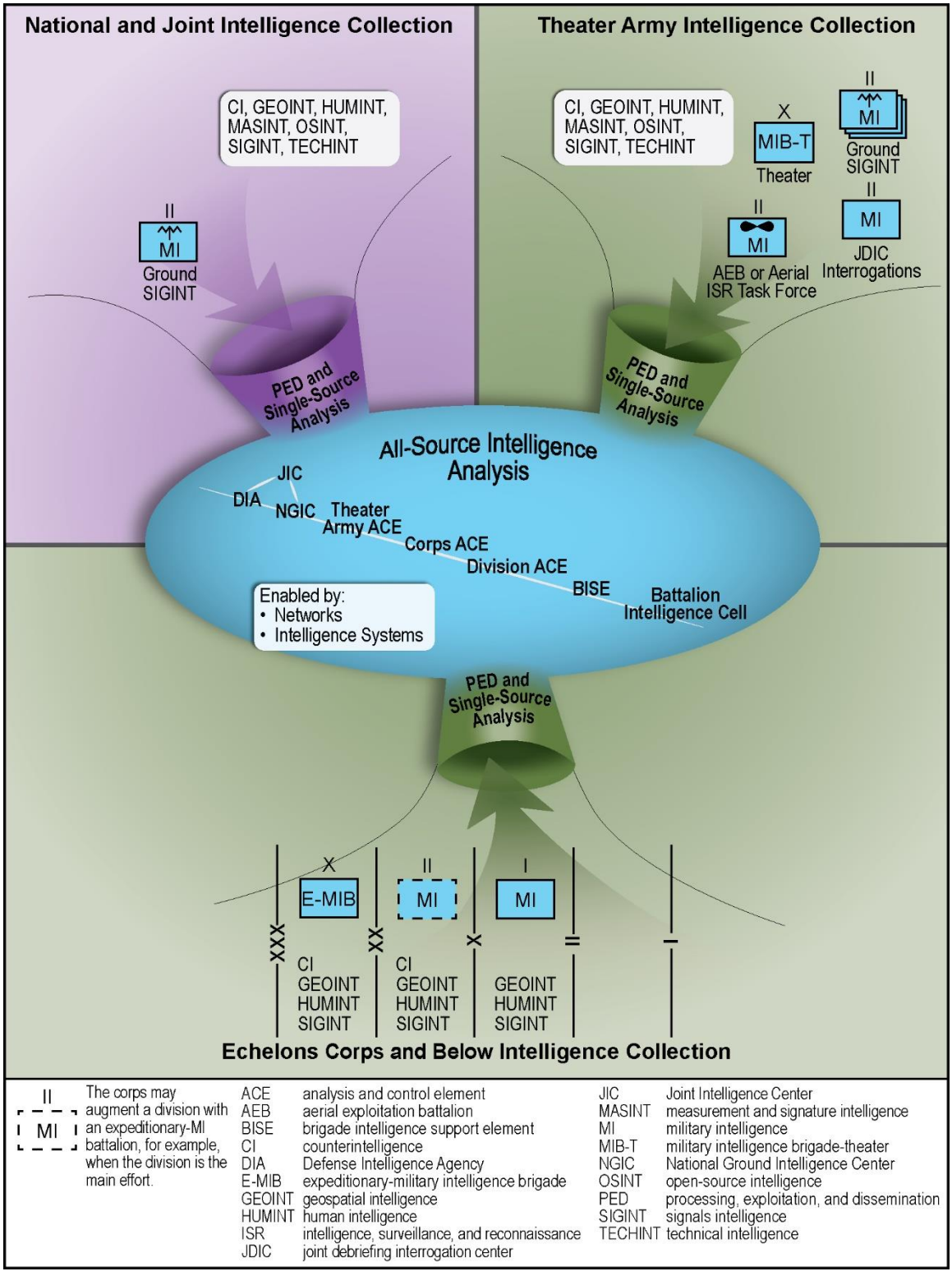


Figure 1-5. All-source analysis across the echelons

INTELLIGENCE ANALYSIS DURING LARGE-SCALE GROUND COMBAT OPERATIONS

1-35. FM 3-0, published in October 2017, provided a new operational focus for the Army and introduced the Army's strategic roles (shape OEs, prevent conflict, prevail in large-scale ground combat, and consolidate gains). FM 3-0 clearly states that while Army forces cannot focus solely on large-scale ground combat operations at the expense of other missions, Army forces cannot afford to be unprepared for large-scale combat operations in an increasingly unstable world. ADP 2-0, published in July 2019, and FM 2-0, published in July 2018, reinforce this focus, providing extensive discussions on intelligence within large-scale ground combat operations.

1-36. ADP 3-0, *Operations*, published in July 2019, provided a definition for large-scale combat operations and created a new term, large-scale ground combat operations. *Large-scale combat operations* are extensive joint combat operations in terms of scope and size of forces committed, conducted as a campaign aimed at achieving operational and strategic objectives (ADP 3-0). *Large-scale ground combat operations* are sustained combat operations involving multiple corps and divisions (ADP 3-0).

1-37. While the fundamentals of intelligence analysis remain constant across the Army's strategic roles, large-scale ground combat operations create some unique challenges for the intelligence analyst. (See table 1-1.) The fluid and chaotic nature of large-scale ground combat operations will cause the greatest degree of fog, friction, uncertainty, and stress on the intelligence analysis effort. Army forces will have to fight for intelligence as peer threats will counter information collection efforts, forcing commanders to make decisions with incomplete and imperfect intelligence. These realities will strain all-source analysis.

Table 1-1. Intelligence analysis during large-scale ground combat operations

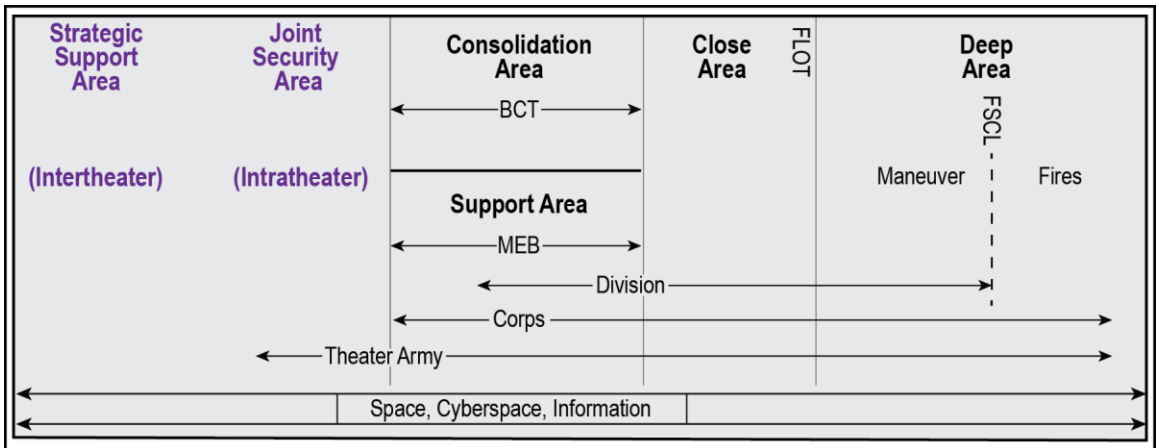
Army strategic role	*Intelligence analysis support*
Prevail in large-scale ground combat	Analysts— • Perform intelligence preparation of the battlefield as part of the military decision-making process to support deployment into a theater of operations. • While collecting and screening information, immediately report relevant combat information to the commander. • Ensure all analysis efforts support the unit commander's intent and guidance, established during the military decision-making process. • Continually update the running estimates and disseminate products to commanders and staffs. • Support current operations—integrate information by updating the common operational picture and continually communicating with other staff sections. • Support target development and detection by ensuring collection plans support the overall targeting plan.

1-38. Over the past 20 years, the Nation's peer threats have increased their capabilities and gained an understanding of United States (U.S.) and allied operations. According to ADP 3-0, a peer threat is an adversary or enemy able to effectively oppose U.S. forces worldwide while enjoying a position of relative advantage in a specific region. Peer threats—

- Can generate equal or temporarily superior combat power in geographical proximity to a conflict area with U.S. forces.
- May have a cultural affinity to specific regions, providing them relative advantages in terms of time, space, and sanctuary.
- Generate tactical, operational, and strategic challenges in order of magnitude more challenging militarily than other adversaries.
- Can employ resources across multiple domains to create lethal and nonlethal effects with operational significance throughout an OE.
- Seek to delay deployment of U.S. forces and inflict significant damage across multiple domains in a short period to achieve their goals before culminating.

1-39. During large-scale ground combat operations, intelligence analysts will have to predict and track rapidly evolving events across the various threat capabilities. (See appendix D.) For this reason, intelligence analysts must understand many of the operational concepts discussed in FM 3-0 and discussed from an intelligence perspective in FM 2-0. These doctrinal concepts include—

- **Multi-domain operations**, including **windows of opportunity**, discussed in FM 3-0, chapter 1, and FM 2-0, chapter 1.
- **Positions of relative advantage**, discussed in FM 3-0, chapter 1.
- **Operational art**, discussed in ADP 3-0, chapter 2, and FM 3-0, chapter 1.
- The new **operational framework**, discussed in FM 3-0, chapter 1, and FM 2-0, chapter 1.
- The new **key physical aspects of the operational framework**, discussed in FM 2-0, chapter 1. (See figure 1-6.)
- **Fighting for intelligence**, discussed in FM 3-0, chapter 2, and FM 2-0, chapter 6.



The strategic support area describes the area extending from a theater of operations to a continental United States base, or another combatant commander's area of responsibility, that contains those organizations, LOCs, and other agencies required in the field. It includes the air and seaports supporting the flow of forces and sustainment into the theater.	The joint security area is a specific surface area, designated by the joint force commander, to facilitate protection of joint bases and their connecting LOCs that support joint operations.	The consolidation area is the portion of the commander's AO that is designated to facilitate the security and stability tasks necessary for freedom of action in the close area and to support the continuous consolidation of gains. The support area is the portion of the commander's AO that is designated to facilitate the positioning, employment, and protection of the base sustainment assets required to sustain, enable, and control operations.	The close area is the portion of a commander's AO assigned to subordinate maneuver forces.	The deep area is the portion of the commander's AO that is not assigned to subordinate units. The deep area is divided into — • Deep area (maneuver): The zone between the FLOT and the FSCL is typically the area over which friendly ground forces intend to maneuver in the near future and is also the area where joint air interdiction operations are normally executed through the air support operations center/direct air support center. • Deep area (fires): Interdiction best describes how Army and joint fires are typically employed in the deep area. *Interdiction* is an action to divert, disrupt, delay, or destroy the enemy's military surface capability before it can be used effectively against friendly forces, or to otherwise achieve objectives (JP 3-03).

AO	area of operations	FLOT	forward line of own troops	LOC	line of communications
BCT	brigade combat team	FSCL	fire support coordination line	MEB	maneuver enhancement brigade

Figure 1-6. Key aspects of the operational framework

1-40. As in all operations, intelligence drives operations and operations support intelligence; this relationship is continuous. The commander and staff need effective intelligence in order to understand threat centers of gravity, goals and objectives, and COAs. Precise intelligence is also critical to target threat capabilities at the right time and place and to open windows of opportunity across domains. Commanders and staffs must have detailed knowledge of threat strengths, weaknesses, equipment, and tactics to plan for and execute friendly operations.

1-41. Commanders and staffs accept some risks and operational uncertainty in all operations, especially during large-scale ground combat operations. The commander must allocate adequate time for information collection and intelligence analysis or determine the balance between time allotted to collection and analysis and to operational necessity. When there is not enough time for adequate information collection and intelligence analysis, the all-source analytical element must inform the G-2/S-2 of the gaps, issues, and risks, so the G-2/S-2 can inform the commander. In those cases, that unit must depend on the higher echelon all-source analytical element for additional support and overwatch.

1-42. One of the ultimate goals of intelligence analysis is to assist the unit in identifying and opening an operational window of opportunity to eventually achieve a position of relative advantage. Opening a window of opportunity often requires a significant amount of intelligence analysis in order to achieve a high degree of situational understanding. This will be difficult as friendly forces are often at a disadvantage in conducting information collection against the threat. Therefore, opening an operational window of opportunity may have to start with operations that support intelligence. In a sense, this is opening an information collection window of opportunity as part of the effort to fight for intelligence.

1-43. The staff must thoroughly plan, find creative solutions, and collaborate across echelons to overcome information collection challenges. Once friendly forces have an open window of opportunity to execute information collection, intelligence analysts will receive more information and should be able to provide timely and accurate intelligence products, updates, and predictive assessments. This timely and accurate intelligence can then assist friendly forces in opening subsequent windows of opportunity to reach positions of relative advantage.

1-44. Facilitating the commander and staff's situational understanding of the various significant aspects of the OE is challenging. Intelligence analysis must address important considerations across all domains and the information environment as well as support multi-domain operations. Intelligence analysis must include all significant operational aspects of the interrelationship of the air, land, maritime, space, and cyberspace domains; the information environment; and the electromagnetic spectrum. Intelligence analysts use information and intelligence from the joint force, U.S. Government, the intelligence community, and allies to better understand and analyze the various domains and peer threat capabilities.

INTELLIGENCE ANALYSIS DURING THE ARMY'S OTHER STRATEGIC ROLES

1-45. As part of a joint force, the Army operates across the strategic roles (shape OEs, prevent conflict, prevail in large-scale ground combat, and consolidate gains) to accomplish its mission to organize, equip, and train its forces to conduct sustained land combat to defeat enemy ground forces and to seize, occupy, and defend land areas. The unique aspects of large-scale ground combat operations were discussed in paragraphs 1-35 through 1-44. Each strategic role presents unique challenges and is often characterized by different analytical tasks, products, product timelines, and specific requirements. (See table 1-2 on page 1-14.)

Table 1-2. Intelligence analysis during the other Army strategic roles

Army strategic role	*Intelligence analysis support*
Shape operational environments	Analysts— • During periods of peace, identify peer threats or hostile element actions in regionally significant areas. This includes supporting contingency planning. • Develop regional expertise and generate intelligence knowledge for possible contingencies. • Provide warning intelligence at echelons above corps. • Identify second and third order effects of all friendly actions based on the operational variables (political, military, economic, social, information, infrastructure, physical environment, and time). • Assist with security force assistance and theater engagement efforts and, when possible, in building an initial allied intelligence analysis architecture. • Support realistic training to improve regional awareness of potential peer threat capabilities and hybrid scenarios. • Conduct focused analysis as regional tensions increase and update operation plans as required.
Prevent conflict	
Consolidate gains	Analysts— • Assess the operational environment and identify how the local population reacts to stability operations. • Use diagnostic structured analytic techniques (see chapter 4) to compare their original estimates of the operational environment and identify changes that may affect stability operations. • Assess operational considerations for improvements to transition control to legitimate civil authorities.

Chapter 2

The Intelligence Analysis Process

OVERVIEW

2-1. Both all-source and single-source intelligence analysts use the intelligence analysis process. The process supports the continuous examination of information, intelligence, and knowledge about the OE and the threat to generate intelligence and reach one or more conclusions. Appendix B provides an overview of three analytic skills: basic thinking abilities, critical and creative thinking, and avoiding analytical pitfalls. Chapters 4 through 6 provide analytic techniques for conducting qualitative analysis. The application of the analytic skills and techniques assist analysts in evaluating specific situations, conditions, entities, areas, devices, or problems.

2-2. The intelligence analysis process includes the continuous evaluation and integration of new and existing information to produce intelligence. It ensures all information undergoes a criterion-based logical process, such as the analytic tradecraft standards established by ICD 203, to determine the relevance and value of the information before updating existing assessments. (See appendix C for a detailed discussion on the analytic tradecraft standards.)

2-3. The intelligence analysis process is flexible and applies to any intelligence discipline. Analysts may execute the intelligence analysis process meticulously by thoroughly screening information and applying analytic techniques, or they may truncate the process by quickly screening collected information using only basic structured analytic techniques. The process becomes intuitive as analysts become more proficient at analysis and understanding their assigned OE. The intelligence analyst uses collected information to formulate reliable and accurate assessments.

THE PHASES OF THE INTELLIGENCE ANALYSIS PROCESS

2-4. The phases of the intelligence analysis process are interdependent. (See figure 2-1 on page 2-2.) Through time and experience, analysts become more aware of this interdependence. The phases of the intelligence analysis process are—

- **Screen (collected information):** Determining the relevance of the information collected.
- **Analyze:** Examining relevant information.
- **Integrate:** Combining new information with current intelligence holdings to begin the effort of developing a conclusion or assessment.
- **Produce:** Making a determination or assessment that can be disseminated to consumers.

Note. *Relevant information* is all information of importance to the commander and staff in the exercise of command and control (ADP 6-0).

2-5. To successfully execute the intelligence analysis process, it is critical for analysts to understand the PIRs and other requirements related to the current OE and mission. This understanding assists analysts in framing the analytic problem and enables them to separate facts and analytical judgments. Analytical judgments form by generating hypotheses—preliminary explanations meant to be tested to gain insight and find the best answer to a question of judgment. (See chapter 6 for more on generating hypotheses.)

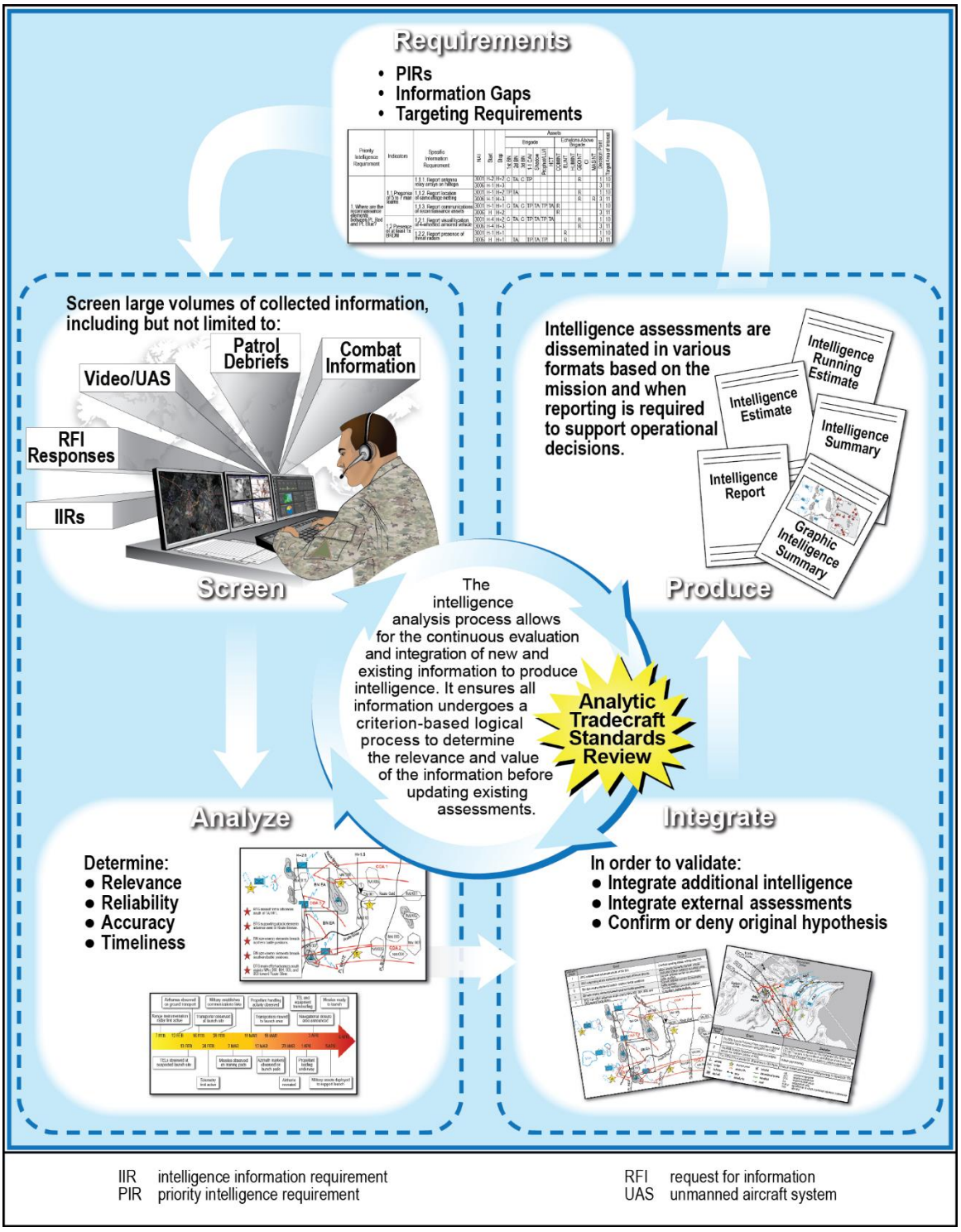


Figure 2-1. The intelligence analysis process

2-6. The following begins a series of examples that walk the reader through the intelligence analysis process from the reporting of requirements to the production and dissemination of intelligence to the commander and staff.

Example: Division Commander's PIRs

PIR 1: Will the motorized rifle division use the tank brigade as a southward exploitation force?

PIR 2: Where is the motorized rifle division's multiple launch rocket system (MLRS) battalion?

PIR 3: Where will displaced civilians impede U.S. combat forces' movement north?

Collection in the past hour provided six pieces of information for analysts to process and answer the commander's PIRs:

- Possible identification of two threat MLRSs as well as support equipment traveling west to east at 20 kilometers per hour along a road 15 kilometers north of the 1 BCT forward locations.
- Threat motorized rifle battalion in company strength engaging adjacent 2 BCT forward positions attempting to seize a hilltop out of sector at a (PK1234) general four-digit grid.
- The 1 BCT reports harassing small arms engagements along forward battalion locations.
- Approximately 28 or 30 threat tanks detected in convoy formations 40 kilometers north of the 1 BCT forward locations.
- Threat air defense elements active near possible headquarters and artillery locations detected.
- Multiple-source reporting that a threat tank brigade is preparing to advance south, seeking to exploit lead division penetration of 1 BCT forward positions.

SCREEN COLLECTED INFORMATION

2-7. During the execution of single-source intelligence or all-source analysis, analysts continuously filter the volume of information or intelligence received through the continuous push and pull of information. It is during the *screen* phase that analysts sort information based on relevancy and how it ties to the analytical questions or hypotheses they developed to fill information gaps. They do this by conducting research and accessing only the information that is relevant to their PIRs, mission, or time. Analysts also screen the volume of information based on the information source's reliability and the information accuracy, as explained in paragraphs 2-12 through 2-15.

2-8. Time permitting, analysts research by accessing information and intelligence from databases, the internet (attributed to open-source information), collaborative tools, broadcast services, and other sources such as automated systems. This screening enables analysts to focus their analytical efforts on only the information that is pertinent to their specific analytic problem. (See ATP 2-22.9 for more information on open-source information; see appendix A for more information on automated systems.)

Note. The relevancy of the information may change as the situation changes. For example, analysts may want to focus their analysis on information not older than 45 days about an armored division in garrison; however, this information may quickly become irrelevant as time elapses and the tactical situation changes.

Example: Screen

Upon screening the six pieces of information in response to collection requirements supporting PIRs 1 and 2, intelligence analysts focused on tank and MLRS/artillery activities. They kept four and discarded two of the pieces of information:

- **Keep for further analysis:** Possible identification of two threat MLRSs as well as support equipment traveling west to east at 20 kilometers per hour along a road 15 kilometers north of the 1 BCT forward locations.
- **Discard:** Threat motorized rifle battalion in company strength engaging adjacent 2 BCT forward positions attempting to seize a hilltop out of sector at a general four-digit grid.
- **Discard:** The 1 BCT reports harassing small arm engagements along forward battalion locations. (It does not relate to the PIRs.)
- **Keep for further analysis:** Approximately 28 or 30 threat tanks detected in convoy formations 40 kilometers north of the 1 BCT forward locations.
- **Keep for further analysis:** Threat air defense artillery elements active near possible headquarters and artillery locations detected.
- **Keep for further analysis:** Multiple-source reporting that a threat tank brigade is preparing to advance south, seeking to exploit lead division penetration of 1 BCT forward positions.

ANALYZE

2-9. Analysts examine relevant information or intelligence using reasoning and analytic techniques, which enable them to see information in different ways and to reveal something new or unexpected. It may be necessary to gain more information or apply a different technique, time permitting, until a conclusion is reached or a determination is made.

2-10. Analysts also analyze the volume of information based on the information source's reliability and the information accuracy, as screening information is continuous. This occurs when analysts receive information they immediately recognize as untrue or inaccurate based on their knowledge or familiarity with the analytic problem. Analysts should not proceed with the analysis when there is a high likelihood that the information is false or part of a deception, as this may lead to inaccurate conclusions. False information and deception are more prevalent today with the proliferation of misinformation commonly found in social media readily available on the internet.

2-11. Analysts may decide to retain or exclude information based on results from the *screen* phase. While the excluded information may not be pertinent to the current analytical question, the information is maintained in a unit repository as it may answer a follow-on question from a new analytical question.

2-12. During operations, intelligence analysts must consider information relevancy, reliability, and accuracy to perform analysis:

- **Relevancy:** Analysts examine the information to determine its pertinence about the threat or OE. Once the information is assessed as relevant, analysts continue with the analysis process.
- **Reliability:** The source of the information is scrutinized for reliability. If the source of the information is unknown, the level of reliability decreases significantly.
- **Accuracy:** Unlike reliability, accuracy is based on other information that can corroborate (or not) the available information. When possible, analysts should obtain information that confirms or denies a conclusion in order to detect deception, misconstrued information, or bad data or information. Additionally, when possible, analysts should characterize their level of confidence in that conclusion.

Note. **Exception:** Combat information, as defined in paragraph 1-14. (See FM 3-13 and FM 3-55.)

2-13. There are marked differences in evaluating the accuracy of information between higher and lower echelons. Higher (strategic) echelons have more sources of information and intelligence than lower (tactical) echelons, giving higher echelons more opportunities to confirm, corroborate, or refute the accuracy of the reported data. The role of higher echelons in evaluating the credibility (or probable truth) of information differs from its role in evaluating the reliability of the source (usually performed best by the echelon closest to the source).

2-14. Information is evaluated for source reliability and accuracy based on a standard system of evaluation ratings for each piece of information, as indicated in table 2-1; *reliability* is represented by a letter and *accuracy* by a number. Single-source intelligence personnel assign the rating, and it is essential for all-source personnel to understand the evaluation of validated intelligence sources.

Table 2-1. Evaluation ratings for source reliability and information accuracy

	Reliability
A	**Completely reliable:** Clearly a known source or reliable information.
B	**Usually reliable:** A known source that provides reliable information.
C	**Fairly reliable:** A source that has reported on information with a degree of reliability.
D	**Not usually reliable:** Typically, a source who provides information with a heavy bias, or past data was not validated.
E	**Unreliable:** Information provided is not reliable; typically, information cannot be confirmed by any means possible with any degree of certainty.
F	**Reliability cannot be judged:** There is no basis for estimating the reliability.
	Accuracy
1	**Confirmed by other sources:** One can state with certainty there is corroborating information.
2	**Probably true:** There is no actual proof, but no reason exits to assess; the source of the information is already available.
3	**Possibly true:** Information may not at present be available to refute the accuracy.
4	**Doubtfully true:** There is information that contradicts the accuracy.
5	**Improbable:** No confirmation, and the information contradicts other reliable/accurate sources.
6	**Truth cannot be judged:** Information does not meet the criteria above.

2-15. Reliable and accurate information is integrated into the analytical production. Data that is less reliable or accurate is not discarded; it is retained for possible additional screening with other established information or if new requirements arise that are relevant to existing data. Analysts are encouraged to read information rated as *F6* (reliability = F; accuracy = 6) to determine if it has relevancy although the source cannot be confirmed and the information accuracy is questionable. As friendly forces collect more information and that information is included in all-source or single-source intelligence analysis, the information originally rated as F6 may subsequently be rated as more reliable and accurate.

Example: Analyze

From the screened information, analysts analyze the retained information (bolded):

- **Possible identification of two MLRSs as well as support equipment traveling west to east at 20 kilometers per hour along a road 15 kilometers north of the 1 BCT forward locations.** Key elements of information include (1) the location of MLRSs maneuvering north, parallel to the division area of operations (AO), which would enable elements to stop and fire, as needed, and (2) the possible identification of two MLRSs with trailing support equipment. Requests for information include (1) the identification of the types of MLRSs and support equipment, (2) the location of the MLRSs if they have stopped, and (3) the observed activity if the location of the MLRSs has been detected.
- **Approximately 28 to 30 threat tanks detected in convoy formations 40 kilometers north of the 1 BCT forward locations.** Analysts determine that the tanks detected are 40 kilometers outside of the 1 BCT AO. However, the predictive analytical assessment identifies this as possible reinforcements likely to enter the AO within the next 24 to 48 hours.
- **Threat air defense elements active near possible headquarters and artillery locations detected.** Key elements of information include the headquarters and artillery locations. The presence of air defense artillery indicates a protected site. The 1 BCT forward positions are in range of threat artillery.
- **Multiple-source reporting that a threat tank brigade is preparing to advance south, seeking to exploit lead division penetration of 1 BCT forward positions**. Key elements of information include a tank brigade preparing to advance in the direction of 1 BCT forward positions. The tank brigade is identified as an exploitation element to penetrate friendly positions.

Note. The information of threat action outside of the immediate division area of interest was passed to the corps; it did not confirm or deny any threat COAs although the report came from a reliable source. The various reports caused some further refinements to the information collection plan.

INTEGRATE

2-16. As analysts reach new conclusions about the threat activities during the *analyze* phase, they should corroborate and correlate this information with prior intelligence holdings using reasoning and analytic techniques. Analysts determine how new information relates to previous analytical conclusions. New information may require analysts to alter or validate initial conclusions. Analysts must continue to evaluate and integrate reliable and accurate information relevant to their mission.

2-17. Analysts resume the analysis based on questions (hypotheses) they established during the *screen* and *analyze* phases. At this point, analysts begin to draw conclusions that translate into an initial determination that is likely to require additional analysis and, in certain instances, additional collection. They employ the analytic tradecraft standards to assess probabilities and confidence levels; they employ the action-metrics associated with analytical rigor to draw accurate conclusions. However, some of these conclusions may present alternative COAs not previously considered during IPB. These COAs must be presented to the commander and staff because they might have operational implications. (Appendix C discusses the analytic tradecraft standards and the action-metrics associated with analytical rigor.)

2-18. Hypotheses are tested and often validated during the *integrate* phase and become the basis for analytical production. To properly validate the hypotheses, analysts must demonstrate analytical rigor to determine the analytical sufficiency of their conclusions and be willing to present those points that prove the accuracy of their assessment.

Example: Integrate

From the four pieces of information, analysts tentatively determine the intent of the tank brigade (likely the motorized rifle division identified during the military decision-making process [MDMP] effort). Analysts conclude the tank brigade will most likely advance south against 1 BCT forward positions within 12 hours if the threat assesses there is a window of opportunity. Additionally, analysis indicates an artillery grouping is repositioning in the range of friendly forces to support the exploitation effort.

Corps, adjacent division, and multinational reporting and confirmation that MLRSs and support equipment are traveling west to east compels the division to collaborate with the adjacent division to confirm the intent and objective of the threat elements.

Note. Analysts must request additional collection on tank, headquarters, and artillery locations to verify current conclusions and initiate the targeting process.

PRODUCE

2-19. Intelligence and operational products are mutually supportive and enhance the commander and staff's situational understanding. Intelligence products are generally categorized by the purpose for which the intelligence was produced. The categories can and do overlap, and the same intelligence and information can be used in each of the categories. JP 2-0 provides an explanation for each of the categories:

- Warning intelligence.
- Current intelligence.
- General military intelligence.
- Target intelligence.
- Scientific and technical intelligence.
- Counterintelligence.
- Estimative intelligence.
- Identity intelligence.

2-20. Intelligence analysis results in the production and dissemination of intelligence to the commander and staff. Intelligence analysts produce and maintain a variety of products tailored to the commander and staff and dictated by the current situation, standard operating procedures (SOPs), and battle rhythms. (See appendix E for a detailed discussion on intelligence production.)

Note. When disseminating intelligence products, intelligence analysts must recognize when intelligence information at a higher classification is essential for the commander's awareness. Intelligence analysts and the intelligence staff must adhere to all appropriate U.S. laws, DOD regulations, classification guidelines, and security protocols. (See AR 380-28.)

The classification of U.S. intelligence presents a challenge in releasing information during multinational operations although sharing information and intelligence as much as possible improves interoperability and trust. Commanders and staffs should understand U.S. and other nations' policies about information sharing, since the early sharing of information (during planning) ensures effective multinational operations.

2-21. An analyst's ultimate goal is finding threat vulnerabilities and assisting the commander and staff in exploiting those vulnerabilities—despite having answered the commander's PIR. If the intelligence analysis does not answer the commander's PIR, the analyst should reexamine the guidance, consider recommending different collection strategies, and review information previously discarded as nonessential. Sometimes, the cause for not answering the requirement is the analyst's misunderstanding of the commander's PIR or guidance, thus the analyst must return to the original question posed by the commander and reevaluate the initial hypothesis.

2-22. In tactical units, analysts must understand that their adjacent and especially their subordinate units may have degraded communications. In those cases, analysts at each echelon must develop their own conclusions and assessments and should use their unit's primary, alternate, contingency, and emergency (known as PACE) plan to facilitate continuous dissemination of their products and assessments (see FM 3-0).

Example: Produce

Following additional collection at specific points of interest, analysts confirm the tank brigade's role as the exploitation force and MLRS battalion locations. Refined collection improves the data and information necessary to target those units and answer PIRs 1 and 2.

Chapter 3
All-Source Analytical Tasks

OVERVIEW

3-1. Through the application of the all-source analytical tasks, intelligence analysis facilitates commanders and other decision makers' ability to visualize the OE, organize their forces, and control operations to achieve their objectives. The all-source analytical tasks are—

- Generate intelligence knowledge.
- Perform IPB.
- Provide warnings.
- Perform situation development.
- Provide intelligence support to targeting and information operations.

3-2. In any operation, both friendly and threat forces will endeavor to set conditions to develop a position of relative advantage. Setting these conditions begins with generate intelligence knowledge, which provides relevant knowledge about the OE that is incorporated into the Army design methodology and used later during other analytical tasks. During the MDMP, the intelligence staff leads IPB and conducts continuous intelligence analysis to understand the OE and the options it presents to friendly and threat forces. The commander and staff continuously assess information, operations, and changes in the OE. Warning intelligence, situation development, and intelligence support to targeting assist them in further shaping the OE to facilitate mission success. These all-source analytical tasks are included within the intelligence warfighting function tasks of the Army Universal Task List (also called AUTL), captured in FM 2-0, appendix B. Each specific task is identified with an Army tactical task (ART) number, such as ART 2.1.4 for the generate intelligence knowledge task. (See figure 3-1.)

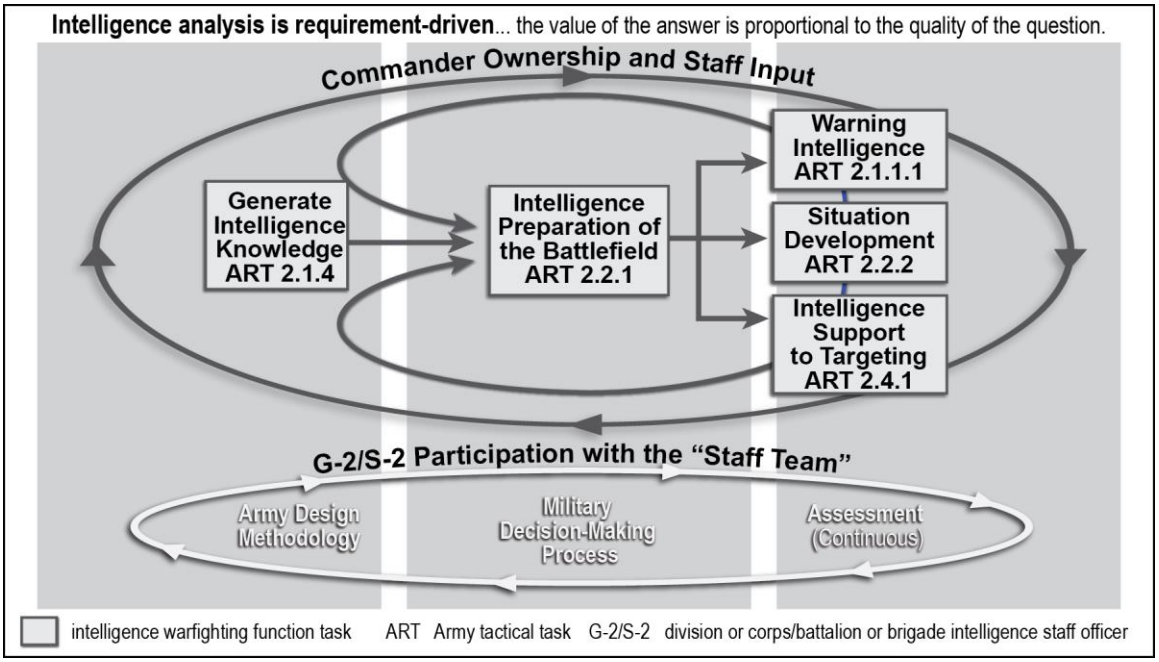


Figure 3-1. The all-source analytical tasks

3-3. The continuous assessment of collected information also mitigates risk to friendly forces while identifying opportunities to leverage friendly capabilities to open a window of opportunity. Analysis presents the commander with options for employing multiple capabilities and gaining a position of relative advantage over the threat.

3-4. For each all-source analytical task, the challenge for the intelligence analyst is understanding the unique requirements and considerations based on the situation, operational echelon, and specific mission. For example, targeting requirements at the brigade level narrowly focus on targets within that brigade's AO. Whereas theater army-level targeting synchronizes and uses operations conducted by one or more corps to reach operational objectives. Another example includes long-term analytical assessments, which are usually produced at the strategic and operational levels of warfare (see chapter 9).

3-5. There are many forms of analysis associated with unique operational activities. One important example of these types of activities is identity activities, which result in identity intelligence. *Identity intelligence* is the intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest (JP 2-0). Identity activities are described as a collection of functions and actions conducted by maneuver, intelligence, and law enforcement components. Identity activities recognize and differentiate one person from another to support decision making. Identity activities include—

- The collection of identity attributes and physical materials.
- The processing and exploitation of identity attributes and physical materials.
- All-source analytical efforts.
- The production of identity intelligence and DOD law enforcement criminal intelligence products.
- The dissemination of those intelligence products to inform policy and strategy development, operational planning and assessment, and the appropriate action at the point of encounter.

GENERATE INTELLIGENCE KNOWLEDGE (ART 2.1.4)

3-6. Generate intelligence knowledge is a continuous task driven by the commander. It begins before receipt of mission and enables the analyst to acquire as much relevant knowledge as possible about the OE for the conduct of operations. Information is obtained through intelligence reach, research, data mining, database access, academic studies, intelligence archives, publicly available information, and other information sources, such as biometrics, forensics, and DOMEX. The information and intelligence obtained can be refined into specific knowledge for use during mission analysis through functional analysis, which is discussed in chapter 6 of this publication.

3-7. Generate intelligence knowledge includes the following five tasks, which facilitate creating a foundation for performing IPB and mission analysis:

- **Develop the foundation to define threat characteristics:** Analysts create a database of known hostile threats and define their characteristics in a general location. Analysts can refine and highlight important threats through functional analysis that can be prioritized later during steps 3 and 4 of the IPB process.
- **Obtain detailed terrain information and intelligence:** Analysts describe the terrain of a general location and categorize it by environment type. For example, desert and jungle environments have distinguishing characteristics that can assist in analyzing terrain during step 2 of the IPB process.
- **Obtain detailed weather and weather effects information and intelligence:** Analysts describe the climatology of a general location and forecast how it would affect future operations. Analysts should rely on the Air Force staff weather officer of their respective echelons to assist in acquiring weather support products, information, and knowledge. If the staff weather officer is not readily available, analysts should use publicly available information and resources. Information regarding climatology characteristics can assist in analyzing weather effects during step 2 of the IPB process.
- **Obtain detailed civil considerations information and intelligence:** Analysts identify civil considerations (areas, structures, capabilities, organizations, people, and events [ASCOPE]) within a general location. Analysts can refine this information further when they receive a designated area of interest and can assist in determining how civil considerations will affect friendly and threat operations during step 2 of the IPB process.

- **Complete studies:** Although analysts do not have a specific operation, mission, or area of responsibility when generating intelligence knowledge, they can compile information into products based on the commander's guidance. This supports the commander's visualization and completes studies for dissemination. Completed studies or products include country briefs, written assessments, or graphics. These products inform the commander and staff on current and historic situations that may affect future operations when a mission is received.

PERFORM INTELLIGENCE PREPARATION OF THE BATTLEFIELD (ART 2.2.1)

3-8. Analytical support begins during the MDMP. The *military decision-making process* is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order (ADP 5-0). Commanders use the MDMP to visualize the OE and the threat, build plans and orders for extended operations, and develop orders for short-term operations within the framework of a long-range plan. During the mission analysis step of the MDMP, intelligence analysts lead the IPB effort; however, they cannot provide all of the information the commander requires for situational understanding. Other staff sections or supporting elements assist in producing and continuously refining intelligence products tailored to the commander's requirements and the operation. (See ATP 2-01.3 for IPB information.)

3-9. As analysts begin the IPB process, they should have a general understanding of their OE based on intelligence produced and acquired when generating intelligence knowledge. IPB is a four-step process:

- **Step 1—Define the OE.** The intelligence staff identifies those significant characteristics related to the mission variables of enemy, terrain and weather, and civil considerations that are relevant to the mission. The intelligence staff evaluates significant characteristics to identify gaps and initiate information collection. During step 1, the AO, area of interest, and area of influence must also be identified and established.
- **Step 2—Describe environmental effects on operations.** The intelligence staff describes how significant characteristics affect friendly operations. The intelligence staff also describes how terrain, weather, civil considerations, and friendly forces affect threat forces. The entire staff determines the effects of friendly and threat force actions on the population.
- **Step 3—Evaluate the threat.** Evaluating the threat is understanding how a threat can affect friendly operations. Step 3 determines threat force capabilities and the doctrinal principles and tactics, techniques, and procedures that threat forces prefer to employ.
- **Step 4—Determine threat COAs.** The intelligence staff identifies and develops possible threat COAs that can affect accomplishing the friendly mission. The staff uses the products associated with determining threat COAs to assist in developing and selecting friendly COAs during the COA steps of the MDMP. Identifying and developing all valid threat COAs minimize the potential of surprise to the commander by an unanticipated threat action.

PROVIDE WARNINGS (ART 2.1.1.1)

3-10. Across the range of military operations, various collection assets provide early warning of threat action. As analysts screen incoming information and message traffic, they provide the commander with advanced warning of threat activities or intentions that may change the basic nature of the operation. These warnings enable the commander and staff to quickly reorient the force to unexpected contingencies and to shape the OE.

3-11. Analysts can use analytic techniques and their current knowledge databases to project multiple scenarios and develop indicators as guidelines for providing warning intelligence. An *indicator* is, in intelligence usage, an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action (JP 2-0). Analysts project future events and identify event characteristics that can be manipulated or affected. Characteristics that cannot be manipulated or affected should be incorporated into unit SOPs as warning intelligence criteria. (See ATP 2-01 and ATP 2-01.3 for more information on indicators.)

PERFORM SITUATION DEVELOPMENT (ART 2.2.2)

3-12. Intelligence analysis is central to situation development, as it is a process for analyzing information and producing current intelligence concerning the relevant aspects of the OE within the AO before and during operations. Analysts continually produce current intelligence to answer the commander's requirements, update and refine IPB products, and support transitions to the next phase of an operation. (For more information on situation development, see FM 2-0.)

Note. In addition to the AO, intelligence analysts should also consider and include relevant aspects of the OE within the area of influence and area of intelligence responsibility that impact the commander's AO.

3-13. Analysts continually analyze the current situation and information to predict the threat's next objective or intention. During step 3 of the IPB process, analysts compare the current situation with their threat evaluations to project multiple scenarios and develop indicators. Understanding how the threat will react supports the planning of branches and sequels, affording the commander multiple COAs and flexibility on the battlefield during current operations. For example, observing a threat unit in a defensive posture may indicate an offensive operation within a matter of hours. Providing this information to the commander enables the staff to pursue a different COA that can place friendly units in a better position of relative advantage. The commander may use a flanking maneuver on the threat since it is in a relatively stationary position, hindering the future offensive operation.

PROVIDE INTELLIGENCE SUPPORT TO TARGETING AND INFORMATION OPERATIONS (ART 2.4)

3-14. *Targeting* is the process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities (JP 3-0). Across all echelons and intelligence disciplines, intelligence analysis provides relevant and timely intelligence to support targeting (both lethal and nonlethal). The staff uses this intelligence during the targeting process, which uses the *decide*, *detect*, *deliver*, and *assess* methodology. (See appendix F for more on intelligence support to targeting.)

3-15. Intelligence analysis, starting with the IPB effort, supports target development and target detection:

- **Intelligence analysis support to target development:** Target development involves the systematic analysis of threat forces and operations to determine high-value targets (HVTs) (people, organizations, or military units the threat commander requires for successful completion of the mission), HPTs (equipment, military units, organizations, groups, or specific individuals whose loss to the threat contributes significantly to the success of the friendly COA), and systems and system components for potential engagement through maneuver, fires, electronic warfare, or information operations.
- **Intelligence analysis support to target detection:** Intelligence analysts establish procedures for disseminating targeting information. The targeting team develops the sensor and attack guidance matrix to determine the sensors required to detect and locate targets. Intelligence analysts incorporate these requirements into the collection management tools, which assist the operations staff in developing the information collection plan.

3-16. *Information operations* is the integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own (JP 3-13). Intelligence support to military information operations pertains to the collection of information essential to define the information environment, understand the threat's information capabilities, and assess or adjust information-related effects. Continuous and timely intelligence is required to accurately identify the information environment across the physical, informational, and cognitive dimensions, including the operational variables (PMESII-PT). Intelligence support to military information operations focuses on the following:

- Aspects of the information environment that influence, or are influenced by, the threat.
- Understanding threat information capabilities.

- Understanding the methods by which messages are transmitted and received in order to assess the cognitive reception and processing of information within the target audience.
- Assessing information-related effects (target audience motivation and behavior, measure of effectiveness, and information indicators of success or failure).

This page intentionally left blank.

PART TWO

Task Techniques

Chapter 4

Analytic Techniques

OVERVIEW

4-1. Intelligence analysts use cognitive processes and analytic techniques and tools to solve intelligence problems and limit analytical errors. The specific number of techniques and tools applied depends on the mission and situation. The basic thinking abilities for intelligence analysis and critical and creative thinking, all described in appendix B, facilitate analysis and improve the probability of accurate conclusions. Intelligence analysts must be as accurate as possible to assist in ensuring mission success.

4-2. The following distinguishes between a technique, tool, and method:

- **Technique** is a way of doing something by using a special knowledge or skill. An analytic technique is a way of looking at a problem, which results in a conclusion, assessment, or both. A technique usually guides analysts in thinking about a problem instead of providing them with a definitive answer as typically expected from a method.
- **Tool** is a component of an analytic technique that facilitates the execution of the technique but does not provide a conclusion or assessment in and of itself. Tools facilitate techniques by allowing analysts to display or arrange information in a way that enables analysis of the information. An example of a tool is a link diagram or a matrix. Not all techniques have an associated tool.
- **Method** is a set of principles and procedures for conducting qualitative analysis.

APPLYING STRUCTURED ANALYTIC TECHNIQUES

4-3. Structured analysis assists analysts in ensuring their analytic framework—the foundation upon which they form their analytical judgments—is as solid as possible. It entails separating and organizing the elements of a problem and reviewing the information systematically. Structured analytic techniques provide ways for analysts to separate the information into subsets and assess it until they generate a hypothesis found to be either feasible or untrue. Structured analytic techniques—

- Assist analysts in making sense of complex problems.
- Allow analysts to compare and weigh pieces of information against each other.
- Ensure analysts focus on the issue under study.
- Force analysts to consider one element at a time systematically.
- Assist analysts in overcoming their logic fallacies and biases.
- Ensure analysts see the elements of information. This enhances their ability to identify correlations and patterns that would not appear if not depicted outside the mind.
- Enhance analysts' ability to collect and review data. This facilitates thinking with a better base to derive alternatives and solutions.

4-4. Applying the appropriate structured analytic technique assists commanders in better understanding and shaping the OE. One technique may not be sufficient to assist in answering PIRs; therefore, analysts should use multiple techniques, time permitting. For example, determining the disposition and composition of the threat in the OE is like attempting to put the pieces of a puzzle together. Employing multiple analytic techniques facilitates the piecing of the puzzle, thus creating a clearer picture. (See figure 4-1.) Structured analytic techniques are categorized as the following and summarized in figure 4-2:

- Basic—provide insight that supports problem solving. (See chapter 5.)
- Diagnostic—make analysis more transparent. (See chapter 5.)
- Advanced:
  - Contrarian—challenge current thinking. (See chapter 6.)
  - Imaginative—develop new insights. (See chapter 6.)

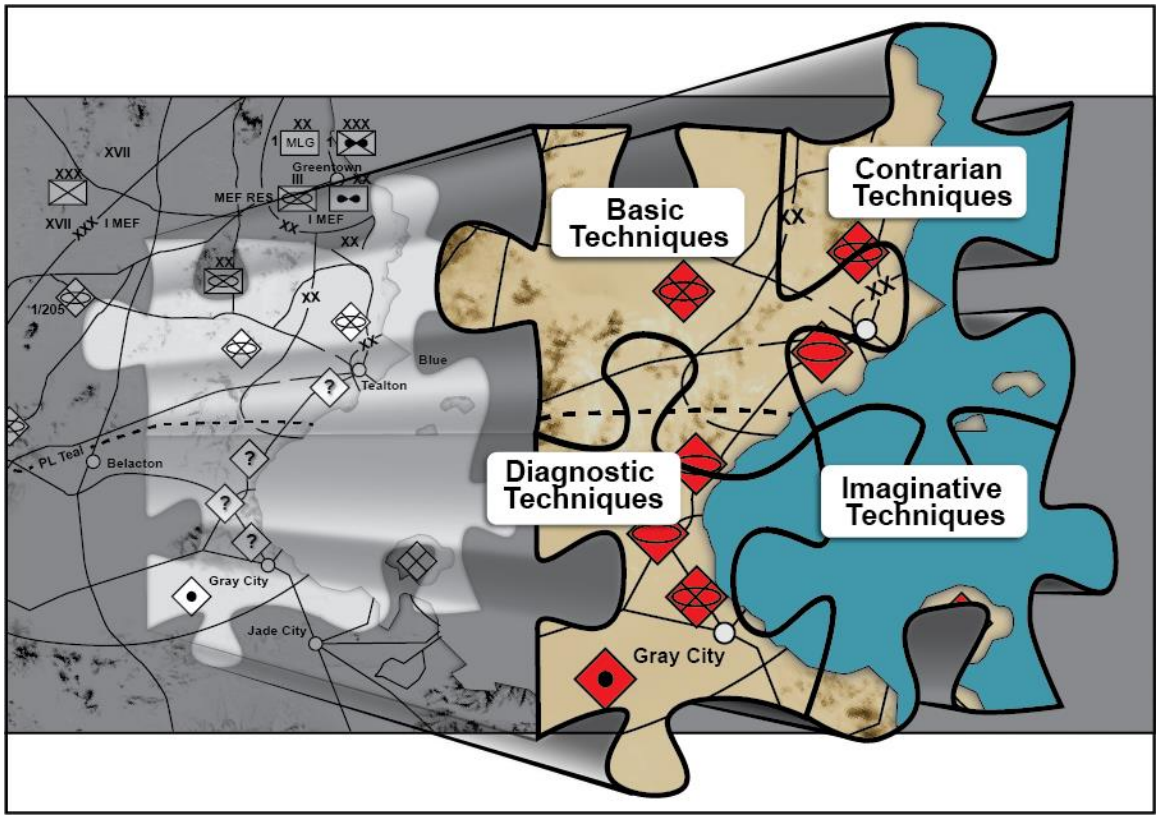


Figure 4-1. Applying analytic techniques to understand the operational environment

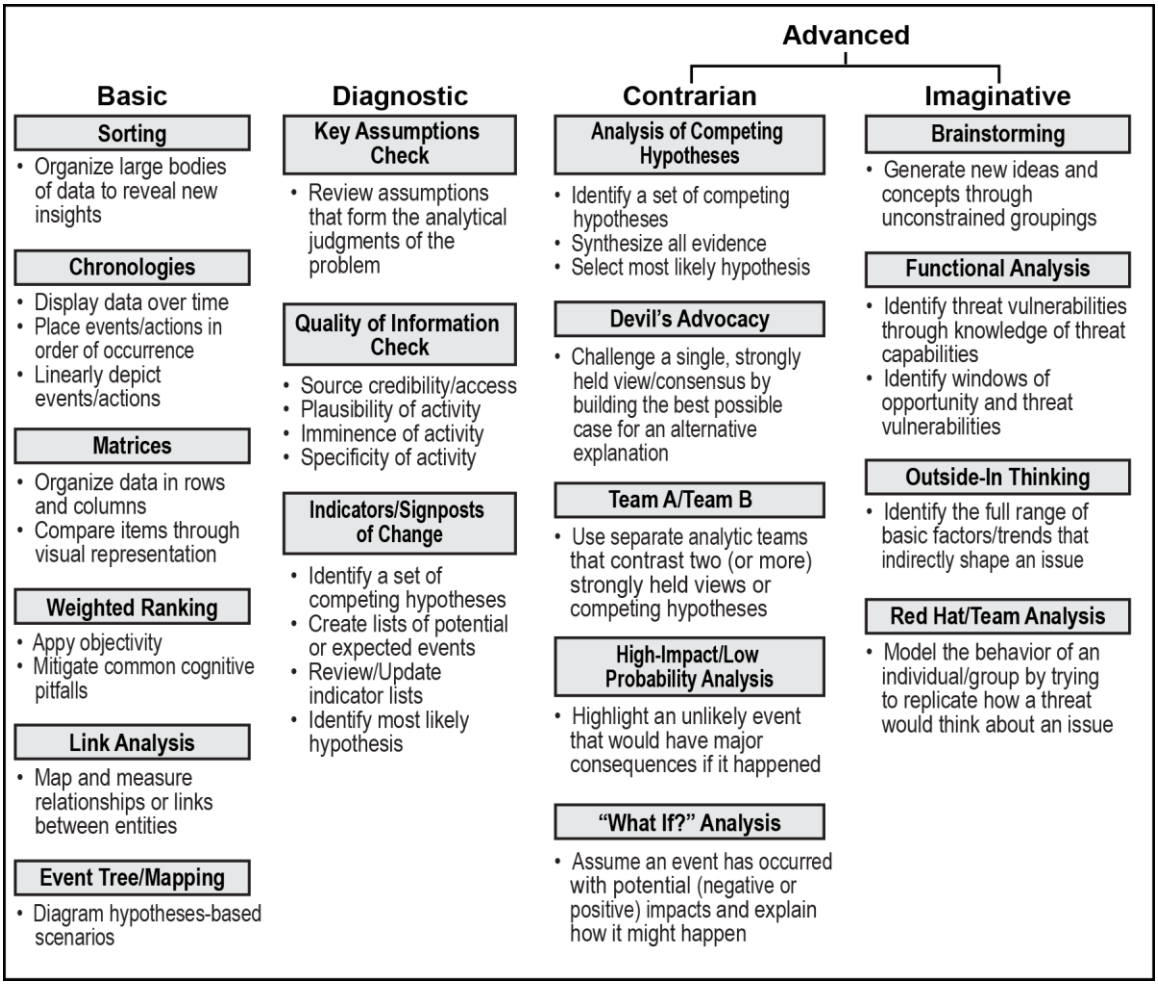


Figure 4-2. Structured analytic techniques summarized

4-5. For thorough analysis, analysts should incorporate as many appropriate techniques as possible into their workflow. Although this may be more time consuming, analysts become more proficient at using these techniques, ultimately reducing the amount of time required to conduct analysis. The exact techniques and tools incorporated, as well as the order in which to execute them, are mission- and situation-dependent. There is no one correct way to apply these techniques as each analyst's experience, preference, and situation are influencing factors.

4-6. Analysts can apply structured analytic techniques in the *analyze* and *integrate* phases of the intelligence analysis process to assist them in solving analytic problems. The analytic problem can vary depending on the echelon or mission. For example, an analytic problem could be forecasting the future stability of a specific country, while another could be trying to identify an HVT. The results of structured analytic techniques and tools, such as link diagrams or quad-charts, are not always incorporated into intelligence products such as intelligence estimates or intelligence running estimates (see FM 2-0). However, analysts may use these results to inform their analytical products; they should maintain these results in a repository for future reference.

4-7. The vast amount of information that analysts must process can negatively affect their ability to complete intelligence assessments timely and accurately; therefore, analysts should be proficient at using both manual and automated methods to conduct structured analysis. Additionally, analysts conduct analysis from varying environments and echelons in which the availability of automation and network connectivity may not be fully mission capable.

Applying Analytic Techniques Throughout the Intelligence Analysis Process

UNDERSTAND THE REQUIREMENTS: A human intelligence analysis cell (HAC) is tasked to help find the composition and disposition of the threat's integrated air defense system (IADS) on the battlefield. This task supports one of the division commander's PIRs. The division's HUMINT elements have been attempting to collect information from captured detainees, defectors, and internally displaced persons. Additionally, HUMINT sources are sensitized to look for radar dishes and missiles.

SCREEN THE COLLECTED INFORMATION: The HAC receives multiple HUMINT reports on various topics, but it focuses on those reports that support the PIR related to IADSs.

The HAC assesses the value of the reports by determining the *relevance* of the information to the PIR, the *reliability* of the source of the information, and the *accuracy* of the information itself:

- **Relevance:** The HAC searches HUMINT databases for all HUMINT reporting in theater related to IADSs and tailors its query to receive reports not older than 120 days (date) and within the boundaries of its AO (location). The HAC discovers that there are 20 reports on hand possibly related to IADSs within the specified date and geographic location. **(Overall relevance is estimated as high.)**
- **Reliability:** The HAC looks for duplication in the reporting, which can occur when one HUMINT source provides multiple HUMINT collection teams the same information. The HAC finds one duplicate report and eliminates it, leaving 19 reports on hand to analyze. The HAC also determines that one of the sources lacks credibility and eliminates the one report associated with that source, reducing the number to 18 reports. **(Overall reliability of sources is estimated as moderate.)**
- **Accuracy:** The HAC examines the 18 reports and determines that most of them have marginally accurate information because they lack grids for any locations. Despite this, the HAC does not eliminate these reports. **(Overall accuracy is estimated as moderate.)**

Screening results: The HAC compiles first-hand information from multiple credible sources about missiles on the backs of large trucks within the division's AO, and from another credible source who reported an increase in the number of trucks with missiles in the last 30 days.

ANALYZE: The HAC considers the information against its current knowledge level and uses sorting, a basic structured analytic technique, to categorize the information and determine what it now reveals or what gaps still exist. The HAC uses the Distributed Common Ground System-Army (DCGS-A) and combatant command-specific databases to further examine the quality of the information to determine if there are any signs of a deception effort. The HAC then generates multiple hypotheses based on the information and determines that the reporting indicates the discovery of a threat supply point. The HAC challenges the hypothesis using contrarian techniques, such as devil's advocacy and team A/team B, to ensure the analysis is thorough (see chapter 6).

Initial analytical determination: Based on the reports and analytic techniques employed, the HAC determines that an unidentified truck with possible missiles will arrive at a general location every few days. The geographical area is a 1,500-meter location on the north side of a specific ridgeline. The HAC postulates that this general location may be a threat supply point for an unknown missile-type weapons system. The HAC reports a moderate level of confidence in its assessment. (See appendix C for more information on likelihoods and confidence levels.)

INTEGRATE: The HAC, requiring more information to further develop the analytic problem, expands the parameters of its previous database query by including the area of interest and HUMINT reporting not older than 150 days. This query returns the same reports as the previous query as well as additional reports from other HUMINT teams and other government agencies operating both inside and outside the division's AO. The reports are assessed as reliable and fairly accurate since the information about these items was preexisting.

Applying Analytic Techniques Throughout the Intelligence Analysis Process (*continued*)

INTEGRATE (*continued*): The following includes key findings in the HUMINT reports:

- The reports from other government agencies contain photographs of trucks with missiles, identified as logistics vehicles, transporting possible SA-17 missiles to and from unknown locations. The photographs were taken at a specific grid location showing the direction of travel towards the division's AO.
- An organic HUMINT report from inside the division's AO, not initially related to IADSs, now reveals links or indicators that, when combined with previous holdings, may provide information related to IADSs. In this report, the source reported loud military trucks travelling frequently near the source's home. Additionally, the source's description of the trucks matched those in the photographs of the other government agencies' reports. The source's residence is located along the main highway between where the photographs were taken and where the increase in trucks with missiles was reported. Furthermore, source reporting indicates that the trucks are loaded with missiles when heading towards the division's AO, but they are empty when heading away from the division's AO.

Note. Single-source analysts may be able to skip to the *produce* phase if no other information on the topic is available.

Final analytical determination: This new information, when integrated with the previous holdings and structured analytic techniques and tools, allows the HAC to refine its initial analytical determination. The HAC postulates that SA-17s are likely to arrive north of Ridgeline Borisenko within the grid square 38JCH1126 every few days. The HAC maintains a moderate level of confidence in its assessment. When the date of the postulated event elapses, the HAC will be able to further define the reliability of the sources and accuracy of the information.

PRODUCE: The HAC disseminates this newly produced intelligence in a summary that contains the determination that SA-17s will arrive north of Ridgeline Borisenko. The summary of HUMINT reporting is disseminated to the commander and shared with all other intelligence elements within the division.

This page intentionally left blank.

Chapter 5
Basic and Diagnostic Structured Analytic Techniques

SECTION I – BASIC STRUCTURED ANALYTIC TECHNIQUES

5-1. Basic structured analytic techniques are the building blocks upon which further analysis is performed. They are typically executed early in the intelligence effort to obtain an initial diagnosis of the intelligence problem through revealing patterns. The basic structured analytic techniques described in this publication are—

- **Sorting technique:** Organizing large bodies of data to reveal new insights.
- **Chronologies technique:**
  - Displaying data over time.
  - Placing events or actions in order of occurrence.
  - Linearly depicting events or actions.
- **Matrices technique:**
  - Organizing data in rows and columns.
  - Comparing items through visual representation.
- **Weighted ranking technique:**
  - Facilitating the application of objectivity.
  - Mitigating common cognitive pitfalls.
- **Link analysis technique:** Mapping and measuring relationships or links between entities.
- **Event tree and event mapping techniques:** Diagramming hypotheses-based scenarios.

5-2. These techniques—

- Improve assessments by making them more rigorous.
- Improve the presentation of the finished intelligence in a persuasive manner.
- Provide ways to measure progress.
- Identify information gaps.
- Provide information and intelligence.

SORTING

5-3. Sorting is a basic structured analytic technique used for grouping information in order to develop insights and facilitate analysis. This technique is useful for reviewing massive data stores pertaining to an intelligence challenge. Sorting vast amounts of data can provide insights into trends or abnormalities that warrant further analysis and that otherwise would go unnoticed. Sorting also assists in reviewing multiple categories of information that when divided into components presents possible trends, similarities, differences, or other insights not readily identifiable. Table 5-1 on page 5-2 briefly describes when to use the sorting technique, as well as the value added and potential pitfalls associated with using this technique.

Table 5-1. Sorting technique

Sorting: *A basic structured analytic technique for organizing a large amount of data in a manner that often yields new insights.*		
When to use	**Value added**	**Potential pitfalls**
Sorting data early in the analysis process is advantageous. It is most effective when information elements can be arranged into categories and subcategories to gain insights not readily identifiable. Sorting is particularly effective during initial data collection and hypotheses generation.	Sorting vast amounts of data can provide insights into trends or anomalies that warrant further analysis. This technique can highlight new or additional analytic insights into an old or new intelligence problem.	Improper sorting can hide valuable insights as easily as it can illuminate them. This occurs more frequently if data is not standardized.

5-4. **Method.** The following steps outline the process of sorting:

- **Step 1:** Arrange the information into categories to determine which categories or combination of categories might show trends or abnormalities that would provide insight into the problem being studied.
- **Step 2:** Review the listed facts, information, or hypotheses in the database to identify key fields that may assist in uncovering possible patterns or groupings.
- **Step 3:** Group those items according to the schema of the categories defined in step 1.
- **Step 4:** Choose a category and sort the information within that category. Look for any insights, trends, or oddities.
- **Step 5:** Review (and re-review) the sorted facts, information, or hypotheses to determine alternative ways to sort them. List any alternative sorting schema for the problem. One of the most useful applications of this technique is sorting according to multiple schemas and examining results for correlations between data and categories. For example, analysts identify from the sorted information that most attacks occurring on the main supply route also occur at a specific time.

5-5. A pattern analysis plot sheet is a common analysis tool for sorting information. (See figure 5-1.) It can be configured to determine threat activity as it occurs within a specified time. The pattern analysis plot sheet is a circular matrix and calendar. Each concentric circle represents one day and each wedge in the circle is one hour of the day. In figure 5-1, the information categories pertain to tactical surface-to-surface missile (also called SSM) launches arranged according to the days of the week and the times of day. For example, four Surface-to-Surface Missile B launches occurred during the last week of the month on alternate weekdays, mainly in the early hours of the day. The threat could be conducting launches during the early morning hours when people are just waking up and at their most vulnerable.

5-6. This method of sorting allows analysts to determine various aspects of an event, such as the type and timing of a particular event, and assists collection managers in allocating collection assets in space and time. Although the pattern analysis plot sheet is a sorting tool, it can also overlap with chronologies since analysts commonly use it to capture and display data over time.

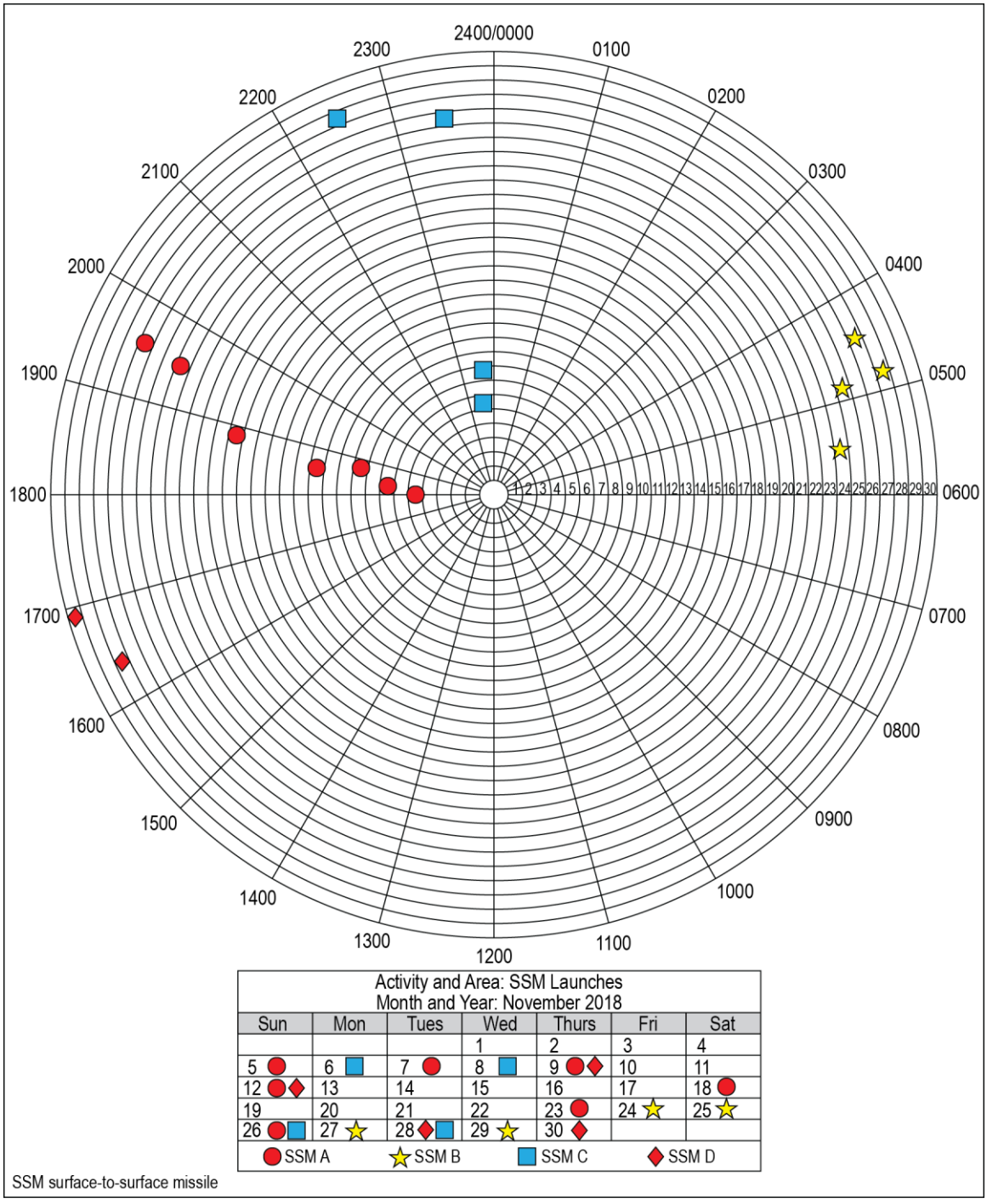


Figure 5-1. Sorting data using a pattern analysis plot sheet example

CHRONOLOGIES

5-7. A chronology is a list that places events or actions in the order they occurred; a timeline is a graphical depiction of those events. Analysts must consider factors that may influence the timing of events. For example, the chronological time of events may be correlated to the lunar cycle (moonset), religious events, or friendly patrol patterns. Timelines assist analysts in making these types of determinations. Table 5-2 briefly describes when to use the chronologies technique, as well as the value added and potential pitfalls associated with using this technique.

Table 5-2. Chronologies technique

Chronologies: *Technique for displaying data over time.*		
When to use	**Value added**	**Potential pitfalls**
The chronologies technique assists in organizing events or actions. It is useful for understanding the timing and sequence of relevant events as well as identifying significant events and gaps. The events may have a cause-and-effect relationship, or they may not. While timelines may be developed at the onset of an analytical task to ascertain the context of the activity being analyzed, they are also used in reviewing intelligence studies to discover causes for intelligence failures as they highlight significant events.	Chronologies assist in identifying patterns and correlations between events. This technique enables analysts to relate seemingly random events to the overarching situation and highlight or identify significant changes. It also assists in discovering trends, issues, or anomalies. Timelines depict information in a format easily understood in a briefing.	Analysts must be careful not to assume that events following earlier events are caused by the earlier events; there may be no causal relationship. The validity of this technique may be minimized if analysts fail to find contextual events that relate to the information in the chronology or timeline.

5-8. **Method.** Creating a chronology or timeline involves three steps:

- **Step 1:** List relevant events by the date or in order each occurred. Analysts should ensure they properly reference the data.
- **Step 2:** Review the chronology or timeline by asking the following questions:
  - What are the temporal distances between key events? If lengthy, what caused the delay? Are there missing pieces of data that may fill those gaps that should be collected?
  - Did analysts overlook pieces of intelligence information that may have had an impact on the events?
  - Conversely, if events seem to happen more rapidly than expected, is it possible that analysts have information related to multiple-event timelines?
  - Are all critical events necessary and shown for the outcome to occur?
  - What are the intelligence gaps?
  - What are indicators for those intelligence gaps?
  - What are the vulnerabilities in the timeline for collection activities?
  - What events outside the timeline could have influenced the activities?
- **Step 3:** Summarize the data along the line. Sort each side of the line by distinguishing between types of data. For example, depict intelligence reports above the timeline and depict significant activities below the timeline. Multiple timelines may be used and should depict how and where they converge.

5-9. Timelines are depicted linearly and typically relate to a single situation or COA. (See figure 5-2.) Multilevel timelines allow analysts to track concurrent COAs that may affect each other. Analysts use timelines to postulate about events that may have occurred between known events. They become sensitized to search for indicators, so the missing events are found and charted. Timelines may be used in conjunction with other structured analytic techniques, such as the event tree technique (see paragraph 5-22), to analyze complex networks and associations.

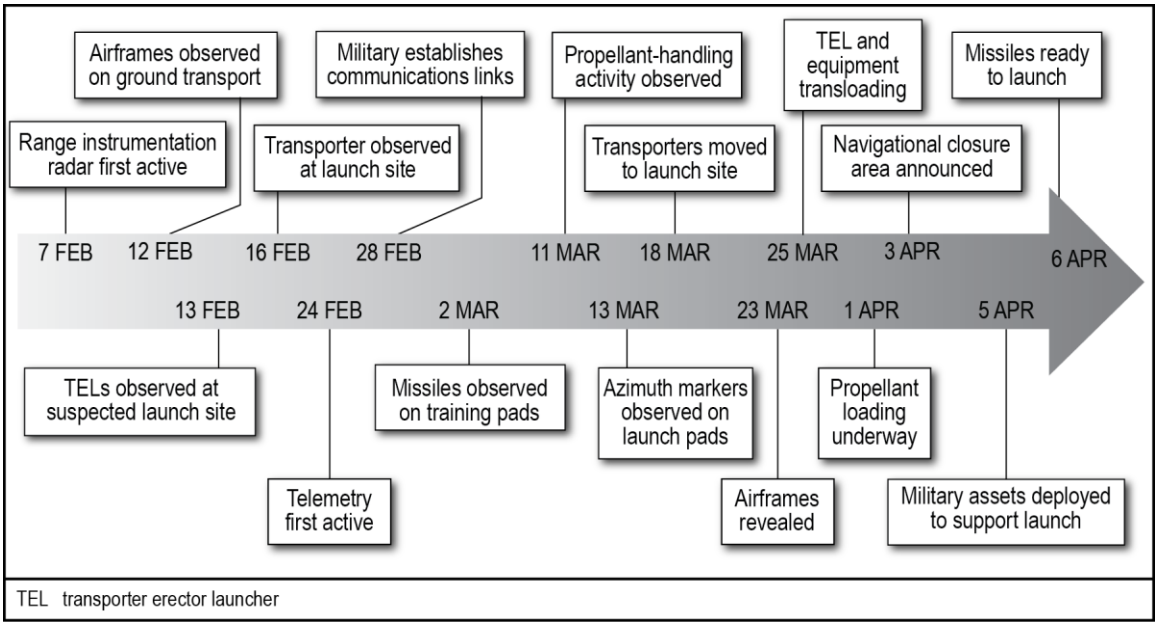


Figure 5-2. Timeline example

5-10. Figure 5-3 illustrates a time event chart, which is a variation of a timeline using symbols to represent events, dates, and the flow of time. While there is great latitude in creating time event charts, the following should be considered when creating them:

- Depict the first event as a triangle.
- Depict successive events as rectangles.
- Mark noteworthy events with an X across the rectangles.
- Display the date on the symbol.
- Display a description below the symbol.
- If using multiple rows, begin each row from left to right.

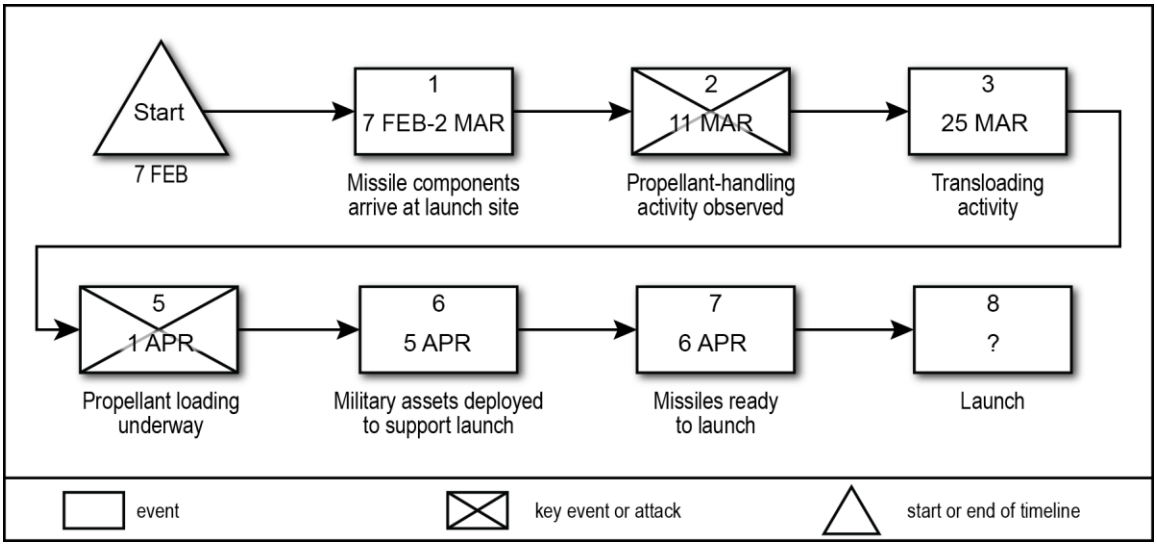


Figure 5-3. Time event chart example

MATRICES

5-11. A matrix is a grid with as many cells as required to sort data and gain insight. Whenever information can be incorporated into a matrix, it can provide analytic insight. A matrix can be rectangular, square, or triangular; it depends on the number of rows and columns required to enter the data. Three commonly used matrices are the—

- **Threat intentions matrix—**assists in efficiently analyzing information from the threat's point of view based on the threat's motivation, goals, and objectives. (See paragraph 5-14.)
- **Association matrix—**identifies the existence and type of relationships between individuals as determined by direct contact.
- **Activities matrix—**determines connections between individuals and any organization, event, entity, address, activity, or anything other than persons.

Note. Since the association and activity matrices closely relate to link analysis, they are described under the link analysis technique. (See paragraph 5-21.)

5-12. A key feature of the matrices analytic technique is the formulation of ideas of what may occur when one element of a row interacts with the corresponding element of a column. This differs from other matrices, such as the event matrix (described in ATP 2-01.3), in which the elements of the columns and rows do not interact to formulate outcomes; the matrix is primarily used to organize information. Table 5-3 briefly describes when to use the matrices technique, as well as the value added and potential pitfalls associated with using this technique. comparison

Table 5-3. Matrices technique

Matrices: *Technique that uses analytic tools for sorting and organizing data to facilitate comparison and analysis.*		
When to use	**Value added**	**Potential pitfalls**
A matrix is useful when there are more options or intricate data to conceptualize at one time without the aid of visual representations.	A matrix is useful for isolating critical data when there are vast amounts of information relevant to an issue, such as collected open-source information for a country study to generate intelligence knowledge; it facilitates comparing the options. When used to review data related to options, such as in a threat intentions matrix, this technique enables the analytical focus on each option, thus improving comparisons.	A matrix's two-dimensional design limits its use for collating data on complex issues; leaving out pertinent data can oversimplify an issue.

5-13. **Method.** The following steps outline the process for constructing a matrix (see figure 5-4):

- **Step 1:** Draw a matrix with enough columns and rows to enter the two sets of data being compared.
- **Step 2:** Enter the range of data or criteria along the uppermost horizontal row and the farthest left vertical column leaving a space in the upper left corner of the matrix.
- **Step 3:** In the grid squares in between, annotate the relationships, or lack thereof, in the cell at the intersection between two associated data points.
- **Step 4:** Review the hypotheses developed about the issue considering the relationships shown in the matrix; if appropriate, develop new hypotheses based on the insight gained from the matrix.

5-14. The following steps pertain to the threat intentions matrix technique (see figure 5-4):

- **Step 1:** Enter the decision options believed to be reasonable from the threat's viewpoint along the farthest left vertical column.
- **Step 2:** Enter the objectives for each option from the threat's viewpoint in the *objectives* column.
- **Step 3:** Enter the benefits for each option from the threat's viewpoint in the *benefits* column.
- **Step 4:** Enter the risks for each option from the threat's viewpoint in the *risks* column.

- **Step 5:** Fill in the *implications* column, which transitions the analyst from the threat's viewpoint to the analyst's viewpoint. Enter the implications from the threat's viewpoint and then add a slash (/) and enter the implications from the analyst's viewpoint.
- **Step 6:** Enter the indicators from the analyst's viewpoint in the *indications* column. This provides a basis for generating collection to determine as early as possible which option the threat selected.

	Objectives	***Benefits***	***Risks***	***Implications***	***Indications***
White House	Destroy most important United States (U.S.) symbol	Ultimate show of power	Miss target or shot down	Threat gains in stature/U.S. drawn into war, bled economically	• Unusual interest in White House air defenses • Extremists taking pilot training
Terrorist Attack	• Mass casualties • Instill fear	• Show of power • Media attention	• Adequate training • Maintain secrecy	Threat gains in stature/mass casualties can damage economy	• Unusual surveillance • Pilot training • Familiarizing with the area
Wall Street	Hurt the U.S. economy	• Aid recruitment • Show of power	• Adequate training • Maintain secrecy	Threat gains in stature/difficult to determine attacker	• Unusual surveillance • Pilot training • Familiarizing with the area

Figure 5-4. Threat intentions matrix example

WEIGHTED RANKING

5-15. The weighted ranking technique is a systematic approach that provides transparency in the derivation and logic of an assessment. This facilitates the application of objectivity to an analytic problem. To simplify the weighted ranking technique, this publication introduces subjective judgments instead of dealing strictly with hard numbers; however, objectivity is still realized. This technique requires analysts to select and give each criterion a weighted importance from the threat's viewpoint. Analysts use the criticality, accessibility, recuperability, vulnerability, effect, and recognizability (also called CARVER) matrix tool to employ this technique to support targeting prioritization. (See ATP 3-60.) The insight gained from how each criterion affects the outcome allows for a clear and persuasive presentation and argumentation of the assessment.

5-16. Weighted ranking assists in mitigating common cognitive pitfalls by converting the intelligence problem into a type of mathematical solution. The validity of weighting criteria is enhanced through group discussions, as group members share insights into the threat's purpose and viewpoint; red hat/team analysis can augment this technique. Weighted ranking uses matrices to compute and organize information. Table 5-4 briefly describes when to use the weighted ranking technique, as well as the value added and potential pitfalls associated with using this technique.

Table 5-4. Weighted ranking technique

Weighted ranking: *Technique that provides clarity among many alternatives by applying weighting to criteria to provide an overall score for each alternative.*		
When to use	**Value added**	**Potential pitfalls**
Analysts should use weighted ranking when there is a need for transparency in the reasoning used to derive an assessment. The targeting selection process is an example of when this technique is advantageous.	Weighted ranking adds validity to an assessment of alternatives, options, and hypotheses by mitigating biases and mindsets, which may result in the unsystematic and therefore inconsistent use of criteria.	Weighted ranking takes more time than many other basic structured analytic techniques and relies on a fair number of mathematical computations. This may cause analysts to avoid the technique.

5-17. **Method.** The following steps describe how to accomplish a simplified weighted ranking review of alternative options:

- **Step 1:** Create a matrix and develop all options and criteria related to the analytical issue. Figure 5-5 depicts the *options* as types of operations and the *criteria* as the five military aspects of terrain (observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment [OAKOC]).
- **Step 2:** Label the left, uppermost column/row of the matrix as options and fill the column with the types of operations generated in step 1.
- **Step 3:** List the criteria (OAKOC) generated in step 1 in the top row with one criterion per column.
- **Step 4:** Assign weights and list them in parentheses next to each criterion. Depending on the number of criteria, use either 10 or 100 points and divide them based on the analyst's judgment of each criterion's relative importance. Figure 5-5 shows how the analyst assigned the weights from the threat's perspective to the OAKOC factors using 10 points.
- **Step 5:** Work across the matrix one option (type of operation) at a time to evaluate the relative ability of the option to satisfy the corresponding criterion from the threat's perspective. Using the 10-point rating scale, assign 1 as low and 10 as high to rate each option separately. (See figure 5-5 for steps 1 through 5.)
- **Step 6:** Work across the matrix again, one option at a time, and multiply the criterion weight by the option rating and record this number in each cell. (See figure 5-6.)

Options	***Criteria***					
	Observation and fields of fire (2)	Avenues of approach (1)	Key terrain (1)	Obstacles (3)	Cover and concealment (3)	Total
Integrated attack	**7**	**8**	**6**	**3**	**6**	
Limited objective attack	**5**	**6**	**8**	**2**	**4**	
Spoiling attack	**7**	**3**	**2**	**5**	**8**	
Counterattack	**4**	**3**	**2**	**5**	**4**	
Maneuver defense	**7**	**3**	**2**	**2**	**8**	
Area defense	**5**	**2**	**4**	**7**	**8**	

Figure 5-5. Weighted ranking (steps 1–5) to determine the threat's most likely COA

Options	***Criteria***					
	Observation and fields of fire (2)	Avenues of approach (1)	Key terrain (1)	Obstacles (3)	Cover and concealment (3)	Total
Integrated attack	**7(2) = 14**	**8(1) = 8**	**6(1) = 6**	**3(3) = 9**	**6(3) = 18**	**55**
Limited objective attack	**5(2) = 10**	**6(1) = 6**	**8(1) = 8**	**2(3) = 6**	**4(3) = 12**	**42**
Spoiling attack	**7(2) = 14**	**3(1) = 3**	**2(1) = 2**	**5(3) = 15**	**8(3) = 24**	**58**
Counterattack	**4(2) = 8**	**3(1) = 3**	**2(1) = 2**	**5(3) = 15**	**4(3) = 12**	**40**
Maneuver defense	**7(2) = 14**	**3(1) = 3**	**2(1) = 2**	**2(3) = 6**	**8(3) = 24**	**49**
Area defense	**5(2) = 10**	**2(1) = 2**	**4(1) = 4**	**7(3) = 21**	**8(3) = 24**	**61**

Figure 5-6. Weighted ranking (step 6) to determine the threat's most likely COA

LINK ANALYSIS

5-18. Link analysis, often known as network analysis, is a technique used to evaluate the relationships between several types of entities such as organizations, individuals, objects, or activities. Visualization tools augment this technique by organizing and displaying data and assisting in identifying associations within complex networks. Although analysts can perform link analysis manually, they often use software to aid this technique. Link analysis programs are standard components in the Army's intelligence systems, from theater to company levels.

Performing Link Analysis Manually

A manual approach to link analysis is using small sticky notes of paper on a whiteboard. The analyst labels the notes to represent different entities and nodes and places them on the whiteboard. Using markers, the analyst links the entities and nodes. This method has several benefits:

- A larger picture may be seen on a whiteboard than on a computer monitor; many automated systems present limited views.
- It allows movement of the entities, quick redrawing of links, and color-coding using different markers.
- It allows analysts to perform link analysis together in OEs with intermittent connectivity and limited bandwidth.

Note. Other manual practices include using a corkboard with thumbtacks, colored string or thread or incorporating a map to add geographic context.

5-19. Analysts may use link analysis to focus on leaders and other prominent individuals, who are sometimes critical factors in the AO. Analysts use personality files—often obtained from conducting identity activities using reporting and biometrics, forensics, and DOMEX data—to build organizational diagrams that assist them in determining relationships between critical personalities and their associations to various groups or activities. This analysis is critical in determining the roles and relationships of many different people and organizations and assessing their loyalties, political significance, and interests. (See ATP 2-01.3 for more information on assessing personalities and personality files.) Table 5-5 briefly describes when to use the link analysis technique, as well as the value added and potential pitfalls associated with using this technique.

Table 5-5. Link analysis technique

Link analysis: *Technique that maps and measures relationships or links among individuals, groups, or organizations.*		
When to use	**Value added**	**Potential pitfalls**
Analysts should use link analysis whenever individuals, groups, group activities, or process networks are being reviewed for insight. Analysts can use this technique to inform the targeting process and for assessing personalities, as accomplished during step 3 of the intelligence preparation of the battlefield process.	Link analysis can clarify what is known and what may be missing about the network being analyzed. Analysts can identify key nodes and hubs for social, organizational, and infrastructure networks, giving insight into relationships and potential vulnerabilities. Link analysis products are easily understood in briefings.	Analysts could assume (incorrectly) that a central figure in a network is the leader because of the number of connections to that figure. Analysts also might ignore the temporal aspect of the relationships and assume they are concurrent. Link analysis provides a freeze-frame look at an activity and seldom conveys change over time unless paired with a timeline or other multidimensional approach.

5-20. **Method.** The following steps describe how to construct a simple link analysis diagram:

- **Step 1:** Extract entities and the information about their relationships from intelligence holdings that include but are not limited to biometrics, forensics, and DOMEX information.
- **Step 2:** Place entity associations into a link chart using link analysis software or a spreadsheet or by drawing them manually:
  - Use separate shapes for different types of entities, for example, circles for people, rectangles for activities, and triangles for facilities. (See figure 5-7 on page 5-10.)
  - Use colored and varying types of lines to show different activities, for example, green solid lines for money transfers, blue dotted lines for communications, and solid black lines for activities. This differentiation typically requires a legend. (See figure 5-7 on page 5-10.)
- **Step 3:** Analyze the entities and links in the link chart.
- **Step 4:** Review the chart for gaps, significant relationships, and the meaning of the relationships based on the activity occurring. Ask critical questions of the data such as—
  - Which entity is central or key to the network?
  - Who or what is the initiator of interactions?
  - What role does each entity play in the network?

- Who or what forms a bridge or liaison between groups or subgroups?
- How have the interactions changed over time?
- Which nodes should be targeted for collection or defeat?

- **Step 5:** Summarize what is observed in the chart and draw interim hypotheses about the relationships.

5-21. The three types of visualization tools used in link analysis to record and visualize information are—

- Link diagram. (See figure 5-7.)
- Association matrix. (See figure 5-8.)
- Activities matrix. (See figure 5-9.)

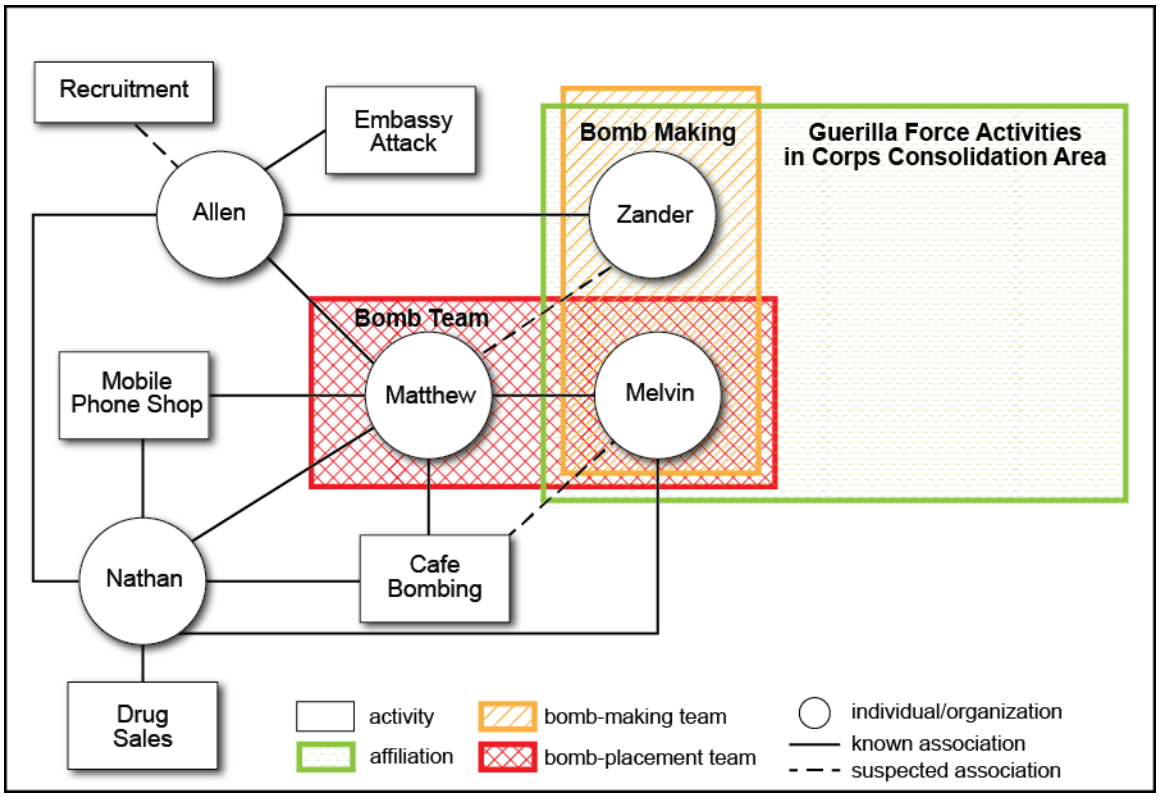


Figure 5-7. Link diagram example

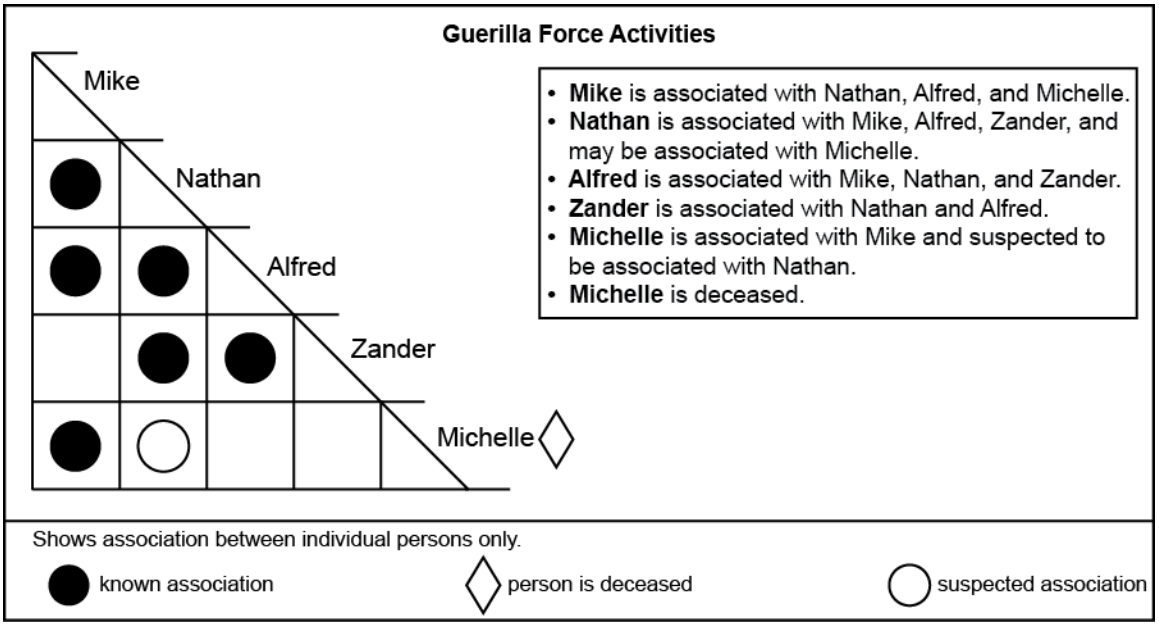


Figure 5-8. Association matrix example

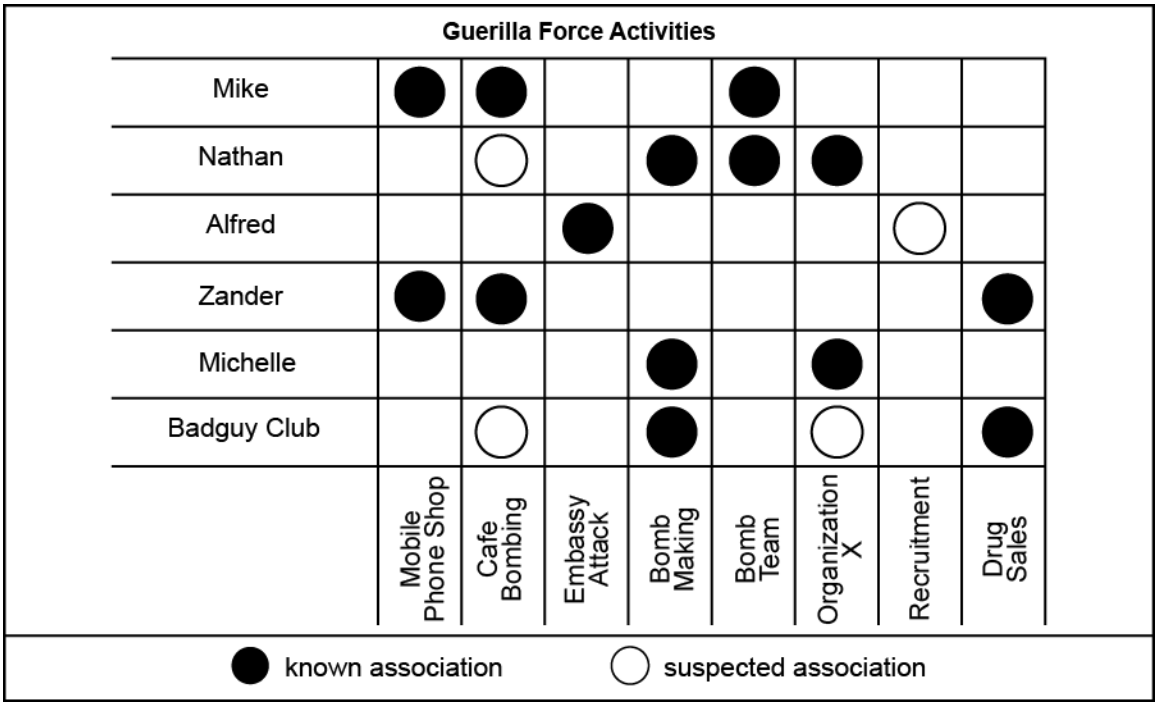


Figure 5-9. Activities matrix example

EVENT TREE

5-22. The event tree is a structured analytic technique that enables analysts to depict a possible sequence of events, including the potential branches of that sequence in a graphical format. An event tree works best when there are multiple, mutually exclusive options that cover the spectrum of reasonable alternatives. It clarifies the presumed sequence of events or decisions between an initiating event and an outcome. Table 5-6 briefly describes when to use the event tree technique, as well as the value added and potential pitfalls associated with this using technique. The following are pointers for analysts using the event tree technique:

- Use this technique in conjunction with weighted ranking, hypothesis-review techniques, and subjective probability to gain added insights.
- Leverage the expertise of a group of analysts during the construction of an event tree to ensure all events, factors, and decision options are considered.

Table 5-6. Event tree technique

Event tree: *A graphical depiction of a potential temporal sequence of events, including potential junctures within the event sequence.*		
When to use	**Value added**	**Potential pitfalls**
Analysts can use an event tree to clarify alternative event sequences with potential future outcomes or at least unknown outcomes related to an intelligence problem.	An event tree is a visual tool that analysts can use to depict a threat's options with decision points, which may provide insight into potential threat vulnerabilities. Event trees also provide an excellent method of determining collection requirements for indications that a decision has been made or events have unfolded in one of the alternative branches of the tree.	An intelligence failure can occur when the threat selects an unforeseen option arising from ignorance or when an unidentified event occurs.

5-23. **Method.** The following outlines the steps for creating event trees (see figure 5-10):

- **Step 1:** Identify the intelligence issue/problem (antigovernment protest in Egypt).
- **Step 2:** Identify the mutually exclusive and complete set of hypotheses that pertain to the intelligence issue/problem (Mubarak resigns or Mubarak stays).
- **Step 3:** Decide which events, factors, or decisions (such as variables) will have the greatest influence on the hypotheses identified in step 2.
- **Step 4:** Decide on the sequencing for when these factors are expected to occur or affect one another.
- **Step 5:** Determine the event options (Mubarak stays—hardline, reforms, some reforms) within each hypothesis and establish clear definitions for each event option to ensure collection strategies to monitor events are effective.
- **Step 6:** Construct the event tree from left to right. Each hypothesis is a separate main branch. Start with the first hypothesis and have one branch from this node for each realistic path the first event can take. Proceed down each event option node until the end state for that subbranch is reached. Then move to the next hypothesis and repeat the process.
- **Step 7:** Determine what would indicate a decision has been made at each decision point for each option to use in generating an integrated collection plan.
- **Step 8:** Assess the implications of each hypothesis on the intelligence problem.

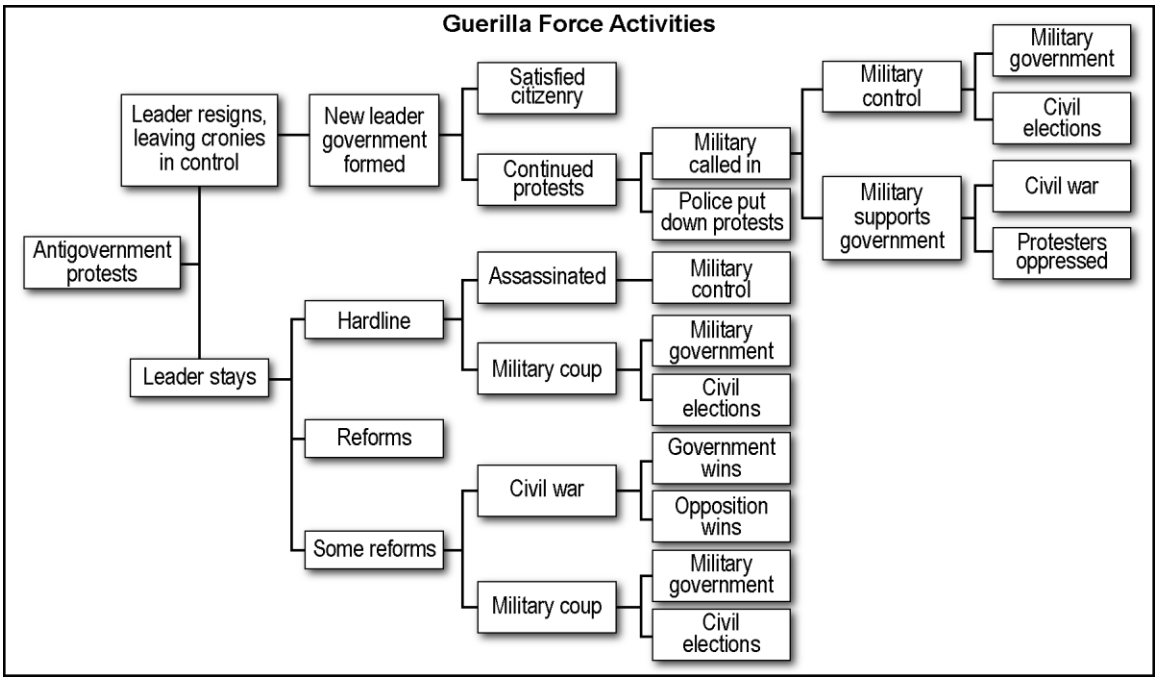


Figure 5-10. Event tree example

EVENT MAPPING

5-24. The event mapping technique uses brainstorming to assist in diagraming scenarios/elements stemming from analyst-derived hypotheses. Scenarios/Elements are linked around a central word or short phrase representing the issue/problem to be analyzed. (See paragraph 6-20 for more information on brainstorming.)

5-25. Event mapping scenarios/elements are arranged intuitively based on the importance of the concepts, and they are organized into groups, branches, or areas. Using the radial diagram format in event mapping assists in mitigating some bias, such as implied prioritization, anchoring, or other cognitive biases derived from hierarchy or sequential arrangements. Table 5-7 on page 5-14 briefly describes when to use the event mapping technique, as well as the value added and potential pitfalls associated with using this technique. The following includes event mapping general rules:

- Start with a blank medium such as paper or use a piece of stationery with adhesive on the back to make notes on a whiteboard.
- Think in terms of key words, phrases, or symbols that represent ideas and words.
- Annotate ideas as they occur, wherever they fit.
- Do not judge or hold back. Develop the map in the direction the topics flow—do not be limited by the map's appearance.
- As the map expands, strive to be more detailed.
- Use arrows or other visual aids to show the links between events in the scenario.
- Use color, as appropriate, to represent key players such as economics, military opposition groups, science, culture, and internal and external political pressures.

Table 5-7. Event mapping technique

Event mapping: *A mind-mapping diagram that represents the scenarios in hypotheses linked around a central issue.*		
When to use	**Value added**	**Potential pitfalls**
Analysts should use this technique when a nonlinear method is desired to generate, visualize, structure, and delineate the events in a scenario or hypotheses related to the intelligence issue/problem.	Event mapping uses a radial diagram that encourages a brainstorming approach. The many associations in event maps promote creativity in generating new ideas and associations not previously considered. This technique facilitates annotating indicators of change in developing collection plans.	Unconstrained event mapping can become overly detailed, lose focus, and include events and scenarios that lack relevance to the issue/problem analysts are studying.

5-26. **Method.** The following outlines the steps for applying event maps (see figure 5-11):

- **Step 1:** Place the word or symbol representing the issue/problem to be analyzed in the center of the medium from which the event map will be constructed.
- **Step 2:** Add symbols/words to represent possible actions/outcomes around the central issue/problem.
- **Step 3:** Link the possible actions/outcomes to the central issue or problem. If desired, use colors to indicate the major influence the link represents. For example, use green for economic links, red for opposition groups, or purple for military forces. Colors may also be used to differentiate paths for ease of reference.
- **Step 4:** Continue working outward, building the scenario of events into branches and subbranches for each hypothesis in detail.
- **Step 5:** If ideas end, move to another area or hypothesis.
- **Step 6:** When creativity wanes, stop and take a break. After the break, return and review the map and make additions and changes as desired.
- **Step 7:** As an option, number the links or decision points for each hypothesis. On a separate piece of paper, write down the evidence for each number to be collected that would disprove that link or decision. Use the lists for each number to develop an integrated collection strategy for the issue/problem.

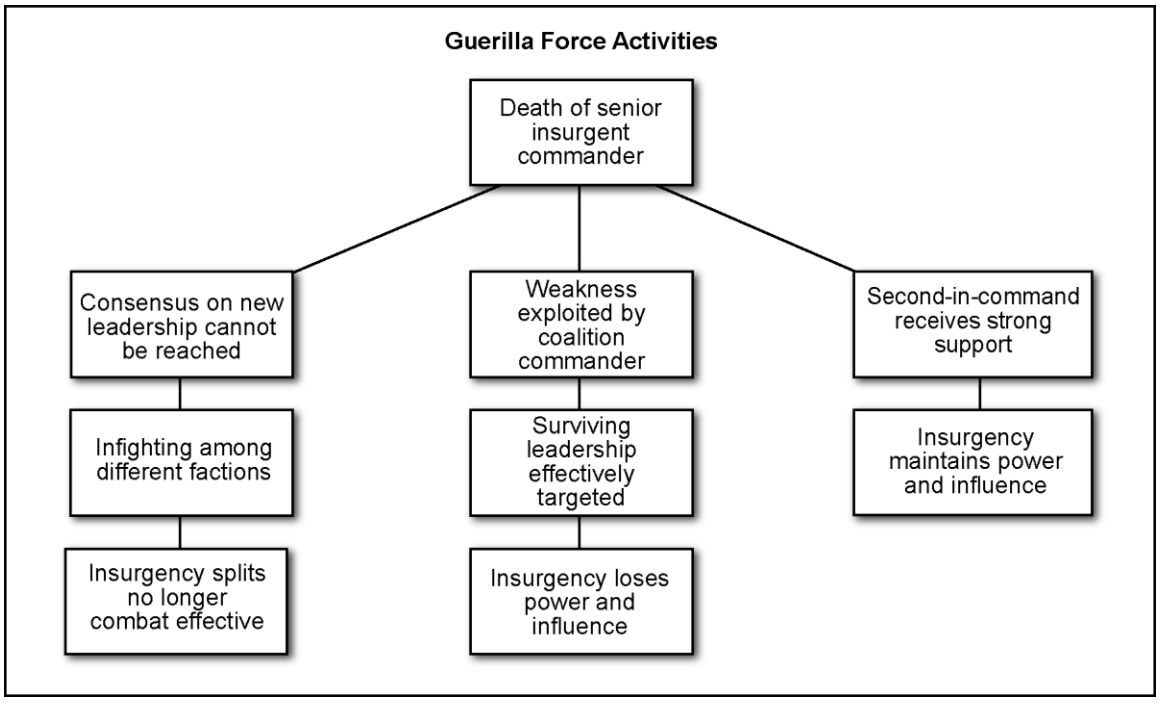


Figure 5-11. Event mapping example

SECTION II – DIAGNOSTIC STRUCTURED ANALYTIC TECHNIQUES

5-27. Diagnostic structured analytic techniques make analytical arguments, assumptions, and/or intelligence gaps more transparent. They are often used in association with most other analytic techniques to strengthen analytical assessments and conclusions. The most commonly used diagnostic techniques are—

- **Key assumptions check technique:** Reviewing assumptions that form the analytical judgments of the problem.
- **Quality of information check technique:**
  - Source credibility and access.
  - Plausibility of activity.
  - Imminence of activity.
  - Specificity of activity.
- **Indicators/Signposts of change technique:**
  - Identifying a set of competing hypotheses.
  - Creating lists of potential or expected events.
  - Reviewing/Updating indicator lists.
  - Identifying most likely hypotheses.

KEY ASSUMPTIONS CHECK

5-28. A key assumption is any hypothesis that analysts have accepted to be true and forms the basis of an assessment. For example, analysts may focus exclusively on analyzing key technical military variables of a military force and assume that a force will operate in a particular environment such as a desert, open plain, or arctic setting. The goal of this technique is not to undermine or abandon key assumptions; rather, it is to make them explicit and identify what information or developments would demand rethinking them.

5-29. Rechecking assumptions is valuable at any time before finalizing judgments. Key assumptions checks should be collaborative because an analyst cannot effectively self-check. Table 5-8 describes when to use this technique, as well as the value added and potential pitfalls associated with using this technique.

Table 5-8. Key assumptions check technique

Key assumptions check: *An exercise in explicitly listing and challenging key working assumptions that underlie the basic analysis.*		
When to use	**Value added**	**Potential pitfalls**
A key assumptions check is most beneficial at the beginning of an analytic project. Analysts typically identify key assumptions during step 2 of the military decision-making process.	Explicitly identifying working assumptions during an analytic project assists analysts in— • Explaining the logic of the analytical argument and exposing faulty logic. • Understanding key factors that shape an issue. • Stimulating thinking about an issue. • Uncovering hidden relationships and links between key factors. • Identifying developments that would cause them to abandon an assumption. • Preparing for changed circumstances that could surprise them.	Identifying hidden assumptions is difficult because they are ideas believed to be true, albeit often subconsciously. Therefore, the assumptions are seldom examined and almost never challenged.

5-30. **Method.** Checking for key assumptions requires analysts to consider how their analysis depends on the validity of certain evidence. The following four-step process assists analysts in checking key assumptions:

- **Step 1:** Review what the current analytic line of thinking on the issue appears to be:
  - What do analysts think they know?
  - What key details assist analysts in accepting that the assumption is true?
- **Step 2:** Articulate the evidence, both stated and implied in finished intelligence, accepted as true.

- **Step 3:** Challenge the assumption by asking why it must be true and is it valid under all conditions. What is the degree of confidence in those initial answers?
- **Step 4:** Refine the list of key assumptions to contain only those that must be true in order to sustain the analytic line of thinking. Consider under what circumstances or based on what information these assumptions might not be true.

5-31. Analysts should ask the following questions during this process:

- What is the degree of confidence that this assumption is true?
- What explains the degree of confidence in the assumption?
- What circumstances or information might undermine this assumption?
- Is a key assumption more likely a key uncertainty or key factor?
- If the assumption proves to be wrong, would it significantly alter the analytic line of thinking? How?
- Has this process identified new factors that require further analysis?

QUALITY OF INFORMATION CHECK

5-32. Weighing the validity of sources is a key feature of any analytical assessment. Establishing how much confidence analysts have in their analytical judgments should be based on the information's reliability and accuracy. Analysts should perform periodic checks of the information for their analytical judgments; otherwise, important analytical judgments may become anchored to poor-quality information.

5-33. Determining the quality of information independent of the source of the information is important in ensuring that neither duly influences the other. Not understanding the context in which critical information has been provided makes it difficult for analysts to assess the information's validity and establish a confidence level in the intelligence assessment. A typically reliable source can knowingly report inaccurate information, and a typically unreliable source can sometimes report high-quality information. Therefore, it is important to keep the two reviews—source and information—separate. Table 5-9 briefly describes when to use the quality of information check technique, as well as the value added and potential pitfalls associated with using this technique. This technique—

- Provides the foundation for determining the confidence level of an assessment and clarity to an analyst's confidence level in the assessment.
- Provides an opportunity to catch interpretation errors and mitigate assimilation or confirmation bias based on the source:
  - **Assimilation bias** is the modification and elaboration of new information to fit prior conceptions or hypotheses. The bias is toward confirming a preconceived answer.
  - **Confirmation bias** is the conditions that cause analysts to undervalue or ignore evidence that contradicts an early judgment and value evidence that tends to confirm already held assessments.
- Identifies intelligence gaps and potential denial and deception efforts.

Table 5-9. Quality of information check technique

Quality of information check: *A way to evaluate the completeness and validity of available information separately from the source.*		
When to use	**Value added**	**Potential pitfalls**
This technique should be initially applied during the screen phase of the analysis process. Periodic reviews of the quality of information should be conducted to prevent assumptions or weak judgments from becoming facts over time. Checking the quality of information is an ongoing, continuous process.	A thorough quality of information check provides analysts with an accurate assessment of "what we know" and "what we do not know." Additionally, this technique provides validity to analysts' confidence levels in assessments.	Analysts can become susceptible to circular reporting and source-based bias when reviewing the quality of information. Analysts may not consider that critical information may sometimes be found in reports from sources judged to have a low level of access or a poor record.

5-34. **Method.** For an information review to be fully effective, analysts need as much background information on sources as is possible. At a minimum, analysts should perform the following steps:

- **Step 1:** Review all sources of information for accuracy; identify any of the more critical or compelling sources. (For example, a human source with direct knowledge is compelling.)
- **Step 2:** Determine if analysts have sufficient and/or strong collaboration between the information sources.
- **Step 3:** Reexamine previously dismissed information considering new facts or circumstances.
- **Step 4:** Ensure any circular reporting is identified and properly flagged for other analysts; analysis based on circular reporting should also be reviewed to determine if the reporting was essential to the judgments made. (For example, a human source's purpose for providing information may be to deceive.)
- **Step 5:** Consider whether ambiguous information has been interpreted and qualified properly. (For example, a signals intelligence transcript may be incomplete.)
- **Step 6:** Indicate a level of confidence analysts can place on sources that may likely figure into future analytical assessments.

5-35. Analysts can use table 5-10 as a questioning guideline. Table 5-10 is not an all-inclusive list of questions, as it does not include every intelligence discipline. It is a start point for analysts to check the quality of the information; analysts can expand the list of questions to include other intelligence disciplines.

Table 5-10. Questioning guideline for checking information quality

Counterintelligence/Human intelligence
• Who wrote the report, and to what organization does the report writer belong? • What changes have been made to the data since the original collection? • What is the collector's evaluation of the information in the report? • Can the source's purpose be ascertained? • Was the information first-, second-, or third-hand? • Is there information from a different intelligence discipline that corroborates this report? • Is the information consistent or inconsistent with previous information? • Does the analyst have any concerns that denial and deception may be in the information? Why?
Geospatial intelligence
• What is the frequency of collection? When does it occur (time/day)? Have there been any recent changes to the frequency of collection or exploitation? • Are additional images being taken at different times? • Is the target aware of overhead imagery capabilities? • Are geospatial intelligence-based indicators being used to assess the site or the activity? • Is there a geospatial aspect to the information?
Signals intelligence
• Communications intelligence: ▪ Is this a complete transcript (verbatim) or a processed (analyzed) summary of the traffic? ▪ Was this report a snippet of a much longer conversation? ▪ Did the collection shortfall preclude capturing all the traffic? • Electronic intelligence: ▪ Is the signal correlated to any events or activities? ▪ What was the duration of the collection? ▪ What is the frequency of the collection? When does it occur (time/day)? ▪ Are additional signals being collected at different times? ▪ Is there additional intelligence that correlates with this emitter activity? ▪ Has the activity been corroborated by another form of intelligence?

Note. Analysts should consciously avoid relating the source to the information until the quality of information check is complete. If relating the source to the quality of information changes the opinion of the information, analysts must ensure they can articulate why. Analysts should develop and employ a spreadsheet to track the information and record their confidence levels in the quality of information as a constant reminder of the findings.

INDICATORS/SIGNPOSTS OF CHANGE

5-36. The indicators/signposts of change technique is primarily a diagnostic tool that assists analysts in identifying persons, activities, developments, or trends of interest. Indicators/Signposts of change are often tied to specific scenarios created by analysts to help them identify which scenario is unfolding. Indicators/Signposts of change are a preestablished set of observable phenomena periodically reviewed to help track events, spot emerging trends, and warn of unanticipated change. These observable phenomena are events expected to occur if a postulated situation is developing. For example, some of the observable events of a potential protest include—

- The massive gathering of people at a specific location.
- People's rallying cries posted as messages on social media.
- An adjacent country's aggressive national training and mobilization drills outside of normal patterns.

5-37. Analysts and other staff members create a list of these observable events and the detection and confirmation of these indicators enable analysts to answer specific information requirements that answer PIRs. Collection managers often use these lists to help create an intelligence collection plan. A list of indicators allows analysts to track developments and build a more concrete case for analytical judgments.

5-38. This technique aids other structured analytic techniques that require hypotheses generation as analysts create indicators that can confirm or deny these hypotheses. Analysts may use indicators/signposts of change to support analysis during all operations of the Army's strategic roles and to assist them in identifying a change in the operations. Table 5-11 briefly describes when to use the indicators/signposts of change technique, as well as the value added and potential pitfalls associated with using this technique.

Table 5-11. Indicators/Signposts of change technique

Indicators/Signposts of change: *A preestablished set of observable phenomena periodically reviewed to help track events, spot emerging trends, and warn of unanticipated change.*		
When to use	**Value added**	**Potential pitfalls**
The technique can be used whenever analysts need to track an event over time to monitor and evaluate changes. It can also amplify other structured analytic techniques and support collection management and current operations.	By providing an objective baseline for tracking events or targets, indicators/signposts of change instill rigor into the analysis process and enhance the credibility of analytical judgments.	Poor indicators can lead to analytic failures. This technique requires analysts to continually check the validity of the indicators as their original assumptions may be outdated or too narrow in focus.

5-39. **Method.** Whether used alone or in combination with other structured analysis, the process is the same. When developing indicators, analysts start from the event, work backwards, and include as many indicators as possible. The following outlines the steps to the indicators/signposts of change technique:

- **Step 1:** Identify a set of competing hypotheses or scenarios.
- **Step 2:** Create separate lists of potential activities, statements, or events expected for each hypothesis or scenario.
- **Step 3:** Regularly review and update the indicator lists to see which are changing.
- **Step 4:** Identify the most likely or most correct hypothesis or scenario based on the number of changed indicators observed.

Note. Analysts should avoid making an assessment based on a single indicator. Integrating multiple indicators is essential for analysts to obtain the clearest picture and assists in mitigating threat deception efforts.

Chapter 6

Advanced Structured Analytic Techniques

SECTION I – CONTRARIAN STRUCTURED ANALYTIC TECHNIQUES

6-1. Contrarian structured analytic techniques challenge ongoing assumptions and broaden possible outcomes. They assist analysts in understanding threat intentions, especially when not clearly stated or known. Contrarian techniques explore the problem from different (often multiple) perspectives. This allows analysts to better accept analytic critique and grant greater avenues to explore and challenge analytical arguments and mindsets. Proper technique application assists analysts in ensuring preconceptions and assumptions are thoroughly examined and tested for relevance, implication, and consequence.

6-2. The contrarian structured analytic techniques described in this publication are—

- **Analysis of competing hypotheses (ACH) technique:** Evaluating multiple hypotheses through a competitive process in order to reach unbiased conclusions and attempting to corroborate results.
- **Devil's advocacy technique:** Challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation.
- **Team A/Team B technique:** Using separate analytic teams that contrast two (or more) strongly held views or competing hypotheses.
- **High-impact/Low-probability analysis technique:** Highlighting an unlikely event that would have major consequences if it happened.
- **What if? analysis technique:** Assuming an event has occurred with potential (negative or positive) impacts and explaining how it might happen.

ANALYSIS OF COMPETING HYPOTHESES

6-3. Analysts use ACH to evaluate multiple competing hypotheses in order to foster unbiased conclusions. Analysts identify alternative explanations (hypotheses) and evaluate all evidence that will disconfirm rather than confirm hypotheses. While a single analyst can use ACH, it is most effective with a small team of analysts who can challenge each other's evaluation of the evidence.

6-4. ACH requires analysts to explicitly identify all reasonable alternatives and evaluate them against each other rather than evaluate their plausibility one at a time. ACH involves seeking evidence to refute hypotheses. The most probable hypothesis is usually the one with the least evidence against it, not the one with the most evidence for it. Conventional analysis generally entails looking for evidence to confirm a favored hypothesis. Analysts sometimes integrate the weighted ranking technique with ACH; this can help elevate one hypothesis in favor of another. Table 6-1 on page 6-2 briefly describes when to use the ACH technique, as well as the value added and potential pitfalls associated with using this technique.

Table 6-1. Analysis of competing hypotheses technique

Analysis of competing hypotheses (ACH): *A technique that uses a matrix as a tool to aid judgment on issues requiring careful weighting of alternative explanations or conclusions.*		
When to use	**Value added**	**Potential pitfalls**
ACH is highly effective when there is a large amount of data to absorb and evaluate. It is particularly appropriate when analysts want to develop a clear record that shows what theories they have considered and how they arrived at their judgments. This technique is useful for generating predictive assessments, as required, during step 4 of the intelligence preparation of the battlefield process.	ACH helps analysts overcome the following common mistakes that can lead to inaccurate forecasts: • Susceptibility to being unduly influenced by a first impression based on incomplete data, an existing analytic line of thought, or a single explanation that seems to fit well enough. • Lack of generating a full set of explanations or hypotheses at the outset of a project. • Reliance on evidence to support their preferred hypothesis, but that is also consistent with other explanations.	There are occasions when there is not enough evidence to arrive at a conclusion using ACH, or when the evidence is unbalanced enough—such as when using intelligence primarily from a single source—to lead to an inaccurate conclusion.

6-5. **Method.** Simultaneous evaluation of multiple competing hypotheses is difficult to accomplish without using tools. Retaining these hypotheses in working memory and then assessing how each piece of evidence interacts with each hypothesis is beyond the mental capabilities of most individuals. To manage the volume of information, analysts use a matrix as a tool to complete ACH. (See figure 6-1.) The following outlines the steps used to complete ACH:

- **Step 1:** Identify the intelligence problem.
- **Step 2:** Identify all possible hypotheses related to the intelligence problem.
- **Step 3:** Gather and make a list of all information related to the intelligence problem.
- **Step 4:** Prepare a matrix with each hypothesis across the top and each piece of information down the left side.
- **Step 5:** Determine if each piece of information is consistent or inconsistent with each hypothesis.
- **Step 6:** Refine the matrix. Reconsider the hypotheses and remove information that has no diagnostic value.
- **Step 7:** Draw tentative conclusions about the relative likelihood of each hypothesis.
- **Step 8:** Analyze if conclusions rely primarily on a few critical pieces of information.
- **Step 9:** Report conclusions.
- **Step 10:** Identify milestones for future observation that may indicate events are taking a different course than expected.

Guerilla Force Activities				
Evidence / Hypothesis (H)	H1 Threat 1/Threat 2 targets SECSTATE at summit.	H2 Threat 1/Threat 2 targets summit to disrupt peace process.	H3 Threat 1 targets SECSTATE at summit.	H4 Threat 1 targets summit to disrupt peace process.
Threat 1 facilitates attack on security force in AO (internet video post crediting Threat 2).	?	C	?	C
Threat 1 coordinates for *exterior talent* to execute security force bombing.	I	C	C	I
Threat 1 is more than a facilitator (completes security force bombing personally).	?	?	?	?
Threat 1 establishes safe house in AO in mid-June.	C	C	C	I
Threat 1 attempts to move targeting resources in AO in mid-June (exterior talent four personnel from unknown country).	C	C	C	I
Threat 1 references *conference* in AO in July and requests for *sales partner* and additional material.	C	C	C	I
Threat 1 facilitates attack on hotel in capital (no video - no credit).	I	C	C	I
No reporting on Threat 1 post attack on hotel in capital.	?	?	?	?
AO area of operations C consistent	I inconsistent SECSTATE Secretary of State			? neutral

Figure 6-1. Analysis of competing hypotheses used during step 4 of the IPB process

DEVIL'S ADVOCACY

6-6. Analysts use the devil's advocacy technique for reviewing proposed analytical conclusions. They are usually not involved in the deliberations that led to the proposed analytical conclusion. Devil's advocacy is most effective when used to challenge an analytic consensus or a key assumption about a critically important intelligence question. In some cases, analysts can review a key assumption and present a product that depicts the arguments and data that support a contrary assessment. Devil's advocacy can provide further confidence that the current analytic line of thought will endure close scrutiny. Table 6-2 briefly describes when to use the devil's advocacy technique, as well as the value added and potential pitfalls associated with using this technique. Devil's advocacy can lead analysts to draw one of three conclusions:

- Analysts ignored data or key lines of argument that undermine their analysis and should restart the analysis process.
- The analysis is sound, but more research is warranted in select areas.
- Key judgments are valid, but a higher level of confidence in the bottom-line judgments is warranted.

Table 6-2. Devil's advocacy technique

Devil's advocacy: *The process of challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation.*		
When to use	**Value added**	**Potential pitfalls**
This technique is useful when there is concern about seemingly widespread unanimity amongst analysts on a critical issue. Analysts should assume the role of the devil's advocate if they have some doubts about a widely held view, or a leader might designate that analysts challenge the prevailing wisdom in order to reaffirm the group's confidence in those assessments.	Devil's advocacy challenges the current consensus to ensure analysts do not overlook alternate possibilities. It highlights the weaknesses in a current analytical judgment or assists in reaffirming analysts' confidence in the conclusion by— • Explicitly challenging key assumptions. • Identifying any faulty logic or information. • Presenting alternative hypotheses.	Those who strongly advocate an analytical judgment will resist a devil's advocacy approach. This technique challenges assumptions, but it can turn into an analytical argument with analysts taking sides rather than exploring the issue at hand.

6-7. **Method.** The following outlines the steps for the devil's advocacy technique:

- **Step 1:** Present the main analytical conclusion.
- **Step 2:** Outline the main points and key assumptions and characterize the evidence supporting the current analytical view.
- **Step 3:** Select one or more assumptions that appear the most susceptible to challenge.
- **Step 4:** Review the data used to determine questionable validity, possible deception, and the existence of gaps.
- **Step 5:** Highlight evidence that supports an alternative hypothesis or contradicts current thinking.
- **Step 6:** Present findings that demonstrate flawed assumptions, poor evidence, or possible deception.

6-8. Analysts should consider the following when conducting the devil's advocacy technique:

- Sources of uncertainty.
- Diagnosticity of evidence.
- Anomalous evidence.
- Changes in the broad environment.
- Alternative decision models.
- Availability of cultural expertise.
- Indicators of possible deception.
- Information gaps.

TEAM A/TEAM B

6-9. Team A/Team B is a process for comparing, contrasting, and clarifying two (or more) equally valid analytical assessments. Multiple teams of analysts perform this process, each working along different lines of analysis. Team A/Team B involves separate analytic teams that analyze two (or more) views or competing hypotheses. Team A/Team B is different from devil's advocacy, which challenges a single dominant mindset instead of comparing two (or more) strongly held views. Team A/Team B recognizes that there may be competing, and possibly equally strong, mindsets on an issue that needs to be clarified. A key requirement to ensure technique success is equally experienced competing mindsets. This mitigates unbalanced arguments. Table 6-3 briefly describes when to use the team A/team B technique, as well as the value added and potential pitfalls associated with using this technique.

Note. If opposing positions are well established, it can be useful to place analysts on teams that advocate positions they normally do not support; forcing analysts to argue the other side can make them more aware of their own mindsets.

Table 6-3. Team A/Team B technique

Team A/Team B: *Use of independent teams to contrast two (or more) strongly held views or competing hypotheses.*		
When to use	**Value added**	**Potential pitfalls**
If there are at least two competing views on a key issue, then team A/team B may be the appropriate technique to apply. Use when there are equally strong mindsets held on an issue that needs to be clarified.	This technique may help opposing groups see merit in each other's perspective. This reduces friction and differences by allowing those holding opposing views to feel their hypotheses have been given equal attention.	If the two teams are unequally matched, then the two views may receive an unequal amount of support.

6-10. **Method.** The following steps outlines the steps of the team A/team B technique (see figure 6-2):

- **Step 1:** Identify the two (or more) competing hypotheses.
- **Step 2:** Form teams and designate individuals to develop the best case for each hypothesis.
- **Step 3:** Review information that supports each respective position.
- **Step 4:** Identify missing information that would support or bolster the hypotheses.
- **Step 5:** Prepare a structured argument with an explicit discussion of—
  - Key assumptions.
  - Key evidence.
  - The logic behind the argument.
- **Step 6:** Set aside the time for a formal debate or an informal brainstorming session.

- **Step 7:** Have an independent jury of peers listen to the oral presentation and be prepared to question the teams about their assumptions, evidence, and/or logic.
- **Step 8:** Allow each team to present its case, challenge the other team's argument, and rebut the opponent's critique of its case.
- **Step 9:** The jury considers the strength of each presentation and recommends possible next steps for further research and collection efforts.

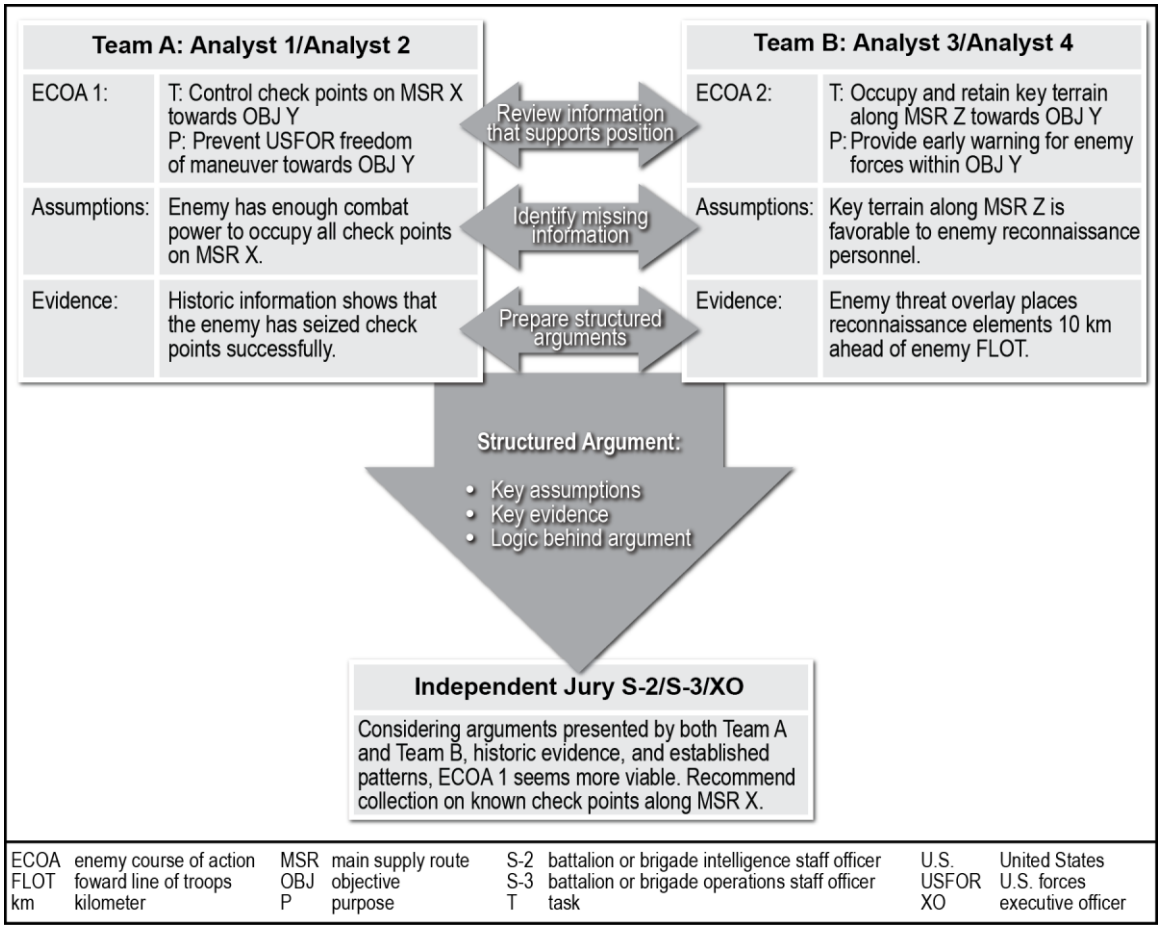


Figure 6-2. Team A/Team B used during step 4 of the IPB process

HIGH-IMPACT/LOW-PROBABILITY ANALYSIS

6-11. The high-impact/low-probability analysis technique sensitizes analysts to the potential impact that seemingly low-probability events could have on U.S. forces. New and often fragmentary data suggesting that a previously unanticipated event might occur is a trigger for applying this technique.

6-12. Mapping out the course of an unlikely, yet plausible event may uncover hidden relationships between key factors and assumptions; it may also alert analysts to oversights in the analytic line of thought. This technique can augment hypotheses-generating analytic techniques.

6-13. The objective of high-impact/low-probability analysis is exploring whether an increasingly credible case can be made for an unlikely event occurring that could pose a major danger or open a window of opportunity. Examining the unlikely allows analysts to develop indicators that may provide early warnings of a shift in the situation. By periodically reviewing those indicators, analysts are likely to counter any prevailing mindset that such a development is highly unlikely. Table 6-4 on page 6-6 briefly describes when to use high-impact/low-probability analysis, as well as the value added and potential pitfalls associated with using this technique.

Table 6-4. High-impact/Low-probability analysis technique

High-impact/Low-probability analysis: *Provides decision makers with an early warning that a seemingly unlikely but impactful event might actually occur.*		
When to use	**Value added**	**Potential pitfalls**
Analysts should use high-impact/low-probability analysis to analyze a threat's worst-case scenario.	This technique allows analysts to explore the consequences of an event—particularly an event not deemed likely by conventional wisdom—without having to challenge the main-line judgment or argue about how likely an event is to occur.	Analysts that communicate the likelihood of low-probability events occurring may cause intelligence assessment consumers to disregard those events. Therefore, analysts should use caution when communicating likelihoods. Additionally, high-impact/low-probability analysis is sometimes confused with "what if" analysis.

6-14. **Method.** An effective high-impact/low-probability analysis involves the following steps:

- **Step 1:** Define the high-impact outcome clearly. This will justify examining what may be deemed a very unlikely development.
- **Step 2:** Devise one or more plausible pathways to the low-probability outcome. Be precise, as it may aid in developing indicators for later monitoring.
- **Step 3:** Insert possible triggers or changes in momentum if appropriate (such as natural disasters, sudden key leader health problems, or economic or political turmoil).
- **Step 4:** Brainstorm plausible but unpredictable triggers of sudden change.
- **Step 5:** Identify a set of indicators for each pathway that help anticipate how events are likely to develop and periodically review those indicators.
- **Step 6:** Identify factors that could deflect a bad outcome or encourage a positive one.

"WHAT IF?" ANALYSIS

6-15. "What if?" analysis is a technique for challenging a strong mindset that an event will not occur or that a confidently made forecast may not be entirely justified. "What if?" analysis is similar to high-impact/low-probability analysis; however, it does not focus on the consequences of an unlikely event. "What if" analysis attempts to explain how the unlikely event might transpire. It also creates an awareness that prepares analysts to recognize early signs of a significant change.

6-16. "What if" analysis can also shift focus from asking whether an event will occur to working from the premise that it has occurred. This allows analysts to determine how the event might have happened. This technique can augment hypotheses-generating analytic techniques using multiple scenario generation or ACH. "What if?" analysis shifts the question from "How likely is the event?" to the following:

- How could the event possibly occur?
- What would be the impact of the event?
- Has the possibility of the event happening increased?

6-17. Like other contrarian techniques, "what if?" analysis must begin by stating the conventional analytic line of thought and then stepping back to consider alternative outcomes that are too important to dismiss no matter how unlikely. Table 6-5 briefly describes when to use the "what if?" analysis, as well as the value added and potential pitfalls associated with using this technique.

Table 6-5. "What if?" analysis technique

"What if?" analysis: *Assumes that an event has occurred with a potential for a major or negative impact and then explains how it came about using hindsight.*		
When to use	**Value added**	**Potential pitfalls**
Using this technique is important when a judgment relies on limited information or unproven assumptions. "What if?" analysis is also a logical follow-up to a key assumptions check that identifies an assumption that is critical to an important estimate but about which there is some doubt.	This technique opens the mind to think differently and creatively. It also provides decision makers a better sense of what can be done to prevent a development from occurring. Additionally, the technique facilitates developing indicators for a potential event.	"What if?" analysis is sometimes confused with high-impact/low-probability analysis. Analysts may waste time if the event hypothesized is inconceivable.

6-18. **Method.** The "what if?" analysis steps are similar to the high-impact/low-probability analysis steps once analysts have established the event itself:

- **Step 1:** Assume the event has happened.
- **Step 2:** Select some triggering events that permitted the scenario to unfold to help make the "what if?" more plausible (for example, the death of key leader, a natural disaster, an economic or political event that might start a chain of other events).
- **Step 3:** Develop a chain of reasoning based on logic and evidence to explain how this outcome could have occurred.
- **Step 4:** Think backwards from the event in concrete ways, specifying what must occur at each stage of the scenario.
- **Step 5:** Identify one or more plausible pathways to the event; it is likely that more than one will appear possible.
- **Step 6:** Generate an indicators/signposts of change list to detect the beginnings of the event.
- **Step 7:** Consider the scope of positive and negative consequences and their relative impact.
- **Step 8:** Monitor the indicators developed periodically.

High-Impact/Low-Probability Analysis Versus "What If?" Analysis

- High-impact/Low-probability analysis primarily warns decision makers that recent, unanticipated developments suggest an event, previously deemed highly unlikely, might occur. It projects forward, extracting from recent evidence or information.
- Conversely, "what if?" analysis does not typically require new evidence or anomalous information as a trigger. It looks back, imagining a surprising outcome and then mapping several ways that outcome could occur.

SECTION II – IMAGINATIVE STRUCTURED ANALYTIC TECHNIQUES

6-19. Imaginative structured analytic techniques assist analysts in approaching an analytic problem from different and multiple perspectives. This technique also broadens analysts' selection of potential COAs, thus reducing the chance of missing unforeseen outcomes. Imaginative techniques facilitate analysts' ability to forecast events and generate ideas creatively. Additionally, the proper application of imaginative techniques can assist in identifying differences in perspectives and different assumptions among analytic team members. The most commonly used imaginative techniques are—

- **Brainstorming technique:** Generating new ideas and concepts through unconstrained groupings.
- **Functional analysis technique:**
  - Identifying threat vulnerabilities through knowledge of threat capabilities.
  - Identifying windows of opportunity and threat vulnerabilities.

- **Outside-in thinking technique:** Identifying the full range of basic factors and trends that indirectly shape an issue.
- **Red hat/team analysis technique:** Modeling the behavior of an individual or group by trying to replicate how a threat would think about an issue.

BRAINSTORMING

6-20. Brainstorming is a widely used technique for stimulating new thinking; it can be applied to most other structured analytic techniques as an aid to thinking. Brainstorming is most effective when analysts have a degree of subject matter expertise on the topic of focus.

6-21. Brainstorming should be a very structured process to be most productive. An unconstrained, informal discussion might produce some interesting ideas, but usually a more systematic process is the most effective way to break down mindsets and produce new insights. The process involves a **divergent thinking phase** to generate and collect new ideas and insights, followed by a **convergent thinking phase** for grouping and organizing ideas around key concepts. Table 6-6 briefly describes when to use the brainstorming technique, as well as the value added and potential pitfalls associated with using this technique.

Table 6-6. Brainstorming structured technique

Brainstorming: *A technique that involves a group process for generating new ideas and concepts.*		
When to use	**Value added**	**Potential pitfalls**
Typically, analysts apply structured brainstorming when they begin a project to help generate a range of hypotheses about an issue or when amplifying other analytic techniques.	This technique can maximize creativity in the thinking process. Structured brainstorming allows analysts to see a wider range of factors that might bear on the topic than they would otherwise consider. It can spark new ideas, ensure a comprehensive look at a problem, raise questions, and prevent premature consensus.	There may not be enough time to apply structured brainstorming correctly, to include establishing rules and generating ideas. Additionally, analysts may censor each other's ideas.

6-22. **Method.** As a two-phase process, brainstorming elicits the most information from brainstorming participants:

- **Phase 1—Divergent thinking phase:**
  - **Step 1:** Distribute a piece of stationery with adhesive and pens/markers to all participants. Typically, a group of 10 to 12 people works best.
  - **Step 2:** Pose the problem in terms of a focal question. Display it in one sentence on a large easel or whiteboard.
  - **Step 3:** Ask the group to write down responses to the question, using key words that will fit on the small piece of stationery.
  - **Step 4:** Stick all of the notes on a wall for all to see—treat all ideas the same.
  - **Step 5:** When a pause follows the initial flow of ideas, the group is reaching the end of its collective conventional thinking, and new divergent ideas are then likely to emerge. End phase 1 of the brainstorming after two or three pauses.
- **Phase 2—Convergent thinking phase:**
  - **Step 6:** Ask group participants to rearrange the notes on the wall according to their commonalities or similar concepts. Discourage talking. Some notes may be moved several times as they begin to cluster. Copying some notes is permitted to allow ideas to be included in more than one group.
  - **Step 7:** Select a word or phrase that characterizes each grouping or cluster once all of the notes have been arranged.
  - **Step 8:** Identify any notes that do not easily fit with others and consider them as either isolated thoughts or the beginning of an idea that deserves further attention.
  - **Step 9:** Assess what the group has accomplished in terms of new ideas or concepts identified or new areas that require more work or further brainstorming.

- **Step 10:** Instruct each participant to select one or two areas that deserve the most attention. Tabulate the votes.
- **Step 11:** Set the brainstorming group's priorities based on the voting and decide on the next steps for analysis.

FUNCTIONAL ANALYSIS USING CRITICAL FACTORS ANALYSIS

6-23. Critical factors analysis (CFA) is an overarching analytic framework that assists analysts in identifying threat critical capabilities, threat critical requirements, and threat critical vulnerabilities that they can integrate into other structured analytic techniques. This assists friendly forces in effectively identifying windows of opportunity and threat vulnerabilities. At echelons above corps, CFA assists in identifying threat centers of gravity that friendly forces can use for operational planning:

- *Critical capability* is a means that is considered a crucial enabler for a center of gravity to function as such and is essential to the accomplishment of the specified or assumed objective(s) (JP 5-0).
- *Critical requirement* is an essential condition, resource, or means for a critical capability to be fully operational (JP 5-0).
- *Critical vulnerability* is an aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects (JP 5-0).

Note. CFA is often presented as a stand-alone technique; however, it shares characteristics found in other imaginative techniques. For the purposes of this publication, CFA is categorized under imaginative techniques.

6-24. To conduct CFA successfully, identify threat critical capabilities. The more specific the threat critical capability, the more specificity analysts can apply to threat critical capabilities, requirements, and vulnerabilities. CFA is more effective when conducted by a team of experienced analysts. Additionally, structured brainstorming can amplify this technique. Analysts can determine windows of opportunity by identifying the common denominator or entity that encompasses those identified threat critical capabilities, requirements, and vulnerabilities. Identified threat critical vulnerabilities are used to develop the HVT list in IPB, step 3, and then later prioritized by the fires cells. (See figure 6-3 on page 6-10.) Table 6-7 briefly describes when to use the functional analysis technique using CFA, as well as the value added and potential pitfalls associated with using this technique.

Table 6-7. Functional analysis technique using critical factors analysis

Functional analysis using critical factors analysis (CFA): The application of the knowledge of common and necessary military functions to specific threat capabilities.		
When to use	**Value added**	**Potential pitfalls**
Analysts should conduct functional analysis using CFA when attempting to identify windows of opportunity and threat vulnerabilities. This is often completed when evaluating the threat during step 3 of the intelligence preparation of the battlefield process.	Functional analysis may also act as the catalyst for other analytic tools such as the criticality, accessibility, recuperability, vulnerability, effect, and recognizability (also called CARVER) matrix tool for prioritizing targets.	Units may not have enough experienced personnel to apply this technique effectively, as multiple analysts are optimal. There may not be enough time to conduct a thorough functional analysis.

6-25. **Method.** The following outlines those steps necessary to conduct CFA (see figure 6-3 on page 6-10):

- **Step 1:** Create a quad-chart. Identify a specific threat mission objective.
- **Step 2:** Identify all threat critical capabilities that are essential to achieve the threat mission objective and input in the top-right quadrant of the chart. (Threat must be able to achieve X.)
- **Step 3:** Identify all threat critical requirements—conditions or resources integral to critical capabilities developed in step 1—and input in the bottom-right quadrant of the chart. (To achieve X, the threat needs Y.)
- **Step 4:** Identify all threat critical vulnerabilities—elements related to threat critical requirements developed in step 2 that appear exposed or susceptible (at risk)—and input in the bottom-left quadrant of the chart. (The threat cannot lose Z.)

- **Step 5:** Analyze the chart to determine the windows of opportunity by identifying the common denominator (or entity) that encompasses those identified threat critical capabilities, requirements, and vulnerabilities and input in the top-left quadrant of the chart.
- **Step 6:** Identify all listed critical factors that friendly forces can directly affect to identify potential targets or topics for further collection.

Windows of Opportunity	**Threat Critical Capabilities**
Friendly force opportunities to attack: • Attack during threat movement because threat command and control limited during maneuver. • Attack at night because threat air limited to daytime.	• Maneuver in depth to disrupt friendly main effort. • Mass combat fire against friendly light reconnaissance force. • Speed presents two options against which to defend. • Capability to seize windows of opportunity.
Threat Critical Vulnerabilities	**Threat Critical Requirements**
• Command and control limited during maneuver. • Maneuver space and routes can be interdicted. • Supply elements vulnerable to attack. • Threat air limited to daytime and visual meteorological conditions. • Special operations forces insertion phase vulnerable to interdiction.	• Command and control. • Maneuver space and routes. • Long-range artillery and multiple launch rocket assets. • Available ammunition. • Available fuel. • Defensive counterair. • Available special operations forces support. • Available air transport to support insertion.

Figure 6-3. Functional analysis using critical factors analysis

OUTSIDE-IN THINKING

6-26. The outside-in thinking technique assists analysts in identifying the broad range of factors, forces, and trends that may indirectly shape an issue—such as global, political, environmental, technological, economic, or social forces—outside their area of expertise, but that may profoundly affect the issue of concern. This technique is useful for encouraging analysts to think critically because they tend to think from inside out, focusing on factors most familiar in their specific area of responsibility.

6-27. Outside-in thinking reduces the risk of missing important variables early in the analysis process; it should be the standard process for any project that analyzes potential future outcomes. This technique works well for a group of analysts responsible for a range of functional and/or regional issues. Table 6-8 briefly describes when to use the outside-in thinking technique, as well as the value added and potential pitfalls associated with using this technique.

Table 6-8. Outside-in thinking technique

Outside-in thinking: *A technique used to identify the range of systemic forces, factors, and trends that could shape an issue, allowing analysts to incorporate this broader conceptual framework into their analysis.*		
When to use	**Value added**	**Potential pitfalls**
Outside-in thinking is most useful in the early stages of an analytic project when the goal is to identify all critical, external factors that could influence how a particular situation will develop.	This technique encourages analysts to think about their issues in a wider conceptual and contextual framework. By recasting the problem in much broader and fundamental terms, analysts are more likely to uncover additional factors, an important dynamic, or a relevant alternative hypothesis.	Analysts tend to think from inside out, focusing on factors that are most familiar in their specific area of responsibility.

6-28. **Method.** The following outlines those steps of outside-in thinking (see figure 6-4):

- **Step 1:** Identify the topic of study.
- **Step 2:** Brainstorm all key factors (operational variables [PMESII-PT]) that could impact the topic.

- **Step 3:** Employ the mission variables (METT-TC) to trigger new ideas.
- **Step 4:** Focus on those key factors over which a commander can exert some influence.
- **Step 5:** Assess how each of those factors could affect the analytic problem.
- **Step 6:** Determine whether those factors can impact the issue based on the available evidence.

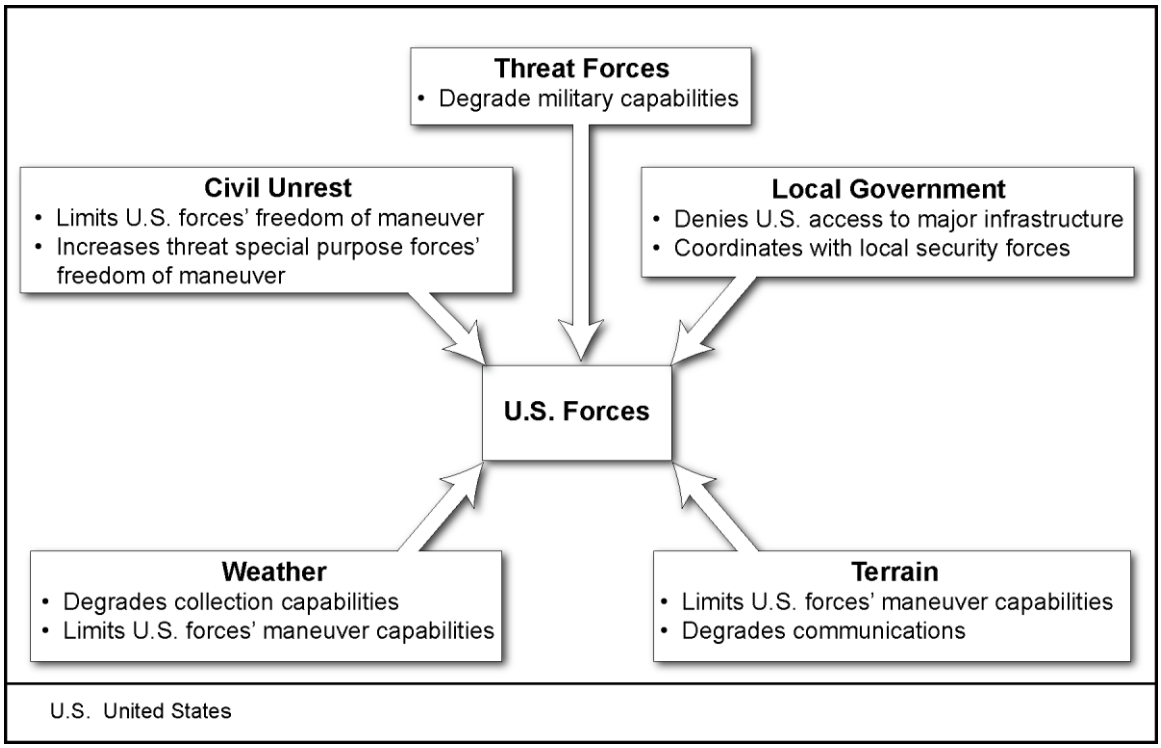


Figure 6-4. Outside-in thinking used during step 2 of the IPB process

RED HAT/TEAM ANALYSIS

6-29. The red hat/team analysis technique facilitates analysts' modeling of threat behavior by attempting to formulate ideas on how the threat would think about an issue. Red hat/team analysis is also a type of reframing technique performed by analysts attempting to solve an intelligence problem by using a different perspective. They attempt to perceive threats and opportunities as would the threat in order to categorize the threat. Categories include but are not limited—

- Command and control.
- Movement and maneuver.
- Intelligence.
- Fires.
- Sustainment.
- Protection.
- Cyberspace.

6-30. Red hat/team analysis is of limited value without a deep understanding of the threat—especially threat doctrine—and the threat's environment, which can affect the threat's decision making. Authoritarian leaders, military leaders, and small cohesive groups, such as terrorist cells, are candidates for this type of analysis. Analysts commonly use red hat/team analysis as a key input to step 2 of the MDMP. Table 6-9 on page 6-12 briefly describes when to use the red hat/team analysis technique, as well as the value added and potential pitfalls associated with using this technique.

Table 6-9. Red hat/team analysis technique

Red hat/team analysis: *A technique that aims to predict the behavior of a threat by trying to replicate how the threat thinks by way of analysts putting themselves "in the threat's shoes."*		
When to use	**Value added**	**Potential pitfalls**
Analysts should use this technique when attempting to forecast behaviors, especially threat behaviors. Analysts typically conduct this type of analysis during step 4 of the intelligence preparation of the battlefield process or when supporting war gaming during the military decision-making process.	The conscious effort to imagine the situation as the target perceives it assists analysts in gaining a different and usually more accurate perspective of the problem or issue.	Analysts challenged to forecast how a threat may behave risk falling into a "mirror-image" exercise. That is, analysts may incorrectly conduct red hat/team analysis from the perspective that the threat shares the same motives, values, or understanding of an issue as they do. Additionally, analysts may assume that the threat will behave according to the same assumptions, culture, and doctrine as analysts would if faced with the same threats or opportunities.

6-31. **Method.** The following outlines the steps to conduct red hat/team analysis:

- **Step 1:** Identify the situation and ask how the threat would respond to the situation.
- **Step 2:** Emphasize the need to avoid mirror imaging. Define the cultural and personal norms that would influence the threat's behavior (use operational variables [PMESII-PT]/civil considerations [ASCOPE] and threat characteristics, threat doctrine, and threat intentions matrices as aids).
- **Step 3:** Develop first-person questions that the threat would ask about the situation.
- **Step 4:** Present results and describe alternative COAs the threat would pursue.

Note. Some publications differentiate between red hat analysis and red team analysis, while others describe them as being the same. When differentiated, red team analysis is categorized as a contrarian technique. For this publication, the two techniques are synonymous.

PART THREE

Intelligence Analysis Considerations

Chapter 7

Analytic Support to Army Forces and Operations

OVERVIEW

7-1. Although the intelligence analysis process does not change, the tasks performed by intelligence analysts differ significantly based on the echelon, the supported functional element, the Army strategic role, and the specific mission. As with many tasks, the most significant factor affecting analysis is time. Time includes both the amount of time to analyze a problem and the timeliness of the final analytical assessment to the decision maker.

7-2. Operations, such as large-scale ground combat operations, are often especially time-constrained for decision makers and analysts. Therefore, care must be taken to provide timely, quality analytical assessments. For example, during large-scale offensive operations, the terrain designated to various echelons to seize, retain, and exploit the initiative dictates the friendly operating tempo within assigned boundaries. A battalion S-2 is assigned a very narrow frontage, while a brigade S-2 looks at a larger area that potentially encompasses a frontage based on assigned and attached maneuver elements according to the assigned mission. However, a brigade conducting consolidation area security might look for bypassed and irregular forces and terrorists within a large and complex area.

ANALYSIS ACROSS THE ECHELONS

7-3. Intelligence analysts conduct analysis during combat operations to support Army forces at all echelons. The commander's need for the continuous assessment of enemy forces focuses intelligence analysis. The analytical output of the intelligence warfighting function assists commanders in making sound and timely decisions. Analysts must understand at which points in an operation the commander needs specific PIRs answered in order to support upcoming decision points. This understanding assists analysts in creating a timeline for conducting analysis and identifying when information is no longer of value to the commander's decision making.

7-4. Analytical elements at NGIC and at echelons above corps focus primarily on strategic- to operational-level analytic problems, analytical elements at the corps level focus on both tactical- and operational-level analytic problems, and analytical elements at echelons below corps focus on tactical-level analytic problems. The strategic, operational, and tactical levels of warfare assist commanders—informed by the conditions of their OEs—in visualizing a logical arrangement of forces, allocating resources, and assigning tasks based on a strategic purpose:

- *Strategic level of warfare* is the level of warfare at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives (JP 3-0). At the strategic level, leaders develop an idea or set of ideas for employing the instruments of national power (diplomatic, informational, military, and economic) in a synchronized and integrated fashion to achieve national objectives.
- *Operational level of warfare* is the level of warfare at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas (JP 3-0). The operational level links the tactical employment of forces to national and military strategic objectives, focusing on the design, planning, and execution of operations using operational art. (See ADP 3-0 for a discussion of operational art.)
- *Tactical level of warfare* is the level of warfare at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces (JP 3-0). The tactical level of warfare involves the employment and ordered arrangement of forces in relation to each other.

NATIONAL AND JOINT ANALYTIC SUPPORT

7-5. Intelligence analysis support to national organizations and the joint force focuses on threats, events, and other worldwide intelligence requirements. For the Army, the United States Army Intelligence and Security Command (INSCOM) is the lead organization to provide all-source and single-source intelligence capabilities to Army Service component commands. INSCOM includes functional brigades, units, and elements that provide general support, general support reinforcing, or direct support to theaters through intelligence reach, or they may be force-tailored for deployment to support the joint force. NGIC, which is under INSCOM, serves as the Army's Service Intelligence Center all-source analytical effort for general military intelligence, science and technology intelligence, and identity intelligence, all of which focus on the land domain. National and joint intelligence activities are continuous and reach across the range of military operations to provide continuous analytic support, including warning intelligence, to senior levels of the U.S. Government and DOD. (See JP 2-01 for more information on national and joint analytic support.)

THEATER ARMY

7-6. At the theater army level, intelligence analysis supports the combatant commander's operational mission requirements by enabling the theater command to apply capabilities to shape and prevent potential threat action. Theater army-level analytical activities include but are not limited to—

- Supporting theater campaign plans.
- Developing expertise to analyze threat characteristics within a region.
- Long-term analysis of a region and/or country that enables warning intelligence of imminent threat ground operations.
- Detailed analysis of multi-domain specific requirements.
- Serving as the Army's interface to national and joint support for operational and tactical forces.

7-7. Analysts assigned to the theater army-level all-source intelligence cell can expect to work with other Services as well as other nations. Analytical assessment support to future operations focuses on threat activities, intent, and capabilities beyond 168 hours within a designated global region assigned to the combatant commander.

CORPS

7-8. The corps G-2 and associated analytical elements, along with the ACE, further refine operational planning provided by the theater army, and they produce and update a broad range of intelligence products to support corps operations. These intelligence products, as well as constant collaboration between echelons, assist subordinate commands (division or brigade) in their planning. The corps ACE provides the most in-depth analysis at the tactical level to support the deep fight. Analytical assessment support to future operations focuses on threat activities, intent, and capabilities for the next 96 to 168 hours. (For more information on intelligence products, see appendix E.)

DIVISION

7-9. The division G-2, supported by the intelligence cell, advises the commander on how to leverage the intelligence warfighting function to support operations. The G-2 assists the commander in synchronizing intelligence operations; coordinates activities and systems that facilitate understanding the threat, terrain and weather, and other relevant aspects of the OE (such as key populations, groups, and organizations); and supervises the intelligence cell. The intelligence cell requests, receives, and analyzes information from multiple sources to produce and distribute intelligence products; it consists of most of the intelligence staff and an attached Air Force weather team.

BRIGADE COMBAT TEAM

7-10. The BCT S-2 is the principal intelligence advisor to the BCT commander. The S-2 coordinates activities and systems that facilitate understanding the threat, terrain and weather, and other relevant aspects of the area of interest (such as key populations, groups, and organizations). Additionally, the BCT S-2 supports security programs and oversees the BCT intelligence cell. The intelligence cell requests, receives, and analyzes information from multiple sources to produce and distribute intelligence products. The cell's geospatial engineer team manages the Standard Sharable Geospatial Foundation and geospatial information and services for the BCT, supporting the entire BCT with geospatial data and terrain analysis products.

BATTALION

7-11. Battalion-level intelligence analysis within the battalion intelligence section is rudimentary and focuses on a 12- to 24-hour period. Specifically, the battalion intelligence section focuses on IPB threat capabilities.

SUPPORT TO FUNCTIONAL ELEMENTS

7-12. The Army is committed to providing intelligence support across most unique functional elements. Although all of these elements perform IPB and collection management, the intelligence analysis requirements for these elements vary significantly based on the commander's designated mission; therefore, when assigned, intelligence analysts must learn the mission-specific intelligence analysis requirements for their functional element, identified in table 7-1.

Table 7-1. Intelligence analysis support to functional elements

Functional element	*Mission*	*Intelligence analysis considerations*	*Doctrinal references*
Air defense (AD) or air and missile defense	AD elements exist across all echelons. They establish AD plans to engage hostile ballistic missiles, aircraft, cruise missiles, and unmanned aircraft systems within the operational environment (OE).	Analysis focuses on air threats consisting of aircraft and missile technologies capable of controlling the air domain and influencing maneuverability within the land domain. Analysts must consider threat-to-friendly AD systems from threat air assets, as this is a United States (U.S.) or coalition Air Force mission.	JP 3-01 FM 3-01
Aviation	Aviation operations consist of aircraft (fixed- and rotary-wing) activities, airfield operations, and Army-level air traffic services.	Analysis support includes basic intelligence activities with additional knowledge of enemy aircraft and AD systems and capabilities. Army aviation operations require intelligence preparation of the battlefield (IPB) and collection support.	FM 3-04

Table 7-1. Intelligence analysis support to functional elements (*continued*)

Functional element	*Mission*	*Intelligence analysis considerations*	*Doctrinal references*
Chemical, biological, radiological, and nuclear (CBRN)	CBRN units support the Army across all echelons by identifying CBRN threats on the battlefield. This includes CBRN passive defense preventive measures to minimize friendly unit vulnerability to CBRN threat/hazard effects. CBRN reconnaissance and surveillance provide the command with detailed, timely, and accurate information to inform decision making or answer the commander's critical information requirements about CBRN threats or hazards.	Analysis support includes basic intelligence activities with additional knowledge of enemy capabilities to employ CBRN capabilities against friendly forces and toxic industrial material or dual-use facilities. Army CBRN operations require IPB and collection support to guide CBRN reconnaissance element collection efforts.	ATP 3-11.36 ATP 3-11.37 FM 3-11
Civil affairs (CA)	CA operations enhance awareness of and manage interactions with the OE civil component, identify and mitigate underlying causes of instability in the civil society, or apply functional specialty skills, which are normally the civil government's responsibility.	Analysis support focuses on IPB and threats to civil considerations (areas, structures, capabilities, organizations, people, and events [ASCOPE]).	FM 3-53 FM 3-57
Cyberspace	Cyberspace elements provide defensive cyberspace operations to the Army as well as to global commands.	Analysis support to cyberspace operations is a developing process and requires examination of current cyberspace operational concepts. Army cyberspace operations require unique cyberspace IPB and collection support.	FM 3-12
Engineer	Engineer activities include geospatial support, construction, real property maintenance activities, sustainment of lines of communications (LOCs), engineer logistics management, base camp development, mobility and countermobility functions, including river speeds, wet gap crossing bank slope, obstacle types and orientation, enemy engagement area development activities, and percentage of enemy survivability positions dug.	Basic analysis support to engineering activities is necessary to identify threats and enemy force activities. Army operational and tactical engineer operations require IPB and collection support. All staff sections rely on Army engineers to provide Standard Sharable Geospatial Foundation and geospatial and terrain analysis for mission planning, command and control/current operations, and geospatial intelligence products.	ATP 3-90.4 ATP 3-90.8 FM 3-34
Explosive ordnance disposal/ Counter-improvised explosive device/ Counter-explosive hazard	Large-scale ground combat operations support includes— • Targeting and remediating threat munitions production, storage, and employment. (Contingency) • Defeating explosive threats to the force. • Mitigating explosive hazards via training the force. • Neutralizing explosive hazards via attacking threat networks.	Analysis supports— • Characterizing threat capabilities in the context of conventional and unconventional munitions and explosive hazards, including CBRN threats. • Detecting, identifying, and targeting threat munition and explosive hazard production and storage capabilities, facilities, and networks. • Describing the threat's use of munitions and explosive hazards to support training.	JP 3-15.1 ATP 3-90.37 ATP 4-32 ATP 4-32.1
Medical	The complexities of the range of military operations require medical support to military and civilian considerations (ASCOPE).	Intelligence analysts advise the medical command on nuclear/chemical surety and CBRN operations. Reference the National Center for Medical Intelligence for all-source medical intelligence assessments.	FM 4-02

Table 7-1. Intelligence analysis support to functional elements (*continued*)

Functional element	*Mission*	*Intelligence analysis considerations*	*Doctrinal references*
Military police (MP)	MPs provide the Army's policing, investigations, and corrections capabilities to enable protection, preserve the force, and promote the rule of law. MPs execute these capabilities via the three MP disciplines: police operations, detention operations, and security and mobility support.	Analysis enables MP commanders' situational understanding, battlefield visualization, and force protection programs by providing relevant criminal threat and friendly information that impacts operational and tactical environments. Army MP operations and overall effects require IPB and collection support.	ATP 3-39.10 ATP 3-39.20 ATP 3-39.30 FM 3-39 FM 3-63
Psychological operations	Military information support operations support corps and divisions in providing tactical-level analysis and augmentation that include language and cultural expertise, regional analysis, and mass communications delivery capabilities.	Analysis support to military information support operations includes performing IPB, specifically threat and civil considerations (ASCOPE) analysis.	FM 3-53
Signal	The signal element supports all levels of Army commands and provides Army communications and communications security—Department of Defense information network (DODIN) operations.	Analysis support is wide-ranging, from global threat analysis to support of threat communications capabilities within a given OE. DODIN operations require IPB and collection support.	FM 6-02
Space	The Army space force is a multicomponent organization of space support elements that conduct theater space operations and planning, integrate and coordinate space capabilities, and support commanders in exercising command and control through space operations.	Analysis support to the Army Space and Missile Defense Command is unique; therefore, it provides new intelligence personnel upon arrival. Army space operations require unique space IPB and collection support.	FM 3-14
Special operations forces (SOF)	*Army special operations forces* are those Active and Reserve Component Army forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to conduct and support special operations (JP 3-05). SOF include CA, psychological operations, Rangers, special forces, special mission units, and Army special operations aviation forces assigned to the U.S. Army Special Operations Command—all supported by the 528th Sustainment Brigade (Special Operations) (Airborne).	Analysis support includes efforts to defeat joint, transregional, all-domain, multifunctional threats and to facilitate Army special operations over a multi-domain extended battlefield in large-scale ground combat operations. Within the range of military operations, analysis assists commanders in developing the appropriate lines of effort and lines of operations to destroy threat networks, shape conditions, deter threats, and influence relevant actors. A common factor of special operations and associated activities is that special operations units conducting operations are either operating among populations or supporting others in permissive or uncertain environments. This factor requires nuanced information and intelligence products to ensure special operations units' consistent interactions with populations contribute to the success of the mission instead of being a detriment to the mission. Most importantly, operating among populations requires an understanding that the populations and subgroups within it are important, potential centers of gravity, sources of power, and often the basis to long-term stability.	ADP 3-05

Table 7-1. Intelligence analysis support to functional elements (*continued*)

Functional element	*Mission*	*Intelligence analysis considerations*	*Doctrinal references*
Sustainment	Sustainment doctrine focuses on the four elements of sustainment: logistics, personnel services, financial management, and health service support to unified land operations.	Analysis support includes basic intelligence activities with additional knowledge of logistics, LOCs, medical or health services, and, to some extent, personnel services and financial management. Army sustainment operations require IPB and collection support.	ADP 4-0

ANALYSIS ACROSS THE ARMY'S STRATEGIC ROLES

7-13. Intelligence analysts must consider all intelligence requirements for operations to shape, prevent, prevail in large-scale ground combat, and consolidate gains. However, the conduct of these operations is associated with the combatant command, as designated by the DOD, and with OE conditions.

SHAPE OPERATIONAL ENVIRONMENTS

7-14. Table 7-2 lists some of the unique considerations and intelligence requirements associated with operations to shape OEs. (For more information on shaping OEs, see FM 2-0's chapter 5.)

Table 7-2. Intelligence requirements associated with operations to shape

Unique considerations	*Intelligence requirements associated with shaping operational environments*
Key leaders	• Identify key leaders (politics, military, economic, social, information, infrastructure). • Evaluate the amount of influence of each leader. • Describe the local populace's opinion of each leader. • Perform link analysis for each leader's social and professional circles. • Research general biographical information.
Threat intent/critical capabilities	• Identify the critical resources the threat requires by capability. • Define the end state the threat is attempting to achieve. • Define decision points to reach the threat organization's end state. • Research open-source reporting on the threat. • Determine the threat's current phase of operations. • Project the threat's likely courses of action and potential crisis issues/flash points. (This should also develop indicators.)
Training activities	• Locate training locations. • Describe the threat training cycle. • Define threat capabilities by warfighting function. • Identify if new threat capabilities are being trained. • Describe how training is sustained.
Political activities	• Evaluate the effectiveness of the government. • Describe the local populace's opinion about the government. • Identify the government's critical requirements by capabilities. • Identify goals the government is attempting to achieve.

PREVENT CONFLICT

7-15. Table 7-3 lists some of the unique considerations and intelligence requirements associated with operations to prevent conflict. (For more information on preventing conflict, see FM 2-0's chapter 5.)

Table 7-3. Intelligence requirements associated with operations to prevent

Unique considerations	*Intelligence requirements associated with preventing conflict*
Mobilization actions	• Describe how the threat will conduct operations. • Evaluate if any windows of opportunity are present from the current situation and disposition. • Identify friendly risks based on the current situation and disposition. • Identify key terrain. • Identify areas that can limit friendly and threat freedom of movement.

PREVAIL IN LARGE-SCALE GROUND COMBAT

7-16. Table 7-4 lists some of the common considerations and intelligence requirements associated with large-scale ground combat operations.

Table 7-4. Intelligence requirements associated with large-scale ground combat operations

Considerations	*Intelligence requirements associated with large-scale ground combat*
Conventional forces and special operations forces	• Describe the threat using intelligence preparation of the battlefield (IPB). • Identify the threat's mission statement and intent. • Identify threat requirements that enable the threat to meet its end state. • Identify the threat commander's acceptable risk. • Identify the threat commander's decision points.
Irregular forces/Terrorists	• Identify irregular forces that friendly forces may encounter. • Describe irregular forces' capabilities by warfighting function. • Determine irregular forces' unique missions. • Identify when irregular forces will interdict/impede friendly force movement. • Locate where irregular forces will observe friendly forces. • Determine irregular forces' high-value targets. • Determine irregular forces' fire support.
Other adversaries (terrorist organizations, criminal organizations, individual relevant actors)	• Identify adversaries' purpose, intent, and motivations. • Identify adversaries' structure, organization, and networks. • Conduct human network analysis. • Identify adversaries' perspectives, intentions, strengths, vulnerabilities, susceptibilities, opportunities, issues, goals, and influence. • Identify nexuses between individual adversarial organizations. • Identify nexuses between adversarial organizations and conventional, special operations, and irregular forces.
Consolidation area	• **Bypassed enemy forces:** ▪ Identify the current disposition of potential stay-behind forces. ▪ Evaluate if the projected attrition of threat personnel is accurate. ▪ Describe how local nationals are reacting to stay-behind forces. ▪ Identify the goals of the stay-behind forces. • **Enemy special operations forces:** ▪ Identify potential safe havens. ▪ Identify potential civilian groups that may provide support. ▪ Identify the most likely tactics, techniques, and procedures that will be employed. ▪ Identify which friendly capabilities are most vulnerable to attack. • **Criminal organizations:** ▪ Identify activities that will impede friendly operations. ▪ Identify activities that will degrade public security. ▪ Determine which organizations can be levied as friendly proxies.

Table 7-4. Intelligence requirements associated with large-scale ground combat operations (*continued*)

Considerations	*Intelligence requirements associated with large-scale ground combat*
Consolidation area (*continued*)	• **Terrorist organizations:** ▪ Identify leaders in the area of operations that may be connected to terrorist activities. ▪ Describe successful terrorist activities that have occurred in the area of operations. ▪ Determine the most plausible, deadliest attack that may potentially occur. ▪ Identify resources terrorists require to conduct attacks. ▪ Describe the tactics, techniques, and procedures employed by terrorists. • **Irregular forces:** ▪ Place large emphasis/focus on civil considerations (ASCOPE). ▪ Identify resources the local populace requires. ▪ Determine if and describe how irregular forces are using those resources as leverage. ▪ Determine which populations are filling irregular force ranks. ▪ Determine which population areas are sympathetic to irregular force activities. ▪ Determine who has influence over irregular forces. • **Local population critical needs:** ▪ Identify the status of the basic infrastructure, including water, heating and cooling resources, electricity, medical, waste collection, roads, bridges, railways, seaports, airports, telecommunications, law enforcement, and emergency services. ▪ Identify key personnel required to manage the infrastructure. ▪ Coordinate analysis with attached or supporting civil affairs and psychological operations forces and organic staffs. ▪ Integrate infrastructure status into the common operational picture. • **Enemy reconsolidation and identification of capabilities.**
Support area	• Evaluate the infrastructure. • Determine refugee flow. • Identify obstacles to continuing activities.

ASCOPE areas, structures, capabilities, organizations, people, and events

OFFENSIVE AND DEFENSIVE OPERATIONS IN LARGE-SCALE GROUND COMBAT

7-17. Whether in offensive or defensive operations, the intelligence analysis process conducted does not differ drastically. In offensive and defensive operations during large-scale ground combat, the operating tempo is accelerated and therefore, intelligence analysis is accelerated. Regardless of the type of operation, all-source intelligence is the primary capability within the intelligence warfighting function that aids commanders' understanding of their OE. (See ADP 3-90 for a detailed discussion on offensive and defensive operations.)

Offensive Operations

7-18. An *offensive operation* is an operation to defeat or destroy enemy forces and gain control of terrain, resources, and population centers (ADP 3-0). The main differences between offensive and defensive operations are the focus and detail level of analysis required for determining the enemy's defensive framework and the effects of terrain on friendly maneuver. Additionally, the enemy often employs capabilities using different tactics and techniques, depending on the specific offensive or defensive operation. Offensive operations are either force-oriented or terrain-oriented. Force-oriented offensive operations focus on the enemy. Terrain-oriented offensive operations focus on seizing and retaining control of the terrain and facilities. Detailed IPB products, such as a modified combined obstacle overlay with intervisibility lines or an event template, must be developed to depict this information. (See ATP 2-01.3.) Table 7-5 lists some of the intelligence requirements associated with offensive operations.

Table 7-5. Intelligence requirements associated with the offense

Determine the enemy's likely purpose and type of defense: area defense, mobile defense, or retrograde.
Determine the enemy's likely end state, objectives, decision points, culmination point, strengths, vulnerabilities, and scheme of maneuver.
Identify military aspects of terrain (OAKOC) and weather effects that support enemy defensive operations: • Terrain that allows reconnaissance and security outposts to be arranged in depth along choke points and terrain features that canalize friendly forces to attrite U.S. forces and diminish U.S. combat power in depth. • Terrain, including subterranean, that allows the enemy to tie obstacles to existing terrain features to support enemy defensive positions. (See ATP 3-21.51 for more on subterranean terrain.) • Favorable air and ground avenues of approach for an enemy counterattack. • Terrain that canalizes friendly attacking forces. • Favorable weather effects (such as visibility, wind, precipitation, cloud cover/ceilings, temperature, thermal crossover, humidity, and atmospheric pressure) for enemy systems compared to friendly systems.
Identify military aspects of terrain (OAKOC) and weather effects that support friendly offensive operations: • Favorable ground and air mobility corridors. • Areas with significant concealment and/or cover. • Terrain that allows forces to bypass obstacles and enemy positions. • Infiltration routes. • Landing zones. • Favorable weather effects (such as visibility, wind, precipitation, cloud cover/ceilings, temperature, thermal crossover, humidity, and atmospheric pressure) for enemy systems compared to friendly systems. • Favorable weather for using obscuration or chemical weapons.
Identify the location and orientation of enemy counterreconnaissance and security units, obstacles, engagement areas, main battle areas, reserve units, and likely counterattack routes.
Within each enemy defensive area, identify specific primary, secondary, tertiary locations of enemy infantry, armored, antitank, mortar, and other units and systems, and the potential use of camouflage.
Determine the likely use and identify the location of enemy command and control nodes, reconnaissance and surveillance assets, long-range fires, artillery and rocket units, air defense systems, rotary aviation units, close air support, engineer units, ammunition and logistics nodes, CBRN units, electronic warfare assets, and special operations forces.
Determine the enemy's likely use of information warfare, cyberattacks, and denial and deception operations.
Determine the impact of significant civil considerations (ASCOPE) on friendly and enemy operations such as hindering movement on lines of communications, medical and health considerations, and the housing and feeding of a displaced population.
ASCOPE areas, structures, capabilities, organizations, people, and events CBRN chemical, biological, radiological, and nuclear OAKOC observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment U.S. United States

Defensive Operations

7-19. A *defensive operation* is an operation to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations (ADP 3-0). Defensive operations retain decisive terrain or deny the enemy access to a vital area, attrite or fix the enemy as a prelude to offensive operations, counter a surprise action by the enemy, or increase the enemy's vulnerability by forcing the enemy to concentrate its forces.

7-20. The main differences between defensive operations and other decisive action are the focus and detail level of analysis required for determining the enemy's offensive framework and the effects of terrain on friendly defensive operations. Table 7-6 on page 7-10 lists some of the intelligence requirements associated with defensive operations.

Table 7-6. Intelligence requirements associated with the defense

Determine the enemy's likely purpose (for example, terrain- or force-oriented) and type of offense.
Determine the enemy's likely end state, objectives, decision points, culmination point, strengths, vulnerabilities, and scheme of maneuver.
Identify military aspects of terrain (OAKOC) and weather effects that support enemy offensive operations: • Favorable ground corridors and air avenues of approach. • Areas with significant concealment and/or cover. • Terrain, including subterranean, that allows forces to bypass obstacles and friendly positions. (See ATP 3-21.51 for more on subterranean terrain.) • Infiltration routes. • Landing zones. • Favorable weather effects (such as visibility, wind, precipitation, cloud cover/ceilings, temperature, thermal crossover, humidity, and atmospheric pressure) for enemy systems compared to friendly systems. • Favorable weather for using obscuration or chemical weapons.
Identify military aspects of terrain (OAKOC) and weather effects that support friendly defensive operations: • Terrain that allows friendly forces to tie obstacles to existing terrain features to supports friendly defensive positions. • Favorable air and ground avenues of approach for a counterattack. • Terrain that canalizes enemy attacking forces. • Favorable weather effects (such as visibility, wind, precipitation, cloud cover/ceilings, temperature, thermal crossover, humidity, and atmospheric pressure) for enemy systems compared to friendly systems.
Identify the location of enemy assembly areas, ammunition and logistics nodes, forward aviation locations, and likely movement routes into the friendly area of operations.
Template and track the composition, disposition, likely routes, and time phase lines of reconnaissance and surveillance, security, advanced engineering, infiltrating, and air assault units.
Template and track the composition, disposition, likely routes, and time phase lines of advance guard, main body, antitank, reserve, and second echelon units.
Template and track specific locations where the enemy will conduct key maneuver tasks, such as occupying support by fire positions and dismounting infantry, or where friendly units may be isolated in defensive positions due to the enemy's use of artillery scatterable mines.
Determine the likely use and template the location of enemy command and control nodes, long-range fires, artillery and rocket units, air defense systems, attack helicopter units, close air support, engineer units, CBRN units, electronic warfare assets, and special operations forces.
Determine the enemy's likely use of information warfare, cyberattacks, and denial and deception operations.
Determine the impact of significant civil considerations (ASCOPE) on friendly and enemy operations such as hindering movement on lines of communications, medical and health considerations, and the housing and feeding of a displaced population.
ASCOPE areas, structures, capabilities, organizations, people, and events CBRN chemical, biological, radiological, and nuclear OAKOC observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment

CONSOLIDATE GAINS

7-21. Commanders continually (through all phases of the operation) consider activities necessary to consolidate gains and achieve the end state. Operations to consolidate gains require a dynamic intelligence effort to conduct offensive and defensive operations that do not create secondary impacts to consolidating gains (for example, destroying key infrastructure) while also supporting the execution of area security and stability operations.

Consolidate Gains Concurrent with Large-Scale Ground Combat Operations

7-22. Table 7-7 lists some of the unique considerations and intelligence requirements associated with operations to consolidate gains during large-scale ground combat operations.

Table 7-7. Intelligence requirements associated with operations to consolidate gains

Unique considerations	*Intelligence requirements associated with consolidating gains*
Assessments	• Conduct battle damage assessments. • Evaluate the effectiveness of friendly operations. • Determine if there are any remaining stay-behind forces. • Describe the composition of any stay-behind forces (bypassed/isolated conventional forces, irregular/special purpose forces, terrorists or insurgents). • Evaluate how remaining threat forces are still able to operate. • Determine if there are any areas still sympathetic to threat forces. • Describe how remaining threat forces are able to sustain operations. • Identify the leadership that remaining forces are looking to for guidance. • Determine the security of hazardous materials and facilities that can be used in the production of weapons of mass destruction.
Transition	• Identify the recipient of the transfer of authority. • Determine if the organization is able to enforce and achieve its intent. • Determine if the organization has enough manpower to meet its intent. • Identify what resources the organization requires to meet its goals. • Determine if the organization can use all information networks to reach the populace effectively.

Consolidate Gains Through Stability Operations

7-23. A *stability operation* is an operation conducted outside the United States in coordination with other instruments of national power to establish or maintain a secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief (ADP 3-0). In stability operations, success is measured differently from offensive and defensive operations. Time may be the ultimate arbiter of success: time to bring safety and security to an embattled populace; time to provide for the essential, immediate humanitarian needs of the people; time to restore basic public order and a semblance of normalcy to life; and time to rebuild the institutions of government and market economy that provide the foundations for enduring peace and stability. (See ADP 3-07 for information on stability operations.)

7-24. The main difference between stability operations and other decisive action is the focus and degree level of analysis required for the civil aspects of the environment. Unlike major combat—an environment dominated by offensive and defensive operations directed against an enemy force—stability operations encompass various military missions, tasks, and activities that are not enemy-centric.

7-25. Constant awareness and shared understanding of civil considerations (ASCOPE) about the environment are crucial to long-term operational success in stability operations. Analysts should classify civil considerations into logical groups (tribal, political, religious, ethnic, and governmental). Intelligence analysis during operations that focus on the civil population requires a different mindset and different techniques than an effort that focuses on defeating an adversary militarily.

7-26. Some situations (particularly crisis-response operations) may require analysts to focus primarily on the effects of terrain and weather, as in the case of natural disasters, including potential human-caused catastrophes resulting from natural disasters. Disasters (such as windstorms, hurricanes, typhoons, floods, tsunamis, wildfires, landslides, avalanches, earthquakes, and volcanic eruptions) may occur without warning. Human-caused catastrophes (such as civil conflict, acts of terrorism, sabotage, or industrial accidents) may develop over time. The speed at which an event occurs dictates how analysts will conduct their assessments and with whom they will share their intelligence.

This page intentionally left blank.

Chapter 8
Analysis and Large-Scale Ground Combat Operations

OVERVIEW

8-1. In future operations, intelligence analysis considerations should include a combination of factors (or elements) that analysts must understand to support the commander. Multi-domain operation considerations differ by echelon. These considerations have their greatest impact on Army operations during large-scale ground combat. Despite the natural tendency to focus on the land domain during large-scale ground combat, analysts must look across the OE or AO to determine how the air, land, and maritime domains affect Army efforts and how those effects may open windows of opportunity for Army forces to create favorable conditions and positions of relative advantages for U.S. and coalition forces.

8-2. Situation development enables commanders to see and understand the battlefield in enough time and detail to make sound tactical decisions. Situation development assists in locating and identifying threat forces; determining threat forces' strength, capabilities, and significant activities; and predicting threat COAs. Situation development assists commanders in effectively employing available combat resources where and when decisive battles will be fought, preventing commanders from being surprised.

8-3. Commanders and staffs require timely, accurate, relevant, and predictive intelligence to successfully execute offensive and defensive operations in large-scale ground combat operations. The challenges of fighting for intelligence during large-scale ground operations emphasize a close interaction between the commander and staff, since the entire staff supports unit planning and preparation to achieve situational understanding against a peer threat. Since each echelon has a different situational understanding of the overarching intelligence picture, the analytical focus differs from one echelon to another. For example, updated intelligence analysis at the corps level could influence a commander's decisions at the BCT level because corps-level requirements differ from BCT-level requirements. Therefore, it is important for intelligence analysts to understand the missions, key tasks, and end state of higher and subordinate forces to ensure they maintain a holistic understanding of the OE. Although each echelon has a different analytical focus, the techniques, tools, and methods employed to conduct analysis do not change. (See FM 2-0 for more information on fighting for intelligence and all-source intelligence capabilities at each echelon.)

TACTICAL TO OPERATIONAL SITUATION: AN ENEMY ATTACK

8-4. The following three examples walk an intelligence analyst from the tactical to operational situation of an enemy attack, demonstrating the necessity for analysts to possess a broad understanding of the OE and the friendly forces' scheme of maneuver. The examples illustrate the situation a unit might encounter along the forward edge of the battle area (FEBA) with friendly and enemy forces poised to engage in large-scale ground combat. In this situation, many friendly and enemy units have deployed to gain a tactical advantage at the onset of combat.

TACTICAL-LEVEL EXAMPLE (BRIGADE COMBAT TEAM)

8-5. The BCT has already completed the MDMP and issued orders, and intelligence analysts have been providing periodic reports and products to support situation development as the situation unfolds. The battle noncommissioned officer receives a spot report that elements of a motorized rifle regiment have crossed the border/FEBA. (See figure 8-1 on page 8-2.) The commander wants to confirm the enemy's intent to cross the border before engaging the enemy.

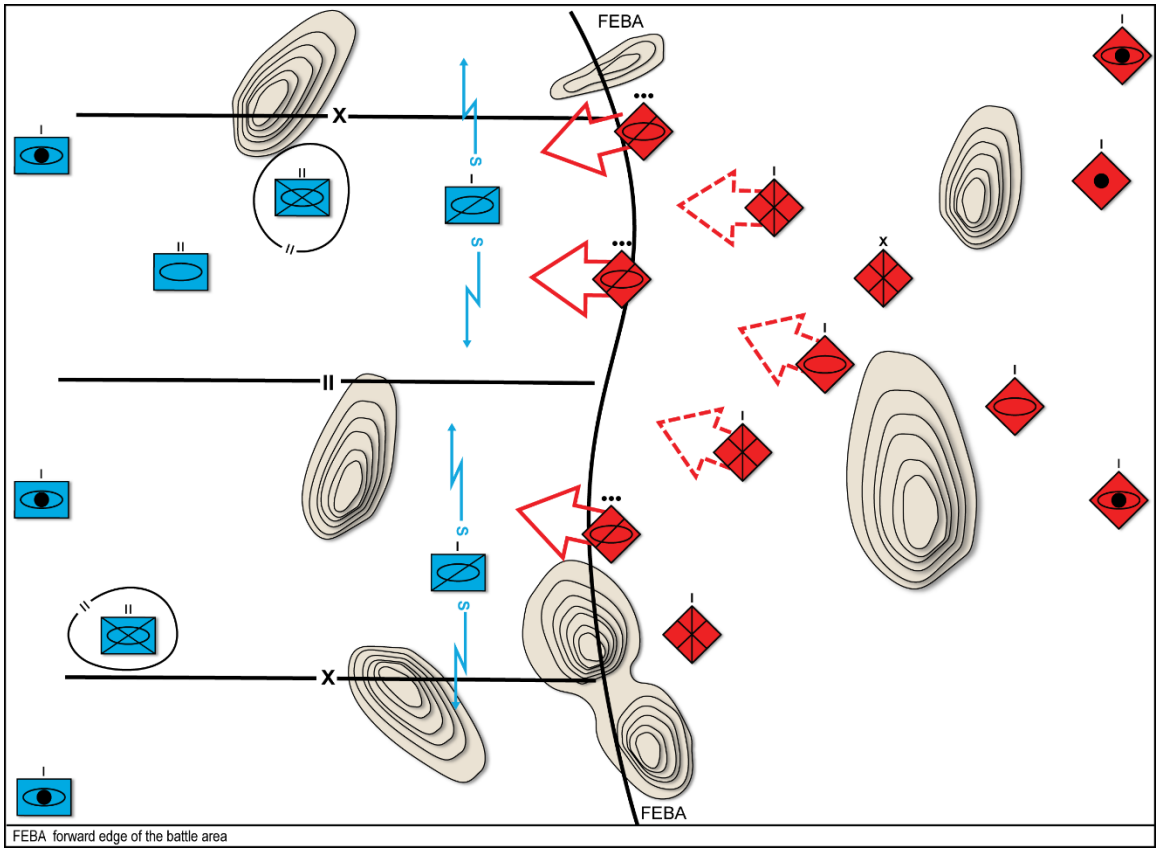


Figure 8-1. Brigade combat team situation example

8-6. Additional information received confirms reporting from forward reconnaissance elements. Intelligence reporting from single-source intelligence analysis indicates movement west of multiple company-sized tank and motorized rifle elements. The intelligence also reveals possible supporting artillery elements. (See table 8-1.)

Table 8-1. Intelligence analysis (brigade combat team) example

Brigade combat team intelligence analysis example			
Action taken			
Screen	***Analyze***	***Integrate***	***Produce***
• General items of relevancy to screen in a tactical sense: ▪ Indicators of threat activities for the next 24 to 48 hours. ▪ Changes in the operational environment that will affect operations. ▪ Enemy maneuvers within the area of operations. • Analysts initiate analysis based on a spot report that meets these criteria.	Analysts should form their initial hypothesis based on information assessed to be relevant in the *screen* phase.	Analysts should compare their new hypothesis to current intelligence holdings.	Analysts make their final assessment and produce a likely course of action (COA) for the commander to make a decision.

Table 8-1. Intelligence analysis (brigade combat team) example (*continued*)

Brigade combat team intelligence analysis example (continued)			
Action taken			
Screen	***Analyze***	***Integrate***	***Produce***
Based on the spot report, the commander provides the following specific requirement, which the intelligence section needs to address: Confirm the enemy's intent to cross the border.	Based on multiple reports indicating enemy forces maneuvering to the west, analysts must assess: • How this movement will support the enemy commander's intent and end state? • How much will the enemy commander commit to this movement? • Will the amount of force committed by the enemy commander drive friendly units to a decision point?	During step 3 of the intelligence preparation of the battlefield (IPB) process, step 3, analysts will have described the enemy to have the minimum products: • Written enemy description (Annex B [Intelligence]). • Situational order of battle. • Threat graphic template. • Threat capabilities matrix.	• Intelligence analysis assessment: At a minimum, battalion plus of motorized rifle supported with tank elements are crossing the border, and an enemy surprise attack by follow-on elements is likely. • Based on the assessment, the friendly commander confirms the enemy's intent to cross the border and provides guidance to assume attack positions to block the enemy advance.
Analysts screen the following based on the specific requirement and tactical guidelines: • Reporting from forward reconnaissance corroborates spot report. • Reporting from single-source analysis indicates movement, including the possible movement of additional elements.	Analysts may use the following analytic techniques: • Chronologies (*Basic*) to understand the enemy's intent and end state by examining historic operations the enemy has conducted. • Key assumptions check (*Diagnostic*) on the enemy's likely intent to enlighten how much the enemy will commit to the movement. • Analysis of competing hypothesis (*Diagnostic*) to project if the friendly commander will be faced with a decision point.	• Based on the enemy description and threat capabilities matrix: Analysts refine enemy movement to add the size of unit (as directed by the commander, but at least two levels down) and type (motorized rifle with tanks). • Based on the situational order of battle: Analysts assess the enemy commander will likely commit follow-on elements. • With a refined size and type of enemy units moving to the west, combined with the projected amount of force committed, the friendly commander must make a decision based on the enemy COA. • Analysts may use the team A/ team B (*Advanced*) analytic technique to war-game their assessed enemy COA, ensuring all variables are considered and their COA is viable. • Analysts may use the red hat/ analysis (*Advanced*) analytic technique in conjunction with their threat capabilities matrix to ensure the enemy intent in their initial hypothesis agrees with current intelligence holdings.	The intelligence analysis process is continuous, and analysts should now consider: • What information can be exploited by combat assessment from the block? • What single-source reporting generates post-mission? • Does the threat model derived in IPB, step 3, require changes? • What should be adjusted for information collection to fully answer the requirement?

TACTICAL-LEVEL EXAMPLE (DIVISION)

8-8. Figure 8-2 illustrates a similar enemy attack but with U.S. division graphics. The enemy's most likely COA is an attack orientated on at least two ground avenues of approach through canalizing terrain. At least one tank division with four brigade elements and two self-propelled artillery battalions will attack as the main effort. In addition to the tank and motorized rifle elements crossing the FEBA, there are elements of at least one tank brigade with self-propelled artillery advancing west.

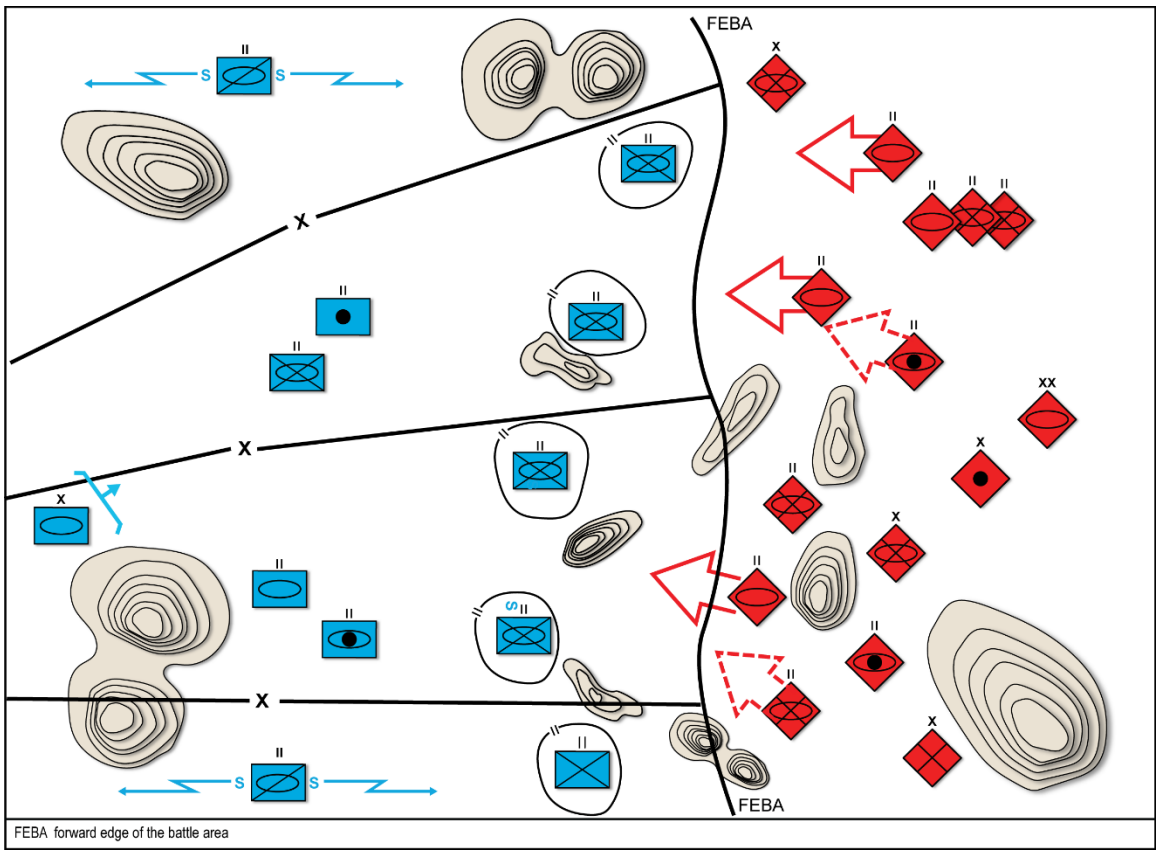


Figure 8-2. Division situation example

8-9. Division analysts assess that elements of the tank division are advancing west to engage friendly forces. The combat information and available intelligence seem to initially support an enemy division frontal attack with infantry and motorized rifle brigades penetrating the FEBA to destroy friendly defenses and allow follow-on units to secure primary and secondary objectives. (See table 8-2.)

Table 8-2. Intelligence analysis (division) example

Division intelligence analysis example			
Action taken			
Screen	***Analyze***	***Integrate***	***Produce***
• General items of relevancy to screen in an operational sense: ▪ Indicators of enemy activities for the next 48 to 168 hours. ▪ Changes in the operational environment that will affect subordinate commands. ▪ Enemy maneuvers that will affect subordinate unit's areas of responsibility (AORs). • Analysts initiate analysis based on reports of enemy orientation on two avenues of approach through canalizing terrain that meets these criteria.	Analysts should form their initial hypothesis based on information assessed to be relevant in the *screen* phase.	Analysts should compare their new hypothesis to current intelligence holdings.	Analysts make their final assessment and produce a likely course of action (COA) for the commander to make a decision.
Based on the orientation, the commander provides the following specific requirement, which the intelligence section needs to address: Project the enemy's future operations for the next 96 to168 hours and how they will affect subordinate units.	Based on the reports indicating enemy forces in attack position, analysts must assess: • What is the enemy commander's end state for this attack? • What resources would be a priority for the enemy commander to commit these forces to an attack? • Will the enemy attack force subordinate units to a decision point?	During intelligence preparation of the battlefield, analysts will have described the enemy and operational environment to have the minimum products: • Modified combined obstacle overlay (MCOO). • Threat model. • Situational order of battle.	• Intelligence analysis assessment: Two motorized rifle brigades are advancing west to engage friendly forces. The enemy is likely to conduct a division frontal attack with infantry and motorized rifle brigades in order to penetrate the forward edge of the battle area to destroy friendly defenses and allow follow-on units to secure primary or secondary objectives. • Based on the assessment, the friendly commander may plan for the enemy's future operations and dispatch orders to subordinate units.
Analysts screen the following based on the specific requirement and operational guidelines: • At least one tank division with four brigade elements in attack position. • Two self-propelled artillery battalions in attack position. • At least one artillery brigade advancing west.	Analysts may use the following analytic techniques: • Quality of information check (*Diagnostic*) to refine and validate the projected orientation and power of enemy forces in the area of operations. • Weighted ranking (*Diagnostic*) to prioritize enemy capabilities to identify critical actions that could greatly affect friendly forces.	• Based on the MCOO: Canalizing terrain will force the armored brigades to engage friendly forces east. • Based on the threat model: The enemy is likely to conduct a divisional attack to cross the border and employ follow-on units to secure the key terrain. • With a refined intent to seize key terrain and a defined method verified by reporting and intelligence analysis, the friendly commander can maneuver subordinate units into a block. • Analysts may use the high impact/low probability (*Advanced*) analytic technique to identify, for subordinate units, indicators of pending offensive operations within their AORs. • Analysts may use the functional analysis (*Advanced*) analytic technique to verify the center of gravity proposed in the initial hypothesis.	The intelligence analysis process is continuous, and analysts should now consider: • What information can be exploited by subordinate units from the block? • How will the enemy benefit from the seizure of the key terrain? • Is there favorable terrain to friendly forces that could mitigate the canalizing terrain in future operations?

Table 8-2. Intelligence analysis (division) example (*continued*)

Division intelligence analysis example (continued)			
Action taken			
Screen	***Analyze***	***Integrate***	***Produce***
	Based on the initial hypothesis, analysts should consider: • What domains can friendly forces leverage to gain an advantage on the enemy? • Are there any windows of opportunity across the domains? • What is the best way to allocate assets based on the windows of opportunity?	• Canalizing terrain can create areas of interest that can be targeted or collected on by air assets. • With an anticipated block, analysts should placement of obstacles for enemy forces. • Are there any elements within the situational order of battle that can apply cyberspace electromagnetic activities (CEMA)? • What effect will CEMA have on navigation and communications assets?	The analyst must disseminate the corresponding products with the applicable domain operator: • Share named and target area of interest overlays with joint force assets. • Share MCOOs and additional terrain analysis with engineer units to support subordinate commands. • Provide electronic warfare and signal units with enemy CEMA capabilities to mitigate system interruptions.

TACTICAL/OPERATIONAL-LEVEL EXAMPLE (CORPS)

8-10. Figure 8-3 provides information about the OE that assists in understanding, at a macro level, the enemy. Understanding that the enemy is conducting a large-scale attack contextualizes the situation for the tactical/operational commander and influences critical decisions. Knowing the enemy is conducting a general attack to likely seize the city of Sawburg influences the tactical and operational commanders' employment of forces, acceptance of risk, and determination to hold key terrain.

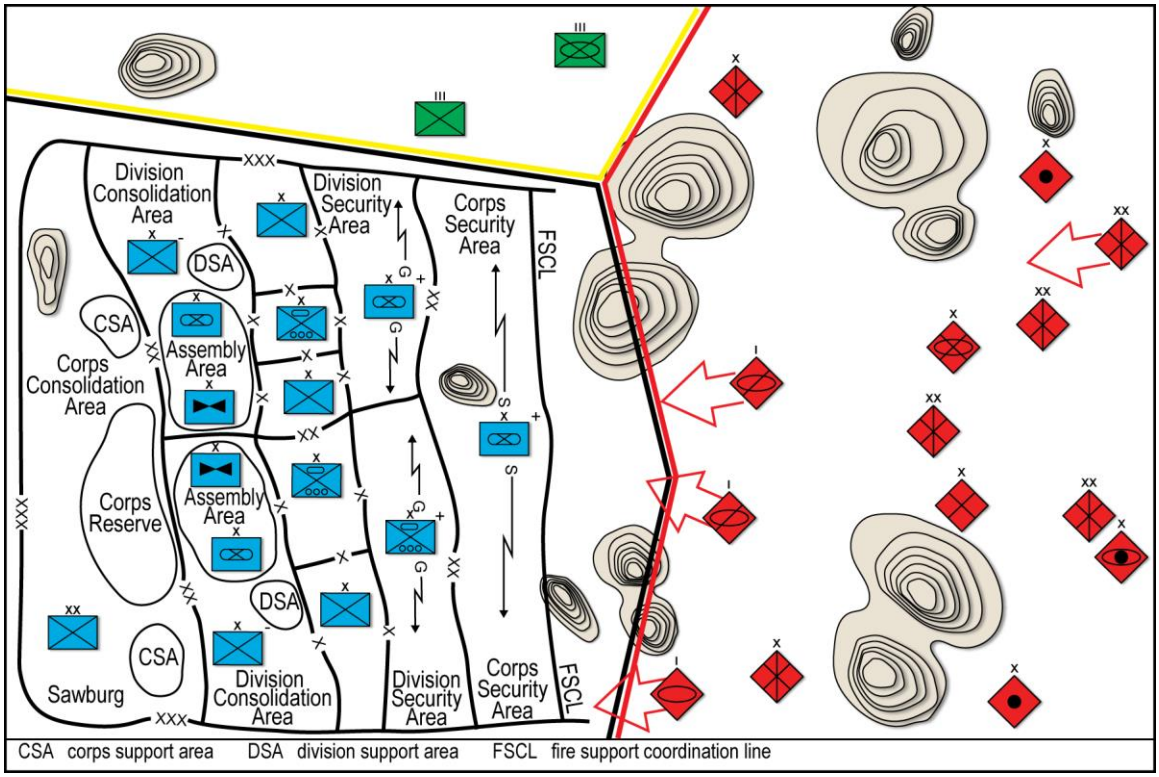


Figure 8-3. Tactical/Operational (corps) situation example

8-11. Based on reporting, the enemy has additional forces in the area, including a second tank division three to four days away in tactical-march formations. The friendly force commander is forced to commit ready forces to stop the enemy force advance since reserve elements are not available. (See table 8-3.)

Table 8-3. Intelligence analysis (tactical/operational [corps]) example

Corps intelligence analysis example			
Action taken			
Screen	***Analyze***	***Integrate***	***Produce***
• Based on the reports indicating enemy forces in attack position, analysts need to assess: ▪ Indicators of threat activities beyond 168 hours. ▪ Changes in the operational environment (OE) that will affect subordinate commands. ▪ Indicators that help shape and prevent potential threat action. • Analysts initiate analysis based on understanding why the enemy is attacking.	Analysts should form their initial hypothesis based on information assessed to be relevant in the *screen* phase.	Analysts should compare their new hypothesis to current intelligence holdings.	Analysts make their final assessment and produce a likely course of action (COA) for the commander to make a decision.
Based on this understanding, the commander provides the following specific requirement, which the intelligence section needs to address: Project the enemy's future operations for the next 96 to168 hours and establish the operational acceptance of risk.	Based on understanding the OE, analysts must assess: • What is the enemy commander's end state for seizing the key terrain? • How will the enemy commander use the key terrain if it is seized? • How much time will it take the enemy commander to maneuver forces to the border?	During mission analysis, analysts will have described the enemy and OE to have the minimum products: • Threat model. • Annex B (Intelligence) (to describe the enemy's likely intentions and end state). • Enemy COAs.	• Intelligence analysis assessment: The enemy conducts a general attack to likely seize Sawburg to influence the tactical and operational commanders' employment of forces, acceptance of risk, and determination to hold key terrain. • Based on the assessment, the friendly commander understands the enemy is attempting to push friendly units to a decision point and must plan to mitigate those operations.
Analysts screen the following based on the specific requirement and operational guidelines: • Location of key terrain is Sawburg. • Enemy composition and disposition in vicinity of friendly units.	Analysts may use the following analytic techniques: • Event trees (*Basic*) to develop initial scenarios of potential enemy actions. • Indicators/Signposts of change (*Diagnostic*) to establish a list of indicators to specific methods of offense being employed by the enemy. • Link analysis (*Basic*) to examine the relationship of resources, organizations, and other entities within the area of operations.	• Based on the threat model: Analysts assess the enemy commander to use armored divisions to conduct an attack. • Based on Annex B (Intelligence): It is likely the enemy will want to control Sawburg for resources. • Based on general enemy COAs: There is likely another tank division 3 to 4 days away from the projected battle zone. • Analysts could use the "what if?" (*Advanced*) analytic technique to generate the multiple outcomes of the operation, applying analytical rigor to their initial hypothesis. • Analysts could use the outside-in thinking (*Advanced*) analytic technique from other members or the staff or organization to gain insight on how favorable the key terrain would be for the enemy commander.	The intelligence analysis process is continuous, and analysts should now consider: • How will adjacent country (green) react to operations? • Are there any maneuvers that can mitigate the offensive enemy operation? • Can information collection refine enemy intentions?

Table 8-3. Intelligence analysis (tactical/operational [corps]) example (*continued*)

Corps intelligence analysis example			
Multi-domain considerations for intelligence analysis			
Screen	***Analyze***	***Integrate***	***Produce***
	Based on the initial hypothesis, analysts should consider: • What domains can friendly forces leverage to gain an advantage over the enemy? • What joint assets should be allocated to subordinate commands?	• Can the information environment develop indicators for enemy intentions? • Has the enemy leveraged information operations on Sawburg? • Reconnaissance in depth may have to be conducted by air assets on tank divisions 3 to 4 days away. • Are cyberspace electromagnetic activities (CEMA) vulnerable within the enemy's navigation and communications systems?	• Analysts must disseminate the corresponding products with the applicable domain operator: ▪ Provide named areas of interest (NAIs) for information collection to gain insight to Sawburg and their disposition to friendly and enemy forces. ▪ Share NAI and target area of interest overlays with joint force assets for reconnaissance in depth. • Analysts should synchronize with the CEMA cell to develop a better understanding of enemy intentions. • Analysts should use CEMA capabilities in conjunction with nonlethal targeting efforts.

Chapter 9
Managing Long-Term Analytical Assessments

OVERVIEW

9-1. Any echelon can conduct long-term intelligence analysis, which is simply analysis over a longer period of time (several months or longer). There are many forms of long-term analysis, such as long-term analytical assessments. Formal (authoritative or exploratory) long-term analytical assessments are usually associated with operational- and strategic-level intelligence units and organizations because these assessments are resource-intensive. Intelligence analysts at the tactical level can use some of the steps and substeps discussed in this appendix in order to improve their analysis, but they rarely apply all of the steps of the process.

9-2. Managing long-term analytical assessments, also referred to as analytic design in this appendix, ensures the analytical effort results in the best possible assessment. Analytic design ensures the analytical effort is properly focused, carefully planned and executed, and that the analytical results are effectively communicated to the requestor. The Defense Intelligence Agency published a helpful document, *Analytic Design: Analytic Tradecraft Guidance from the DI Research Director*, which served as the basis for this appendix.

9-3. Long-term analytical assessments are produced using a deliberate and specific execution of the intelligence analysis process over a longer period of time that closely complies with the Intelligence Community Analytic Standards (to include the analytic tradecraft standards) established in ICD 203. This form of analysis includes the careful management of the overall effort, dedicating significant resources to the effort (for example, analysis is conducted by an analytic team), executing various iterations of analysis, and applying advanced structured analytic techniques within the effort.

Note. Intelligence personnel should not use this appendix to develop criteria and standards for tactical-level intelligence analysis. This appendix covers the basics of analytic design but does not cover all the information needed to develop formal long-term analytical assessments. Specifically, some of the analytic techniques and the use of models and automated simulations are not discussed in this publication.

THE BASICS OF ANALYTIC DESIGN

9-4. Managing long-term analytical assessments is accomplished by performing seven analytic design steps, as shown in figure 9-1 on page 9-2:

- **Step 1:** Frame the question/issue.
- **Step 2:** Review and assess knowledge.
- **Step 3:** Review resources.
- **Step 4:** Select the analytic approach/methodology and plan project.
- **Step 5:** Develop knowledge.
- **Step 6:** Perform analysis.
- **Step 7:** Evaluate analysis.

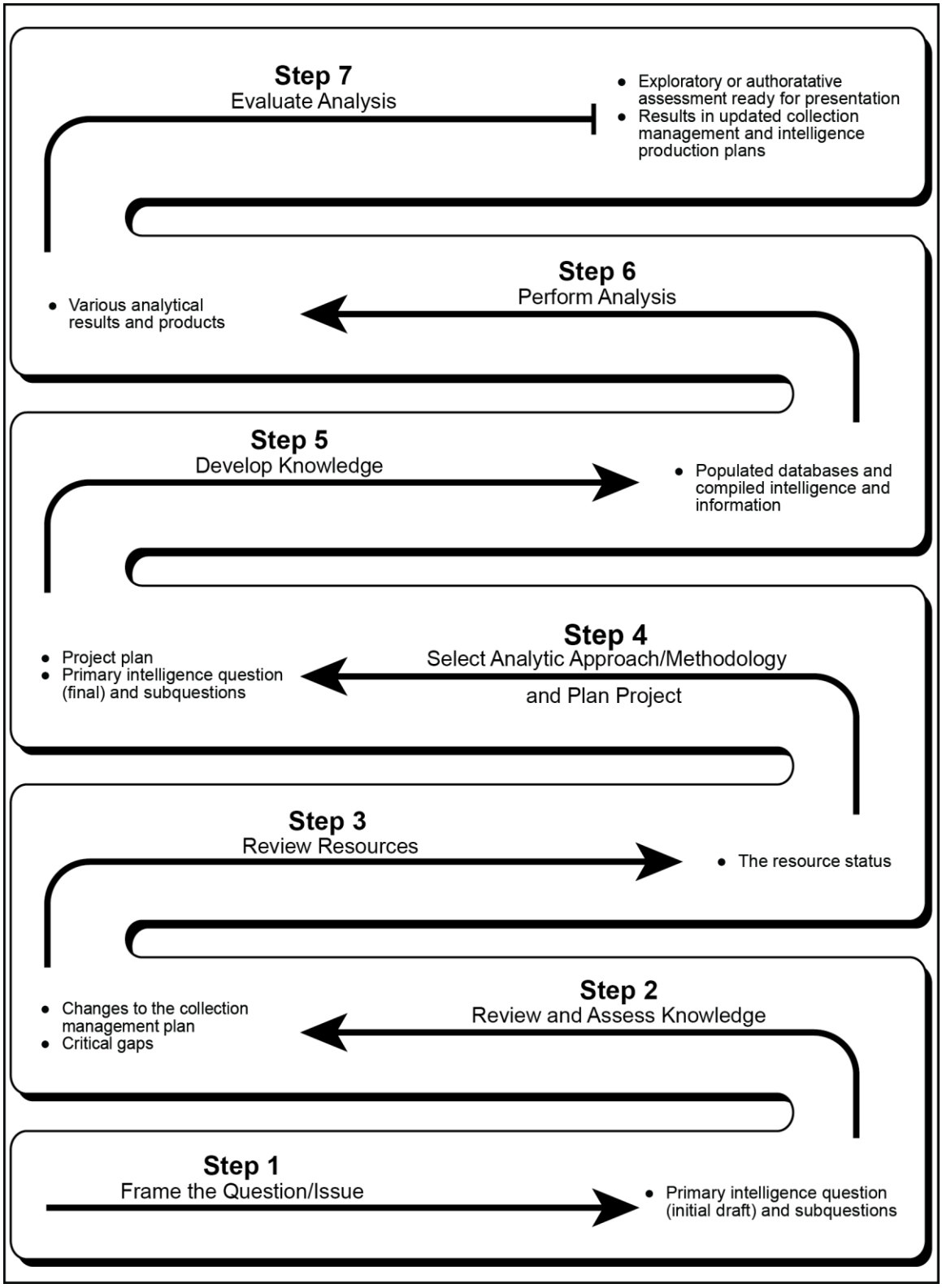


Figure 9-1. Analytic design steps

FRAME THE QUESTION/ISSUE

9-5. Properly framing the question greatly increases the chance of successful long-term analysis. The analytic team starts with understanding the requestor's requirement by identifying relevant topics and issues that break down into a primary question that can be analyzed. Framing the question includes refining and scoping the question to carefully capture the requestor's expectations, mitigate bias, craft an objective analytic question, and develop subquestions. This step results in an initial draft of the primary intelligence question and is followed by reviewing and assessing existing knowledge. (See figure 9-2.)

Note. Do not confuse the frame the question/issue step with the "frame" activities associated with the Army design methodology. (For information on the Army design methodology, see ATP 5-0.1)

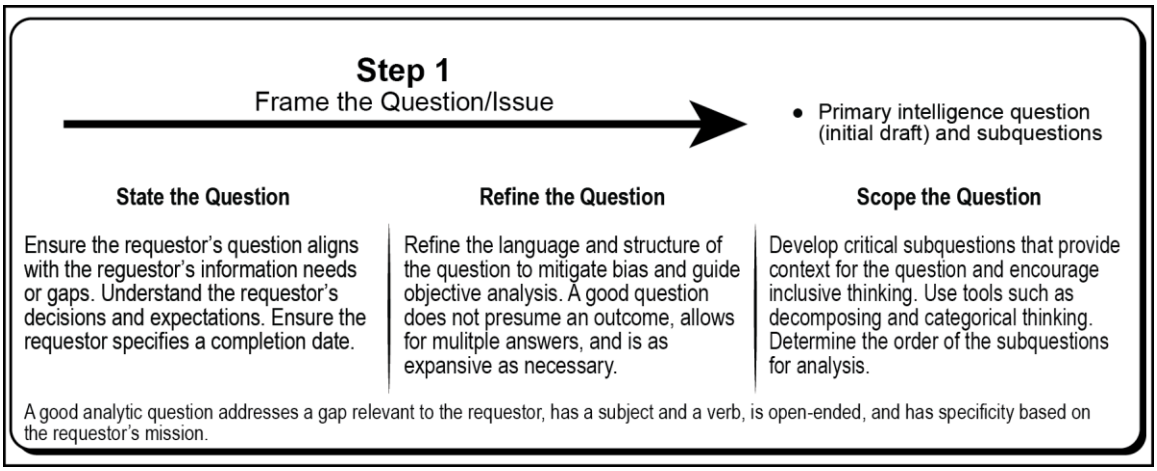


Figure 9-2. Frame the question/issue

REVIEW AND ASSESS KNOWLEDGE

9-6. Reviewing and assessing knowledge involves an overlap of the analytical effort with collection management. Step 2 includes reviewing available information and intelligence, the collection management plan, and results of on-going intelligence collection, as well as identifying information gaps. (See figure 9-3.)

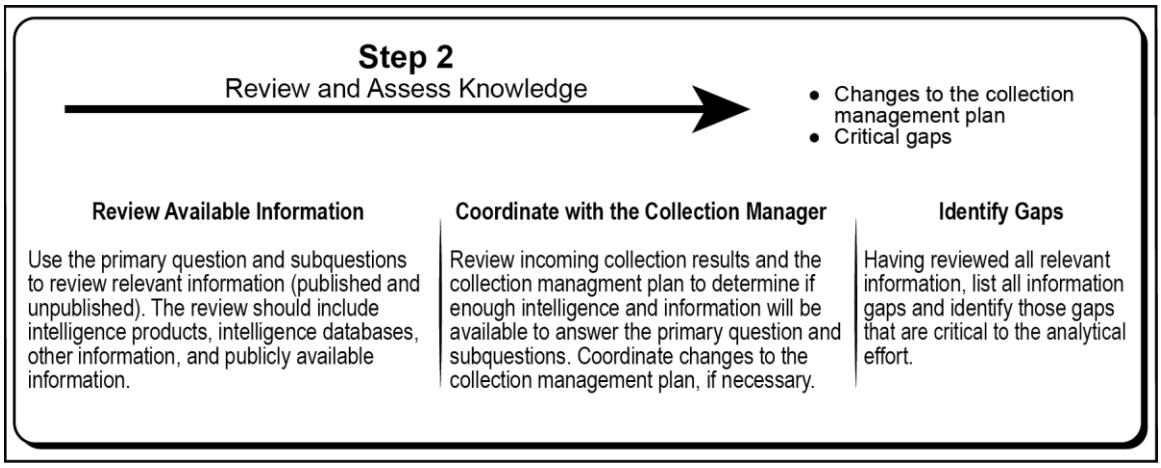


Figure 9-3. Review and assess knowledge

REVIEW RESOURCES

9-7. After understanding what knowledge is available and identifying information gaps, the next step is reviewing available resources, such as tools, personnel, and time. (See figure 9-4.)

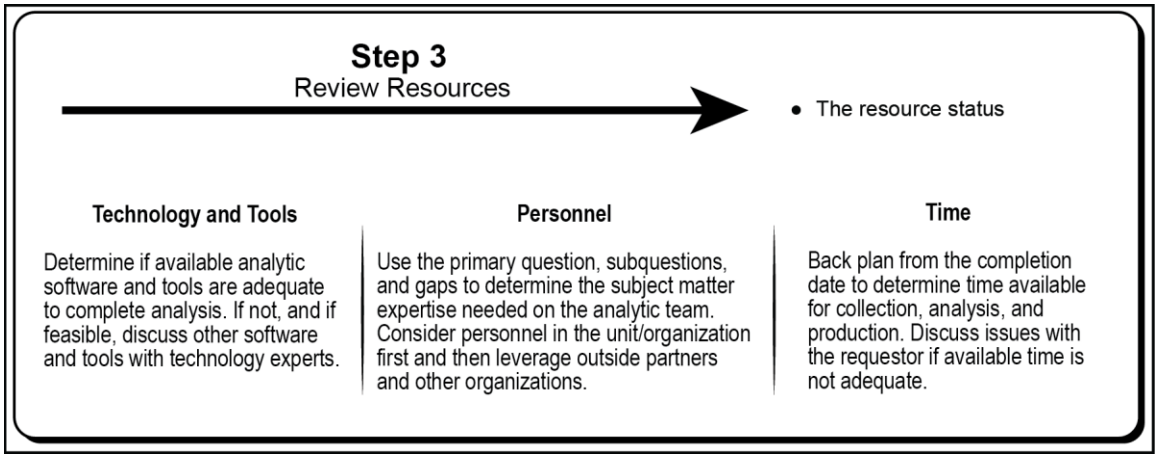


Figure 9-4. Review resources

SELECT THE ANALYTIC APPROACH/METHODOLOGY AND PLAN PROJECT

9-8. Using the results of steps 1 through 3, the analytic team finalizes the primary intelligence question and subquestions, selects the analytic approach/methodology, and develops a project plan. The analytic approach/methodology includes the specific analytic techniques, who will perform each technique, and the sequence of those techniques to ensure analytic insight and mitigate bias. (See figure 9-5.)

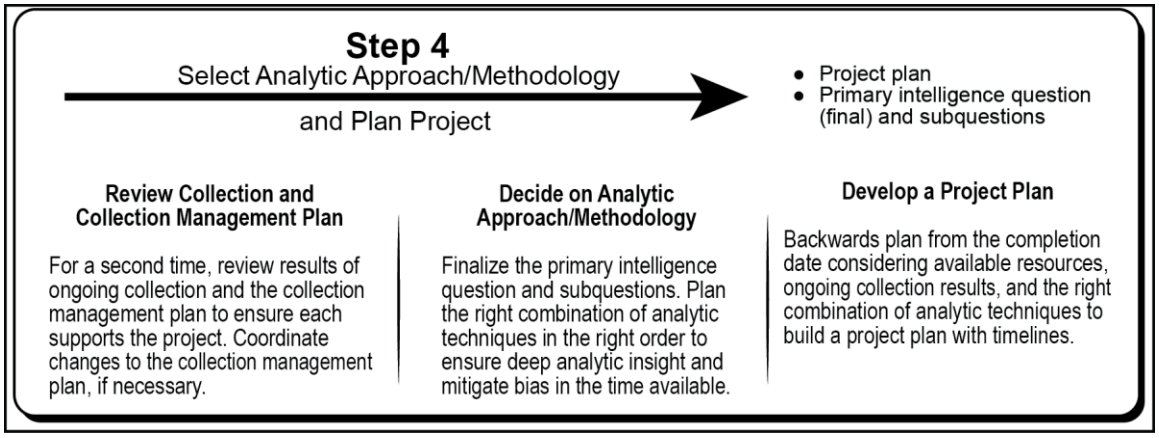


Figure 9-5. Select the analytic approach/methodology and plan project

DEVELOP KNOWLEDGE

9-9. Developing knowledge is the last step before performing analysis. Although discussed as a separate step in the process, developing knowledge occurs continually throughout the process. The analytic team gathers all relevant intelligence and information through ongoing collection, intelligence reach, and internal research. (See figure 9-6.)

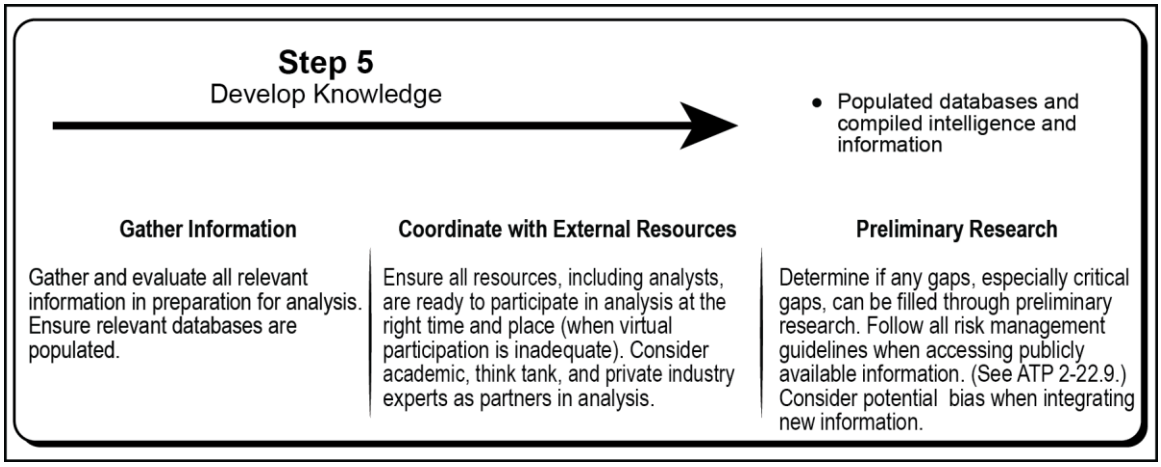


Figure 9-6. Develop knowledge

PERFORM ANALYSIS

9-10. Steps 1 through 5 set the stage for the deliberate execution of analytic techniques, to include adjusting the project plan, if necessary, and assessing the analytical results using the context that was developed while framing the question/issue. (See figure 9-7.)

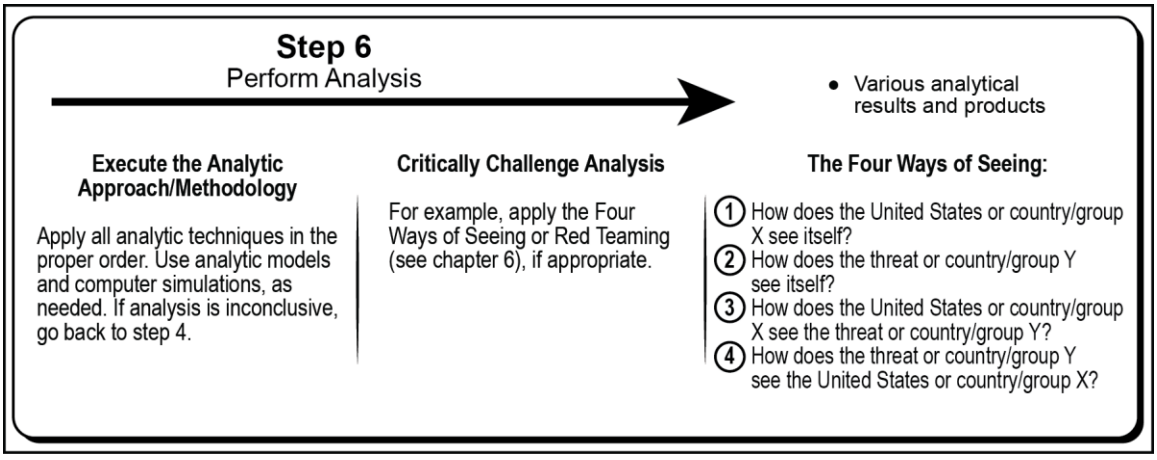


Figure 9-7. Perform analysis

EVALUATE ANALYSIS

9-11. Evaluating analysis, the final step of the process, results in the final analytical results and associated information necessary to make a presentation to the requestor. Evaluating analysis includes assessing the analytical results and the impact of analytic gaps and unconfirmed assumptions, performing analysis of alternatives, and assigning a confidence level to the analytic answer. (See figure 9-8.)

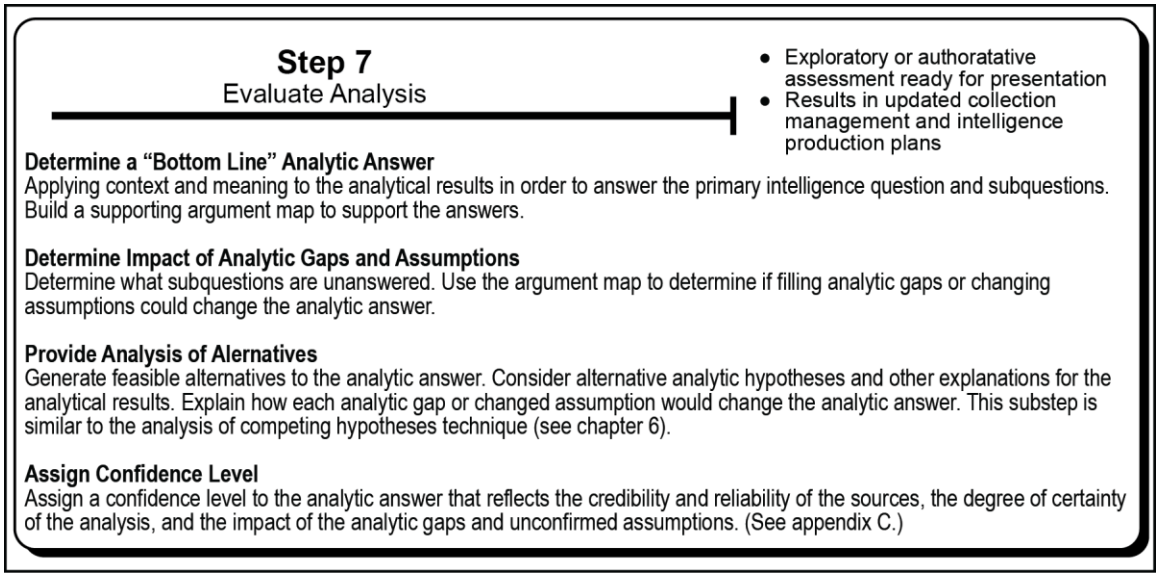


Figure 9-8. Evaluate analysis

COLLABORATION DURING ANALYTIC DESIGN

9-12. Collaboration is critical to long-term analytical assessments and occurs between different stakeholders across the intelligence community. This collaboration ensures a diversity of perspective and depth in expertise that is impossible through any other means. Four specific areas in which collaboration is invaluable are—

- **Bias mitigation:** Analytic teams with diverse backgrounds and different perspectives can effectively identify and check assumptions, interpret new information, and determine the quality of various types of information.
- **Framing/Knowledge review:** Analytic teams can engage early in the process to build context, craft analytic questions, share information sources, and develop analytical issues.
- **Methodology building:** Analytic teams assess the credibility of the analytic approach and clarity of the argument through various means, including peer reviews.
- **Perform analysis:** Analytic teams can perform various analytic techniques, identify hypotheses, and analyze alternatives as a group to improve the quality of the analytical effort.

TRANSITIONING FROM THE ANALYTIC DESIGN PROCESS TO PRESENTING THE RESULTS

9-13. Managing long-term analytical assessments includes not only presenting an analytic answer but also a confidence level to the answer and alternative hypotheses or explanations for gaps and uncertainty. During evaluate analysis, the last step of the process, the analytic team decides whether the question requires more analysis, and therefore, whether the assessment is exploratory or authoritative and ready to present to the requestor. If the results are ready for presentation, the analytic team deliberately prepares to present those results. Transitioning from long-term analysis to presenting the analytic answer includes stepping back from that analysis, reviewing the assessment, and clarifying the relevance of the analytical results. Then the analytic team determines—

- **What is the message:** The message characterizes whether the assessment is authoritative or exploratory and includes the "bottom line" of the assessment. Additionally, the assessment includes any shifts in analysis that occurred over time, any impacts on the requestor (decisions and future focus areas), the confidence level, alternative hypotheses, and indicators.
- **What is the analytical argument:** The analytic team develops an outline for logically progressing through the analytical assessment. An argument map is a useful tool to ensure a logical analytical flow during the presentation and to ensure the message is easily understood. The team may use basic interrogatives (*who, what, when, where, why,* and *how*) or a similar tool to capture the critical elements of the message to present to the requestor.
- **What are critical gaps and assumptions:** Gaps and assumptions identified during the evaluate analysis step become limitations to the certainty of the analytical assessment, and, in some cases, drive future analytical efforts. The analytic team may insert gaps and assumptions within the message and clearly discuss the level of impact on the assessment (for example, in the source summary statement or in the "bottom line" statement).
- **What reasonable analytical alternatives remain:** For authoritative assessments, answering the questions *"what if I am wrong"* and *"what could change my assessment"* provides analysis of alternatives that should be included in the assessment to explain what remains uncertain.
- **What product or products should be presented:** Determine the best format for the presentation that facilitates the discussion of the argument. If it is exploratory analysis, the format should allow the analytic team to effectively describe the new understanding of the topic and its relevance to the requestor. The team should consider the following when choosing the format: requestor preference, specific tasking/requirement, complexity of the argument, urgency/time constraints, and potential interest of others.

CROSSWALKING ANALYTIC DESIGN WITH TACTICAL INTELLIGENCE ANALYSIS

9-14. Tactical intelligence analysis and analytic design have similarities but also differ in a number of ways. Tactical operations are often chaotic and time-constrained, and therefore, driven by specific commander-centric requirements (for example, PIRs and targeting requirements). The commander and staff plan and control operations by employing several standard Army planning methodologies, including but not limited to the Army design methodology, the MDMP, and Army problem solving. (See ADP 5-0 for a discussion of these methodologies.) Large portions of steps 1 through 5 of analytic design equate to the Army's time-tested planning processes, namely the Army design methodology, the MDMP (including IPB), and Army problem solving. Parts of steps 1 through 5 also equate to generate intelligence knowledge, which is a continuous task that develops general intelligence knowledge for subsequent intelligence analysis (see paragraphs 3-6 and 3-7).

9-15. Many of the doctrinal concepts presented in this and other publications are consistent with the analytic design steps discussed in this appendix. Table 9-1 provides a crosswalk of the analytic design steps to various Army doctrinal concepts and their associated references.

Table 9-1. Analytic design to tactical intelligence analysis crosswalk

Analytic design step	*Doctrinal concepts and references*
Step 1: Frame the question/ issue	• ATP 2-33.4: ▪ Develop commander's PIRs, par. 1-30. ▪ Frame the analytic problem with PIRs and other requirements, par. 2-5 and figure 2-1. ▪ Commander's visualization of the OE and threat, pars. 3-8 and 3-9. • ADP 5-0: Identify requirements to support decision points, pars. 1-40–1-43. • ATP 2-01: Refine PIRs into SIRs and indicators, par. 2-9. • ATP 5-0.1: Frame OEs, chapter 3.
Step 2: Review and assess knowledge	• ATP 2-33.4: ▪ Include information and intelligence from all available sources, par. 1-44. ▪ Screen collected information, pars. 2-7 and 2-8. ▪ Review information previously discarded as nonessential, par. 2-21. • ATP 2-01: Plan collection management, par. 1-4. • ATP 5-0.1: Share knowledge and build consensus, par. 1-32. • ATP 2-01.3: Identify intelligence gaps in knowledge, par. 1-16.

Table 9-1. Analytic design to tactical intelligence analysis crosswalk (*continued*)

Analytic design step	*Doctrinal concepts and references*
Step 3: Review resources	• ATP 2-33.4: ▪ Identify planning and execution deadlines, par. 1-23. ▪ Collaborate with available analytic assets, pars. 1-25 and 1-26. ▪ Identify all-source intelligence architecture requirements, pars. 1-32 and 1-33. ▪ Identify availability of time, tools, services, and other sources, pars. 2-8 and 7-2. • FM 2-0: ▪ Leverage intelligence, par. 1-19. ▪ Determine intelligence reach relationships, par. 1-25. • FM 3-55: Conduct information collection with organic and nonorganic resources, par. 1-28. • ATP 2-01: Evaluate resources, par. 4-2. • MI Pub 2-01.2: ▪ Plan the intelligence architecture, chapter 1. ▪ Prepare the intelligence architecture, chapter 2.
Step 4: Select analytic approach/methodology and plan project	• ATP 2-33.4: ▪ Determine optimal all-source structure to address the question, par. 1-34. ▪ Chapter 4, *Analytic Techniques.* ▪ Chapter 5, *Basic and Diagnostic Structured Analytic Techniques*. ▪ Chapter 6, *Advanced Structured Analytic Techniques.* • ATP 2-01: Plan collection management, par. 3-2. • ATP 5-0.1: Plan to facilitate decision making, pars. 1-7–1-10.
Step 5: Develop knowledge	• ATP 2-33.4: ▪ Think critically, par. 1-24. ▪ Screen collected information, pars. 2-7 and 2-8. ▪ Integrate new information with prior holdings, pars. 2-16–2-18. ▪ Review information previously discarded as nonessential, par. 2-21. ▪ Generate intelligence knowledge, pars. 3-6 and 3-7. • ADP 2-0: Generate knowledge through the intelligence process, par. 3-4. • FM 2-0: Access information through intelligence reach, pars. 1-25–1-33. • FM 3-55: Gather data to support primary information collection tasks and operations, par. 1-30.
Step 6: Perform analysis	• ATP 2-33.4: ▪ Conduct intelligence analysis, pars. 1-15 and 1-16. ▪ Reach determination based on facts and assumptions, par. 1-24. ▪ Chapter 2, *The Intelligence Analysis Process.* ▪ Chapter 4, *Analytic Techniques.* ▪ Chapter 5, *Basic Diagnostic Structured Analytic Techniques.* ▪ Chapter 6, *Advanced Structured Analytic Techniques.* ▪ Appendix B, *Cognitive Considerations for Intelligence Analysts.* (This appendix describes thinking abilities, critical and creative thinking, and avoiding analytical pitfalls.)
Step 7: Evaluate analysis	• ATP 2-33.4: ▪ Answer the *'so what'* from the commander's perspective, par. 1-21. ▪ Determine relevancy before producing assessments, par. 1-27. ▪ Appendix B, *Cognitive Considerations for Intelligence Analysts.* (This appendix describes thinking abilities, critical and creative thinking, and avoiding analytical pitfalls.) ▪ Appendix C, *Analytic Standards and Analysis Validation.* (This appendix discusses the analytic standards that govern intelligence analysis.)

Doctrinal references:	**Legend:**	
ADP 2-0, *Intelligence*	MI Pub	military intelligence publication
ADP 5-0, *The Operations Process*	OE	operational environment
ATP 2-01.3, *Intelligence Preparation of the Battlefield*	par./pars.	paragraph/paragraphs
ATP 2-33.4, *Intelligence Analysis*	PIR	priority intelligence requirement
ATP 5-0.1, *Army Design Methodology*	SIR	specific information requirement
FM 2-0, *Intelligence*		
FM 3-55, *Information Collection*		
MI Pub 2-01.2, *Establishing the Intelligence Architecture*		

Appendix A

Automation Support to Intelligence Analysis

AUTOMATION ENABLERS

A-1. Many different automation and communications systems are vital to intelligence analysis; they facilitate real-time collaboration, detailed operational planning, and support to collection management. Software updates and emerging technologies continue to improve current intelligence analysis systems to operate more effectively in garrison and in deployed environments.

A-2. Automation processing capabilities and tools readily available on today's computers enable the intelligence analysis process. The software or related programs in current automation systems allow intelligence analysts to screen and analyze significantly more data than in previous years. The development of analytical queries, data management tools, and production and dissemination software enhances the intelligence analysis process, facilitating the commander's situational understanding and timely decision making across all echelons.

A-3. Automation is crucial to intelligence analysis; there are four aspects for analysts to consider:

- Automation is a key enabler to the processing and fusion of compatible information and intelligence, but the individual analyst remains essential in the validation of any assessment.
- The analyst must still be heavily involved in building specific queries, analyzing the final assessment, and releasing intelligence.
- Automation relies on the cyberspace domain, which requires extensive defensive actions to ensure data is not corrupted from collection to dissemination. Deception and corruption within the cyberspace domain are likely occurrences; therefore, they require monitoring by both cyberspace experts and intelligence analysts.
- Automation relies on available communications to receive, assess, and disseminate information across the command at all echelons. During periods of disrupted or degraded communications, the intelligence analyst must understand and may have to execute intelligence analysis without the aid of automation.

DISTRIBUTED COMMON GROUND SYSTEM-ARMY

A-4. All communications, collaboration, and intelligence analysis within the intelligence warfighting function are facilitated by the DCGS-A—the intelligence element of Army command and control systems and an Army program of record. DCGS-A can leverage the entire national, joint, tactical, and multinational intelligence community for intelligence reach and federated analysis. DCGS-A enables the intelligence analysis process through software tools, as shown in figure A-1 on page A-3. The following highlights some of the most significant tools across the phases of the intelligence analysis process:

- **Screen:**
  - ***Axis Pro/Link Diagram*** is a software product used for data analysis and investigations that assists in mapping and understanding threat networks comprising threat equipment, units, facilities, personnel, activities, and events.
  - ***Threat Characteristics Workstation*** provides tools to develop and manage threat characteristics, track battle damage assessments (BDAs), and create doctrinal and dynamic situation templates. The workstation also allows analysts to create graphic and written comparisons of threat capabilities and vulnerabilities, which are included in the intelligence estimate.
  - ***Weather Client*** allows analysts to identify segments of the battlefield that require an in-depth evaluation of weather effects on friendly and threat operations. This evaluation gives the commander a general overview of potential effects throughout the AO.

- ***MovINT Client*** provides an integrated, temporal view of the battlefield, and aggregates air- and ground-force locations, moving target intelligence, aircraft videos, sensor points of interest, and target locations.

- **Analyze**:
  - ***SOCET GXP*** (also known as Softcopy Exploitation Toolkit Geospatial Exploitation Product), an advanced geospatial intelligence software solution, uses imagery from satellite and aerial sources to identify, analyze, and extract ground features, allowing for rapid product creation.
  - ***Terra Builder/Explorer*** provides professional-grade tools for manipulating and merging imagery and elevation data of different sizes and resolutions into a geographically accurate terrain database. It also allows analysts to view, query, analyze, edit, present, and publish geospatial data.
  - ***Text Extraction*** allows analysts to quickly extract information from reports, associate elements with relationships, and identify existing matches in the database.
  - ***ArcGIS*** (also known as Arc Geographic Information System) allows analysts to visualize, edit, and analyze geographic data in both two- and three-dimensional images and has several options for sharing with others.
- **Integrate:**
  - ***Multifunction workstation interface***, a customizable interface that streamlines workflow, supports the commander's operations by providing accurate and timely intelligence and analysis to support Army forces.
  - ***ArcGIS***. (See description under **Analyze**.)
  - ***Google Earth***, a geo-browser that accesses satellite and aerial imagery, ocean bathymetry, and other geographic data of a network, represents the Earth as a three-dimensional globe.
- **Produce:**
  - ***Office 2013*** is a suite of productivity applications that includes Microsoft Word, Excel, PowerPoint, Outlook, OneNote, Publisher, Access, InfoPath, and Link.
  - ***Multifunction workstation interface***. (See description under **Integrate**.)
  - ***i2 Analyst Notebook*** is a software product used for data analysis and investigation. It is part of the Human Terrain System, an Army program that embeds social scientists with combat brigades.

A-5. DCGS-A, like any automation system, is subject to software updates, including changes to the current hardware as well as lifecycle replacements. As such, future versions may include greater analytical cross discipline and domain collaboration and improved interoperability with command and control systems and knowledge management components. (See figure A-1.)

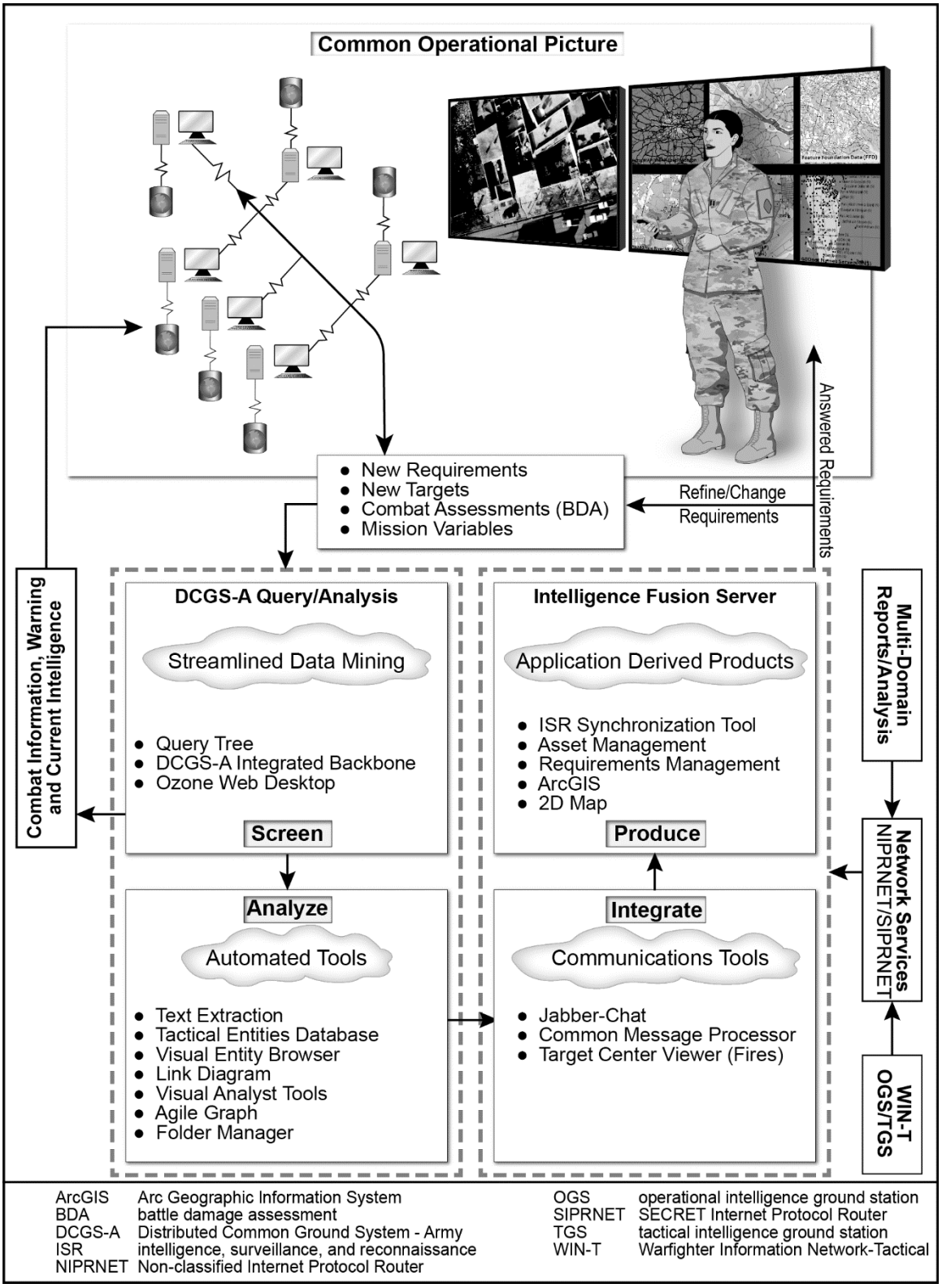


Figure A-1. Intelligence analysis enabled by DCGS-A

This page intentionally left blank.

Appendix B

Cognitive Considerations for Intelligence Analysts

OVERVIEW

B-1. Analytic skills are the ability to collect, visualize, and examine information in detail to make accurate analytical conclusions. Analytic skills enable Army Soldiers to complete simple and complex tasks; they enable intelligence analysts to use deliberate thought processes to examine a situation critically and without bias.

THE INTELLIGENCE ANALYST

B-2. Intelligence analysis support to any operation involves separating useful information from misleading information, using experience and reasoning, and reaching an assessment or conclusion based on fact and/or sound judgment. The conclusion is based on the intelligence analyst's—

- Experience, skill, knowledge, and understanding of the operation.
- Knowledge of the various intelligence disciplines.
- Knowledge of information collection.
- Understanding of the threats within an OE.
- In-depth understanding of the threat's military and political structure.

B-3. The intelligence personnel conducting the analysis of information and intelligence use basic to advanced tradecraft skills and tools and integrated automated programs to sort raw forms of data and information and apply research skills to formulate an assessment. Analysts are responsible for the timely dissemination and/or presentation (proper writing and presentation techniques) of known facts and assumptions regarding the OE to the commander and staff. There are established tradecraft standards that direct the individual or group of analysts to ensure the analysis meets a common ethic to achieve analytical excellence.

B-4. Intelligence analysts follow guidelines, such as the ICD 203 Intelligence Community Analytic Standards, that promote a common ethic for achieving analytical rigor and excellence and personal integrity in analytical practices. (See appendix C.) Additionally, they must build their foundational understandings and integrate their learned skills—critical thinking and embracing ambiguity. Intelligence analysts must be willing to change their determinations over time. Training, knowledge, and experience further develop analysts' expertise, as these aspects are essential in helping analysts deal with the uncertain and complex environments.

B-5. The OE is complex, and the threat attempts to hide its objectives, intent, and capabilities when possible. Therefore, intelligence analysts embrace ambiguity, recognize and mitigate their own or others' biases, challenge their assumptions, and continually learn during analysis. To assist in mitigating some of the uncertainty associated with conducting intelligence analysis, analysts should increase their proficiency in using analytic techniques and tools, including automated analytic tools and systems, to identify gaps in their understanding of the OE. Furthermore, to be effective, intelligence analysts must have a thorough understanding of their commanders' requirements and the intelligence analysis process (see chapter 2), which directly contributes to satisfying those requirements.

BASIC THINKING ABILITIES

B-6. Army intelligence personnel are required to use basic thinking abilities and complex skills to analyze information. These skills relate to an analyst's ability to think. Intelligence analysis focuses primarily on thinking. Intelligence analysts must continually strive to improve the quality of their thinking to support the commander's requirements. The three basic thinking abilities for intelligence analysis are

- Information ordering.
- Pattern recognition.
- Reasoning.

INFORMATION ORDERING

B-7. *Information ordering* is the ability to follow previously defined rules or sets of rules to arrange data in a meaningful order. In the context of intelligence analysis, this ability allows analysts, often with technology's assistance, to arrange information in ways that permit analysis, synthesis, and a higher level of understanding. The arrangement of information according to certain learned rules leads analysts to make conclusions and disseminate the information as intelligence. However, such ordering can be inherently limiting—analysts may not seek alternative explanations because the known rules lead to an easy conclusion.

PATTERN RECOGNITION

B-8. Humans detect and impose patterns on apparently random entities and events in order to understand them, often doing this without awareness. Intelligence analysts impose or detect patterns to identify relationships, and often to infer what they will do in the future. Pattern recognition lets analysts separate the important from the less important, even the trivial, and conceptualize a degree of order out of apparent chaos. However, imposing or seeking patterns can introduce bias. Analysts may impose culturally defined patterns on random aggregates rather than recognize inherent patterns, thereby misinterpreting events or situations.

REASONING

B-9. *Reasoning* is what allows humans to process information and formulate explanations in order to assign meaning to observed actions and events. The quality of any type of reasoning is based on how well analysts' analytic skills have been developed, which occurs through practice and application. Improving analytic skills occurs by implementing individual courses of study and organizational training strategies.

B-10. There are four types of reasoning that guide analysts in transforming information into intelligence:

- **Deductive reasoning** is using given factual information or data to infer other facts through logical thinking. It rearranges only the given information or data into new statements or truths; it does not provide new information. Therefore, deductive reasoning is, *"If this is true, then this is also true."*
- **Inductive reasoning** is looking at given factual information or data for a pattern or trend and inferring the trend will continue. Although there is no certainty the trend will continue, the assumption is it will. Therefore, inductive reasoning is, *"Based on this trend, this is probably true."*
- **Abductive reasoning** is similar to inductive reasoning since conclusions are based on probabilities or "guessing." Therefore, abductive reasoning is, "*Because this is probably true, then this may also be true."*
- **Analogical reasoning** is a method of processing information that relies on an analogy to compare the similarities between two specific entities; those similarities are then used to draw a conclusion—the more similarities between the entities, the stronger the argument.

Note. Of the four types of reasoning, only deductive reasoning results in a conclusion that is always true. However, during the conduct of intelligence analysis, this statement can be misleading. During operations, there are few situations in which both a rule is always true and there is adequate collection on the threat to apply deductive reasoning with certainty.

Even in the best of circumstances, inductive, abductive, and analogical reasonings cannot produce conclusions that are certain. All of the types of reasoning rely on accurate information, clear thinking, and freedom from personal bias and group thinking.

B-11. Figure B-1 provides hypothetical examples for each type of reasoning. The examples are based on a peer threat with multiple divisions. The threat designates its divisions as first-tier, second-tier, or third-tier based on their equipment, end strength, and ability to conduct complicated operations. Effective execution of a relief-in-place is very complicated.

Deductive Reasoning	*Inductive Reasoning*	*Abductive Reasoning*	*Analogical Reasoning*
General Rule ↓ Specific Conclusion (always true)	**Specific Observations** ↓ General Conclusion (probably true)	**Incomplete Observations** ↓ Best Prediction (may be true)	**Incomplete Observations** ↓ Possible Prediction (may be true) (Requires Further Analysis)
P1: All first-tier divisions are capable of conducting an effective relief-in-place. **P2:** The 87th Tank Division is designated as a first-tier division. **Conclusion:** The 87th Tank Division is capable of conducting an effective relief-in-place.	**P1:** The 87th Tank Division is designated as a first-tier division. **P2:** The 87th Tank Division is capable of conducting an effective relief-in-place. **Conclusion:** All first-tier divisions are capable of conducting an effective relief-in-place.	**P1:** All first-tier divisions are capable of conducting an effective relief-in-place. **P2:** The 87th Tank Division is capable of conducting an effective relief-in-place. **Conclusion:** The 87th Tank Division is designated as a first-tier division.	**Similarities:** The 46th Tank Division has key leaders who all received exceptional ratings throughout their career; the division is manned at 90% strength. **Similarities:** The 87th Tank Division has key leaders who all received exceptional ratings throughout their career; the division is manned at 90% strength. **P3:** The 46th Tank Division is designated as a first-tier division. **Conclusion:** The 87th Tank Division is designated as a first-tier division.
P premise			

Figure B-1. Types of reasoning examples

CRITICAL AND CREATIVE THINKING

B-12. Combining good analytic techniques with an understanding of the requirements, area knowledge, and experience is the best way of providing accurate, meaningful assessments to commanders and leaders. However, subject matter expertise alone does not guarantee the development of logical or accurate conclusions. Intelligence analysts apply critical thinking skills to provide more holistic, logical, ethical, and unbiased analysis and conclusions. Critical thinking ensures analysts fully account for the elements of thought, the intellectual standards of thought, and the traits of a critical thinker.

B-13. *Critical thinking* is a deliberate process of analyzing and evaluating thought with a view to improve it. The elements of thought (the parts of a person's thinking) and the standards of thought (the quality of a person's thinking) support critical thinking. Key critical thinking attributes include human traits such as intellectual courage, integrity, and humility. *Creative thinking* involves creating something new or original.

B-14. Analysts use thinking to transform information into intelligence. Critical thinking can improve many tasks and processes across Army operations, especially the conduct of intelligence analysis. Critical thinking includes the intellectually disciplined activity of actively and skillfully analyzing and synthesizing information. The key distinction in critical thinking is a reflective and self-disciplined approach to thinking.

B-15. For the analyst, the first step in building critical thinking skills is to begin a course of personal study and practice with a goal of improving the ability to reason. This means moving outside the Army body of doctrine and other Army professional writing when beginning this study. Most of the body of thought concerning critical thinking extends throughout various civilian professions, particularly those in academia. The discussion in this publication provides a glimpse of what should become a professional endeavor.

B-16. The Army has used many different sources in its doctrinal discussions of critical thinking. Among those most cited, as well as those used in the development of this discussion, are Dr. Richard Paul and Dr. Linda Elder of the Foundation for Critical Thinking. This foundation has developed many products and tools that assist Army leaders and Soldiers in developing critical thinking skills. Of those, the elements of thought, intellectual standards, and intellectual traits are the most useful tools analysts can initially apply to further their critical thinking skills. These tools can also assist analysts in avoiding the common pitfalls of undisciplined thinking (see paragraph B-30).

ELEMENTS OF THOUGHT

B-17. Whenever people think, they think for a purpose within a point of view based on assumptions leading to implications and consequences. People use concepts, ideas, and theories to interpret data, facts, and experiences in order to answer questions, solve problems, and resolve issues. These eight elements of thought assist in describing how critical thinking works:

- **Element 1—Purpose.** All thinking has a purpose. Critical thinkers will state the purpose clearly. Being able to distinguish the purpose from other related purposes is an important skill that critical thinkers possess. Checking periodically to ensure staying on target with the purpose is also important.
- **Element 2—Question at issue.** All thinking is an attempt to figure something out, to settle some question, or to solve some problem. A critical thinker can state questions clearly and precisely, express the questions in several ways to clarify their meaning and scope, and break the questions into subquestions.
- **Element 3—Information.** All thinking is based on data, information, and evidence. Critical thinkers should support their conclusions with relevant information and be open to actively searching for information that supports and contradicts a position. All information should be accurate, clear, and relevant to the situation being analyzed.
- **Element 4—Interpretation and inference.** All thinking contains interpretations and inferences by which to draw conclusions and give meaning to data. Critical thinkers should be careful to infer only what the evidence implies and to crosscheck inferences with each other. They should clearly identify the assumptions and concepts that led to the inferences, as well as consider alternative inferences or conclusions. Developing and communicating well-reasoned inferences represent the most important parts of what intelligence analysts provide because they aid situational understanding and decision making.
- **Element 5—Concepts.** All thinking is expressed through, and shaped by, concepts. A concept is a generalized idea of a thing or a class of things. People do not always share the same concept of a thing. For example, the concept of happiness means something different to each individual because happiness comes in many different forms. For a star athlete, happiness may be winning; for a mother, happiness may be seeing her children do well. To ensure effective communications, critical thinkers identify the meaning they ascribe to the key concepts used in their arguments and determine if others in their group ascribe different meanings to those concepts.
- **Element 6—Assumptions.** All thinking is based, in part, on assumptions. In this context, an assumption is a proposition accepted to be true without the availability of fact to support it. Assumptions are layered throughout a person's thinking and are a necessary part of critical thinking. The availability of fact determines the amount of assumption an analyst must use in analysis. Critical thinkers clearly identify their assumptions and work to determine if they are justifiable.
- **Element 7—Implications and consequences.** All thinking leads somewhere or has implications and consequences. Analysts should take the time to think through the implications and consequences that follow from their reasoning. They should search for negative as well as positive implications.
- **Element 8—Point of view.** All thinking is performed from some point of view. To think critically, analysts must recognize a point of view, seek other points of view, and look at them fair-mindedly for their strengths and vulnerabilities.

B-18. By applying the eight elements of thought, analysts can develop a checklist for reasoning. Developing and using a checklist, as shown in table B-1, can help analysts focus their efforts to a specific problem and avoid wasting time on irrelevant issues or distractions.

Table B-1. Checklist for reasoning

Element	*Explanation*
Purpose	All reasoning has a purpose. Failure to identify the purpose causes problems throughout the analytical effort: • Express the purpose only. • Distinguish the purpose from similar purposes. • Check periodically to remain on target. • Choose significant and realistic purposes.
Question at issue	All reasoning is an attempt to figure something out, to answer some question, to meet some requirement: • State the question at issue clearly and precisely • Express the question in several ways to clarify its meaning and scope. • Carefully break the question into subquestions. • Distinguish between questions that have definitive answers from those that are a matter of opinion and from those that require consideration of multiple viewpoints.
Information	All reasoning is based on data and information: • Only state facts as facts and clearly identify the assumptions used to help form conclusions. • Search for information that opposes one's position as well as information that supports it. • Ensure all information used is clear, accurate, and relevant to the question at issue. • Gather sufficient information.
Interpretation and inference	All reasoning contains inferences or interpretations from which to draw conclusions and give meaning to data: • Infer only what the evidence implies. • Check inferences for their consistency with others. • Identify assumptions, underlying one's inferences. ***Note.*** Inferring involves uncertainty. Analysts must deal with different degrees of uncertainty. Both the complexity of a situation and the availability of information determine the amount of uncertainty that will exist.
Concepts	All reasoning is expressed through, and shaped by, concepts and ideas: • Identify key concepts and explain them clearly. • Consider alternative concepts or alternative definitions to concepts. • Use concepts with precision.
Assumptions	All reasoning includes assumptions: • Clearly identify and justify assumptions to the audience. • Ascertain those deep-held personal assumptions that can affect one's analysis.
Implications and consequences	All reasoning leads somewhere or has implications and consequences: • Trace the implications and consequences that follow from one's reasoning. • Search for negative and positive implications. • Consider all possible consequences.
Point of view	All reasoning is performed from some point of view: • Identify one's point of view. • Seek points of view from other analysts related to the threat and other significant aspects of the operational environment and identify their strengths and vulnerabilities. • Strive to be fair-minded when considering other points of view.

INTELLECTUAL STANDARDS

B-19. When critical thinkers take apart their thinking and examine its parts, they use standards of quality referred to as the intellectual standards or standards for thought. While the elements of thought provide a framework for analyzing thinking, the standards of thought provide criteria that critical thinkers use to assess the quality of thinking. The effectiveness of intelligence analysis and resulting products can be measured against nine intellectual standards:

- **Standard 1—Clarity.** Clarity is the gateway standard. If the questions a person tries to answer, the information a person uses, the inferences a person makes, and the assumptions that guide a person's thinking are unclear, one cannot determine whether the information the person provides is accurate, relevant, logical, or justifiable. Therefore, analysts should strive to provide information clearly, so the audience understands it.
- **Standard 2—Accuracy.** To be accurate is to represent something in accordance with the way it actually is. People often describe things or events inaccurately. Critical thinkers listen carefully to statements and, when there is reason for skepticism, they question whether what they hear is true or accurate. A statement describing an implication, assumption, inference, or the very question a person tries to answer may be clear but not accurate. ***Note.*** Since people tend to think from an egocentric and/or socio-centric perspective, assessing the accuracy of their own ideas can be difficult. People tend to believe their thoughts are accurate just because the thoughts belong to them; therefore, the thoughts of those that disagree with theirs are inaccurate. Additionally, people often fail to question statements made by others that agree with what the people already believe.
- **Standard 3—Precision.** To be precise is to give the details needed for someone to understand exactly what is meant. Precise thinking seeks more details and greater specificity when necessary. People can apply the standard of precision to evaluate how detailed the question is that one is answering, or how detailed it needs to be. Precision is also the standard to determine if assumptions and facts contain enough detail to evaluate them using the standards of relevance, clarity, and accuracy. However, one should never sacrifice clarity for precision.
- **Standard 4—Relevance.** Something is relevant when it is connected with and bears upon the question people are reasoning through. Something is also relevant when it is pertinent or applicable to a problem people are trying to solve. Relevant thinking also encourages people to identify facts, information, questions, assumptions, implications, and points of view that they should set aside as not being pertinent to the main issue. Thinking that is relevant stays on track. People are often irrelevant in their thinking because they lack discipline in their thinking. They wander into side issues that may be intellectually satisfying to discuss but have no bearing on the issue or question.
- **Standard 5—Depth.** People think deeply when they get beneath the surface of an issue or problem. Depth of thinking is also present when people identify its inherent complexities, and then deal with those complexities not superficially but in an intellectually responsible way. Intelligence analysis generally involves the examination of complex situations and requires deep conclusions.
- **Standard 6—Breadth.** When people consider the issue from every relevant viewpoint, they think broadly. Multiple points of view that are pertinent to the issue are given due consideration. People think broadly about an issue when they recognize other viewpoints and intellectually empathize with those contrary viewpoints so as to understand them. Breadth of thinking improves the quality of the inferences and recommendations developed during intelligence analysis.
- **Standard 7—Logic.** When people think, they bring together thoughts in some order. When the combined thoughts are mutually supporting and make sense, the thinking is logical. If information, inferences, and so forth, are contradictory, if they do not make sense together, they are illogical.
- **Standard 8—Significance.** When people reason, they want to concentrate on the most important information and consider the most important ideas or concepts to answer the question. Too often, people fail in their thinking because they do not recognize that although many ideas may be relevant to an issue, the ideas are not equally important.

- **Standard 9—Fairness.** To think fairly is to think in accordance with reason and to consider the views of others. Fairness as a standard helps one deal with one's propensity for self-deception. Personal biases and ego creep easily into people's thinking. When gauging the fairness of a decision, the critical thinker asks, "Do my selfish interests distort this thinking or is my decision fair to all concerned?" The fairness standard seeks to prevent egocentric thinking. As a person's ego enters the thought process, critical thinking becomes poisoned.

APPLYING THE ELEMENTS AND STANDARDS

B-20. When an analyst exercises self-discipline and thoughtfully analyzes thinking (using the elements of thought) and then assesses the quality of the elements using intellectual standards, the result is a solid foundation for critical thinking. It is important to remember that critical thinking is a deliberate choice. Critical thinking requires self-discipline and a commitment to improve the skills that support this approach. While critical thinking cannot necessarily solve every problem an analyst may face (because some are so complex), it can ensure that every analyst is more effective and efficient while conducting the different analytical tasks, especially those that are the most complicated or ambiguous.

ESSENTIAL INTELLECTUAL TRAITS

B-21. Intellectual traits are the traits of mind and character necessary to support reasoning. Analysts should repeatedly apply and practice the elements of thought and intellectual standards to help develop intellectual traits. The following provides brief descriptions of the essential intellectual traits and related questions that foster their development.

Fair-Mindedness

B-22. A fair-minded thinker strives to treat every relevant viewpoint in an unbiased, unprejudiced way. Fair-mindedness entails an awareness that people tend to prejudge the views of others, placing them into favorable (agrees with others) and unfavorable (disagrees with others) categories. People tend to give less weight to a contrary view than to their own. This is especially true when people have selfish reasons for opposing such views. Fair-minded thinkers try to see the strengths and vulnerabilities of any reasoning they assess. Fair-mindedness entails a conscious effort to treat all viewpoints alike in spite of one's feelings or selfish interests, or the feelings of one's friends, company, community, or social organization. Questions that foster fair-mindedness include—

- "Am I considering how my behavior might make others feel?"
- "Is my reason for doing that fair to everyone?"

Intellectual Humility

B-23. Intellectual humility is knowledge of ignorance, sensitivity to what one knows and what one does not know. It means being aware of one's biases, prejudices, self-deceptive tendencies and the limitations of one's viewpoint. Questions that foster intellectual humility include—

- "What do I really know (about myself, about the situation, about another person, about what is going on in the world)?"
- To what extent do my prejudices or biases influence my thinking?"

Intellectual Courage

B-24. Intellectual courage is the disposition to question beliefs one feels strongly about. It includes questioning the beliefs of one's culture and the groups to which one belongs, and a willingness to express one's views even when those views are unpopular. Questions that foster intellectual courage include—

- "To what extent have I analyzed and questioned the beliefs I hold?"
- "To what extent have I demonstrated a willingness to give up my beliefs when sufficient evidence is presented against them?"
- "To what extent am I willing to stand up against the majority (even though people ridicule me)?"

Intellectual Empathy

B-25. Intellectual empathy is awareness of the need to actively entertain views that differ from one's views, especially those one strongly disagrees with. It is to accurately reconstruct the viewpoints and reasoning of one's opponents and to reason from premises, assumptions, and ideas other than one's own. Questions that foster intellectual empathy include—

- "To what extent do I accurately represent viewpoints I disagree with?"
- "Can I summarize the views of my opponents to their satisfaction? Can I see insights in the views of others and prejudices in my own?"
- "Do I sympathize with the feelings of others in light of their thinking differently from me?"

Intellectual Integrity

B-26. Intellectual integrity consists of holding oneself to the same intellectual standards one expects others to honor (no double standards). Questions that foster intellectual integrity include—

- "Do I behave in accordance with what I say I believe, or do I tend to say one thing and do another?"
- "To what extent do I expect the same of myself as I expect of others?"
- "To what extent are there contradictions or inconsistencies in my views?"
- "To what extent do I strive to recognize and eliminate self-deception in my views?"

Intellectual Perseverance

B-27. Intellectual perseverance is the disposition to work one's way through intellectual complexities despite the frustration inherent in the task. Questions that foster intellectual perseverance include—

- "Am I willing to work my way through complexities in an issue or do I tend to give up when I experience difficulty?"
- "Can I think of a difficult intellectual problem with which I have demonstrated patience and determination in working through the difficulties?"

Confidence in Reason

B-28. Confidence in reason is based on the belief that one's higher interests and those of humankind are best served by giving the freest play to reason. It means using standards of reasonability as the fundamental criteria by which to judge whether to accept or reject any belief or position. Questions that foster confidence in reason include—

- "Am I willing to change my position when the evidence leads to a more reasonable position?"
- "Do I adhere to principles of sound reasoning when persuading others of my position or do I distort matters to support my position?"
- "Do I deem it more important to 'win' an argument or see the issue from the most reasonable perspective?"
- "Do I encourage others to come to their own conclusions or do I try to force my views on them?"

Intellectual Autonomy

B-29. Intellectual autonomy is thinking for oneself while adhering to standards of rationality. It means thinking through issues using one's thinking rather than uncritically accepting the viewpoints of others. Questions that foster intellectual autonomy include—

- "To what extent am I a conformist?"
- "Do I think through issues on my own or do I merely accept the views of others?"
- "Having thought through an issue from a rational perspective, am I willing to stand alone despite the irrational criticisms of others?"

AVOIDING ANALYTICAL PITFALLS

B-30. Critical thinking is a mental process that is subject to numerous influences. Intelligence analysts involved in analyzing complex situations and making conclusions are prone to the influences that shape and mold their view of the world and their ability to reason. These influences are referred to as analytical pitfalls. The elements of thought, intelligence standards, and intellectual traits assist analysts in recognizing these pitfalls in their analysis and the analysis performed by others. Logic fallacies and biases are two general categories of analytical pitfalls.

LOGIC FALLACIES

B-31. Logic fallacies are errors in the reasoning process caused by the failure to apply sound logic. Although usually committed unintentionally, these fallacies are sometimes used deliberately to persuade, convince, or deceive. An analyst must be able to recognize logic fallacies so a false line of reasoning will not distract them and lead to poor conclusions. This appendix discusses the fallacies of relevance, omission, and assumption.

Fallacies of Relevance

B-32. Fallacies of relevance appeal to evidence or examples that are irrelevant to the argument at hand:

- **Appeal to force ("argumentum ad baculum" or the "might-makes-right" fallacy):** This argument uses force, the threat of force, or some other unpleasant backlash to make the audience accept a conclusion. It commonly appears as a last resort when evidence or rational arguments fail to convince. Logically, this consideration has nothing to do with the merits of the points under consideration.
- **Genetic fallacy:** The genetic fallacy is the claim that, because an idea, product, or person must be wrong because of its origin. For example, "That car cannot possibly be any good! It was made outside of the United States!" Or, "Why should I listen to her argument? She comes from California, and we all know those people are not critical thinkers." This type of fallacy is closely related to the fallacy of argumentum ad hominem, below.
- **Argumentum ad hominem (literally "argument to the man"; also called "poisoning the well" and "personal attack"):** This fallacy seeks to discount evidence before it is presented, most often by discrediting the source. For example, an ardent spokesman against the value of strategic bombing states, "You cannot trust that man's testimony regarding the effectiveness of strategic bombing; he's employed by the Air Force." The speaker is trying to discredit contrary evidence by creating the specific impression that the testimony is biased because the testifier represents a certain organization. There are two subcategories:
  - ***Abusive:*** To argue that proposals, assertions, or arguments must be false or dangerous because of an irrational psychological transference with the originator.
  - ***Circumstantial:*** To argue that opponents should accept or refute an argument only because of circumstances in their lives is a fallacy. If one is an environmentalist, suggesting that this environmentalist should not accept hunting because to do so would be incompatible with environmentalism is a circumstantial fallacy. The opponent's special circumstances do not affect the truth or untruth of a specific contention. The speaker or writer must find additional evidence beyond that to make a strong case.
- **Argumentum ad populum ("argument to the people"):** This fallacy uses an appeal to popular assent, often by arousing the feelings and enthusiasm of the multitude rather than building an argument. It is a favorite device with the propagandist, the demagogue, and the advertiser. There are three basic approaches:
  - ***Bandwagon approach:*** "Everybody is doing it." This argumentum ad populum asserts that, since the majority of people believes an argument or chooses a particular COA, the argument must be true or the COA must be the best one. For instance, "Over a million people purchased that phone rather than a competing phone; all those people cannot be wrong. That company must make the best phones." Popular acceptance of any argument does not prove it to be valid.

- ***Patriotic approach:*** This argument asserts that a certain stance is true or correct because it is somehow patriotic, and that those who disagree are somehow unpatriotic. It overlaps with pathos and argumentum ad hominem to a certain extent. The best way to spot it is to look for emotionally charged terms like Americanism, rugged individualism, motherhood, patriotism, or godless communism, for example, "A true American would never use this approach," or, "A truly free man will exercise his American right to drink beer, since beer belongs in this great country of ours."
- ***Snob approach:*** This type of argumentum ad populum does not assert "everybody is doing it," but rather that "all the best people are doing it." For instance, "The top analysts at the Central Intelligence Agency agree that my analytic approach is correct." The implication is that anyone who fails to recognize the truth of the analyst's assertion is not an equal to the "top analysts of the Central Intelligence Agency," and thus has no right to question the analytical conclusions.

- **Appeal to tradition (argumentum ad traditio [also referred to as argumentum ad antiquitatem]):** This line of thought asserts that a premise must be true because people have always believed it or done it. Alternatively, it may conclude that the premise has always worked in the past and will thus always work in the future.

Fallacies of Omission

B-33. Fallacies of omission occur when an analyst leaves out necessary material in a conclusion or inference. Some fallacies of omission include oversimplification, composition, division, post hoc, false dilemma, hasty generalization, and special pleading:

- **Oversimplification** is a generality that fails to adequately account for all the complex conditions bearing on a problem. Oversimplification results when one or more of the complex conditions pertaining to a certain situation is omitted and includes ignoring facts, using generalities, and/or applying an inadequately qualified generalization to a specific case. For example, an ordnance specialist inspecting a captured, hand-carried, surface-to-air missile launcher concludes that the threat has no effective low-level air defense. The assessment is based on the fact that the weapons system is equipped with antiquated guidance mechanisms. The ordnance specialist's conclusion omits the following considerations:
  - That this piece of equipment may not be the threat's only low-level air defense weapon.
  - That the launcher may have been planted by the threat to give a misleading picture of the threat's true capabilities and deceive weapons experts.
  - That the threat abandoned the launcher because it was ineffective and more capable systems were available.
- **Fallacy of composition** is committed when a conclusion is drawn about a whole based on the features of parts of that whole when, in fact, no justification is provided for that conclusion. For example, during a battle with an ethnic militia, a single detainee was captured. This detainee was suffering from malnutrition and low morale. It was noted that the detainee was equipped with a semiautomatic weapon of World War II vintage. After a brief interrogation, the intelligence analyst reported the threat militia recently engaged was starving, diseased, and poorly armed. The intelligence analyst failed to consider that—
  - The detainee may have been captured because the detainee was too sick to keep up with the rest of the unit.
  - The weapon of early vintage did not necessarily make it ineffective.
  - Few captured detainees have high morale; in fact, low morale could just as easily result from being captured as it could contribute to being captured.
- **Fallacy of division** is committed when a person infers that what is true of a whole must also be true of the parts of that whole. For example, members of the threat guard's brigade had never surrendered in previous combat. After a recent engagement, a detainee stated it was a member of the guard brigade. The interrogator doubted the detainee's statement because personnel from that brigade never surrender.

- **Fallacy of post hoc ergo propter hoc** (after this, therefore because of this) is consideration of other factors that might have accounted for the same result that are omitted. Post hoc fallacies often occur when trying to establish cause and effect. For example, an aircraft equipped with a new jamming pod was not fired on while flying over threat-controlled territory. It was concluded that, since the aircraft was not intercepted or fired upon, the jamming pod was extremely effective in suppressing threat electronic systems. The conclusion may or may not account for the aircraft not being attacked. Other considerations include—
  - The threat was obtaining electronic intelligence on this new pod.
  - The threat recently relocated several surface-to-air missile units and did not want to reveal their new positions.
- **False dilemma** (also known as black-and-white thinking) is a fallacy in which a person omits consideration of more than two alternatives when in fact there are more than two alternatives. For example, an S-2 reports to the commanding officer that the threat only has the capability to either defend in place or retreat. The S-2 committed the fallacy of false dilemma by failing to anticipate or ignoring that the threat could attack if it were willing to accept high casualties, withdraw to an alternate defensive position, or conduct a delaying action.
- **Hasty generalizations** are conclusions drawn from samples that are too few or from samples that are not truly representative of the population. For example, after interrogating a detainee, the interrogation officer reports the threat's morale as extremely low and that surrender is imminent. In this case, the interrogator is making a hasty generalization because the sample population considered, one detainee, is too small.
- **Special pleading** is a fallacy in which the writer creates a universal principle, then insists that the principle does not for some reason apply to the issue at hand. For instance, "John Doe claimed to be psychic, but when his 'abilities' were tested under proper scientific conditions, they magically disappeared. John explained this saying that one had to have faith in his abilities for them to work."

Fallacies of Assumption

B-34. Fallacies of assumption implicitly or explicitly involve assumptions that may or may not be true. Some fallacies of assumption include begging the question, stating hypotheses contrary to fact, and misusing analogies:

- **Begging the question** (also known as circular reasoning) is a fallacy in which the conclusion occurs as one of the premises.
  - It is an attempt to support a statement by simply repeating the statement in different and stronger terms. For example, a particular group wants democracy. America is a democratic nation. Therefore, that group will accept American-style democracy.
  - When asked why the enemy was not pinned down by fire, the platoon leader replied, "Our suppressive fire was inadequate." The fallacy in this response is that by definition suppressive fire pins down the enemy or is intended to pin him down. Since the platoon failed to pin down the enemy, the inadequacy of this fire was self-evident.
- **Stating hypotheses contrary to fact** occurs when someone states decisively what would have happened had circumstances been different. Such fallacies involve assumptions that are either faulty or simply cannot be proven. For example, the statement, "If we had not supported Castro in his revolutionary days, Cuba would be democratic today" is contrary to fact. Besides being a gross oversimplification, the assumption made in the statement cannot be verified.
- **Misusing analogies** occurs when one generalizes indiscriminately from analogy to real world. One method for weakening an analogous argument is by citing a counter-analogy. Analogies are strong tools that can impart understanding in a complex issue. In the absence of other evidence, intelligence analysts may reason from analogy. Such reasoning assumes that the characteristics and circumstances of the object or event being looked at are similar to the object or event in the analogy.

B-35. The strength of a conclusion drawn from similar situations is proportional to the degree of similarity between the situations. The danger in reasoning from analogy is assuming that because objects, events, or situations are alike in certain aspects, they are alike in all aspects. Conclusions drawn from analogies are inappropriately used when they are accepted as evidence of proof. Situations may often be similar in certain aspects, but not in others. A counter-analogy weakens the original analogy by citing other comparisons that can be made on the same basis.

BIASES

B-36. A subjective viewpoint, bias indicates a preconceived notion about someone or something. Biases generally have a detrimental impact on intelligence analysis because they obscure the true nature of the information. Intelligence analysts must be able to recognize cultural, organizational, personal, and cognitive biases and be aware of the potential influence they can have on judgment.

Cultural Bias

B-37. Americans see the world in a certain way. The inability to see things through the eyes of someone from another country or culture is cultural bias. Biases interfere with the analyst's ability to think the way a threat commander might think or to give policymakers informed advice on the likely reaction of foreign governments to U.S. policy. Also known as mirror imaging, cultural bias attributes someone else's intentions, actions, or reactions to the same kind of logic, cultural values, and thought processes as the individual analyzing the situation. Although cultural bias is difficult to avoid, the following measures can lessen its impact:

- Locate individuals who understand the culture:
  - Include them in the intelligence analysis process.
  - Ask their opinion about likely responses to friendly actions.
  - Take care when using their opinions since they may be subject to biases regarding ethnic groups or cultures in the region and their knowledge may be dated or inaccurate.
- Locate regional experts, such as foreign and regional area officers, who have lived or traveled through the area and are somewhat conversant regarding the culture. Assess the quality of the information provided against the level of knowledge and experience the individual has for that culture or region.

Organizational Bias

B-38. Most organizations have specific policy goals or preconceived ideas. Analysis conducted within these organizations may not be as objective as the same type of analysis done outside the organization. Groupthink and best case are organizational biases that can significantly skew internal analysis.

- **Groupthink.** This bias occurs when a judgment is unconsciously altered because of exposure to selective information and common viewpoints held among individuals. Involving people outside the organization in the analysis can help identify and correct this bias.
- **Best case.** This bias occurs when an analyst presents good news or bad news in the most optimistic light. The judgment is deliberately altered to provide only the information the commander wants to hear. Analysts can avoid this bias by having the moral courage to tell the commander the whole story, good and bad.

A Useful Tool in Logic: Occam's Razor

The term “Occam's Razor” comes from a misspelling of the name William of Ockham. Ockham was a brilliant theologian, philosopher, and logician in the medieval period. One of his rules of thumb has become a standard guideline for thinking through issues logically. Occam's Razor is the principle that, if two competing theories explain a single phenomenon, and they both generally reach the same conclusion, and they are both equally persuasive and convincing, and they both explain the problem or situation satisfactorily, the logician should always pick the less complex one. The one with the fewer number of moving parts, so to speak, is most likely to be correct. The idea is always to cut out extra unnecessary bits, hence the name "razor." An example will help illustrate this.

Suppose you come home and discover that your dog has escaped from the kennel and chewed large chunks out of the couch. Two possible theories occur to you:

- Theory one is that you forgot to latch the kennel door, and the dog pressed against it and opened it, and then the dog was free to run around the inside of the house. This explanation requires two entities (you and the dog) and two actions (you forgetting to lock the kennel door and the dog pressing against the door).
- Theory two is that some unknown person skilled at picking locks managed to disable the front door, then came inside the house, set the dog free from the kennel, then snuck out again covering up any sign of his presence and then relocked the door, leaving the dog free inside to run amok in the house. This theory requires three entities (you, the dog, and the lock-picking intruder) and several actions (picking the lock, entering the house, releasing the dog, hiding the evidence, relocking the door). It also requires us to come up with a plausible motivation for the intruder-a motivation that is absent at this point.

  Either theory would be an adequate and plausible explanation. Both explain the same phenomenon (the escaped dog) and both employ the same theory of how, for example, that the latch was opened somehow, as opposed to some farfetched theory.

  Which theory is most likely correct? If you do not find evidence like strange fingerprints or human footprints or missing possessions to support theory two, William of Ockham would say that the simpler solution (theory one) is most likely to be correct in this case. The first solution only involves two parts-two entities and two actions.

On the other hand, the second theory requires at least five parts-you, the dog, a hypothetical unknown intruder, some plausible motivation, and various actions. It is needlessly complex. Occam's basic rule was: "Thou shalt not multiply extra entities unnecessarily," or to phrase it in modern terms: "Don't speculate about extra hypothetical components if you can find an explanation that is equally plausible without them." All things being equal, the simpler theory is more likely to be correct.

Personal Bias

B-39. Personal bias is the tendency to base assessments on personal beliefs. This can cause the rejection of valid arguments that conflict with these beliefs. A racially or religiously prejudiced person may reject arguments because of the source. A person with strong political views may discount every argument from another political group.

B-40. There are several types of personal bias. Three common biases exhibited by analysts are—

- **Confirmation bias.** This bias causes analysts to undervalue or ignore evidence contradicting an early judgment and value evidence that tends to confirm already held assessments.
- **Assimilation bias.** This bias involves the modification and elaboration of new information to fit prior conceptions or hypotheses. The bias is toward confirming a preconceived answer.
- **Anchoring bias.** This bias involves the use, often unwitting, of arbitrary values in decision making, including the use of conclusions developed by others.

Cognitive Bias

B-41. The intelligence analyst evaluates information from a variety of sources. The degree of reliability, completeness, and consistency varies from source to source and even from report to report. This variance often creates doubt about the reliability of some sources. Cognitive biases that affect the analyst are—

- **Vividness.** Clear and concise or vivid information has a greater impact on analytical thinking than abstract and vague information. A clear piece of information is held in higher regard than a vague piece of information that may be more accurate. Analysts must consider that an enemy may use deception to portray vivid facts, situations, and capabilities that they want the friendly intelligence effort to believe.
- **Absence of evidence.** Lack of information is the analyst's most common problem, especially in the tactical environment. Analysts must do their best with limited information and avoid holding back intelligence because it is inconclusive. To avoid this bias, the analyst should—
  - Realize that information will be missing.
  - Identify areas where information is lacking and consider alternative conclusions.
  - Adapt or adjust judgments as more information becomes available.
  - Consider whether a lack of information is normal in those areas or whether the absence of information itself is an indicator.
- **Oversensitivity to consistency.** Consistent evidence is a major factor for confidence in the analyst's judgment. Information may be consistent because it is appropriate, or it may be consistent because it is redundant, is from a small or biased sample, or is the result of the enemy's deception efforts. When making judgments based on consistent evidence, the analyst must—
  - Be receptive to information that comes in from other sources regardless of whether it supports the hypothesis or not.
  - Be alert for circular reporting, which is intelligence already obtained by the unit that is then reformatted by other units and intelligence organizations, modified slightly, and disseminated back to the unit. This is a common problem; particularly in digital units, where large volumes of information are being processed. It helps to know, to the degree possible, the original source for all intelligence to ensure that a circular report is not used as evidence to confirm an intelligence estimate or conclusion.
- **Persistence on impressions.** When evidence is received, there is a tendency to think of connections that explain the evidence. Impressions are based on these connections. Although the evidence eventually may be discredited, the connection remains and so do the impressions.
- **Dependency on memory.** The ability to recall past events influences judgment concerning future events. Since memory is more readily available, it is easy to rely on memory instead of seeking new information to support analysis.
- **Acceptance of new intelligence.** Often new intelligence is viewed subjectively; either valued as having more value or less value than current intelligence.

Appendix C

Analytic Standards and Analysis Validation

INTELLIGENCE COMMUNITY ANALYTIC STANDARDS

C-1. During intelligence analysis, the conclusions reached should also adhere to analytic standards, such as those established by the Director of National Intelligence in ICD 203. This directive establishes the analytic standards that govern the production and evaluation of national intelligence analysis to meet the highest standards of integrity and rigorous analytic thinking. The ICD 203 Intelligence Community Analytic Standards act as guidelines and goals for analysts and leaders throughout the intelligence community who strive for excellence in their analytical practices and products. The following identify and describe the five ICD 203 Intelligence Community Analytic Standards, including the nine analytic tradecraft standards:

- **Objective:** Analysts must perform their functions with objectivity and awareness of their own assumptions and reasoning. They must employ reasoning techniques and practical mechanisms that reveal and mitigate bias. Analysts should be alert to the influences of existing analytical positions or judgments and must consider alternative perspectives and contrary information. Analysis should not be unduly constrained by previous judgments when new developments indicate a modification is necessary.
- **Independent of political consideration:** Analytical assessments must not be distorted by, nor shaped for, advocacy of a particular audience, agenda, or policy viewpoint. Analytical judgments must not be influenced by the force of preference for a particular policy.
- **Timely:** Analysis must be disseminated in time for it to be actionable. Analytical elements must be continually aware of events of intelligence interest and of intelligence requirements and priorities in order to provide useful analysis at the right time.
- **Based on all available sources of intelligence information:** Analysis should be informed by all relevant information available. Analytical elements should identify and address critical information gaps and work with collection managers and data providers to develop access and collection strategies.
- **Implement and exhibit the analytic tradecraft standards:** See paragraphs C-3 through C-14.

ANALYSIS VALIDATION

C-2. Intelligence analysis and the resultant judgments are incomplete without the estimative language that provides both the probability that an event will occur and the confidence level of the analyst making this assessment. Analysts employ the analytic tradecraft standards to assess probabilities and confidence levels and the actions associated with analytical rigor to draw accurate conclusions.

ANALYTIC TRADECRAFT STANDARDS

C-3. Intelligence analysts exhibit and implement the nine analytic tradecraft standards, one of the five ICD 203 Intelligence Community Analytic Standards. Specifically, they—

- Properly describe the quality and credibility of all underlying sources, information, and methodologies.
- Properly express and explain uncertainties associated with major analytical judgments.
- Properly distinguish between underlying intelligence information and analysts' assumptions and judgments.
- Incorporate analysis of alternatives.
- Demonstrate customer relevance and address implications.

- Use clear and logical argumentation.
- Explain change to or consistency of analytical judgments.
- Make accurate judgments and assessments.
- Incorporate effective visual information where appropriate.

Properly Describe the Quality and Credibility of All Underlying Sources, Information, and Methodologies

C-4. Analytical products should include all underlying sources, information, and methodologies from which analytical judgments are based. Factors affecting source quality and credibility should be described using source descriptors in accordance with ICD 206, *Sourcing Requirements for Disseminated Analytic Products*. Such factors can include accuracy and completeness, possible denial and deception, age and continued currency of information, and technical elements of collection, as well as source access, validation, motivation, possible bias, or expertise. Source summary statements, described in ICD 206, should be used to provide a holistic assessment of the strengths or vulnerabilities in the source base and explain which sources are most important to key analytical judgments.

Properly Express and Explain Uncertainties Associated with Major Analytical Judgments

C-5. Analysts must properly express and explain uncertainties associated with any major analytical judgment. When briefing their analytical results, analysts, at a basic level, must be able to assess the likelihood of an event happening, expressed by using estimative language. Then, they must express their confidence level—high, moderate, or low—in that assessment. (See figure C-1.) For intelligence analysts to reach a high level of confidence in the accuracy of their analytical assessment, they must apply the actions of high analytical rigor found in table C-1 on page C-5.

Expressions of Likelihood	Almost no chance	Very unlikely	Unlikely	Roughly even chance	Likely	Very likely	Almost certain
	Remote	Highly improbable	Improbable	Roughly even odds	Probable	Highly probable	Nearly certain
Probability	01-05%	05-20%	20-45%	45-55%	55-80%	80-95%	95-99%
Confidence Levels	Low				Moderate		High

Figure C-1. Estimative language: expressions of likelihood

Note. For expressions of likelihood, analysts are strongly encouraged not to mix terms from the different rows. Additionally, commanders are all different and their individual acceptance of the various probability and confidence levels may be different than those of previous commanders.

Assessing the Likelihood of an Event Happening

C-6. Phrases (such as *we judge*, *we assess*, and *we estimate*) commonly used to convey analytical assessments and judgments, are not facts, proofs, or knowledge. Intelligence analysts use estimative language, shown in figure C-1, to convey their assessment of the probability or likelihood of an event and the level of confidence ascribed to the judgment.

Expressing Confidence in Assessments

C-7. Confidence levels express the strength of the assessment given the reasoning, methodologies, gaps, and assumptions; the number, quality, and diversity of sources; and the potential for deception. (See figure C-1.) To avoid confusion, assessment language and confidence levels are no longer combined in the same sentence. Confidence levels are ascribed using high, moderate, and low levels of confidence in analytical assessments:

- **High confidence level.** High confidence generally indicates that sound reasoning and/or methodologies have been applied; no linchpin assumptions have been made; no critical gaps relevant to the issue are evident; consistent evidence from a variety of independent sources supports the judgment; the potential for deception is low; the body of reporting is not consistent with a plausible alternative; and/or the nature of the issue allows one to render a solid judgment. A *high confidence judgment*, however, is not a fact or a certainty, and such judgments still carry a risk of being inaccurate.
- **Moderate confidence level.** Moderate confidence generally indicates that potentially critical assumptions are used to fill gaps; some inconsistencies exist, but the preponderance of evidence supports the judgment; the information is credibly sourced and plausible but is not of sufficient quality or is not sufficiently corroborated to warrant high confidence; moderate potential for deception exists; and/or the body of reporting leaves open the possibility of a plausible alternative explanation of events.
- **Low confidence level.** Low confidence generally indicates that key assumptions have been used to fill critical gaps; significant inconsistencies or questions exist regarding the evidence; the information is fragmented or uncorroborated or is of questionable credibility and/or plausibility; high potential for deception exists; and/or the body of reporting supports an alternative explanation of events.

Properly Distinguish Between Underlying Intelligence Information and Analysts' Assumptions and Judgments

C-8. Analytical products should clearly distinguish statements that convey underlying intelligence information used in analysis from statements that convey assumptions or judgments. *Assumptions* are suppositions used to frame or support an argument; assumptions affect analytical interpretation of underlying intelligence information. *Judgments* are conclusions based on underlying intelligence information, analysis, and assumptions. Products should state assumptions explicitly when they serve as the linchpin of an argument or when they bridge key information gaps. Products should explain the implications for judgments if assumptions prove to be incorrect. As appropriate, products should also identify indicators that, if detected, would alter judgments.

Incorporate Analysis of Alternatives

C-9. *Analysis of alternatives* is the systematic evaluation of differing hypotheses to explain events or phenomena, explore near-term outcomes, and imagine possible futures to mitigate surprise and risk. Analytical products should identify and assess plausible alternative hypotheses. This is particularly important when major judgments must contend with significant uncertainties, or complexity, such as forecasting future trends, or when low probability events could produce high-impact results. In discussing alternatives, products should address factors such as associated assumptions, likelihood, or implications related to Army forces. Products should also identify indicators that, if detected, would affect the likelihood of identified alternatives.

Demonstrate Relevance and Address Implications

C-10. Analytical products should provide information and insight on issues relevant to the commanders and address the implications of the information and analysis they provide. Products should add value by addressing prospects, context, threats, or factors affecting opportunities for action.

Use Clear and Logical Argumentation

C-11. Analytical products should present a clear main analytical conclusion up front. Products containing multiple judgments should have a main analytical conclusion that is drawn collectively from those judgments. All analytical judgments should be effectively supported by relevant intelligence information and coherent reasoning. Products should be internally consistent and acknowledge significant supporting and contrary information affecting judgments.

Explain Change To or Consistency Of Analytical Judgments

C-12. Analysts should state how their major judgments on a topic are consistent with or represent a change from those in previously published analysis or represent initial coverage of a topic. Products need not be lengthy or detailed in explaining change or consistency. They should avoid using reused or unoriginal language and should make clear how new information or different reasoning led to the judgments expressed in them. Recurrent products should note any changes in judgments; absent changes, recurrent products need not confirm consistency with previous editions. Significant differences in analytical judgment, such as between two intelligence community analytical elements, should be fully considered and brought to the attention of customers.

Make Accurate Judgments and Assessments

C-13. Analytical products should apply expertise and logic to make the most accurate judgments and assessments possible, based on the information available and known information gaps. In doing so, analytical products should present all judgments that would be useful to commanders and should include difficult judgments in order to minimize the risk of being wrong. Inherent to the concept of accuracy is that the analytical conclusion that the analyst presents to the commander should be the one the analyst intended to send. Therefore, analytical products should express judgments as clearly and precisely as possible, reducing ambiguity by addressing the likelihood, timing, and nature of the outcome or development.

Incorporate Effective Visual Presentations When Feasible

C-14. Analysts should present intelligence in a visual format to clarify an analytical conclusion and to complement or enhance the presentation of intelligence and analysis. In particular, visual presentations should be used when information or concepts, such as spatial or temporal relationships, can be conveyed better in graphic form, such as tables, flow charts, and images coupled with written text. Visual presentations may range from a plain display of intelligence information to interactive displays for complex issues and analytical concepts. Visual presentations should always be clear and pertinent to the product's subject. Analytical content in a visual format should also adhere to other analytic tradecraft standards.

ANALYTICAL RIGOR

C-15. *Analytical rigor* is the application of precise and exacting standards to better understand and draw conclusions based on careful consideration or investigation. There are eight primary action-metrics that lead to analytical rigor. When analysts combine these action-metrics with the intelligence analysis process, they can determine the analytical sufficiency of their conclusions. (See table C-1.)

Table C-1. Analytical actions and levels of rigor

Analytical rigor actions	*Levels of analytical rigor*		
	Low rigor	*Moderate rigor*	*High rigor*
Consider alternative hypotheses: Hypothesis exploration describes the extent to which multiple hypotheses were considered in explaining data.	• Little to no consideration of alternatives to primary or initial hypotheses. • Interpretation of ambiguous or conflicting data such that they are compatible with existing beliefs. • Fixation or knowledge shielding behaviors.	• Some consideration of how data could support alternative hypotheses. • An unbalanced focus on a probable hypothesis or a lack of commitment to any particular hypothesis.	• Significant generation and consideration of alternative explanations via the direct evaluation of specific hypotheses. • Incorporation of "outside" perspectives in generating hypotheses. • Evolution and broadening of hypothesis set beyond an initial framing. • Ongoing revision of hypotheses as new data are collected.
Evaluate depth of research: Information search relates to the depth and breadth of the search process used in collecting data.	• Failure to go beyond routine and readily available data sources. • Reliance on a single source type or on data that are far removed from original sources. • Dependence upon “pushed” information, rather than on actively collected information. • Use of stale or dated source data.	• Collection from multiple data types or reliance on proximal sources to support key findings. • Some active information seeking.	• Collection of data from multiple source types in addition to the use of proximal sources for all critical inferences. • Exhaustive and detailed exploration of data in the relevant sample space. • Active approach to information to information collection
Validate information accuracy: Information validation details the levels at which information sources are corroborated and cross-validated.	• General acceptance of information at face value, with little or no clear embellishment of underlying veracity. • Lack of convergent evidence. • Poor tracking and citation of original sources of collected data.	• Use of heuristics to support judgments of source integrity. For example, relying on sources that have previously proven to be consistently accurate. • A few “key” high-quality documents are relied on heavily. • Recognizes and highlights inconsistencies between sources.	• Systematic and explicit processes employed to verify information and to distinguish facts from judgments. • Seeks out multiple, independent sources of converging evidence. • Concerned both with consistency between sources and with validity and credibility within a given source.
Examine source bias: Stance analysis is the evaluation of data with the goal of identifying the stance or perspective of the source and placing it into a broader context of understanding.	• Little consideration of the views and motivations of source data authors. • Recognition of only clearly biased sources or sources that reflect a well-defined position on an issue.	• Perspectives and motivations of authors are considered and assessed to some extent. • Incorporates basic strategies to compare perspectives of different sources. For instance, by dividing issues into “for” or “against” positions.	• Involves significant research into, or leverages a preexisting knowledge of, the backgrounds and views of key players and thought leaders. • May involve more formal assessments of data sources, such as faction analysis, social network analysis, or deception analysis.

Table C-1. Analytical actions and levels of rigor (*continued*)

Analytical rigor actions	*Levels of analytical rigor*		
	Low rigor	*Moderate rigor*	*High rigor*
Scrutinize strength of analysis: Sensitivity analysis considers the extent to which the analyst considers and understands the assumptions and limitations of their analysis.	• Explanations are appropriate and valid at a surface level. • Little consideration of critical "what if?" questions, such as, "What if a given data source turns out to be unreliable?" or "What if a key prediction does not transpire as anticipated?"	• Considers whether being wrong about some inferences would influence the overall best explanation for the data. • Identifies the boundaries of applicability for an analyzed information.	• Goes beyond simple identification to specify the strength of explanations and assessments in the event that individual supporting evidence or hypotheses were to prove invalid or unreliable. • Specifies limitations of the analysis, noting the most vulnerable explanations or predictions on which the analysis is at risk of erring.
Amalgamate information: Information synthesis refers to how far beyond simply collecting and listing data an analyst went in their process.	• Little insight with regard to how the analysis relates to the broader analytical context or to more long-term concerns. • Lack of selectivity, with the inclusion of data figures that are disconnected from the key arguments or central issues. • Extensive use of lists or the restatement of material copied directly from other sources with little interpretation.	• Explicit, though perhaps not systematic, efforts to develop the analysis within a broader framework of understanding. • Depiction of events in context and framing of key issues in terms of tradeoff dimensions and interactions. • Provides insight beyond what is available in the collected data.	• Extracted and integrated information in terms of relationships rather than components and with a thorough consideration of diverse interpretations of relevant data. • Reconceptualization of the original task, employing cross-checks on abstractions. • Performed by individuals who are "reflexive" in that they are attentive to the ways in which their cognitive processes may have hindered effective synthesis.
Incorporate expert input: Specialist collaboration describes the degree to which an analyst incorporates the perspectives of domain experts into their assessments.	• Minimal direct collaboration with experts. • Little if an on-topic, "outside" expertise is accessed or sought out directly.	• Involves some direct interaction with experts, though usually via readily available specialists. • Expertise is drawn from within preexisting personal or organizational networks.	• Independent experts in key content areas are identified and consulted. • Efforts to go beyond a "core network" of contacts to seek out domain-relevant experts, with additional resources and "political capital" potentially expended to gain access to such specialist expertise.
Assess breadth of collaboration: Explanation critique is a different form of collaboration that captures how many different perspectives were incorporated in examining the primary hypotheses.	• Few if any instances of alternative or "outside" criticisms being considered. • Reliance on preexisting channels of critiquing, primarily supervisory.	• Brings alternative perspectives to bear in critiquing the overall intelligence analysis process. • Leverages personal or organizational contacts to examine analytical reasoning. For example, peer analysts or proxy decision makers.	• Familiar as well as independent perspectives have examined the chain of analytical reasoning, explicitly identifying which inferences are stronger and weaker. • Use of formal techniques, such as devil's advocacy or team A/team B (see chapter 6, to challenge and vet hypotheses and explanations. • Expenditure of capital, political or otherwise, in critiquing the intelligence analysis process.

Appendix D

Threat Considerations During Large-Scale Ground Combat Operations

OVERVIEW

D-1. A *threat* is any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland (ADP 3-0). While the Army must be manned, equipped, and trained to operate across the range of military operations, large-scale ground combat against a peer threat represents the most significant readiness requirement.

D-2. Intelligence analysts must be proficient in understanding the threat to ensure they provide quality products and recommendations to commanders and staffs. They should continuously strive to be experts on threat doctrine, capabilities, and equipment. Threat doctrine provides the guidelines a threat often follows or tries to follow during military operations; threat tactics are derived from threat doctrine. Many peer threats require their forces to follow threat doctrine and do not allow these forces to exercise the initiative. Identifying *how* and *when* a threat follows threat doctrine is key to developing COAs. Intelligence analysts must seek the most current (by nation) threat doctrine, capabilities, and equipment from the various U.S. intelligence agencies: Defense Intelligence Agency, NGIC, INSCOM, and several of the DOD organizations responsible for maintaining national threat databases and assessments.

D-3. After mission receipt, analysts should have a basic knowledge of the fundamental maneuver tactics and the combat equipment related to the warfighting functions, which are used to generate threat combat power and access joint and multinational capabilities. Setting the conditions begins with generate intelligence knowledge. Databases and threat signatures developed during generate intelligence knowledge assist in assessing threat capabilities and vulnerabilities during IPB. This information facilitates decision making during the MDMP and provides a common understanding of how friendly forces may gain a position of relative advantage across multiple domains.

D-4. During mission analysis and IPB, analysts reference current intelligence holdings to develop the initial intelligence estimate of the threat situation for the warning order produced during the MDMP. An understanding of the current threat situation enables analysts to recognize potential threat vulnerabilities, which will be developed further during IPB.

D-5. During large-scale ground combat operations, analysts apply their knowledge of threat doctrine, capabilities, and equipment to the OE in order to assess the threat. While maintaining an accurate intelligence threat assessment during combat operations, analysts must be able to—

- **Confirm or deny analytical predictions.** Analysts identify whether or not the threat's actions are consistent with the analytical assessment (for example, validation of the most likely and most dangerous threat COAs).
- **Update the situation template, event template and matrix, and running estimate.** Analysts should recognize the threat's balance of risk and opportunity to create and maintain the conditions necessary to seize, retain, and exploit the threat initiative and achieve decisive results.
- **Assist the commander and staff to update planning.** Analysts continually update the situation template and running estimate to reflect current operations in order to identify windows of opportunity to seize, retain, and exploit the initiative to shape the OE.

THREAT ANALYSIS BY WARFIGHTING FUNCTION

D-6. Analysts must have a detailed knowledge of threat doctrine and capabilities to portray how the threat will conduct operations in a given environment. During the war-gaming step of the MDMP, analysts apply their knowledge of threat doctrine and capabilities. This knowledge enables the staff to determine the threat's likely reaction to friendly COAs and assists the staff in refining the plan recommended to the commander.

D-7. The analysis and predicted implementation of threat doctrine and capabilities must be as accurate and detailed as possible because its inclusion in IPB drives planning. During IPB, this analysis assists the S-2 and S-3 in identifying additional planning considerations and potential operational windows of opportunity for the commander to exploit. Categorizing potential threat capabilities and requirements by warfighting function is a basic way of analyzing the threat. A peer threat force commander is likely to have similar requirements as the Army force commander's requirements. Therefore, categorizing threat elements by warfighting function enables analysts to efficiently convey and commanders and staffs to easily understand threat requirements. Determining the threat's likely requirements assists in determining the threat force commander's likely decision points.

D-8. Intelligence analysts apply techniques and tools to assist them in identifying likely threat requirements, categorized by warfighting function. (See table D-1.) After identifying threat requirements, the S-2 and S-3 collaborate to determine how best to influence the threat's decision-making process.

Table D-1. Threat analysis by warfighting function example

Threat element	*Threat requirements*	*Considerations*	*Support to future friendly operations*
Command and control	Commander's critical information requirements	What must threat commander know to meet the end state?	Provide EEFIs for protection and security.
	CP positioning	How is the threat arrayed on the battlefield?	• Contribute information to the threat overlay. • Provide potential NAIs.
		Does the terrain favor the location of the CPs?	• Identify key terrain. • Identify natural defensive terrain.
		Where are the LOCs that connect CPs across the AO?	Identify AAs
	Commander's location	Which CP has the best defensive posture?	Identify natural defensive terrain.
		What security measures are emplaced at the location?	Identify obstacles for maneuver elements.
		What weapons systems are colocated with the commander?	Develop targets.
	Succession of command	Which personalities would be able to continue operations?	Develop targets.
	Communications guidance	How does the threat communicate throughout the AO?	• Refine the collection plan. • Assess the threat's operations security. • Identify possible bypass routes.
Intelligence	Most likely COA/Most dangerous COA	How much influence can friendly forces apply on the threat?	Identify the threat threshold that would force commitment to a decisive operation.
	Key terrain	What terrain would be advantageous to the threat's mission?	• Develop NAIs. • Identify potential objectives for seizure.
	Weather	What effect will certain weather have on threat operations?	Refine threat COAs.
	Information gaps	What does the threat not know about friendly forces?	• Refine collection plans. • Identify potential threat priority intelligence requirements.
	Intelligence collection guidance	What capabilities is the threat employing to collect information?	• Develop counterreconnaissance plans. • Develop operational security guidelines.

Table D-1. Threat analysis by warfighting function example (*continued*)

Threat element	*Threat requirements*	*Considerations*	*Support to future friendly operations*
Movement and maneuver	Commander's intent	What is the end state the commander is attempting to achieve?	Develop COA criteria.
	Task and purpose of subordinate units	Do projected threat COAs support the threat commander's intent?	COA development
	Task organization	What is the threat command structure?	Develop targets.
	Forms of maneuver	How does the threat conduct specific operations?	Develop threat TTP.
	Reserve composition, mission, priorities, and control measures	How many personnel does the threat have in reserve?	Identify the overall threat strength.
		What is the threat commander's threshold for committing reserve forces onto the battlefield?	Develop COA criteria.
		How will reserve forces operate?	COA development
Fires	• Task and purpose of lethal and nonlethal fires • Schemes of fire	Do projected lethal and nonlethal fires in COAs support the threat commander's intent?	COA development
		What lethal and nonlethal fires capabilities can the threat use?	Develop threat TTP.
		What is the location of fires systems?	Develop NAIs.
		Where would the threat emplace observers?	Develop NAIs.
	Special munitions	Does the threat possess any special munitions?	Adjust planning considerations.
		How much special munitions does the threat possess?	Anticipate potential resupply points.
Protection	Protection priorities	What structures or locations require additional protection?	Refine the collection plan.
		What is the significance of the structures or locations to the threat commander?	Develop high-value targets.
	Terrain factors	Does any terrain provide protection for the threat?	Identify obstacles for maneuver elements.
		What LOCs will the threat prioritize for protection?	• Identify possible AAs. • Develop ways to restrict threat freedom of maneuver.
Sustainment	Sustainment priorities—manning, fueling, fixing, arming, moving the force, and sustaining Soldiers and systems	How will the threat conduct resupply operations?	Develop threat TTP.
		How will the threat refuel vehicles?	• Identify potential LOAs. • Identify AAs. • Identify LOCs for collection.
	Construction of facilities and installations	What types of systems will be needed to degrade threat facilities?	• Identify threat vulnerabilities. • Provide accurate recommendations to friendly capabilities.
	Anticipated requirements of classes III (fuel), IV (fortification), V (ammunition)	How often will the threat require a resupply?	Identify potential threat battle rhythm.

AA avenue of approach
AO area of operations
COA course of action
CP command post
EEFI essential element of friendly information
LOA limit of advance
LOC line of communications
NAI named area of interest
TTP tactics, techniques, and procedures

THREAT EQUIPMENT

D-9. The strengths, vulnerabilities, and functionality of a threat's equipment influence that threat's tactics. Analysts should conduct basic threat equipment analysis combined with threat doctrine for accurate threat capability assessments. Analysis results assist in understanding the threat's ability to employ its capabilities. Understanding the strengths and vulnerabilities of threat equipment by warfighting function assists analysts in identifying key factors about the threat, such as how the threat's equipment status may affect its ability to fight based on threat doctrine, or whether an enemy can go on the offensive, and if so, how far can the enemy advance based on its logistic support. From those factors, analysts can further identify limits of advance and determine the threat's likely objectives. Table D-2, while not all inclusive, provides one way to assist analysts in identifying key factors to consider during large-scale ground combat.

Note. Understanding equipment strengths and vulnerabilities may encompass more than one warfighting function because the equipment may have multiple capabilities. For example, an armored reconnaissance vehicle can fall under the movement and maneuver, intelligence, and protection warfighting functions, as indicated in table D-2, based on its capabilities. In this instance, it is important for analysts to analyze the specific role of the vehicle or unit in order to explain its strengths and vulnerabilities.

Table D-2. Analyst considerations based on threat equipment capabilities

Equipment	*Threat element*	*Description*	*Considerations*	*Strengths and vulnerabilities*
BRM-3K/Kredo 1 (modified BRM for reconnaissance)	**Movement and maneuver**	**Range:** Frag-HE 4000 m (day) 1200–1500 m (night passive sight) 3000 m+ (night-active sight); 4000 m (antiaircraft)	Threat has not been observed conducting night training in 18 months.	• Vehicle can outrange 25-mm bushmaster during daylight hours. • It is unlikely the threat will be proficient on night scopes, providing the advantage to friendly forces.
		Speed: Max road: 70 km/hour Max off-road: 45 km/hour Average cross-country: 35 km/hour Max swim: 10 km/hour **Range:** 600 km (highway)	Open terrain exists throughout the area of operations.	Vehicle will have minimally restricted movement throughout the area of operations.
	Intelligence	• 2-3-m mast with a Kredo-1 radar system • Catherine 2d generation thermal sight extends night range to 5-7 km • 1D22 laser target designator ranges to 7 km	Division capable of detecting radar within 10 seconds of activation.	Threat uses radar to spot targets and call for fire, then quickly transitions to a new location to prevent being targeted.
			Laser designators will enable the threat to send locations rapidly for indirect fires.	When within 7 km of the corps disruption zone and templated reconnaissance positions, units are at an increased risk for indirect fire attack.
	Protection	Six smoke grenade launchers, vehicle engine exhaust systems	Division has reported critical shortages of smoke canisters for the past year.	It is unlikely that smoke will be used for obscuring positions and movement.
		CBRN-automatic overpressure system	Not applicable	Not applicable
		30-355 mm-turret armor (front glacis)	Not applicable	Direct fires from 25 mm or higher are required to penetrate the turret. Tracks are susceptible to .50 caliber direct fire and above for mobility kill.

CBRN chemical, biological, radiological, and nuclear
km kilometer
m meter
mm millimeter

D-10. In-depth analysis of threat equipment assists in nominating equipment critical to the success of the threat's mission. This information assists analysts in nominating HVTs and HPTs for targeting and the S-2 and S-3 in recommending PIRs to the commander. Additionally, it provides friendly forces the ability to exploit threat vulnerabilities by creating defeat mechanisms.

Appendix E
Intelligence Production

OVERVIEW

E-1. The fundamental requirement of intelligence analysis is providing timely, accurate, reliable, and predictive intelligence assessments about the threat and OE to the commander and staff. Therefore, intelligence production requires the dissemination of reports and presentations to support operations. These reports involve various updates to IPB and collection management templates and matrices.

Notes. The development of production and dissemination software in current automation systems enhances intelligence production. DCGS-A and other operational systems must be identified and a location or internet protocol address provided to find maps, overlays, templates, charts, and other analytic techniques and tools.

This appendix contains specific collection requirements and instructions. Unit-level SOP information should not be repeated in the intelligence annex.

INTELLIGENCE PRODUCTS

E-2. The intelligence products described in this appendix are organized based on the following:

- Threat and OE analysis reports.
- Current intelligence reports.
- Supplemental analytical reports.
- Analytical assessments that support orders and briefings.

THREAT AND OPERATIONAL ENVIRONMENT ANALYSIS REPORTS

E-3. The intelligence estimate, intelligence running estimate, and Annex B (Intelligence) to the operation order (OPORD) each maintain an analytical assessment of threat forces' strengths, vulnerabilities, tactics, composition, disposition, training, equipment, and personnel, as well as other OE considerations before, during, and after operations (revision of the original estimate).

Annex B (Intelligence) to the Operation Order

E-4. Commanders and staffs use Annex B (Intelligence) to describe how intelligence supports the concept of operations described in the base plan or order. (See figure E-1 on page E-2.) The purpose of Annex B (Intelligence) is to provide detailed information and intelligence on the characteristics of the OE and to direct intelligence activities. (For more information, see FM 6-0.)

[CLASSIFICATION]

ANNEX B (INTELLIGENCE) to OPERATION ORDER 001

(U) References:
(a) (U) Maps. See base order.
(b) (U) ADP 2-0, FM 2-0, FM 6-0.

(U) Time Zone Used Throughout the Order: *Identify the appropriate time zone.*

1. (U) Situation.
a. (U) Area of Interest. *Describe the area of interest.*
b. (U) Area of Operations (AO). *Describe the AO.*
(1) (U) Terrain. See Tab A (Terrain) to Appendix 1 (Intelligence Estimate) to this annex.
(2) (U) Weather. See Tab B (Weather) to Appendix 1 (Intelligence Estimate) to this annex.
c. (U) Enemy Forces. See Appendix 1 (Intelligence Estimate) to this annex.
d. (U) Friendly Forces. See Annex A (Task Organization).
e. (U) Interagency, Intergovernmental, and Nongovernmental Organizations. See Annex V (Interagency Coordination).
f. (U) Civil Considerations. See Tab C (Civil Considerations) to Appendix 1 (Intelligence Estimate) to this annex and Annex K (Civil Affairs Operation).
g. (U) Attachments and Detachments. See Annex A (Task Organization).
2. (U) Mission. *Restate the unit's mission*.
3. (U) Execution.
a. (U) Scheme of Intelligence Support. *Describe the intelligence unit's roles and responsibilities in relation to the operation and define priorities of support to subordinate units.*
b. (U) Tasks to Subordinate Units.
(1) (U) *Perform intelligence preparation of the battlefield and situation development, as well as provide analytic support to targeting, information-related activities, protection, and civil affairs operations.*
(2) (U) *Conduct information collection. See Annex L (Information Collection) for specific requirements.*
(3) (U) *Support stability operations, such as Noncombatant Evacuation Operations and foreign humanitarian assistance.*
c. (U) Counterintelligence. See Appendix 2 (Counterintelligence) to this annex.
d. (U) Coordinating Instructions.
(1) (U) Requirements.
(a) (U) Priority Intelligence Requirements (PIRs).
1. (U) PIR #1. *Identify all PIRs in relation to the operation.*
2. (U) PIR #2.
3. (U) PIR #3.
(b) (U) Friendly Force Information Requirements. See base order.
(c) (U) Request for Information (RFI). *Describe the process for handling RFIs.*
(2) (U) Measures for Handling Personnel, Documents, and Materiel.
(a) (U) Prisoners of War, Deserters, Repatriates, Inhabitants, and Other Persons.
(b) (U) Captured Documents and Materiel.
(c) (U) Documents or Equipment Required.

[page number]
[CLASSIFICATION]

Figure E-1. Annex B (Intelligence) to the operation order example

[CLASSIFICATION]

ANNEX B (INTELLIGENCE) to OPERATION ORDER 001

(3) (U) Distribution of Intelligence Products.

(a) (U) *Describe requirements and the process for dissemination of products to and from subordinate units.*

(b) (U) *Subordinate units will submit a daily graphic intelligence summary (GRINTSUM) covering 24 hours (0001L - 2400L) NLT 0600L. The GRINTSUM must include a summary of all significant activities within subordinate units' AOs, a current near-term assessment of the AO, and a rollup of all reporting across every intelligence discipline (signals intelligence, human intelligence, and any interrogation summaries) originating in the AO.*

3. (U) Sustainment. See Annex F (Sustainment).

4. (U) Command and Signal.

a. (U) Command.

(1) (U) Location of Key Intelligence Leaders. *The division G-2 will be colocated with the division commander during all phases of the operation.*

(2) (U) Intelligence Liaison Requirements. *The division G-2 does not require intelligence liaison personnel from subordinate units. Subordinate units' organic liaison officer can execute intelligence liaison duties.*

b. (U) Control.

(1) (U) Command Posts (CPs). *The division main CP is located in the vicinity of military grid reference system (MGRS) 12A BC 1234 5678. The division main CP in the vicinity of MGRS 12A BC 2345 6789.*

(2) (U) Intelligence Coordination Line. See Annex L (Information Collection).

c. (U) Signal. See Annex H (Signal).

ACKNOWLEDGE:

COMMANDER
BG

OFFICIAL:

DEBORD
G-2

ATTACHMENTS:
Appendix 1–Intelligence Estimate
Appendix 2–Counterintelligence
Appendix 3–Signals Intelligence
Appendix 4–Human Intelligence
Appendix 5–Geospatial Intelligence
Appendix 6–Measurement and Signature Intelligence
Appendix 7–Open-Source Intelligence

[page number]
[CLASSIFICATION]

Figure E-1. Annex B (Intelligence) to the operation order example (*continued*)

Intelligence Estimate

E-5. An *intelligence estimate* is the appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view of determining the courses of action open to the enemy or adversary and the order of probability of their adoption (JP 2-0). Since intelligence analysts will have performed IPB to support the commander's MDMP effort and likely participated in a thorough staff war-gaming effort to validate friendly and threat COAs, the intelligence estimate is a version of the staff planning effort and part of the larger OPORD. (See figure E-2 on page E-4.)

E-6. The intelligence staff develops and maintains the intelligence estimate to disseminate information and intelligence that define the threat COA along with the requirements to determine the adoption of a COA. The assessments in the intelligence estimate of COA development, including threat strengths, compositions, dispositions, and vulnerabilities, form the basis for future intelligence analytical requirements.

[CLASSIFICATION]

APPENDIX 1 (INTELLIGENCE ESTIMATE) to ANNEX B (INTELLIGENCE) OPERATION ORDER 001

(U) References:
(a) (U) Maps. See base order.
(b) (U) ADP 2-0, FM 2-0, FM 6-0, ATP 2-01.3, World Equipment Guide (2016).

(U) Time Zone Used Throughout the Order: *Identify the appropriate time zone.*

1. (U) Situation.
a. (U) Area of Interest. See Exhibit 1 to Tab A.
b. (U) Area of Operations. See Exhibit 2 to Tab A.
(1) (U) Terrain. See Tab A (Terrain) to this appendix.
(2) (U) Weather. See to Tab B (Weather) to this appendix.
c. (U) Enemy Forces.
(1) (U) Composition. *The Operational Strategic Command-South (OSC-S) comprises four division tactical groups and one Reserve Component unit*.
(2) (U) Disposition. *The OSC-S underwent intense collective maneuver training before advancing south*.
(3) (U) Capability.
(a) (U) *OSC-S regular formations maintain an overall 80% operational readiness rate*.
(4) (U) Enemy Courses of Action (ECOAs). See Exhibit 3 (ECOA Sketch) to Tab D (Intelligence Preparation of the Battlefield-Products) to this appendix.
(a) (U) ECOA 1.
(b) (U) ECOA 2.
c. (U) Friendly Forces. See Annex A (Task Organization).
d. (U) Interagency, Intergovernmental, and Nongovernmental Organizations. See Annex V (Interagency Coordination).
e. (U) Civil Considerations. See Tab C (Civil Considerations) to this appendix.
f. (U) Attachments and Detachments. See Annex B (Intelligence).
g. (U) Assumptions. See Annex B (Intelligence).
2. (U) Mission. See Annex B (Intelligence).
3. (U) Execution. See Annex B (Intelligence).
4. (U) Sustainment. See Annex B (Intelligence).
5. (U) Command and Signal. See Annex B (Intelligence).

ACKNOWLEDGE:

COMMANDER
BG

OFFICIAL:

DEBORD
G-2

ATTACHMENTS:
Tab A–Terrain
Tab B–Weather
Tab C–Civil Considerations
Tab D–Intelligence Preparation of the Battlefield-Products

[CLASSIFICATION]

Figure E-2. Appendix 1 (Intelligence Estimate) example

Intelligence Running Estimate

E-7. Effective plans and successful execution hinge on accurate and current running estimates. A *running estimate* is the continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if the planned future operations are supportable (ADP 5-0). Failure to maintain accurate running estimates may lead to errors or omissions that result in flawed plans or bad decisions during execution. Each staff element is responsible for updating its portion of the running estimate as the operation unfolds.

E-8. The intelligence running estimate enables the intelligence operational officer/noncommissioned officer to continually update the commander on the mission execution from the intelligence perspective. Unlike other intelligence products, the intelligence running estimate combines both the analysis of friendly and allied forces' intelligence activities to support current operations.

E-9. Figure E-3 illustrates an example intelligence running estimate. The analysis focuses on current threat activities, strengths, and assessed intent/objectives to provide the commander and associated reporting requirements with a consistent summary of the threat. As the operation progresses, the collaborative effort may involve further analysis of the terrain and weather, monitoring the flow of displaced persons on the battlefield as inhibitors to friendly force maneuverability, and, when necessary, additional security requirements.

Note. In the highly volatile large-scale ground combat environment, the intelligence operational officer along with the all-source intelligence analyst are likely to maintain the running estimate.

[CLASSIFICATION]

INTELLIGENCE RUNNING ESTIMATE NUMBER___

(U) DATE-TIME GROUP:

(U) REFERENCES: Maps, charts, or other documents.

1. (U) MISSION: The commander determines the unit's mission.
2. (U) AREA OF OPERATIONS (AO): Describe the existing situation in the AO based on:
a. Terrain. How terrain affects a functional area's capabilities.
b. Civil Considerations. Description of areas, structures, capabilities, organizations, people, and events.
c. Weather. How weather affects friendly and threat warfighting function capabilities.
3. (U)ENEMY SITUATION: Summary of each threat characteristic that can influence mission accomplishment:
a. Composition.
b. Disposition. Geographic location of threat elements and how they are deployed or employed.
c. Strength. Committed forces, reinforcements, air, and chemical, biological, radiological, nuclear, and high-yield explosive weapons.
d. Tactics and Training. Strategy, methods of operations, doctrine, tactics, and training.
e. Sustainment. Procurement, maintenance, distribution, and materiel replacement.
f. Operational Effectiveness. Threat morale, weapons effectiveness, equipment readiness, leadership, and personnel.
g. Intelligence. Estimate of the threat's intelligence collection capability.
h. Communications. The threat's communications modes.
i. Other.
4. (U) ENEMY CAPABILITIES: In conventional operations:
a. State Enemy's Capabilities. *What*, *where*, *when*, and in what *strength* for each capability.
b. State Enemy's Limitations. Cause and effect of each limitation.
c. Analysis and Discussion. Effect of capabilities on terrain, civil considerations, weather.
5. (U) CONCLUSIONS: Conclusions based on information and analysis about the total effects of the AO on threat operations.
ACKNOWLEDGE: [Designated Staff Officer's Name and Designation]
OFFICIAL: [Authenticator's Name and Position]

[CLASSIFICATION]

Figure E-3. Intelligence running estimate example

CURRENT INTELLIGENCE REPORTS

E-10. Current intelligence reports address the current reporting of threat activities on the battlefield. The goal is to provide the commander with predictive analysis of the threat's intentions for future operations based on what conditions occurred by either threat or friendly actions during the past reporting period. This requires extensive intelligence analytical rigor in assessing threat activities and vigilance to the friendly scheme of maneuver.

Intelligence Summary

E-11. The intelligence summary (also known as INTSUM) is a periodic publication of the G-2/S-2 assessment of the threat situation on the battlefield. It provides the commander with context to support decision making based on the G-2/S-2's interpretation and conclusions about the threat, terrain and weather, and civil considerations over a designated period of time. This is typically identified in unit SOPs and in associated OPORD reporting instructions. The intelligence summary also provides COA updates based on the current situation. Unit SOPs designate the command's format for preparing and disseminating an intelligence summary. At a minimum, the intelligence summary should contain the paragraphs and subparagraphs as shown in figure E-4.

[CLASSIFICATION]

INTELLIGENCE SUMMARY (INTSUM) NUMBER____

(U) References: Maps, charts, overlays, and other relevant documents are available at internet protocol address.

(U) Time Zone Used Throughout the Order: ZULU

1. (U) WEATHER. The weather occurring within the operational environment (OE) will affect friendly and threat warfighting capabilities. This assessment is based on the weather officer and intelligence analyst's evaluation of the impact of specific environment conditions on friendly and threat forces. Normally, current and future weather conditions are displayed as far out as five days.

2. (U) SITUATION HIGHLIGHTS. A summary of the OE situation as it has evolved over the reporting period. Highlighted subparagraphs are as follows:

a. **Air:** Highlights of the current air situation. When in conflict with a threat possessing a capable air force, it is critical to the commander to identify whether or not friendly air power has achieved control of the operational airspace. This includes aircraft and air defense interlocking measures.

b. **Land:** Highlights of the current ground situation, usually divided by area of operations. If there are three divisions forming, the forward battle area along with a corps consolidation area and multiple division consolidation areas, then the land portion can be divided in that manner. Additionally, the main effort is often annotated first followed by the secondary and then any guerrilla or insurgent activities in the consolidation areas.

c. **Maritime:** Highlights of the current maritime situation. Maritime operations are as critical as air lift and air supremacy.

d. **Space:** Highlights of the current space situation. Space operations, including space weather, is critical to all operations whether the threat is capable of operating in this domain.

e. **Cyberspace:** Highlights of the current cyberspace situation. Cyberspace operations are critical to all operations whether the threat is capable of operating in this domain.

f. **Information Environment:** Highlights of the current information environment situation.

g. **Electromagnetic Spectrum:** Highlights of the current electromagnetic spectrum situation.

h. **Civil or Other Considerations:** Highlights of the current civil situation. Knowledge of the civilian population and civilian authorities/government is critical to the commander's situational understanding.

[CLASSIFICATION]

Figure E-4. Intelligence summary example

[CLASSIFICATION]

3. (U) SUMMARY OF THE ENEMY SITUATION. Each subparagraph of the threat situation is oriented on the commander's priority intelligence requirements (PIRs) and other information requirements as the basis for the analysis and assessment. The subparagraphs are as follows:

a. **Land:** The analysis of the land situation must include threat and possible insurgent activities detected during the INTSUM reporting period. Each echelon should publish at least one INTSUM daily, but it is likely that brigade and below commands in the forward combat zones will publish an INTSUM every 12 hours and in some missions even sooner. Based on the echelon, it is important for the analysis to consider terrain, weather, and the threat composition and disposition over the next 12 or more hours of combat. If in the consolidation area, the assessment must focus on the friendly forces' ability to support the forward battle with supplies and reinforcements as needed.

b. **Air:** The analysis of the air and air defense situation must focus on the threat air capability to gain or retain control of the air domain. Even when the threat air power is near depletion, ground air defense and even artillery or missile threats may still have a direct impact on friendly air operations—fixed or rotary wing.

c. **Maritime:** The analysis of the maritime situation must focus on the threat naval capability to gain or retain control of the maritime domain. This includes the ability of the threat maritime assets to support threat ground operations within distance of the sea.

d. **Other Domains:** Advise the commander of the other domains in which the threat may have opportunities to deny, impede, or disrupt friendly operations.

e. **Other:** The battlefield will be congested before, during, and after engagements. Any other considerations that answer PIRs or other requirements may enable the commander's decision making.

4. (U) UNIT ASSESSMENT. In each subparagraph, provide an analysis of current and possibly future threat courses of actions (COAs). All discussions of threat COAs must match what has been identified in the military decision-making process effort. If the threat COA has changed since that time, the G-2/S-2 should update the commander and staff to ensure the INTSUM is not the first notification. The subparagraphs are as follows:

a. **Most Likely COA:**

b. **Most Dangerous COA:**

c. **Other:** Other is reserved for other likely developments in civil considerations or a reiteration of pending serve weather.

5. (U) ENEMY MOVEMENT DURING THE REPORTING PERIOD. Provide all-source intelligence analysts a way to present various forms of identifying major threat units (including at least two levels below that of the reporting command) and coordinates to the last known positions. The information may be presented in written form, on a spreadsheet, or as a graphic summary, which should include where in DCGS-A other intelligence organizations may find this information.

6. (U) PIRs. Provide the commander's PIR list and, when possible, identify which PIRs have been answered. PIRs that have not been answered require explanations as to why they have yet to be answered.

7. (U) REPORTS AND DISTRIBUTION. Provide key reporting and distribution instructions from each echelon as well as reporting guidance from subordinate units. This includes the dissemination of reports, summaries, and dissemination requirements from subordinate echelon reporting. The Army uses DSCG-A and each echelon publishes associated procedures for the exchange/publication of various threat databases and reporting. Also provide authentication of the report.

[CLASSIFICATION]

Figure E-4. Intelligence summary example (*continued*)

Graphic Intelligence Summary

E-12. The graphic intelligence summary (also known as GRINTSUM) can be included with the intelligence summary or disseminated as a separate analytical report. It is a graphical representation of the intelligence summary, with emphasis on the threat forces location compared to friendly forces' location. The graphic intelligence summary also includes current PIRs and a summary of threat activities. (See figure E-5 on page E-8.) Since the emphasis of a graphic intelligence summary is graphical, most of the written details should be captured in the intelligence summary or an accompanying report.

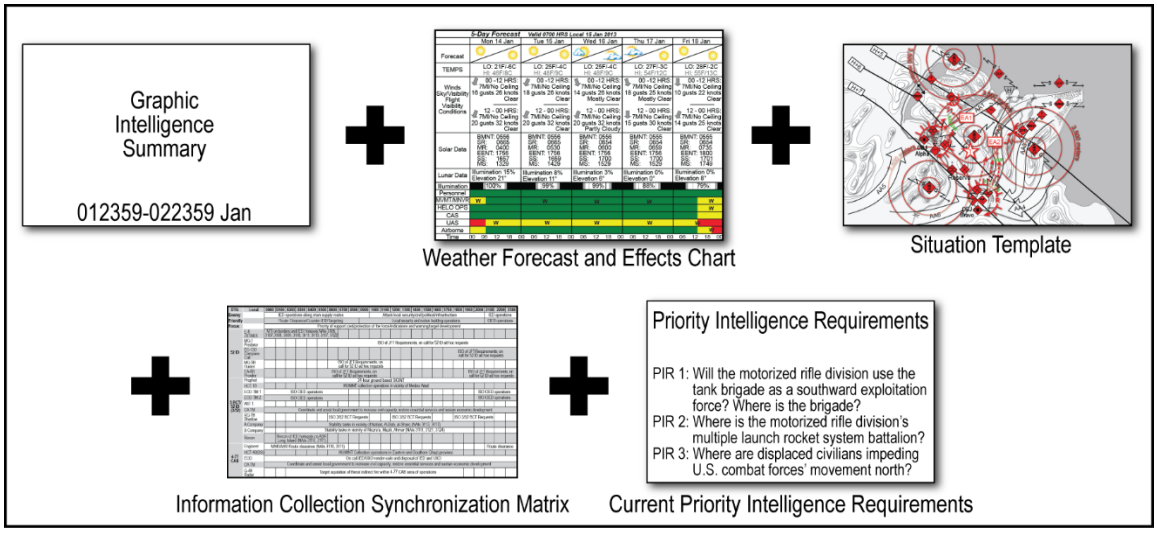


Figure E-5. Graphic intelligence summary example

E-13. There are challenges with using the graphic intelligence summary:

- The size of the graphical portrayal of the OE is often driven by critical facts about the threat that must be shown. Therefore, it is advisable to begin with a general OE map and zoom in on key areas. Ensure the written assessment includes the necessary details by either referencing the accompanying intelligence summary or other report or including the details in the Notes page of a PowerPoint slide.
- The file size must follow the commander's guidance or unit SOPs. Typically, the graphic intelligence summary is one or two graphics (PowerPoint slides) and limited in bit size for ease in emailing and posting on unit web portals. In a tactical large-scale ground combat environment, a brigade or lower command may be unable to send or receive a megabit plus-size file.

Intelligence Report

E-14. The intelligence report (also known as INTREP) demonstrates the importance of intelligence analysis. It is a standardized report, typically one page, used to establish a near current-threat operational standpoint. It points to the threat's responses to friendly actions and the battlefield environment. Intelligence reports may also highlight time-sensitive critical activities that require corroboration with other units and higher echelons. An intelligence report's basic information requirements describe *who*, *what*, *when*, *where*, *why*, and *how* facts in order to provide a conclusion. (See figure E-6.) There is no established timeline for disseminating an intelligence report. Some units may publish one or two daily, while others may publish 15 or 20 reports daily, depending on the activity level of engaging threat forces.

[CLASSIFICATION]

INTELLIGENCE REPORT NUMBER____

(U) References: Maps, charts, overlays, and other relevant documents used to create the intelligence report.

(U) Time Zone Used Throughout the Order: Applicable time zone during the time or reporting.

(U) Commander's Priority Intelligence Requirement: The applicable priority intelligence requirement to which the intelligence report is related.
(U) Summary of Activity: Brief discussion of the threat's general situation or activities, covering the *who*, *what*, *when*, *where*, *why*, and *how*, which support the analyst's conclusion.
(U) Authentication: Authentication by and instructions on handling and destroying.

[CLASSIFICATION]

Figure E-6. Intelligence report example

SUPPLEMENTAL ANALYTICAL REPORTS

E-15. Supplemental analytical reports, such as the periodic intelligence and supplementary intelligence reports, do not fall into a predetermined dissemination timeline. Periodic intelligence reports and supplementary intelligence reports follow a similar format, designated by a senior operational intelligence officer and staff. These reports allow for expanded analytical efforts, providing assessments of a technical or historical comparative nature. However, once the analysis begins to shape an assessment of threat intentions or capabilities, the urgency for releasing these analytical reports may increase.

Periodic Intelligence Report

E-16. The periodic intelligence report (also known as PERINTREP) is a summary of the intelligence situation that covers a longer period than the intelligence summary. (See figure E-7.) It is a means of disseminating detailed information and intelligence, including threat losses, morale, assessed strength, tactics, equipment, and combat effectiveness.

E-17. The periodic intelligence report includes but is not limited to sketches, overlays, marked maps or graphics, and annexes, providing a written and visual representation of the information and/or intelligence. The report is disseminated through the most suitable means based on its volume and urgency.

[CLASSIFICATION]

PERIODIC INTELLIGENCE REPORT NUMBER_____

(U) Period Covered: Date and time to date and time.

(U) References: Maps or charts.

(U) Disposal Instructions: If applicable.

(U) GENERAL ENEMY SITUATION. Briefly summarize threat operations during the period. Furnish amplifying details in the paragraphs that follow and in appropriate annexes or both. Also provide brief highlights of the threat situation and the significance of the threat's major activities, including marked changes in morale, strength, tactics, equipment, and combat effectiveness. Data that is lengthy or can conveniently be shown graphically is presented in annexes.

(U) ENEMY ACTIVITIES. Provide, in conjunction with the paragraphs that follow, details of the situation summarized in paragraph 1. Maximum use of sketches, overlays, marked maps or graphics, and annexes provide written and visual representations of the information and/or intelligence. Omit subparagraphs when appropriate intelligence is not available or is adequately covered by other portions of this report.

(U) ENEMY ORDER OF BATTLE. As appropriate, provide the threat order of battle in the following subparagraphs:

a. **Composition and Disposition.** Include land (airborne, artillery, rocket/missiles, air defense) air, maritime, space, cyberspace, information environment, and the electromagnetic spectrum.
b. **Strength.** Personnel and equipment/weapon losses.
    1. Losses (Killed in Action, Wounded in Action, and Captured).
    2. Assessed or Known Battle Damage Assessment.
    3. Key Personalities and Morale if Known.
    4. Current Strength.
c. **Tactics and Training.**
d. **New Tactics, Weapons, and Equipment.**
e. **Combat Service Support.**
f. **Combat Effectiveness.**
g. **Miscellaneous Details.**
    1. Civil.
    2. Communications (Electronics and Telecommunications).
    3. Electronic Warfare.
    4. Counterintelligence (Sabotage or Espionage).

[page number]

[CLASSIFICATION]

Figure E-7. Periodic intelligence report example

[CLASSIFICATION]

(U) OTHER INTELLIGENCE. Provide a detailed summary of the findings of other intelligence such as technical reports, interrogations, and/or document translations.

a. Technical intelligence summary includes detailed analysis of captured military equipment, communications devices, and can include explosive reports. While this information may not provide current information on the threat situation, it details enemy tactics, techniques, and procedures; new or modified equipment details, and critical information on improvised explosives. Most of the technical information comes from the Department of Defense and the national analysis from the Army's National Ground Intelligence Center.
b. Enemy prisoner of war interrogation reports from human intelligence teams provide key information about the threat forces' leadership, strength, and other details to support future cross-cuing efforts.
c. Translation of captured enemy documents provides similar details of threat capabilities, possible information on supplies, communications securities, and other key military operational details.
d. Additional details on weather and climate summaries.

(U) WEATHER. Provide an update on the impact of weather on future operations. Weather graphics can be presented in the annex as necessary.

(U) TERRAIN. Provide an update on the impact of terrain on future operations. If necessary, use annexes to provide special maps, overlays, and electronic data.

(U) ANALYSIS AND DISCUSSION. List and briefly discuss threat capabilities and vulnerabilities based on the information revealed. The conclusions present the commander's assessment of the most probable courses of actions available to the threat, probability of their adoption, and vulnerabilities that are exploitable by own, higher, adjacent, or lower commanders.

a. Enemy Capabilities.
b. Enemy Vulnerabilities.
c. Conclusions.

(U) REPORTS AND DISTRIBUTION. Provide key reporting and distribution instructions from each echelon as well as reporting guidance from subordinate units. Include the dissemination of reports, summaries, and dissemination requirements from the subordinate echelon's reporting. The Army uses DSCG-A, and each echelon publishes associated procedures for the exchange/publication of various threat databases and reporting. Also provide authentication of the report.

[page number]
[CLASSIFICATION]

Figure E-7. Periodic intelligence report example (*continued*)

Supplementary Intelligence Report

E-18. The supplementary intelligence report (also known as SUPINTREP) is a comprehensive analysis of one or more specific subjects, typically the result of a request or to support a particular operation. This report is formatted similarly to a periodic intelligence report, but it addresses analysis over an extended period of time. Typically, the detailed analysis is from an accumulation of national assessments of threat actions, tactics, and doctrine identified during combat—normally a post-combat review. Maximum use of sketches, photos, overlays, marked maps or graphics, and annexes provides a written and visual representation of the information and/or intelligence. The supplementary intelligence report is disseminated based on the intelligence it contains and the commander's requirements.

E-19. Specific reports may pertain to but are not limited to the following:

- Technical intelligence summary includes detailed analysis of captured military equipment, communications devices, and can include post-explosive reports.
- Enemy prisoner of war interrogation reports from tactical to national sources.
- Translation of captured enemy documents (DOMEX).
- Cyberspace security updates.
- Medical or environmental hazards.
- Changes to civil political and other civilian authorities.

ANALYTICAL ASSESSMENTS THAT SUPPORT ORDERS AND BRIEFINGS

E-20. In addition to designated intelligence production requirements, the intelligence staff also provides analytical assessments to orders, briefings, and staff events, as described in FM 6-0. (See table E-1.) Normally, the intelligence analysis identifies the current threat situation and assessed threat capabilities (often tied to a threat COA); the same information exists in the intelligence summary, intelligence report, and intelligence running estimate. For intelligence analysts, the commander, and often the key staff officer, defines the requirement and may provide additional detailed requirements in unit SOPs.

Table E-1. Support to orders and briefings

Orders			
Reports	***Echelon***	***Dissemination timeline***	***General description***
Operations summary	All	Daily	The commander provides to higher, adjacent, and lower a daily (or twice daily) operations summary that includes an intelligence assessment of threat forces' actions, intent, and assessed strength.
Operation order	All	As needed	The operation order is the same as the intelligence estimate identified in the operation order as Annex B (Intelligence).
Warning order	All	As needed	The G-2/S-2 provides a summary update to paragraph 1.c *Enemy Forces* to the warning order.
Fragmentary order	All	As needed	The G-2/S-2 provides a summary of the threat activity to paragraph 1 *Situation* and as the mission requires to paragraph 3 *Execution*.
Staff briefings			
Briefing	***Echelon***	***Dissemination timeline***	***General description***
Battle update brief	All	Daily	The G-2/S-2 provides an assessment of the threat forces and identifies collection opportunities or requirements to answer the commander's priority intelligence requirement (PIR).
Military decision-making process (MDMP)	All	As needed	The G-2/S-2 provides intelligence analysts to support the planning and war-gaming efforts associated with the commander's MDMP requirements. Normally, the intelligence analysis is in the form of the intelligence preparation of the battlefield steps.
Operations and intelligence brief	All	Likely daily	The G-2/S-2 provides an assessment of the threat forces and identifies collection opportunities or requirements to answer the commander's PIR.
Targeting board	All	As needed	The G-2/S-2 provides an assessment of the threat actions in the high-payoff target and high-value target criteria established by the commander. (See appendix F for more details on intelligence analysis support to targeting.)
After action report	All	As needed	The after action report is a method of capturing lessons learned or, in some cases, identifying what caused a friendly action to occur. In specific cases, the G-2/S-2 may be required to provide a summary assessment of the threat actions that caused a friendly action. (See FM 6-0.)
G-2/S-2 division or corps/battalion or brigade intelligence staff officer			

This page intentionally left blank.

Appendix F

Intelligence Support to Targeting

OVERVIEW

F-1. The targeting effort is cyclical and closely tied to combat assessments. Targeting is a complex and multidiscipline effort that requires coordinated interaction among many command and staff elements. The functional element necessary for effective collaboration is represented in the targeting working group. Intelligence analysts perform a number of critical tasks as part of this working group and the overall targeting effort. (See ATP 3-60 for more information on targeting.)

TARGETING GUIDELINES

F-2. The threat presents a large number of targets that must be engaged with available information collection assets and attack assets. The targeting process assesses the benefits and the costs of engaging various targets in order to achieve the desired end state. Adhering to the five targeting guidelines should increase the probability of creating desired effects while diminishing undesired or adverse collateral effects:

- Targeting focuses on achieving the commander's objectives.
- Targeting seeks to create specific desired effects through lethal and nonlethal actions.
- Targeting directs lethal and nonlethal actions to create desired effects.
- Targeting is a fundamental task of the fires warfighting function that encompasses many disciplines and requires participation from many staff elements and components.
- Targeting creates effects systematically.

TARGETING GUIDANCE AND CATEGORIES

F-3. The commander's targeting guidance must be articulated clearly and simply to enhance understanding. The guidance must be clearly understood by all warfighting functions, especially by the intelligence staff. Targeting guidance must focus on essential threat capabilities and functions that interfere with the achievement of friendly objectives.

F-4. The commander's targeting guidance describes the desired effects to be generated by fires, physical attack, cyberspace electromagnetic activities, and other information-related capabilities against threat operations. Targeting enables the commander, through various lethal and nonlethal capabilities, the ability to produce the desired effects. Capabilities associated with one desired effect may also contribute to other effects. For example, delay can result from disrupting, diverting, or destroying threat capabilities or targets. Intelligence personnel should understand and only use the 14 terms used in ATP 3-60 to describe desired effects:

- Deceive.
- Defeat.
- Degrade.
- Delay.
- Deny.
- Destroy.
- Destruction.
- Disrupt.
- Divert.
- Exploitation.
- Interdict.
- Neutralize.
- Neutralization.
- Suppress.

F-5. To effectively target the threat, friendly forces use deliberate and dynamic targeting. Deliberate targeting prosecutes planned targets, while dynamic targeting prosecutes targets of opportunity and changes to planned targets. During both categories of targeting, friendly forces may prosecute normal, time-sensitive, and sensitive targets.

TARGETING METHODOLOGY

F-6. The targeting methodology organizes the efforts of the commander and staff to accomplish key targeting requirements. This methodology is referred to as the *decide*, *detect*, *deliver*, and *assess* methodology. The methodology assists the commander and staff in deciding which targets must be acquired and engaged and in developing options to engage those targets. Options can be lethal or nonlethal, organic, or supporting assets at all levels as listed—maneuver, electronic attack, psychological, attack aircraft, surface-to-surface fires, air to surface, other information-related capabilities, or a combination of these operations.

F-7. The *decide*, *detect*, *deliver*, and *assess* methodology is an integral part of the MDMP. During the MDMP, targeting becomes more focused based on the commander's guidance and intent. A very important part of targeting is identifying potential fratricide situations and the necessary coordination measures to positively manage and control the attack of targets. These measures are incorporated in the coordinating instructions and appropriate annexes of the operation plan or OPORD.

DECIDE

F-8. The *decide* function of the targeting methodology provides the overall focus and sets priorities for information collection and attack planning. It is the most important targeting function and requires close interaction between the intelligence, plans, operations, and fires cells, and the servicing judge advocate. This step draws heavily on the staff's knowledge of the threat, a detailed IPB (which occurs simultaneously), and a continuous assessment of the situation. Targeting priorities are addressed for each phase or critical event of an operation. The decisions made are reflected in visual products as follows:

- **HPT list.** The *high-payoff target list* is a prioritized list of high-payoff targets by phase of the operation (FM 3-09). A *high-payoff target* is a target whose loss to the enemy will significantly contribute to the success of the friendly course of action (JP 3-60). An HPT is an HVT that must be acquired and successfully engaged for the success of the friendly commander's mission. A *high-value target* is a target the enemy commander requires for the successful completion of the mission (JP 3-60).
- **Information collection plan.** The information collection plan focuses the collection effort to answer PIRs and other significant requirements. If an HPT is not designated as a PIR, it must still be supported by collection. The information collection plan usually supports the acquisition of more HPTs. (See ATP 2-01.)
- **Target selection standard matrices.** These matrices address accuracy or other specific criteria requiring compliance before targets can be attacked.
- **Attack guidance matrix.** The *attack guidance matrix* is a targeting product approved by the commander, which addresses the how and when targets are engaged and the desired effects (ATP 3-60).

Intelligence Preparation of the Battlefield

F-9. In the same manner that targeting involves coordinated interactions among the commander and entire staff, IPB involves the active participation of the entire staff. The interactions between intelligence personnel and fires personnel are important during the IPB process. (For more information on staff collaboration during IPB, see ATP 2-01.3.) Many of the IPB products significantly influence or are brought forward into the targeting effort. These products assist in target value analysis and war gaming. Some examples of important IPB products include—

- The modified combined obstacle overlay.
- Civil considerations (ASCOPE) products.
- Weather effects products.

- Threat models with recommended HVTs.
- Situation templates with threat time phase lines.
- Event templates and matrices, which have named areas of interest (NAIs).

Target Value Analysis and War Gaming

F-10. From the coordination and work performed during the IPB effort, the targeting working group, especially the intelligence staff and targeting officer, perform target value analysis that yields HVT lists (which may include high-value individual lists) for a specific threat COA. Target value analysis continues the detailed analysis of relevant threat factors, including doctrine, tactics, equipment, capabilities, and expected actions for a specific threat COA. The target value analysis process identifies HVT sets associated with critical threat functions.

F-11. Target spreadsheets (or target folders, as appropriate) identify an HVT compared to a type of operation. Target spreadsheets give detailed targeting information for each HVT, which is used during IPB and war gaming. The intelligence staff and targeting officer collaborate to develop and maintain the target spreadsheet.

F-12. The targeting working group develops HVTs for lethal and nonlethal targeting. For nonlethal targeting, there is no limit on how creative and flexible the working group can be when focusing targeting requirements to support the commander's guidance. In certain circumstances, an HVT may not be focused on a certain geographic area.

F-13. The following assists in identifying and evaluating HVTs:

- Identify HVTs from threat models, situation templates with time phase lines, existing intelligence studies, database evaluations, patrol debriefs, and reporting. The following provide useful information:
  - A review of threat tactics, techniques, and procedures.
  - Previous threat operations.
  - Understanding the threat's objective, tasks, purpose, and intent.
- Identify assets that are key to executing the primary operation or sequels.
- Determine how the threat might react to the loss of each identified HVT. Consider the threat's ability to substitute other assets and adopt branches or sequels.
- After identifying HVTs, place them in order of their relative worth to the threat's operation and record them as part of the threat model. The value of HVTs varies over the course of an operation. Identify and annotate changes in value by phase of the operation. The following are additional considerations:
  - Use all available intelligence sources (for example, patrol debriefs, reporting) to update and refine the threat models.
  - Categorize the updates to reach a conclusion concerning the threat's operations, capabilities, and vulnerabilities.

F-14. HVTs are finalized and prioritized during war gaming. The staff analyzes and identifies those HVTs that must be attacked to ensure mission success. Additionally, the staff analyzes all implications of attacking those HVTs and possible threat counteractions. Those critical HVTs that the staff confirms as acquired and attacked are nominated as HPTs. Then, the staff groups HPTs into a list, associating the HPTs to a specific point in the battle. The completed HPT list is submitted to the commander for approval.

F-15. During war gaming, the commander and staff identify the best places to attack an HPT. These places are known as target areas of interest (TAIs). A TAI is a point or area where the commander can acquire and engage HPTs. The shape of a TAI reflects the type of threat, target, and weapon system that will engage the target.

F-16. The staff may need to develop additional NAIs to support TAIs. NAIs for nonlethal targets may include religious buildings, places of worship, and shrines that are important to assessing key civil considerations (ASCOPE). Decision points or decision time phase lines are used to ensure the decision to engage or not to engage occurs at the proper time. Decision points and TAIs are recorded on the decision support template.

F-17. A thorough war gaming effort ensures the staff sets the foundation for a successful targeting effort. The purpose of war gaming includes building staff running estimates and developing the scheme of maneuver, scheme of fires, and decision support template. The process also synchronizes the attack guidance matrix with the decision support template and ensures the information collection plan supports all HPTs.

Target Selection

F-18. Target selection depends on the ability to acquire the target. The collection manager must be closely involved in ensuring information collection on HPTs is carefully synchronized into the information collection plan. This task includes breaking HPTs into subsets, when necessary; developing adequate collection tasks; and considering the use of cueing, collection redundancy, and sensor mix during the development of the information collection synchronization matrix. (See ATP 2-01 for more information.)

High-Payoff Target List

F-19. Once prioritized, targets are placed on the HPT list and approved by the commander. Figure F-1 provides an example of an HPT list. The list identifies HPTs by operational phase or specific time windows and order of priority. Other considerations include—

- The sequence or order or appearance.
- The ability to detect, identify, classify, locate, and track the target.
- The degree of accuracy of the acquisition system.
- The ability to engage the target.
- The ability to achieve the desired effects based on the attack guidance.

Threat element	*Time (H-hour)*	*Priority*	*Targets*	*Desired effect*
Intelligence	H-24-H+10	1	Air defense radar	Destroy
Fires		2	Air missile defense (SA-13, SA-18)	
Intelligence		3	Artillery locating radar (ARK-1M)	
Fires	H-H+10	4	Field artillery companies (2S1)	
Command and control	H-H+10	4	• Control node/Government Complex • Threat communications networks	Neutralize
H-hour specific hour at which a particular operation commences				

Figure F-1. High-payoff target list example

Target Selection Standards

F-20. Target selection standards are criteria applied to threat activity and used to decide whether the activity is a target. There are two target selection standard categories:

- Targets, which meet accuracy and timeliness requirements for engagement.
- Suspected targets, which must be confirmed before any engagement.

F-21. Target selection standards are based on the threat's activity and available weapon system. The following elements are used to develop the standards:

- Weapon system target location accuracy requirements (target location error).
- Size of threat activity.
- Status of the activity (moving or stationary).
- Timeliness of the information.

F-22. The BCT can develop target selection standards based on anticipated threat characteristics and template threat activities. Different target selection standards may exist for a given threat activity based on different attack systems. For example, a threat artillery battery may have a 150-meter target location error criterion for attack by cannon artillery and a one-kilometer requirement for attack helicopters. The fires cell develops target selection standards in conjunction with the intelligence cell. Units may develop their own worksheet format. Intelligence analysts use the standards to quickly determine targets from combat information and pass the targets to the fires cell.

F-23. The fires cell uses target selection standards to identify targets for attack. Certain situations require the systems to identify friendly and neutral from threats before approval to engage in lethal fire. HPTs that comply with the criteria are tracked until they are attacked in accordance with the attack guidance matrix. Target locations that do not comply with the standards are confirmed before attacked.

F-24. Target selection standards can be depicted in a matrix. Figure F-2 is an example of a target selection standard matrix. Although not shown in figure F-2, it may include a column that lists each friendly information collection system that forwards targets directly to the fires cell or fires direction center. The effects of terrain and weather on information collection assets and threat equipment are considered. While target selection standards are developed specific to the situation, the greatest emphasis is on considering the threat situation, possibility of threat deception, and the reliability of the source or agency that is reporting.

High-Payoff Target	*Timeliness*	*Accuracy*
2S3	30 minutes	500 meters
M-46	30 minutes	500 meters
Air and missile defense	15 minutes	500 meters
Command posts	3 hours	500 meters
Ammunition	6 hours	1 kilometer
Maneuver	1 hour	150 meters

Figure F-2. Example target selection standard matrix

Attack Guidance

F-25. Analyzing target vulnerabilities and the effect an attack has on threat operations within the context of the commander's targeting guidance allows the staff to propose the most efficient available engagement option. During war gaming, decision points linked to events, areas (NAIs and TAIs), or points within the AO are developed. These decision points cue command decisions and staff actions when a tactical activity is needed.

F-26. Based on the commander's guidance, the targeting team recommends target engagement in terms of the effects of fire and attack options. The intelligence staff must understand the definitions of and nuances for each of the 14 terms used to describe desired effects. Desired effects are then translated into automation system values to more effectively engage targets.

F-27. Deciding on which attack system to use occurs simultaneously as deciding when to acquire and attack the target. When deciding to attack by two different means, such as electronic warfare and combat air operations, coordination is required. Coordination requirements are recorded during the war game.

F-28. The commander, with recommendations from the targeting working group, approves the attack guidance, which is more than the attack guidance matrix. The attack guidance details the following:

- An updated prioritized HPT list.
- When, how, and the desired effects of engagement.
- Special instructions.
- BDA requirements.

F-29. This information is developed during the war game. Attack guidance is provided to weapon systems managers via the attack guidance matrix, which, at a minimum, includes—

- Specific HPTs.
- Timing of engagement.
- How targets are engaged.
- Desired effects.
- Remarks, including restrictions.

Target Development

F-30. *Target development* is the systematic examination of potential targets and their components, individual targets, and even elements of targets to determine the necessary type and duration of the action that must be exerted on each target to create an effect that is consistent with the commander's specific objective (JP 3-60). This analysis includes deconfliction, aim point recommendations, target materials production, and collateral damage estimation. Target development generally results in products such as target folders, information collection requirements, and target briefs. Detailed analysis should characterize the function, criticality, and vulnerabilities of each target, linking targets back to targeting objectives and measures of effectiveness. Target development includes target vetting and target validation.

Note. Although target development is discussed under *detect* in ATP 3-60, for this publication, it is more useful to discuss this step under *decide*.

Target Vetting

F-31. *Vetting* is a part of target development that assesses the accuracy of the supporting intelligence to targeting (JP 3-60). Vetting establishes a reasonable level of confidence in a target's designated functional characterization. The BCT intelligence cell accomplishes this by reviewing all target data for accuracy. At a minimum, the assessment includes at a review of target identification, significance, collateral damage estimation, geospatial or location issues, impact on the threat or friendly forces, impact of not conducting operations on the target, environmental sensitivity, and intelligence gain or loss concerns. Vetting does not include an assessment of compliance with the law of war or rules of engagement.

Target Validation

F-32. *Validation* is a part of target development that ensures all candidate targets meet the objectives and criteria outlined in the commander's guidance and ensures compliance with the law of war and rules of engagement (JP 3-60). Targets are validated against multinational concerns during some operations. Target vetting and validation should recur as new intelligence is collected or the situation changes. Target validation is performed by targeting personnel, in coordination with planners, servicing judge advocate, and other experts, as required. (See ATP 3-60 for a list of useful target validation questions.)

DETECT

F-33. As much as possible, the procedures and supporting products that are used during the *detect* function should be developed during the *decide* function. However, the targeting team must periodically update decisions made during the *decide* function concerning IPB products, HPT lists, target synchronization matrices, attack guidance matrices, the information collection plan, and the OPORD. Updating these products can occur throughout the *detect*, *deliver*, and *assess* functions of the targeting methodology.

F-34. Based on targeting priorities, the targeting working group establishes target detection and tracking priorities. Target tracking is inherent in target detection. The fires cell provides the intelligence cell with the degree of accuracy required and dwell time for a target to be eligible for engagement. Then the collection manager can match those requirements to the target location error of the information collection asset.

F-35. Execution of the information collection plan begins as early as possible during planning and continues all the way through the *assess* function and even helps transition operations into the next mission. The execution of the information collection plan to answer targeting information requirements is central to the *detect* function. Targets are detected by using the appropriate information collection assets. ATP 3-60 discusses this effort as detection procedures.

F-36. The *detect* function comprises target detection and additional target development, when necessary. The current operations integration cell is the primary cell responsible for directing the execution of the information collection effort to detect HPTs identified in the *decide* function. The intelligence cell (with the current operations integration cell) must focus their intelligence analysis efforts to support both situation development and the targeting effort. Therefore, close coordination between the intelligence cell and the fire support element is critical. Key staff members in this effort include the G-3/S-3, G-2/S-2, information

operations officer, field artillery intelligence officer (when staffed), targeting officer, and fire support coordinator/officer.

F-37. When detecting a planned HPT, the information is quickly disseminated to the field artillery intelligence officer to determine if the target is an HPT, the target's priority, and if the target complies with target selection standards. To ensure the target information is disseminated quickly, the field artillery intelligence officer should be located in the intelligence cell with communications to the fires cell. If the target is an HPT, the field artillery intelligence officer coordinates with the intelligence cell and disseminates the target directly to the fires cell or fire support element. If the commander approves the target, it is transferred to a firing unit.

F-38. In those cases, where the situation dictates the development of a new HPT or when the staff assesses a significant change to an existing HPT, subsequent target development must occur. When subsequent target development is necessary, the targeting information is forwarded for intelligence analysis and the target development process must occur quickly. Upon identifying a target specified for attack, analysts pass the target to the fire support element. The fire support element executes the attack against the target.

DELIVER

F-39. The *deliver* function executes the target attack guidance and supports the commander's plan once HPTs have been located and identified. Target engagement requires several decisions and actions, which are grouped into tactical and technical decisions.

Tactical Decisions

F-40. Tactical decisions are made based on the analysis that was accomplished during target development. Tactical decisions reconfirm or determine the—

- Time of the engagement.
- Desired effect, degree of damage, or both.
- Delivery system to be used through weaponeering and collateral damage estimation.

Time of Engagement and Desired Effect

F-41. Time of engagement and the desired effect that will be achieved on the target are critical considerations. The commander needs to weigh the operational risk of tactical patience balanced against the immediacy of the planned action in the attack guidance matrix. As the operation evolves, the commander may decide to change the time of engagement or the desired effect on a particular HPT. When a target is a target of opportunity, then the commander and staff must quickly decide on the desired effects.

Delivery System

F-42. This step builds on the analysis performed during target development and includes weaponeering and collateral damage estimation. If the target was already planned, then this step starts with determining if the delivery means is available and still the best weapon or means for the engagement. When the target is a target of opportunity then some analysis is necessary to work through completion of a quick target development.

F-43. *Weaponeering* is the process of determining the specific means required to create a desired effect on a given target (JP 3-60). As much as possible, weaponeering should be planned during the plan function during target development. Weaponeering considers munitions delivery error and accuracy, damage mechanisms and criteria, probability of kill, weapon reliability, and trajectory. Targeting personnel quantify the expected results of fires against targets to produce the desired effects. ATP 3-60 provides a general weaponeering process that can be adapted as needed.

F-44. Collateral damage estimation builds on target validation to assist the commander and unit in staying within the law of war and rules of engagement. Failure to observe these obligations can be very significant to operations and considered a law of war violation. The staff has the responsibility to mitigate unintended or incidental risk of death, injury, or damage according to the law of war and rules of engagement as described in ATP 3-60.

Technical Decisions

F-45. Once the tactical decisions have been made, the G-3/S-3 directs the appropriate unit to engage the target. The fires cell provides the asset or system manager with selected time of engagement, desired effects, and any special restraints or requests for particular munitions types.

F-46. The asset or system manager (for example, field artillery battalion S-3, air liaison officer, or brigade naval gunfire officer) determines if the system can meet the requirements. The fires cell is notified when a delivery system or asset is unable to meet the requirements. In those cases, the fires cell must decide if the selected delivery asset or system should engage the target under a different criterion or if a different delivery asset or system should be used.

ASSESS

F-47. The *assess* function of the targeting methodology is nested in the overall continuous assessment of operations within the operations process. Assessment is directly tied to the commander's decisions throughout the planning, preparation, and execution of operations. Planning for assessment identifies key aspects of the operation that the commander directs be closely monitored, and where the commander wants to make the decisions. Commanders and staffs consider assessment ways, means, and measures. ADP 5-0 discusses overall operational assessment, including measures of effectiveness, measures of performance, and indicators. Intelligence plays a major role in operational assessment.

F-48. Intelligence also plays a major role in assessment as a part of the targeting methodology. The assess function of the targeting methodology is performed through combat assessment. *Combat assessment* is the determination of the effectiveness of force employment during military operations (JP 3-60). Combat assessment comprises three elements:

- BDA.
- Munitions effectiveness assessment.
- Reengagement recommendation.

F-49. Together, BDA and munitions effectiveness assessment provide the commander and staff with an assessment of the effects achieved against targets and whether the targeting guidance was met. Based on this information, the staff can recommend reengagement when necessary.

Battle Damage Assessment

F-50. *Battle damage assessment* is the estimate of damage composed of physical and functional damage assessment, as well as target system assessment, resulting from the application of lethal or nonlethal military force (JP 3-0). The staff determines how combat assessment relates to specific targets by completing BDA. Producing BDA is primarily an intelligence cell responsibility but requires coordination across the staff, similarly to IPB and most steps of intelligence support to targeting. BDA requirements should be captured as PIRs or as similar high-priority information collection requirements. BDA provides—

- Commanders with an assessment of the target's mission effectiveness, overall status, capabilities (whether full or partial), and likely reactions or any change to their intent. This assists the staff in determining if the engagement is meeting the targeting guidance and is critical to any recommendation to reengage the target.
- Important analysis used to conduct quick target development and decide on the allocation or redirection of assets or weapon systems for any reengagement.

F-51. BDA has three components (see table F-1):

- **Physical damage assessment.** The staff estimates the extent of physical damage to a target based on observed or interpreted damage. It is a post-attack target analysis coordinated among all units.
- **Functional damage assessment.** All-source intelligence analysts assess the remaining functional or operational capability of the threat. The assessment focuses on measurable effects and estimates the threat's ability to reorganize or find alternative means to continue operations. The targeting cell and staff integrate analysis with external sources to determine if the commander's intent for fires has been met.

- **Target system assessment.** The staff conducts a broad assessment of the overall impact and effectiveness of all types of engagement against an entire target system capability (for example, threat air defense artillery systems). All-source intelligence analysts assist the staff in assessing the threat's combat effectiveness or major threat subordinate elements or capabilities needed to accomplish a threat mission. This is a relatively permanent assessment (compared to functional damage assessment) that can be used for more than one mission.

Table F-1. Battle damage assessment components

Component	*Description*
Physical damage assessment	• Quantitative physical damage from munitions blast, fragmentation, or fire. • Based on observed or interpreted damage.
Functional damage assessment	• Estimates the effects on the target's capability to perform its mission. • Assessment based on all-source intelligence. • Includes a time estimate required to reconstitute or replace the target. • Temporary assessment—compared to a target system assessment—used for specific missions.
Target system assessment	• The overall effect on an entire target system's capability. • Applicable against a threat's combat effectiveness. • May address significant subdivisions of a target. • A more permanent assessment.

F-52. BDA requirements for specific HPTs are determined during the *decide* function. Often information collection assets can answer either target development and target acquisition requirements or BDA, but not both types of requirements. An asset used for BDA may be unavailable for target development and target acquisition requirements. The intelligence cell receives, processes, and disseminates results that are analyzed based on desired effects to the targeting team attack.

F-53. The targeting team should consider the following BDA principles:

- BDA should measure what is important to commanders, not make important what is easily measurable.
- BDA should be objective. When receiving a BDA product from another echelon, the conclusions should be verified (time permitting) to identify and resolve discrepancies among BDA analysts at different headquarters.
- The degree of reliability and credibility of BDA relies largely on information collection assets. The quantity and quality of information collection assets influence whether the assessment is highly reliable (concrete, quantifiable, and precise) or has low reliability (estimation). Effective BDA uses more than one source to verify each conclusion.

F-54. BDA is more than determining the number of casualties or the amount of equipment destroyed. The targeting team can use other information such as—

- Whether the targets are moving or hardening in response to the attack.
- Changes in deception efforts and techniques.
- Whether the damage achieved is affecting the threat's combat effectiveness as expected.

F-55. Units may choose to use BDA charts. Figures F-3 and F-4 on page F-10 display two techniques for creating these charts. Figure F-3 is based on the threat's organization; figure F-4 is based on the BDA reported at locations within the AO. Units may choose to use figure F-4 when conducting offensive operations because it provides the commander and staff with an estimation of threat strength at a specific location.

F-56. BDA may simply be compiled information about a particular target or area (for example, the area's cessation of fires). If BDA is developed, the targeting team gives the collection management team and operations cell adequate warning to task information collection units and prepare and orient intelligence collection systems to the right target at the right time. BDA outcomes may result in changed plans and earlier decisions. The targeting team periodically updates earlier decisions during the *decide* function concerning IPB products, HPT lists, target selection standards, attack guidance matrices, collection management tools, and operation plans or OPORDs.

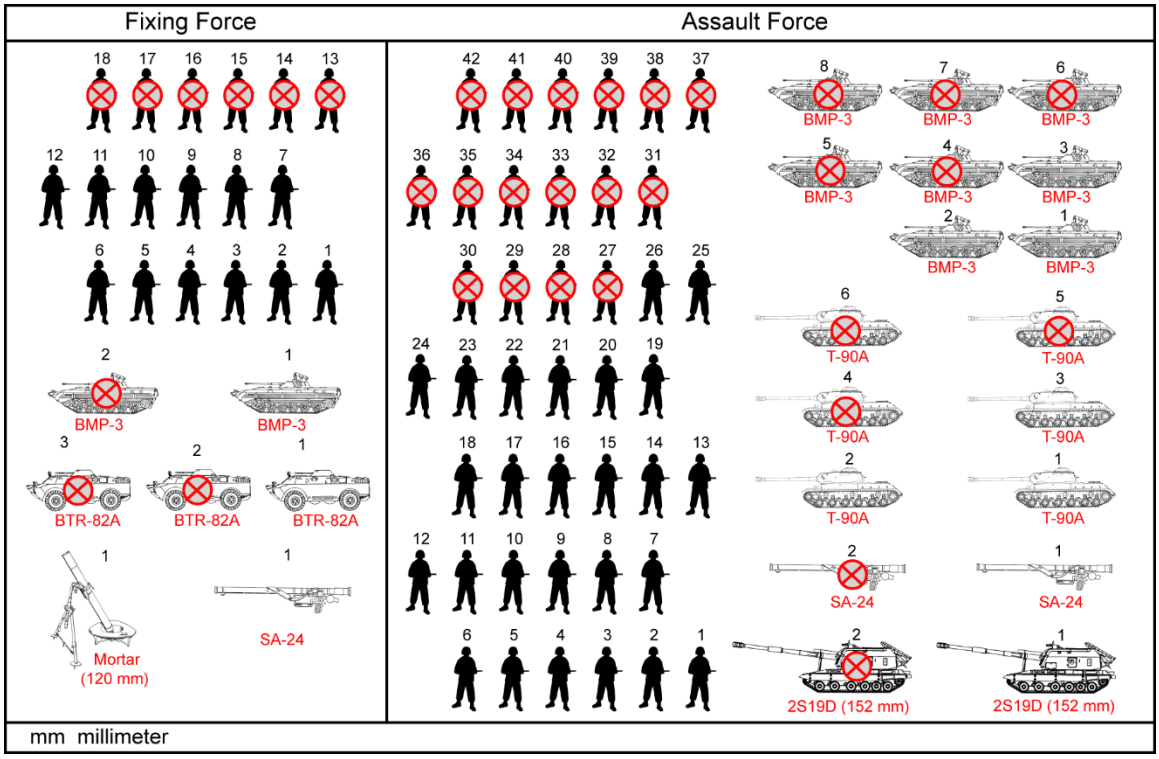


Figure F-3. Battle damage assessment chart (based on threat organization)

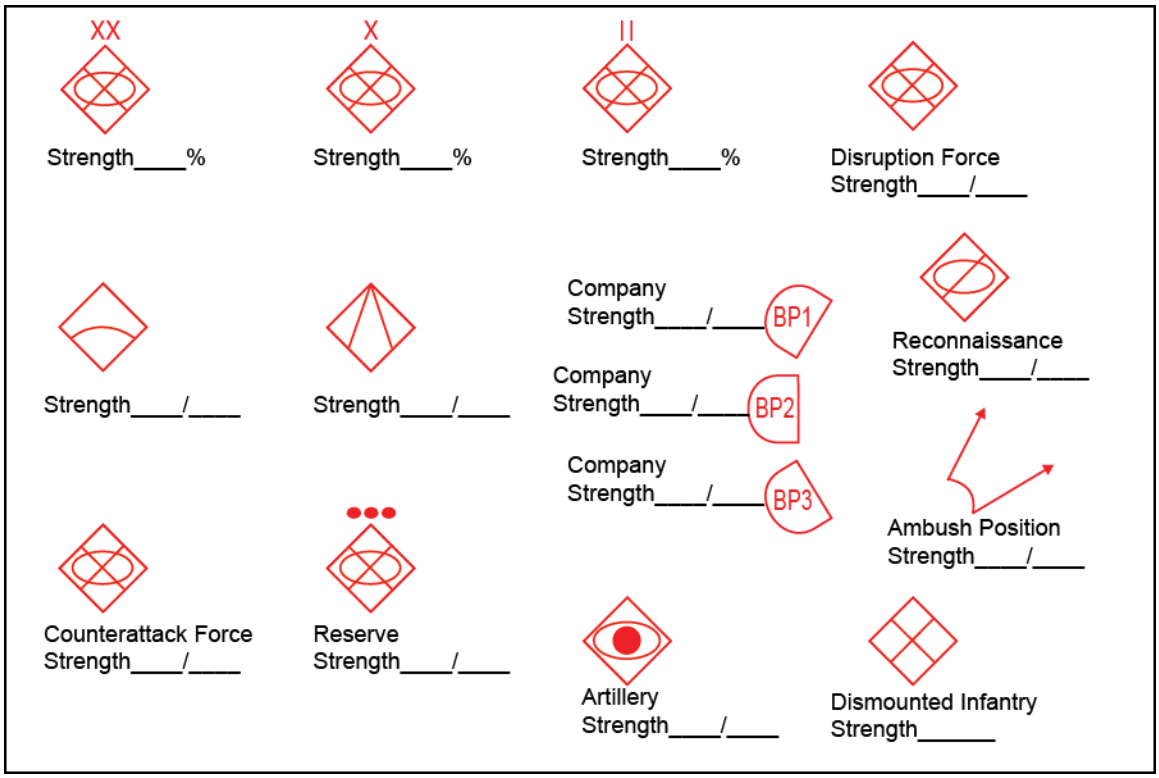


Figure F-4. Battle damage assessment chart (based on location)

Munitions Effectiveness Assessment

F-57. The intelligence cell is not normally involved in the munitions effectiveness assessment but should track them to better understand the unit targeting effort. The G-3/S-3, in coordination with the fires cell and targeting working group, conducts the munitions effectiveness assessment concurrent with BDA. The munitions effectiveness assessment focuses on the munitions effectiveness of the specific threat weapons or other types of systems. The fires cell uses specific weaponeering software. Then the G-3/S-3 and fires cell conducts the munitions effectiveness assessment to increase the effectiveness of the targeting methodology, tactics, weapon systems, munitions, and weapon delivery patterns. Based on the assessment, the targeting working group may recommend modifying the commander's guidance about the unit basic load, required supply rate, and controlled supply rate.

Reengagement Recommendation

F-58. Unlike the munitions effectiveness assessment, the intelligence cell is involved in a reengagement recommendation. When delivery of fires does not achieve a predecided effect or reach a preset BDA criterion, a decision from the commander is necessary. The targeting team and current operations cell must assess the operational risk associated with reengaging or not reengaging an HPT. Based on the BDA and munitions effectiveness assessment, the G-2/S-2, in conjunction with the fire support coordinator and G-3/S-3, considers to what degree the targeting objective has been achieved and makes a recommendation to the commander. Reengagement and other recommendations should address objectives relative to targets, target critical elements, target systems, threat combats for strength, and friendly maneuver.

This page intentionally left blank.

Glossary

The glossary lists acronyms and terms with Army or joint definitions. Where Army and joint definitions differ, (Army) precedes the definition. The proponent publication for terms is listed in parentheses after the definition.

SECTION I – ACRONYMS AND ABBREVIATIONS

ACE	analysis and control element
ACH	analysis of competing hypotheses
ADP	Army doctrine publication
AO	area of operations
AR	Army regulation
ART	Army tactical task
ASCOPE	areas, structures, capabilities, organizations, people, and events (civil considerations)
ATP	Army techniques publication
BCT	brigade combat team
BDA	battle damage assessment
CFA	critical factors analysis
COA	course of action
DCGS-A	Distributed Common Ground System-Army
DOD	Department of Defense
DOMEX	document and media exploitation
FEBA	forward edge of the battle area
FM	field manual
G-2	assistant chief of staff, intelligence
G-3	assistant chief of staff, operations
HAC	human intelligence analysis cell
HPT	high-payoff target
HUMINT	human intelligence
HVT	high-value target
IADS	integrated air defense system
ICD	intelligence community directive
INSCOM	U.S. Army Intelligence and Security Command
IPB	intelligence preparation of the battlefield
JP	joint publication
MDMP	military decision-making process
METT-TC	mission, enemy, terrain and weather, troops and support available, time available, and civil considerations (mission variables)
MLRS	multiple launch rocket system

NAI	named area of interest
NGIC	National Ground Intelligence Center
OAKOC	observation and fields of fire, avenues of approach, key terrain, obstacles, and cover and concealment (military aspects of terrain)
OE	operational environment
OPORD	operation order
PIR	priority intelligence requirement
PMESII-PT	political, military, economic, social, information, infrastructure, physical environment, and time (operational variables)
S-2	battalion or brigade intelligence staff officer
S-3	battalion or brigade operations staff officer
SOP	standard operating procedure
TAI	target area of interest
U.S.	United States

SECTION II – TERMS

Army special operations forces

Those Active and Reserve Component Army forces designated by the Secretary of Defense that are specifically organized, trained, and equipped to conduct and support special operations. (JP 3-05)

attack guidance matrix

A targeting product approved by the commander, which addresses the how and when targets are engaged and the desired effects. (ATP 3-60)

battle damage assessment

The estimate of damage composed of physical and functional damage assessment, as well as target system assessment, resulting from the application of lethal or nonlethal military force. (JP 3-0)

combat assessment

The determination of the effectiveness of force employment during military operations. (JP 3-60)

combat information

Unevaluated data, gathered by or provided directly to the tactical commander which, due to its highly perishable nature or the criticality of the situation, cannot be processed into tactical intelligence in time to satisfy the user's tactical intelligence requirements. (JP 2-01)

critical capability

A means that is considered a crucial enabler for a center of gravity to function as such and is essential to the accomplishment of the specified or assumed objective(s). (JP 5-0)

critical requirement

An essential condition, resource, or means for a critical capability to be fully operational. (JP 5-0)

critical vulnerability

An aspect of a critical requirement which is deficient or vulnerable to direct or indirect attack that will create decisive or significant effects. (JP 5-0)

defensive operation

An operation to defeat an enemy attack, gain time, economize forces, and develop conditions favorable for offensive or stability operations. (ADP 3-0)

fusion

(Army) Consolidating, combining, and correlating information together. (ADP 2-0)

high-payoff target

A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. (JP 3-60)

high-payoff target list

A prioritized list of high-payoff targets by phase of the operation. (FM 3-09)

high-value target

A target the enemy commander requires for the successful completion of the mission. (JP 3-60)

identity intelligence

The intelligence resulting from the processing of identity attributes concerning individuals, groups, networks, or populations of interest. (JP 2-0)

indicator

In intelligence usage, an item of information which reflects the intention or capability of an adversary to adopt or reject a course of action. (JP 2-0)

information

In the context of decision making, data that has been organized and processed in order to provide context for further analysis. (ADP 6-0)

information operations

The integrated employment, during military operations, of information-related capabilities in concert with other lines of operation to influence, disrupt, corrupt, or usurp the decision-making of adversaries and potential adversaries while protecting our own. (JP 3-13)

intelligence analysis

The process by which collected information is evaluated and intgrated with existing information to facilitate intelligence production. (ADP 2-0)

intelligence estimate

The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view of determining the courses of action open to the enemy or adversary and the order of probability of their adoption. (JP 2-0)

knowledge

In the context of decision making, information that has been analyzed and evaluated for operational implications. (ADP 6-0)

large-scale combat operations

Extensive joint combat operations in terms of scope and size of forces committed, conducted as a campaign aimed at achieving operational and strategic objectives. (ADP 3-0)

large-scale ground combat operations

Sustained combat operations involving multiple corps and divisions. (ADP 3-0)

military decision-making process

An iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order. (ADP 5-0)

offensive operation

An operation to defeat or destroy enemy forces and gain control of terrain, resources, and population centers. (ADP 3-0)

operational level of warfare

The level of warfare at which campaigns and major operations are planned, conducted, and sustained to achieve strategic objectives within theaters or other operational areas. (JP 3-0)

relevant information

All information of importance to the commander and staff in the exercise of command and control. (ADP 6-0)

running estimate

The continuous assessment of the current situation used to determine if the current operation is proceeding according to the commander's intent and if the planned future operations are supportable. (ADP 5-0)

stability operation

An operation conducted outside the United States in coordination with other instruments of national power to establish or maintain a secure environment and provide essential governmental services, emergency infrastructure reconstruction, and humanitarian relief. (ADP 3-0)

strategic level of warfare

The level of warfare at which a nation, often as a member of a group of nations, determines national or multinational (alliance or coalition) strategic security objectives and guidance, then develops and uses national resources to achieve those objectives. (JP 3-0)

tactical level of warfare

The level of warfare at which battles and engagements are planned and executed to achieve military objectives assigned to tactical units or task forces. (JP 3-0)

target development

The systematic examination of potential targets and their components, individual targets, and even elements of targets to determine the necessary type and duration of the action that must be exerted on each target to create an effect that is consistent with the commander's specific objective. (JP 3-60)

targeting

The process of selecting and prioritizing targets and matching the appropriate response to them, considering operational requirements and capabilities. (JP 3-0)

threat

Any combination of actors, entities, or forces that have the capability and intent to harm United States forces, United States national interests, or the homeland. (ADP 3-0)

validation

A part of target development that ensures all candidate targets meet the objectives and criteria outlined in the commander's guidance and ensures compliance with the law of war and rules of engagement. (JP 3-60)

vetting

A part of target development that assesses the accuracy of the supporting intelligence to targeting. (JP 3-60)

weaponeering

The process of determining the specific means required to create a desired effect on a given target. (JP 3-60)

References

All URLs accessed on 19 November 2019.

REQUIRED PUBLICATIONS

These documents must be available to intended users of this publication.

DOD Dictionary of Military and Associated Terms. November 2019.

ADP 1-02. *Terms and Military Symbols*. 14 August 2018.

ADP 2-0. *Intelligence*. 31 July 2019.

ADP 3-0. *Operations*. 31 July 2019.

ATP 2-01. *Plan Requirements and Assess Collection*. 19 August 2014.

ATP 2-01.3. *Intelligence Preparation of the Battlefield*. 01 March 2019.

FM 1-02.1. *Operational Terms*. 21 November 2019.

FM 2-0. *Intelligence*. 06 July 2018.

FM 3-0. *Operations*. 06 October 2017.

JP 3-60. *Joint Targeting*. 28 September 2018.

RELATED PUBLICATIONS

These documents contain relevant supplemental information.

JOINT AND DEPARTMENT OF DEFENSE PUBLICATIONS

Most joint publications are available online: https://www.jcs.mil/Doctrine/.

JP 2-0. *Joint Intelligence*. 22 October 2013.

JP 2-01. *Joint and National Intelligence Support to Military Operations*. 05 July 2017.

JP 3-0. *Joint Operations*. 17 January 2017.

JP 3-01. *Countering Air and Missile Threats.* 21 April 2017.

JP 3-05. *Special Operations*. 16 July 2014.

JP 3-13. *Information Operations*. 27 November 2012.

JP 3-15.1. *Counter-Improvised Explosive Device Activities*. 17 July 2018.

JP 5-0. *Joint Planning*. 16 June 2017.

ARMY PUBLICATIONS

Most Army doctrinal publications are available online: https://armypubs.army.mil/.

ADP 3-05. *Army Special Operations*. 31 July 2019.

ADP 3-07. *Stability*. 31 July 2019.

ADP 3-90. *Offense and Defense*. 31 July 2019.

ADP 4-0. *Sustainment*. 31 July 2019.

ADP 5-0. *The Operations Process*. 31 July 2019.

ADP 6-0. *Mission Command: Command and Control of Army Forces.* 31 July 2019.

AR 380-28. *Army Sensitive Compartmented Information Security Program*. 13 August 2018.

ATP 2-19.1. *(U) Echelons Above Corps Intelligence Organizations (S).* 17 December 2015.

ATP 2-19.3. *Corps and Division Intelligence Techniques*. 26 March 2015.

ATP 2-19.4. *Brigade Combat Team Intelligence Techniques*. 10 February 2015.

ATP 2-22.2-1. *Counterintelligence Volume I: Investigations, Analysis and Production, and Technical Services and Support Activities (U)*. 11 December 2015.

ATP 2-22.6-2. *(U) Signals Intelligence Volume II: Reference Guide*. 20 June 2017.

ATP 2-22.9. *Open-Source Intelligence*. 15 August 2019.

ATP 2-22.82. *Biometrics-Enabled Intelligence (U)*. 02 November 2015.

ATP 2-91.8. *Techniques for Document and Media Exploitation*. 05 May 2015.

ATP 3-11.36. *Multi-Service Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Planning*. 24 September 2018.

ATP 3-11.37. *Multi-Service Tactics, Techniques, and Procedures for Chemical, Biological, Radiological, and Nuclear Reconnaissance and Surveillance*. 25 March 2013.

ATP 3-21.51. *Subterranean Operations*. 01 November 2019.

ATP 3-39.10. *Police Operations*. 26 January 2015.

ATP 3-39.20. *Police Intelligence Operations*. 13 May 2019.

ATP 3-39.30. *Security and Mobility Support*. 30 October 2014.

ATP 3-60. *Targeting*. 07 May 2015.

ATP 3-90.4. *Combined Arms Mobility*. 08 March 2016.

ATP 3-90.8. *Combined Arms Countermobility Operations*. 17 September 2014.

ATP 3-90.37. *Countering Improvised Explosive Devices*. 29 July 2014.

ATP 4-32. *Explosive Ordnance Disposal (EOD) Operations*. 30 September 2013.

ATP 4-32.1. *Explosive Ordnance Disposal (EOD) Group and Battalion Headquarters Operations*. 24 January 2017.

ATP 5-0.1. *Army Design Methodology*. 01 July 2015.

FM 2-22.3. *Human Intelligence Collector Operations*. 06 September 2006.

FM 3-01. *U.S. Army Air and Missile Defense Operations*. 02 November 2015.

FM 3-04. *Army Aviation*. 29 July 2015.

FM 3-09. *Field Artillery Operations and Fire Support*. 04 April 2014.

FM 3-11. *Chemical, Biological, Radiological, and Nuclear Operations*. 23 May 2019.

FM 3-12. *Cyberspace and Electronic Warfare Operations*. 11 April 2017.

FM 3-13. *Information Operations.* 06 December 2016.

FM 3-14. *Army Space Operations*. 30 October 2019.

FM 3-34. *Engineer Operations*. 02 April 2014.

FM 3-39. *Military Police Operations*. 09 April 2019.

FM 3-53. *Military Information Support Operations*. 04 January 2013.

FM 3-55. *Information Collection*. 03 May 2013.

FM 3-57. *Civil Affairs Operations*. 17 April 2019.

FM 3-63. *Detainee Operations*. 28 April 2014.

FM 4-02. *Army Health System*. 26 August 2013.

FM 6-0. *Commander and Staff Organization and Operation*s. 05 May 2014.

FM 6-02. *Signal Support to Operations*. 13 September 2019.

FM 6-27. *The Commander's Handbook on the Law of Land Warfare*. 07 August 2019.

OTHER PUBLICATIONS

ICD 203. *Analytic Standards.* 02 January 2015. Available online: https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives.

ICD 206. *Sourcing Requirements for Disseminated Analytic Products*. 22 January 2015. Available online: https://www.dni.gov/index.php/what-we-do/ic-related-menus/ic-related-links/intelligence-community-directives.

SOURCES USED

Defense Intelligence Agency. *Analytic Design: Analytic Tradecraft Guidance from the DI Research Director*. Available by contacting the DI Analytic Development Office via email at DIA_Tradecraft@coe.ic.gov.

Paul, Richard and Linda Elder. *The Miniature Guide to Critical Thinking: Concepts and Tools*. 2014. Dillon Beach, CA: Foundation for Critical Thinking. Available online: http://www.criticalthinking.org/.

Elder, Linda and Richard Paul. *The Thinker's Guide to Analytic Thinking*. 2017. Dillon Beach, CA: Foundation for Critical Thinking. Available online: http://www.criticalthinking.org/.

PRESCRIBED FORMS

This section contains no entries.

REFERENCED FORMS

Unless otherwise indicated, DA forms are available on the Army Publishing Directorate website: https://armypubs.army.mil/.

DA Form 2028. *Recommended Changes to Publications and Blank Forms*.

This page intentionally left blank.

Index

Entries are by paragraph number unless indicated otherwise.

A

abductive reasoning. *See* reasoning, types of.

ACH. *See* contrarian structured analytic techniques.

action-metrics. *See* analysis validation.

activities matrix. *See* tool.

all-source analysis, 1-7, 1-10–1-14

all-source analytical element, 1-7, 1-8, 1-10, 1-13, 1-34

all-source analytical task, 3-1–3-5
- generate intelligence knowledge, 3-1, 3-2, 3-6
- perform IPB, 3-1, 3-2, 3-8
- perform situation development, 3-1, 3-2, 3-12, 3-13
- provide intelligence support to information operations, 3-16
- provide intelligence support to targeting, 3-14, 3-15
- provide warnings, 3-1, 3-2, 3-10, 3-11

all-source production, 1-10–1-14

analogical reasoning. *See* reasoning, types of.

analysis,1-1, 1-2. *See also* intelligence analysis; threat.

analysis, across the echelons, 1-33, 1-34, 7-3, 7-4
- battalion, 1-7, 2-6, 2-8, 2-22, 7-2, 7-11
- BCT, 1-7, 1-8, 2-6, 2-8, 2-15, 2-18, 7-10, 8-3, 8-5, F-22, F-31
- corps, 1-7, 1-14, 3-4, 6-23, 7-4, 7-8, 8-3, 8-10, 8-11
- division, 1-7, 2-6, 2-8, 2-15, 2-18, 4-7, 7-9, 8-8, 8-9
- national and joint, 7-5
- theater army, 1-7, 3-4, 7-6–7-8

analysis of competing hypotheses. *See* ACH.

analysis validation
- analytic tradecraft standards, C-2–C-14
- analytical rigor, 2-17, 2-18, B-4, C-2, C-15 (table C-1, action-metrics), E-10

analytic design
- collaboration during, 9-12
- managing long-term analytical assessments, 9-2, 9-4, 9-13
- results of, 9-13

analytic design, steps of, 9-4
- step 1, frame the question/issue, 9-5
- step 2, review and assess knowledge, 9-6
- step 3, review resources, 9-7
- step 4, select the analytic approach/methodology and plan project, 9-8
- step 5, develop knowledge, 9-9
- step 6, perform analysis, 9-10
- step 7, evaluate analysis, 9-11, 9-13

analytic problem, 2-8, 5-15, 6-19
- familiarity with, 2-10
- framing of, 2-5, 9-15 (table 9-1)
- solving, 4-6

analytic standards, 1-27, C-1

analytic technique. *See also* structured analytic techniques.
- using, 2-9, 2-16

analytic tradecraft standards, 1-27 (figure 1-4), 2-2. *See also* analysis validation.

analytical judgments, 5-37, 6-6 (table 6-2), C-1
- change to/consistency of, C-12
- confidence in/credibility in, 5-32, 5-38 (table 5-11), C-3–C-5

analytical judgments (*continued*)
- forming, 2-5, 4-3, 5-27

analytical pitfalls, 1-26
- avoiding, B-30
- biases, B-36–B-41
- logic fallacies, B-32–B-35

analytical rigor. *See* analysis validation.

Army design methodology, 3-2, 9-5, 9-14

Army strategic roles, 1-35, 5-38, 7-1. *See also* intelligence requirements.
- shape OEs, 1-45
- prevent conflict, 1-45
- prevail in large-scale ground combat, 1-37
- consolidate gains, 1-45

association matrix. *See* tool.

automation systems, 1-11, 4-7, E-1, F-26
- DCGS-A, 4-7, A-4, A-5, E-1

B

basic structured analytic techniques, 5-1, 5-2
- chronologies, 5-1, 5-7-5-10
- event mapping 5-1, 5-24–5-26
- event tree 5-1, 5-22, 5-23
- link analysis, 5-1, 5-18–5-21
- matrices, 5-1, 5-11–5-14
- sorting, 5-1, 5-3–5-6
- weighted ranking, 5-1, 5-15–5-17

basic thinking abilities, 1-16, 4-1, B-6
- information ordering, 1-16, B-7
- pattern recognition, 1-16, B-8
- reasoning, 1-16, B-6, B-9–B-11

battalion level. *See* analysis, across the echelons.

battle damage assessment (BDA), A-4, F-50–F-56

Entries are by paragraph number unless indicated otherwise.

BCT level. *See* analysis, across the echelons.

bias. *See also* analytical pitfalls.
 assimilation and confirmation biases, 5-33

brainstorming. *See* imaginative structured analytic techniques.

brigade combat team. *See* BCT.

C

collaboration, 1-25, 1-26
 across the echelons, 1-33, 1-43
 between intelligence analysis and collection management, 1-30, 1-32
 during the analytic design process, 9-12

collection management, A-1
 and intelligence support to targeting, 3-15, F-56
 in relation to intelligence analysis, 1-28–1-32
 performed by functional elements, 7-12

combat information. *See* information.

complementary intelligence capability
 as a single-source intelligence capability, 1-7, 1-9

conclusion, accurate. *See* analysis validation, analytical rigor.

confidence level
 assessing, 2-17
 expressing, C-7

contrarian structured analytic techniques, 6-1, 6-2
 ACH, 6-2–6-5, 6-16
 devil's advocacy, 4-7, 6-2, 6-6–6-9, C-15 (table C-1)
 high-impact/low-probability analysis, 6-2, 6-11–6-14, 6-18
 team A/team B, 4-7, 6-2, 6-9, 6-10, C-15 (table C-1)

convergent thinking. *See* imaginative structured analytic techniques, brainstorming.

corps level. *See* analysis, across the echelons.

creative thinking, 1-16, 2-1, 4-1
 described, B-13

critical capability. *See* imaginative structured analytic techniques, functional analysis.

critical factors analysis (CFA). *See* imaginative structured analytic techniques, functional analysis.

critical requirement. *See* imaginative structured analytic techniques, functional analysis.

critical thinking, 1-24, 1-26, 4-1, B-12–B-16

critical thinking, application tools
 elements of thought, 1-24, B-16–B-18, B-20, B-30
 essential intellectual traits, 1-24, B-16, B-21–B-30
 intellectual standards, 1-24, B-16, B-19, B-20, B-30

critical vulnerability. *See* imaginative structured analytic techniques, functional analysis.

D

DCGS-A. *See* automation systems.

deductive reasoning. *See* reasoning, types of.

defensive operations. *See* large-scale ground combat operations.

diagnostic structured analytic techniques, 5-27
 indicators/signposts of change 5-27, 5-36–5-39
 key assumptions check 5-27–5-31
 quality of information check 5-27, 5-32–5-35

Distributed Common Ground System-Army. *See* DCGS-A.

divergent thinking. *See* imaginative structured analytic techniques, brainstorming.

division level. *See* analysis, across the echelons.

E

echelons, 1-31, 1-43. *See also* analysis, across the echelons.

echelons (*continued*)
 and multi-domain operations, 8-1
 and the analytical focus, 8-3

elements of thought. *See* critical thinking, application tools.

essential intellectual traits. *See* critical thinking, application tools.

F

fallacies. *See* analytical pitfalls.

fight for intelligence, 1-37, 1-42
 during large-scale ground combat operations, 1-39, 8-3

functional analysis, 3-6. *See also* imaginative structured analytic techniques.

fusion (as part of all-source analysis and production), 1-11

G

generate intelligence knowledge, 1-45 (table 1-2), 9-14
 as an all-source analytical task. *See* all-source analytical task.
 tasks, 3-7
 to assess the threat, D-3

H

high-payoff target list, F-8, F-19

hypothesis, 2-7, 2-17
 ACH, 6-2–6-5, 6-16
 alternative, 6-7, 9-12, 9-13, C-9
 comparing, 6-9, 6-10
 generating, 2-5, 4-3, 5-3 (table 5-1), 5-4, 5-38, 6-12, 6-16
 reviewing, 5-23–5-26
 validating, 2-18

I

identity intelligence, 1-9, 3-5, 7-5. *See also* intelligence, categories of.

imaginative structured analytic techniques, 6-19
 brainstorming, 6-19–6-22
 functional analysis, 6-19, 6-23–6-25
 outside-in thinking 6-19, 6-26–6-28

Entries are by paragraph number unless indicated otherwise.

imaginative structured analytic techniques (*continued*)
red hat/team analysis, 6-19, 6-29–6-31
indicator, F-47
defined, 3-11
threat, 1-31, 3-13
inductive reasoning. *See* reasoning, types of.
information, 1-1
accuracy, 2-7, 2-12–2-16
combat information, 1-14, 1-37 (table 1-1), 2-12, F-22
corroboration of, 1-13, 2-12, 2-13, 2-16, C-7
refining. *See* fusion.
relevancy, 2-8, 2-12
relevant information, 2-4, 2-9
reliability, 2-7, 2-12–2-16
information collection 1-4, 1-28, 1-29, 1-31, 1-37, B-2
information collection plan, F-8
information operations. *See* all-source analytical task.
information ordering. *See* basic thinking abilities.
INSCOM, 7-5, D-2
intellectual standards. *See* critical thinking, application tools.
intelligence
categories of, 2-19
support to information operations, 3-16
support to targeting, 3-14, 3-15
intelligence analysis
as discussed in ADP 2-0, 1-6, 1-7
automation support, A-1–A-3
comprises, 1-7
conducting, 1-15, 1-16
crosswalking with analytic design, 9-14, 9-15
defined, 1-3
effective analysis, six aspects of, 1-16–1-27
facilitating situational understanding, 1-12, 1-44, 2-19, A-2
large-scale ground combat operations, effect on, 1-37, 1-39
support to functional elements, 7-12
unique aspects of, 1-5
intelligence analysis process, 2-1–2-3, 2-6
analyze phase, 2-4, 2-9–2-15, 8-6 (table 8-1), 8-9 (table 8-2), 8-11 (table 8-3)
and long-term analytical assessment, 9-3
integrate phase, 2-4, 2-16–2-18, 8-6 (table 8-1), 8-9 (table 8-2), 8-11 (table 8-3)
produce phase, 2-4, 2-19–2-22, 8-6 (table 8-1), 8-9 (table 8-2), 8-11 (table 8-3)
screen phase, 2-4, 2-7, 2-8, 8-6 (table 8-1)
intelligence analyst. *See also* analytical judgments.
and mission-specific requirements, 7-12
avoiding analytical pitfalls. *See* analytical pitfalls.
challenges, 1-4, 1-17, 1-18, 1-37
cognitive considerations for, B-2–B-5
doctrinal concepts, understanding of, 1-39
employing analytic tradecraft standards, C-2
understanding the threat, D-2
intelligence architecture, 1-34
Intelligence Community Directive (ICD) 203. *See* analytic standards.
Intelligence Community Directive (ICD) 206, C-4
intelligence discipline
as a single-source intelligence capability, 1-7, 1-9
intelligence preparation of the battlefield. *See* IPB.
intelligence product, 2-19, 2-20, E-2
analytical support to orders and briefings, E-20
Annex B (Intelligence) to the operation order, E-3, E-4
graphic intelligence summary, E-12, E-13
intelligence estimate, E-3, E-5, E-6
intelligence report, E-14
intelligence running estimate, E-3, E-7–E-9
intelligence product (*continued*)
intelligence summary, E-11
periodic intelligence report, E-15–E-17
supplementary intelligence report, E-15, E-18, E-19
intelligence requirements (associated with the Army strategic roles), 7-13
shape OEs, 7-14
prevent conflict, 7-15
prevail in large-scale ground combat, 7-16–7-20
consolidate gains, 7-21–7-26
intelligence warfighting function, 1-3, 1-30, 3-2, 7-3, 7-17, A-4
IPB, 3-7, 9-14
and targeting, F-9
as an all-source analytical task. *See* all-source analytical task.
assessing the threat, D-3, D-4
performed by functional elements, 7-12
situation development and, 3-12, 3-13
steps of, 3-9

K

knowledge, defined, 1-1

L

large-scale combat operations, defined, 1-36
large-scale ground combat operations, 1-35–1-37, 7-2. *See also* Army strategic role; fight for intelligence; intelligence requirements.
and consolidating gains, 7-22
and the threat, D-1–D-5
defensive operations in, 7-17, 7-19, 7-20
offensive operations in, 7-17, 7-18
levels of warfare, 7-4
operational, 1-27, 1-38, 3-4, 7-4, 8-4, 8-10, 8-11, 9-1
strategic, 1-38, 2-13, 3-4, 7-4, 9-1
tactical, 1-14, 1-27, 1-38, 2-13, 7-4, 8-4–8-11

Entries are by paragraph number unless indicated otherwise.

link analysis. *See* basic structured analytic techniques.

link diagram. *See* tool.

long-term analytical assessment, 3-4
  described, 9-1, 9-3
  managing. *See* analytic design.

M

MDMP, 3-2, D-3
  and analytical support, 3-8, 3-9
  employing, 9-14
  input to, 6-30

method (pertaining to analysis), 4-2

military decision-making process. *See* MDMP.

multi-domain operations, 1-39, 1-44, 8-1, 8-11 (table 8-3)

N

National Ground Intelligence Center (NGIC), 1-7, 7-4, 7-5, D-2

national to tactical intelligence, 1-25

O

OE
  assessing the threat, D-5
  intelligence assessments about, E-1, E-3
  relevent aspects of, 3-12
  shaping, 3-2, 4-4. *See also* Army strategic role; intelligence requirements.
  visualizing, 1-2, 3-1, 3-8, 9-15 (table 9-1)

offensive operations. *See* large-scale ground combat operations.

operational art, 1-39

operational environment. *See* OE.

operational framework, 1-39

operational level of warfare. *See* levels of warfare.

P

pattern analysis plot sheet. *See* tool.

pattern recognition. *See* basic thinking abilities.

peer threat, 1-44, 1-45 (table 1-2), 8-3, D-1, D-2, D-7
  countering information collection, 1-37

explained, 1-38

PIR, 2-6, 2-8, 2-22
  answering, 2-21, 4-4, 7-3
  information relevant to, 2-7
  understanding, 2-5

position of relative advantage, 1-39, 1-42, 1-43, 3-2

priority intelligence requirement. *See* PIR.

R

reasoning, 1-16, B-6, B-9
  types of, B-10, B-11
  using, 2-9, 2-16

relevant information. *See* information.

S

single-source analysis, 1-7–1-9

single-source analytical elements, 1-7, 1-8

situation development, 8-2
  as an all-source analytical task. *See* all-source analytical task.

situational understanding. *See* intelligence analysis.

stability operations, 7-21, 7-23–7-26

strategic level of warfare. *See* levels of warfare.

structured analytic techniques. *See also* basic structured analytic techniques; contrarian structured analytic techniques; diagnosic, structured analytic techniques; imaginative structured analytic techniques.
  applying, 4-3–4-7

T

tactical level of warfare. *See* levels of warfare.

target detection. *See* targeting methodology, detect.

target development, F-30–F-32

target value analysis, F-10–F-17

targeting. F-1–F-4. *See also* all-source analytical task.

targeting methodology, F-6, F-7
  decide, F-8–F-32
  detect, F-33–F-38
  deliver, F-39–F-46
  assess, F-47–F-58

technique (pertaining to analysis), 4-2

theater army level. *See* analysis, across the echelons.

threat
  analysis by warfighting function, D-6–D-8
  and analysis, 1-3, 3-13
  and critical factors analysis (CFA), 6-23–6-25
  and large-scale ground combat operations, D-1–D-5
  categorizing and understanding, 6-29–6-31
  defined, D-1
  equipment, D-9, D-10
  intelligence assessments, about, E-1, E-3

threat intentions matrix. *See* tool.

time event chart.*See* tool.

timeline. *See* tool.

tool (pertaining to analysis), 4-2
  activities matrix, 5-11, 5-21
  association matrix, 5-11, 5-21
  link diagram, 5-21
  pattern analysis plot sheet, 5-5, 5-6
  threat intentions matrix, 5-11, 5-14
  time event chart, 5-10
  timeline, 5-9

U

U.S. Army Intelligence and Security Command. *See* INSCOM.

W

warning intelligence, 1-45 (table 1-2). *See also* intelligence, categories of.
  as an all-source analytical task. *See* all-source analytical task.

window of opportunity, 1-39, 1-42, 1-43

ATP 2-33.4
10 January 2020

By Order of the Secretary of the Army:

JAMES C. MCCONVILLE
General, United States Army
Chief of Staff

Official:

KATHLEEN S. MILLER
Administrative Assistant
to the Secretary of the Army
1936404

DISTRIBUTION:
Active Army, Army National Guard, and United States Army Reserve: To be distributed in accordance with the initial distrubution number (IDN) 111117 requirements for ATP 2-33.4.

This Page Is Intentionally Left Blank

USMC

MCTP 2-10B
(Formerly MCWP 2-3)

MAGTF Intelligence Production and Analysis

U.S. Marine Corps

DISTRIBUTION STATEMENT A: Approved for public release; distribution is unlimited.

PCN 147 000012 00

USMC

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, D.C. 20350-3000

4 April 2018

CHANGE 1 to MCTP 2-10B
MAGTF Intelligence Production and Analysis

1. This publication has been edited to ensure gender neutrality of all applicable and appropriate terms, except those terms governed by higher authority. No other content has been affected.

2. File this transmittal sheet in the front of this publication.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

Robert S. Walsh

ROBERT S. WALSH
Lieutenant General, U.S. Marine Corps
Deputy Commandant for Combat Development and Integration

Publication Control Numbers:
Publication: 147 000012 00
Change: 147 000012 01

CD&I (C 116)

2 May 2016

ERRATUM

to

MCWP 2-3

MAGTF INTELLIGENCE PRODUCTION AND ANALYSIS

1. Change all instances of MCWP 2-3, *MAGTF Intelligence Production and Analysis*, to MCTP 2-10B, *MAGTF Intelligence Production and Analysis.*

2. Change PCN 143 000076 00 to PCN 147 000012 00

3. File this transmittal sheet in the front of this publication.

PCN 147 000012 80

MCCDC (C 42)
13 Jul 2004

E R R A T U M

to

MCWP 2-3

MAGTF INTELLIGENCE PRODUCTION AND ANALYSIS

1. Change the publication short title to read “MCWP 2-3” (vice MCWP 2-12).

PCN 143 000076 80

DEPARTMENT OF THE NAVY
Headquarters United States Marine Corps
Washington, D.C. 20380-1775

27 September 2001

FOREWORD

Marine Corps Doctrinal Publication 2, *Intelligence*, and Marine Corps Warfighting Publication (MCWP) 2-1, *Intelligence Operations,* provide the doctrine and higher order tactics, techniques, and procedures for intelligence operations. MCWP 2-12, *MAGTF Intelligence Production and Analysis,* complements and expands upon this information by detailing doctrine, tactics, techniques, and procedures for the conduct of intelligence production and analysis in support of the Marine air-ground task force (MAGTF).

The target audience of this publication is intelligence personnel responsible for the planning and execution of intelligence production and analysis operations.

The MCWP 2-12 provides the information needed by Marines to understand, plan, and execute intelligence production and analysis to support MAGTF operations. It describes intelligence doctrinal fundamentals, the nature of analytical thinking, intelligence preparation of the battlespace, and intelligence support to targeting. This publication also discusses intelligence command and control, communications and information systems support, intelligence products and formats, planning, execution, and training.

Reviewed and approved this date.

BY DIRECTION OF THE COMMANDANT OF THE MARINE CORPS

EDWARD HANLON, JR.
Lieutenant General, U.S. Marine Corps
Commanding General
Marine Corps Combat Development Command

DISTRIBUTION: 143 000076 00

MAGTF INTELLIGENCE PRODUCTION AND ANALYSIS

TABLE OF CONTENTS

Chapter 1 Fundamentals

What is Intelligence Production and Analysis? 1-1
- Intelligence Functions 1-1
- Intelligence Cycle. 1-1

Production Steps. 1-3
- Preparation for Analysis. 1-3
- Analytical Process 1-4
- Product Preparation 1-5

Operations and Command and Control 1-5
Production and Analysis Company, Intelligence Battalion 1-5

Chapter 2 Organizations and Responsibilities

MAGTF Commander 2-1
- Focus the Analytical and Production Effort. 2-1
- Participate in the Analytical Process 2-1
- Evaluate the Product 2-1

Marine Expeditionary Force Command Element Intelligence Officer 2-2
Intelligence Battalion Commander 2-2
- Responsibilities in Garrison 2-2
- Responsibilities During Operations 2-2

Intelligence Battalion 2-3
Production and Analysis Company 2-3
- All-Source Fusion Platoon 2-3
- Organization for Support 2-3

Production and Analysis Cell. 2-4
- Tasks 2-4
- Organization. 2-4
- Supporting Organizations. 2-6

Principal Staff Officers 2-7
Unit Intelligence Officer 2-8
Organic Intelligence Sections 2-8
Organization for Employment 2-8
- Combat Intelligence Center 2-8
- Command and Control 2-9
- Senior Marine Expeditionary Force Intelligence Staff Officers 2-10
- Intelligence Production Support Flow 2-10
- Organization for Combat Operations 2-10

Communications and Information Systems 2-12
Basic Requirements 2-12
Information Systems 2-13

Chapter 3 Filtering, Recording, and Evaluating

Section I Filtering

Filtering Criteria 3-2
Subject Matter 3-2
Location 3-2
Time of Occurrence 3-2
Redundancy 3-2
Methodology 3-2
Manual Filtering 3-2
Automated Filtering 3-2

Section II Recording

Methodology 3-3
Recording Tools 3-3
Intelligence Journal 3-4
Enemy Situation Map 3-5
Intelligence Workbook 3-6
Order of Battle Files 3-6
Target Files 3-11
Tools Automation 3-11

Section III Evaluation

Relevance 3-12
Reliability 3-12
Accuracy 3-12
Evaluation Rating System 3-12
Reliability Evaluation Codes 3-13
Accuracy Evaluation Codes 3-13

Chapter 4 Analytical Thinking

Section I Analytical Process

Analysis 4-1
Synthesis 4-2
Estimation 4-2

Section II Analytic Problem Solving

Analytical Theories 4-3
Proposition or Premise 4-3
A Priori 4-4
Applied Logic 4-4
Facts 4-4
Opinions 4-4
Inferences 4-4
Reasoning 4-5
Deductive 4-5
Inductive 4-6
Tests of Truth 4-7
Correspondence Test of Truth 4-7
Coherence Test of Truth 4-7
Pragmatic Test of Truth 4-8

Section III Pitfalls of Analysis

Logical Fallacies 4-9
Omission 4-9
Assumption 4-11
Biases 4-12
Cultural 4-12
Organizational 4-13
Personal 4-13
Cognitive 4-13

Section IV Decisionmaking

Analytical 4-15
Intuitive 4-15
Comparison 4-15

Chapter 5 Intelligence Preparation of the Battlespace

Section I Step 1—Define the Battlespace Environment

Identify Significant Characteristics of the Environment 5-2
Identify the Command's Area of Operations and Battlespace Limits 5-2
Area of Influence 5-2
Area of Interest 5-4
Battlespace 5-4
Establish the Area of Interest Limits 5-4
Identify the Detail Required for the Time Available 5-5

Evaluate Existing Intelligence Data Bases and Identify Intelligence Gaps 5-5
Collect the Required Intelligence and Materials. 5-6

Section II Step 2—Describe the Battlespace Effects

Analyze the Battlespace Environment 5-6
Terrain. 5-6
Weather. 5-10
Other Characteristics of the Battlespace. 5-11
Describe the Battlespace Effects on Threat and Friendly Capabilities and Broad Courses of Action. 5-12

Section III Step 3—Evaluate the Threat

Update or Create Threat Models. 5-13
Doctrinal Templates 5-13
Description of Tactics and Options 5-13
Identification of Center(s) of Gravity 5-14
Critical Vulnerabilities 5-14
Identification of Type High-Value Targets 5-14
Identify Threat Capabilities 5-14

Section IV Step 4—Determine Threat Courses of Action

Identify the Threat's Likely Objectives and Desired End State 5-15
Identify the Full Set of Courses of Action Available to the Threat 5-15
Evaluate and Prioritize Each Course of Action 5-17
Develop Each Threat Course of Action in the Amount of Detail Time Allows 5-18
Situation Template 5-18
Description of the Threat's Courses of Action and Options. 5-19
High-Value Targets. 5-21
Identify Initial Intelligence Collection, Production, and Dissemination Requirements 5-22
Event Template. 5-23
Event Matrix 5-24

Section V Decision Support Template

Targeted Areas of Interest. 5-25
Decision Points 5-26
Types. 5-26
Considerations 5-26

Section VI Abbreviated Intelligence Preparation of the Battlespace Process

Work Ahead 5-27
Focus on Essentials 5-28
Stay Objective Oriented 5-28
Minimize Essentials 5-28
Output 5-29
Intelligence Estimate 5-29
Target and Objective Studies 5-29

Chapter 6 Analysis of the Battlespace

Section I Responsibilities

Section II Characteristics of the Battlespace

Section III Terrain Analysis

Responsibilities 6-2
Sources of Information 6-3
Geospatial Factors 6-3
Surface Configuration 6-3
Hydrologic Features 6-3
Vegetation Features 6-4
Surface Materials 6-5
Military Aspects of Terrain Evaluation 6-5
Key Terrain 6-5
Observation and Fields of Fire 6-6
Cover and Concealment 6-6
Obstacles 6-6
Avenues of Approach and Mobility Corridors 6-7

Section IV Hydrographic Analysis

Sources of Information 6-9
Hydrographic Conditions 6-9
Seas, Swells, and Surf 6-9
Tides 6-9
Currents 6-9
Beach Selection Considerations 6-10
Size 6-10
Approaches 6-11
Gradient 6-11
Composition 6-11
Trafficability 6-11

Vegetation 6-11
Natural Obstacles 6-11
Manmade Obstacles 6-12
Exits 6-12

Section V Airspace Analysis

Geospatial Analysis Support 6-13
Airspace Evaluation 6-13
Military Aspects of Terrain Evaluation 6-14
Key Terrain 6-14
Observation and Fields of Fire 6-14
Cover and Concealment 6-14
Obstacles 6-14
Avenues of Approach 6-15
Weather 6-15

Section VI Weather Analysis

Responsibilities 6-15
Weather Effects 6-15
Temperature and Humidity 6-16
Precipitation 6-16
Visibility 6-17
Wind Speed and Direction 6-17
Cloud Conditions 6-18
Atmospheric Pressure 6-18
Weather Forecast and Weather Effects Products 6-18

Section VII Infrastructure Analysis

Sources of Information 6-20
Transportation System 6-20
Highway or Road Network 6-20
Railroad Network 6-21
Port and Harbor Facilities 6-21
Airfields 6-22
Structures and Crossings 6-22
Inland Waterways 6-24
Supply Systems 6-24
Power System or Grid 6-24
Petroleum, Oils, and Lubricants Facilities 6-25
Water 6-25
Telecommunications 6-25

Urban Areas 6-25
Characteristics 6-25
Urban Area Classification 6-25
Evaluation Factors 6-26
Construction Resources 6-26

Section VIII Political, Economic, and Sociological Analysis

Political Intelligence. 6-26
Basic Governmental Principles 6-27
Governmental Operations 6-27
Foreign Policy 6-27
Political Parties. 6-27
Pressure Groups 6-27
Electoral Procedures. 6-28
Subversive Movements 6-28
Criminal and Terrorist Organizations 6-28
Economic Intelligence 6-28
Sources of Economic Intelligence 6-29
Evaluation Factors 6-29
Narcotics and Terrorism. 6-29
Sociological Analysis. 6-29
Population 6-29
Characteristics of the People 6-29
Public Opinion 6-30
Education 6-30
Religion 6-30
Public Welfare 6-30
Narcotics and Terrorism Tolerance 6-30

Chapter 7 Threat Analysis Techniques

Section I Intelligence Preparation of the Battlespace Techniques

Threat Order of Battle 7-1
Order of Battle Factors. 7-1
Analytical Considerations 7-5
Threat Model Development 7-5
Doctrinal Templates. 7-5
Description of Tactics and Options 7-5
Identification of Type High-Value Targets 7-7
Threat Courses of Action Determination. 7-8
Criteria for Testing Threat Courses of Action 7-8
Considerations 7-8
Course of Action Evaluation and Prioritization. 7-9

Course of Action Development 7-9
Course of Action Parts 7-10
Considerations 7-10
Course of Action Key Elements 7-10

Section II Specialized Analytical Techniques

Subsystem Threat Analysis. 7-11
Air Defense. 7-11
Artillery. 7-12
Aviation 7-12
Counterintelligence. 7-13
Command and Control Warfare 7-13
Engineer 7-14
Combat Service Support. 7-15
Pattern Analysis 7-15
Coordinates Register. 7-16
Pattern Analysis Plot Sheet. 7-16
Matrix Analysis. 7-17
Activities Matrix. 7-17
Association Matrix 7-19
Link Analysis 7-19
Indicator List. 7-20

Chapter 8 Target Development and Combat Assessment

Section I Targeting

Targeting Cycle. 8-1
Target Development 8-2
Intelligence Preparation of the Battlespace 8-3
Target Value Analysis 8-3
High-Value and High-Payoff Target Identification 8-3
High-Payoff Target List 8-4
Target Analysis. 8-4
Target System Analysis 8-4
Target Complex Analysis. 8-6
Target Element Analysis. 8-6
Role of the Target Analyst 8-7
Target Analysis Products 8-7
List of Targets. 8-7
No-Strike Target List 8-7
Restricted Target List 8-7
Target File. 8-8
Collection Requirements. 8-8
Target or Objective Studies 8-8

Section II Combat Assessment

Battle Damage Assessment 8-9
Munitions Effects Assessment 8-9
Reattack Recommendations 8-9
Battle Damage Assessment Components 8-10
Physical Damage Assessment 8-10
Functional Damage Assessment 8-11
Target System Assessment 8-12
Responsibilities 8-13
Battle Damage Assessment Methodology 8-14
Battle Damage Assessment Principles 8-14
Objectivity 8-14
Reliability 8-14
Accuracy 8-15
Battle Damage Assessment Reporting 8-15
Reports 8-15
Reporting Methods 8-15

Chapter 9 Intelligence Production

Production Categories 9-1
Deliberate Production 9-1
Immediate Production 9-2
Principles 9-2
Purpose and Use of Intelligence 9-2
Objectivity 9-2
Provision of Integrated and Tailored Products 9-2
Coordination Among Echelons 9-2
Responsibilities 9-2
Management 9-3
Production Cycle 9-3
Define Intelligence Requirements 9-3
Define and Prioritize Intelligence Production Requirements and Tasks 9-3
Develop Intelligence Production Plan and Schedule 9-4
Allocate Resources 9-4
Assign Tasks 9-4
Prepare the Product(s) 9-5
Review and Quality Control 9-5
Approve and Distribute the Product(s) 9-5
Follow Up 9-5
Production Management 9-5
Functions 9-5
Production Managers 9-5
Production Management Elements 9-6

Intelligence Products. 9-6
MAGTF Contingency Intelligence Study. 9-7
Intelligence Estimate and Supporting Studies 9-7
Target or Objective Study. 9-7
Intelligence Summary. 9-7
Intelligence Report 9-7
Briefings 9-8
Organic MAGTF Intelligence Production 9-8
Unit Intelligence Sections. 9-8
Intelligence Direct Support Teams 9-9
Production and Analysis Company, Intelligence Battalion 9-9
External Production Support. 9-9
Department of Defense Support 9-9
National Production Support 9-10
Unified Command Production Support 9-10
Services Production Support. 9-11
Non-Department of Defense Intelligence Production Support. 9-12
Production Support Requests 9-12
Request Process 9-14
Request Format. 9-14
Automated Production Request Procedures 9-14

Chapter 10 Operations

Section I Operational Maneuver From the Sea

Requirements 10-1
Considerations 10-2
Support During Planning 10-2
Support During Execution 10-3

Section II Sustained Operations Ashore

Considerations 10-4
Support During Planning 10-4
Support During Execution 10-4

Section III Military Operations Other Than War

Requirements 10-5
Considerations 10-5
Support During Planning 10-5

MOOTW IPB Requirements 10-6
Define the Battlespace Environment 10-6
Describe the Battlespace Effects 10-6
Evaluate the Threat 10-7
Determine Threat Courses of Action 10-8
MOOTW IPB Products 10-8
Population Status Overlay 10-8
Logistics Sustainability Overlay 10-8
Lines of Communications Overlay 10-8
Key Facilities and Target Overlay 10-10
Coordinates Register and Pattern Analysis Plot Sheet. 10-10

Section IV Joint Operations

Responsibilities 10-11
Marine Corps Component Production and Analysis 10-11
Joint Task Force Headquarters Production and Analysis 10-11
Key Functions 10-11
Support During Planning 10-12
Support During Execution 10-12

Section V Combined Operations

Principles 10-12
Adjustment of National Differences Among Nations 10-12
Unity of Effort Against Common Threat. 10-12
Intelligence Determination and Planning. 10-12
Special Arrangements 10-13
Full Exchange of Intelligence 10-13
Complementary Intelligence Operations 10-13
Combined Intelligence Centers 10-13
Liaison Exchange. 10-13
Foreign Disclosure and Releasability. 10-13
Policies and Procedures 10-13
Security 10-14
Product Format Considerations 10-14
Information Sources. 10-14

Section VI Pre-Crisis Phase

Data Base Management 10-15
Intelligence Reference Library. 10-15
Statement of Intelligence Interest. 10-15
Intelligence Data Bases 10-16

Production 10-16
Contingency Intelligence 10-16
Intelligence Preparation of the Battlespace 10-17
Exercise Intelligence 10-18
Other Intelligence 10-18
Production and Analysis Training 10-18
Individual Training 10-18
Element Training 10-19
Unit Training 10-19
MAGTF Training 10-20

Section VII Warning and Deployment Phase

Initial Production and Analysis 10-20
Determine Initial Requirements 10-20
Assemble and Focus Data Bases 10-20
Develop Initial Estimate and Supporting Studies 10-20
Develop Collection, Production, and Dissemination Requirements 10-21
Production Management 10-21
Standardization of Products 10-21

Section VIII Execution Phase

Production Management 10-21
Support to Current Operations 10-22
Support to Future Operations 10-22
Support to Future Plans 10-23
Support to Targeting 10-23

Appendices

A Intelligence Estimate Format A-1
B Weather Critical Values B-1
C Tactical Indicators C-1
D Battle Damage Assessment Report Format D-1
E MAGTF Intelligence Production Plan Format E-1
F Intelligence Summary Format F-1
G Intelligence Report Format G-1
H Intelligence Information Brief H-1
I Production Requirement and Request for Intelligence Format I-1
J Glossary J-1
K References K-1

Figures

1-1 Intelligence Cycle. 1-1
1-2 Intelligence Cycle in Support of Commander's Decision 1-2
1-3 Intelligence Support to Planning and Decisionmaking 1-6

2-1 Intelligence Battalion Organization 2-3
2-2 IIP Organization. 2-6
2-3 Topographic Platoon Organization 2-6
2-4 CI/HUMINT Company Organization 2-7
2-5 IOC Organization. 2-10
2-6 C2 and Staff Cognizance of Intelligence Production Support Flow 2-11
2-7 Notional MEF CIS Architecture 2-14

3-1 Example of an Intelligence Journal Page. 3-4
3-2 Example of a Unit Workbook Page 3-8
3-3 Example OOB Overlay 3-9
3-4 Sample OOB Record 3-10

5-1 Battlespace Examination 5-3
5-2 AO and AOI. 5-3
5-3 Battlespace Dimensions and Factors 5-4
5-4 Regimental Ground AA 5-7
5-5 Air AAs Overlay 5-8
5-6 Mobility Corridors Grouped to Form an AA. 5-9
5-7 Lines of Communications and Likely Ambush Sites. 5-9
5-8 Combined Obstacle Overlay 5-10
5-9 Doctrinal Template. 5-13
5-10 Combining Doctrine and Battlespace Effects to Develop Threat COAs 5-16
5-11 Enemy COA 1—Counterattack 5-17
5-12 Enemy COA 2—Withdrawal from the Current Position and Set Up Defense on Eastern Shore of River. 5-17
5-13 Counterattack Situation Template with TPLs and HVTs 5-19
5-14 Threat COA Overlay with Text Description 5-20
5-15 Intelligence Synchronization Matrix 5-20
5-16 Intelligence Synchronization Sheet 5-21
5-17 Templated Locations of HVTs for Enemy COA 1 5-22
5-18 Event Template 5-23
5-19 Event Template Development by Comparing and Contrasting Each COA's NAIs and Indicators. 5-24
5-20 Detailed Event Matrix for a Specific NAI 5-25
5-21 Decision Support Template 5-26

6-1 Concealment and Cover Overlay. 6-6
6-2 Weather Forecast Graphic 6-19
6-3 Weather Effects Matrix 6-19

Figures (Continued)

7-1 Threat Synchronization Matrix 7-6
7-2 Threat Model with Target Value Matrix 7-7
7-3 Coordinates Register 7-16
7-4 Pattern Analysis Plot Sheet 7-17
7-5 Activities Matrix 7-18
7-6 Association Matrix 7-19
7-7 Link Diagram 7-19

8-1 Joint Targeting Cycle and D3A 8-2
8-2 Target System, Components, and Elements 8-5
8-3 Combat Assessment Process 8-9
8-4 Phase I BDA or PDA Information Flow 8-10
8-5 Phase II BDA or FDA Information Flow 8-12
8-6 Phase III BDA or TSA Information Flow 8-13

9-1 IPR Flow 9-13

10-1 Population Status Overlay 10-9
10-2 Logistics Sustainability Overlay 10-9
10-3 Sewers and Subterranean Overlay 10-10

Tables

2-1 P&A Company Organization for Support 2-3
2-2 MEF CE's CIC Key Elements 2-9
2-3 Senior Intelligence Staff Officers 2-11

6-1 Landform Elevations 6-3

8-1 Example of Combat Strength Assessment 8-11

CHAPTER 1. FUNDAMENTALS

Marine air-ground task force (MAGTF) intelligence provides decision-makers with an understanding of the battlespace. This understanding encompasses a sophisticated knowledge of the threat and the physical, political, economic, and cultural environment in the area of operations (AO). That knowledge is developed through intelligence production and analysis (P&A).

What is Intelligence Production and Analysis?

P&A is the filtering, recording, evaluating, and analyzing of information, and product preparation of developed intelligence.

Analysis is a process that involves sifting and sorting evaluated information to isolate significant elements related to the mission of the command, determining the significance of the information relative to information and intelligence already known, and drawing deductions about the probable meaning of the evaluated information. Production is the conversion of evaluated material or information into intelligence. All sources of information are integrated, analyzed, evaluated, and interpreted to prepare intelligence products or all-source intelligence in support of known or anticipated user requirements. Production or the process of analysis and synthesis is the most important action in developing usable intelligence for the commander. Production, the fourth step in the intelligence cycle, helps forecast the effect gathered intelligence will have on the commander's ability to accomplish the mission.

Intelligence Functions

To support the commander, MAGTF intelligence organizations carry out six intelligence functions of which the P&A function is an integral part. In each function, data is synthesized into intelligence that provides a portion of the knowledge from which the commander can reach an acceptable level of understanding before making a decision. Intelligence answers the all-important question: "What effect does all this have on our ability to accomplish the mission?" Intelligence organizations—

- Support the commander's estimate.
- Develop the situation.
- Provide indications and warning.
- Support force protection.
- Support targeting.
- Support combat assessment.

Intelligence Cycle

The intelligence cycle consists of a series of related activities that translate the need for intelligence about a particular aspect of the battlespace or threat into a knowledge-based product that is provided to the commander for use in the decision-making cycle (see fig. 1-1).

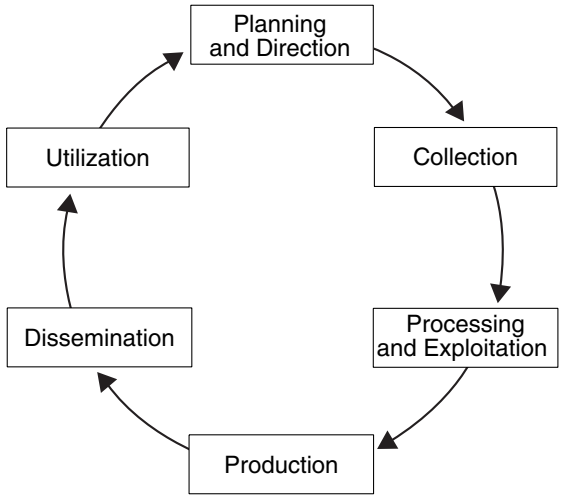


Figure 1-1. Intelligence Cycle.

Planning and Direction

The initial step identifies intelligence needs and develops a plan for satisfying those needs.

Collection

In this step, information used to generate intelligence is drawn from—

- Intelligence data that is derived from assets primarily dedicated to intelligence collection (e.g., imagery systems, electronic intercept equipment, human intelligence sources).
- Sensor data that is derived from sensors whose primary mission is surveillance or target acquisition, air surveillance radar, counterbattery radar, and remote ground sensors.
- Combat data that is derived from reporting by operational units.

Processing and Exploitation

This step converts collected information into an understandable form suitable for the production of intelligence. Processing is accomplished during collection or production. Data collected in a form suitable for analysis is processed automatically during collection. Other types of data require extensive processing, which can affect the timeliness and accuracy of the resulting information. Because processing and production are often accomplished by the same organization, production management generally encompasses processing functions that are required to convert raw data into a usable format. Examples of processing and exploitation include—

- Film processing.
- Document translation.
- Signals intercept.

Production

Production, the fourth step, converts data into intelligence and creates the knowledge (see fig. 1-2) needed for the planning and execution of operations. The intelligence must deliver knowledge, in

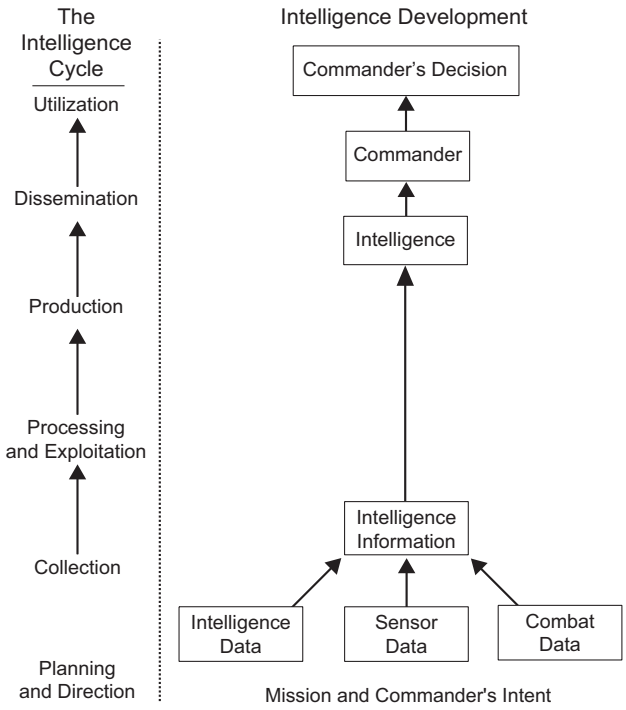


Figure 1-2. Intelligence Cycle in Support of Commander's Decision.

context, in time, and in a form usable in the decisionmaking process. In any situation, providing timely, accurate, and relevant intelligence to commanders and planners is a critical consideration. Production (analysis and synthesis) can be complex, such as comprehensive and detailed intelligence studies required to support the planning of a Marine expeditionary force (MEF) in a major theater war (MTW), or simple, such as direct answers to rapidly changing questions needed to support the ongoing battle at the battalion level. For this reason, production is distinguished as—

- Deliberate production makes full use of available information to provide a complete and extensive product that satisfies non-time sensitive intelligence requirements (IRs). This type of production normally supports operations planning.
- Immediate production identifies information directly applicable to current operations, the information is subjected to a compressed ver-

sion of the production process, and the resulting product is rapidly disseminated to those affected. This production is associated with mission execution.

Dissemination

This step conveys intelligence to users.

Utilization

During utilization, the processed intelligence is used to influence the conduct of operations.

Production Steps

Production (analysis and synthesis) encompasses the following steps, which begin with the receipt of processed information and end with the completion of an intelligence product that is ready for dissemination:

- Filtering is the discarding of irrelevant or repetitive information prior to its entering the production process.
- Recording is the reduction of information to writing or graphical representation and then the arranging of that information into groups of related items.
- Evaluating is the determining of the pertinence, reliability, and accuracy of information.
- Analyzing is the process in which information is analyzed and synthesized to predict possible outcomes.
- Product preparation is the incorporating of developed intelligence into an appropriate product (e.g., text reports and studies, graphics, overlays, or combinations) for dissemination.

Preparation for Analysis

The first three production steps are tools used to prepare information for analysis. The objective is to discard information not pertinent to the situation, organize and document the information in a manner that facilitates analysis, and assess the quality of the individual elements of information to determine the reliability and importance of each report or piece of information.

In deliberate production, comprehensive procedures are often employed to accomplish filtering, recording, and evaluating. The complexity of these procedures increases with the level of command, scope of the operation, and number of agencies or elements participating in the production process. However, it is important to note that filtering, recording, or evaluation systems are tools to support the analytical effort, not an end unto themselves. Intelligence personnel must be thoroughly familiar with the methodology being employed in preparing information for analysis to ensure that the pertinent information is available to the right analyst when needed.

In immediate production, a central node or individual, normally the intelligence watch in the combat operations center, makes a rapid assessment of each piece of incoming information to determine its pertinence and to evaluate its reliability and accuracy. The intelligence watch personnel's evaluation is based on their knowledge and understanding of the enemy situation, the current intelligence estimate, and ongoing and planned friendly operations and IRs. The watch performs the minimal collating and recording necessary so that an immediate tactical analysis may be completed and judgments made. Simultaneous with or upon completion of immediate production, the information is entered into the formal recording and evaluation system for further use in deliberate production. At lower tactical echelons, the entire process, from receipt of information to dissemination and utilization, can take a matter of seconds or minutes. Organization, established standing operating procedures, and individual and unit training are key components of effective preparation for, and conduct of, P&A.

Analytical Process

Intelligence analysis provides the commander with the battlespace and threat knowledge required for planning and executing combat operations. Intelligence analysts lessen the uncertainty facing a commander, permitting the commander to make decisions and to focus combat power on courses of action (COAs) that maximize the opportunity for success. The analysis framework used by intelligence analysts is described as analysis, synthesis, and estimation. This framework provides a disciplined approach to gathering and understanding information and a means for the analyst to place information in context and relate it to planned or ongoing operations.

Analysis

Effective analysis requires that intelligence analysts—

- Possess a thorough knowledge of—
  - Military operations.
  - Characteristics of the battlespace.
  - Friendly situation and IRs.
  - Threat situation (current situation, doctrine, and past practices).
- View collected information in relation to the—
  - Unit's mission.
  - Commander's intent.
  - Commander's IRs.
- Divide the battlespace into component parts to isolate and define the individual elements of significant information that include—
  - Physical dimensions (i.e., length, depth, width, and altitude).
  - Time.
  - Threat force structure (e.g., divisions, wings,groups, task forces).
  - Battlespace activities (e.g., command and control [C2], air and space defense, fire support).
  - Other characteristics that facilitate understanding and satisfy the MAGTF's needs.
- Identify key elements of the situation to—
  - Formulate hypotheses.
  - Make deductions from those hypotheses.
  - Reach conclusions.
- Compare the existing situation to new pieces of information to determine if they relate to the identified key elements and to assess the impact of the new information on the current intelligence estimate.

Synthesis

In this step, intelligence analysts—

- Identify and integrate relationships between individual significant pieces of information with the existing battlespace picture to provide a new image of the situation.
- View the battlespace as a coherent whole.
- Discern emerging patterns in environmental conditions or enemy activity.

Estimation

The bottom line of the analytical process, estimation is based on the detailed study of the tactical situation, experience, intelligence successes, the application of specific tools and methods, and the supported commander's intelligence needs. Estimation is not guessing and it is not predicting! Estimation must describe the current conditions and present an image of future possibilities. Well-founded estimates reduce uncertainty and help the commander plan and execute successful MAGTF operations. Building on the image developed during analysis and synthesis, intelligence analysts determine a threat's—

- Capabilities.
- Intent.
- Probable COA.
- Likely reactions to friendly operations.

Product Preparation

Products are prepared by translating the results of analysis into usable intelligence formats that are timely, accurate, and tailored to both the unit and its mission. Intelligence analysts must strive to provide knowledge that the decisionmaker can easily and quickly visualize and absorb. A series of standard intelligence products are used to support MAGTF operations. Standard production formats facilitate rapid preparation, mutual support between intelligence sections, ease of dissemination, and, most importantly, familiarity for the user. The baseline production formats provided in this manual can be tailored to meet the requirements of any operational situation. The following standard all-source intelligence products are prepared in MAGTF:

- Intelligence preparation of the battlespace (IPB) graphics, matrices, and charts.
- MAGTF contingency intelligence studies.
- Intelligence estimates.
- Target or objective studies.
- Intelligence summaries.
- Intelligence reports.

Operations and Command and Control

Intelligence drives the planning and execution of operations by providing a menu of factors that the commander considers when making a decision. The analytical and production effort identifies these factors and presents them to decisionmakers in a form that enables them to understand the battlespace, place intelligence in context, and use the product to carry out successful operations. P&A shapes operations by—

- Identifying potential advantages offered by the environment.
- Defining the limitations imposed by the environment.
- Locating and assessing enemy strengths to be avoided.
- Determining enemy vulnerabilities to be exploited.
- Providing an estimate of likely enemy actions and reactions based on reasoned analysis, synthesis, and judgment.

Intelligence and operations must be linked throughout the planning, decision, execution, and assessment (PDE&A) cycle at all command echelons. The PDE&A cycle provides the framework for the implementation of C2, which enhances the commander's ability to make sound and timely decisions. Whether the commander uses the analytical or intuitive decisionmaking approach, intelligence P&A reduces uncertainty.

Deliberate intelligence production shapes the operations plan and provides the knowledge that facilitates execution (see fig. 1-3 on page 1-6). Immediate intelligence production identifies situation changes that modify the plan or trigger decisions during execution of the operation. Intelligence production provides the basis for assessing the effectiveness of current operations, while operations drive the P&A effort. The mission and commander's intent focus the initial IPB, while the potential COAs, the concept of operations, the future planning effort, and IRs determine the scope and content of the production process. Intelligence products must be relevant to the mission and be used to satisfy specific operational and tactical IRs.

Production and Analysis Company, Intelligence Battalion

The P&A company is the MEF's primary all-source P&A element. An organic unit within the intelligence battalion (intel bn), P&A company is composed of an imagery intelligence platoon, a topographic platoon, an all-source fusion platoon, and two direct support teams. The P&A company is in general support of the MAGTF and provides direct support teams to MAGTF

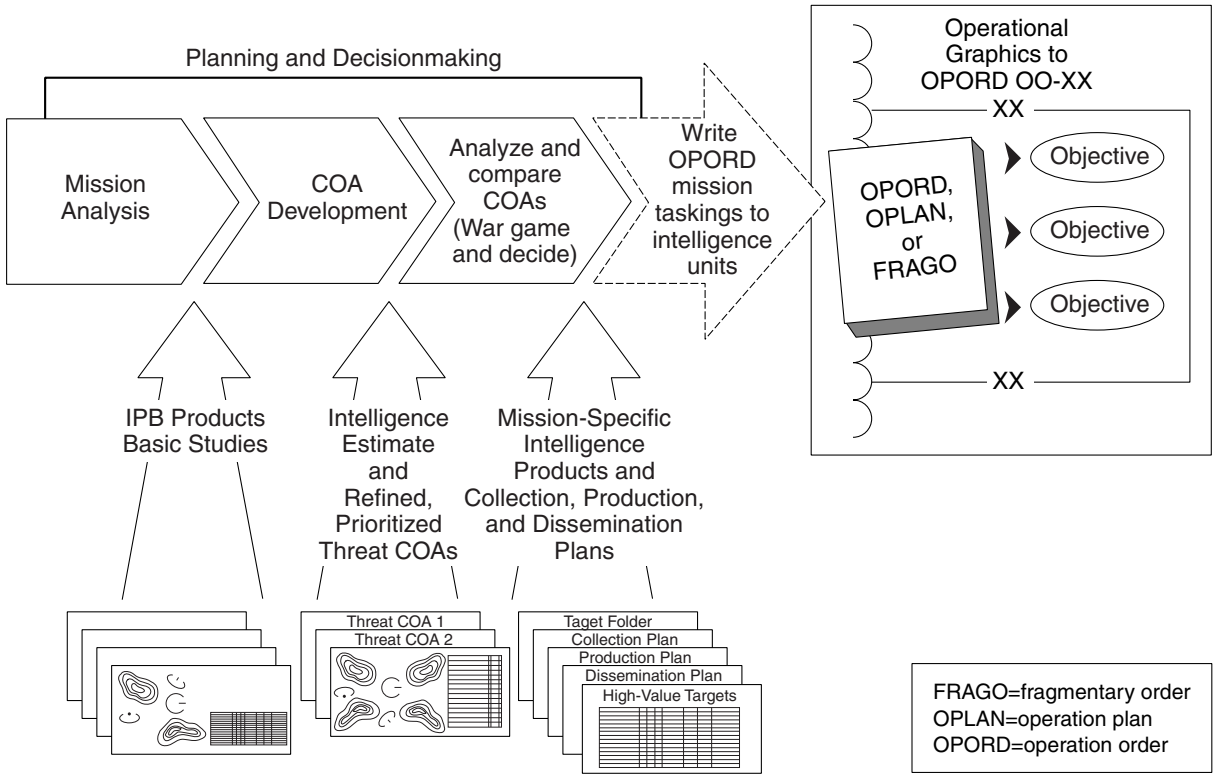


Figure 1-3. Intelligence Support to Planning and Decisionmaking.

subordinate elements, as required. The P&A company performs the following tasks:

- Assists the intel bn commander with planning, developing, and directing the MAGTF intelligence production plan and its integration with the collection and dissemination plans.
- Provides and maintains centralized all-source P&A in support of the MAGTF within the MAGTF P&A cell.
- Maintains an all-source picture of MAGTF AO and area of interest (AOI) threat situation.
- Provides MAGTFs and other commands with geographic intelligence (GEOINT) and geospatial information and services.
- Provides command and control of the topographic platoon.
- Provides imagery analysis and imagery intelligence (IMINT) production support for MAGTFs and other commands.
- Provides command and control of the imagery intelligence platoon.
- Provides task-organized, trained, and equipped detachments or teams to assist MAGTFs or designated commands in the processing, exploitation, evaluation, integration, analysis, interpretation, production, and dissemination of all-source intelligence.

Although the P&A company is a subordinate element of the MEF intel bn and the MAGTF's only dedicated production element, the company responds to the IRs of the entire force. The MAGTF G-2, through the intel bn commander in the role as intelligence support coordinator, establishes the P&A company's analytical and production priorities based on the MAGTF's mission, commander's intent, priority intelligence requirements (PIRs), the current and projected enemy situation, and ongoing planning for future operations. The P&A company focuses primarily on deliberate

production. In garrison or a pre-crisis environment, the P&A company conducts mainly IPB of potential contingency areas to produce MAGTF contingency intelligence studies. During operations and exercises, the P&A company develops intelligence to support future operations, deliberate targeting, and development of the key target or objective area studies. A detailed discussion of the P&A company organization, functions, and employment is provided in chapter 2.

CHAPTER 2. ORGANIZATIONS AND RESPONSIBILITIES

Marine Corps operational forces are organized for combat as MAGTFs. Marine intelligence P&A operations are conducted primarily to facilitate planning and execution of MAGTF operations through the development of tactical intelligence. This chapter discusses responsible officers, organization, supporting organizations, and communications and information systems (CIS) architecture necessary to conduct MAGTF intelligence P&A.

MAGTF Commander

Intelligence is an inherent responsibility of command, and commanders must—

- Be personally involved in the conduct of intelligence activities.
- Specify intelligence requirements and establish PIRs.
- Provide guidance to ensure a timely and useful product.
- Develop an appreciation for the capabilities and limitations of intelligence.
- Make the final synthesis of intelligence.
- Supervise the overall intelligence effort to ensure the product is timely, relevant, and useful.
- Ensure intelligence activities support subordinate commanders as well as the parent unit.
- View intelligence training of all personnel as a command responsibility.

To ensure the timely development of useful intelligence products, the commander has specific P&A responsibilities.

Focus the Analytical and Production Effort

The commander must—

- Provide guidance and direction to ensure that the intelligence developed satisfies requirements.
- Issue a statement of intent and approval of the command's priority intelligence requirements, focusing the analytical and production effort.
- Supervise the process to ensure that it is responding to the intent and intelligence needs.
- Provide direction in the scope of the IPB effort, preferred product formats, and priorities among subordinates' production requirements (PRs).

Participate in the Analytical Process

The commander must understand and participate in the analytical process. Since intelligence analysis is based on incomplete information and involves assumptions and judgments, the commander must scrutinize the process by analyzing intelligence operations and resulting products to determine the operational impact and overall effectiveness.

Evaluate the Product

To provide the basis for continued improvement of the P&A effort, the commander must—

- Evaluate key areas (e.g., product content, presentation, timeliness).
- Identify where the intelligence provided met expectations and where and how it fell short.

- Provide timely and constructive feedback to the intelligence officer, the supporting intel bn commander or detachment officer in charge, and P&A elements.

Marine Expeditionary Force Command Element Intelligence Officer

The MEF assistant chief of staff (AC/S) G-2 focuses on overall C2 and direction of MEF intelligence, counterintelligence (CI), and reconnaissance operations, to include P&A. The MAGTF commander relies on the AC/S G-2 to provide the necessary information on the weather, terrain, and enemy capabilities, status, and intentions. Through intelligence operation plans (OPLANs) and supporting intelligence and reconnaissance and surveillance plans, the AC/S G-2—

- Plans and coordinates intelligence priorities.
- Integrates collection, production, and dissemination.
- Allocates resources.
- Assigns specific missions to subordinate elements.
- Supervises the overall intelligence and reconnaissance efforts.

Intelligence Battalion Commander

The intel bn commander is responsible for planning and directing, collecting, processing, producing, and disseminating intelligence, and providing CI support to the MEF and MEF major subordinate commands (MSCs).

Responsibilities in Garrison

In garrison, the principal task of the intel bn commander is to organize, train, and equip detachments that support MAGTFs or other designated commands to execute integrated collection, intelligence analysis, production, and product dissemination.

Responsibilities During Operations

During operations the intel bn commander is dual-hatted as the intelligence support coordinator (ISC), serving under the direct staff cognizance of the MEF AC/S G-2. The intel bn S-3 section and the MEF G-2 operations center element form the core of the ISC support effort and conduct planning, directing, and C2 within the intelligence operations center (IOC) support cell. Generally, the IOC is collocated with the main command post of the MEF command element (CE). As ISC, the intel bn commander is responsible to the MEF AC/S G-2 for the overall MEF IR management. During operations, the ISC is responsible for—

- Implementing the concept of intelligence operations developed by the G-2 plans officer and approved by the AC/S G-2.
- Establishing and supervising the MEF IOC, which includes P&A cell, surveillance and reconnaissance cell (SARC), and support cell.
- Developing, consolidating, validating, and prioritizing recommended PIRs and IRs to support MAGTF planning and operations.
- Planning, developing, integrating, and coordinating MEF intelligence collection, production, and dissemination plans.
- Exercising C2 staff cognizance of supporting intelligence and reconnaissance organizations to ensure unity of effort and production of all-source intelligence.
- Developing, in conjunction with the G-2 plans officer and G-2 operations officer, and completing Annex B (Intelligence) to MEF operation order (OPORD), supporting appendices, and intelligence input to other OPORD annexes.
- Providing intelligence support to MEF CE G-2 section and MSCs.

- Preparing the intelligence and CI estimates to support G-2 plans.
- Planning, developing, integrating, and coordinating intelligence and CI support to the commander's estimate, situation development, indications and warning, force protection, targeting, and combat assessment.

Intelligence Battalion

Within the MEF, the intel bn is organized to conduct intelligence operations for the MEF, MEF MSCs, subordinate MAGTFs, and other commands as directed (see fig. 2-1).

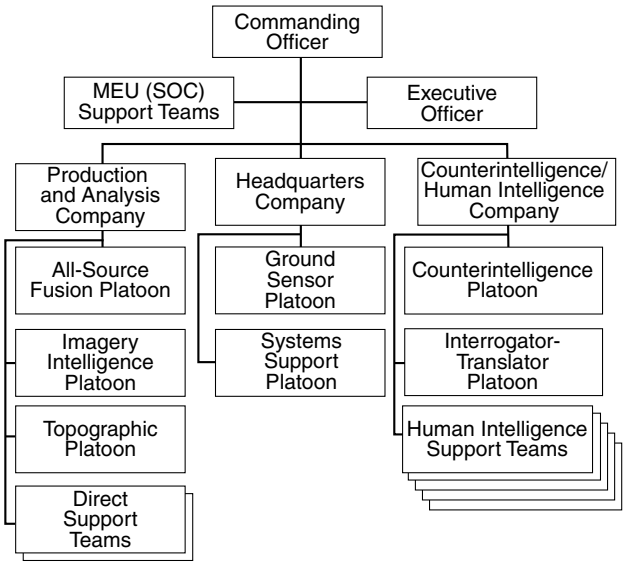


Figure 2-1. Intelligence Battalion Organization.

Production and Analysis Company

The P&A company, intel bn, is the focal point for deliberate intelligence production within the MEF. Although all P&A company elements contribute to the deliberate production process, the focal point for all-source analysis, order of battle (OOB), target intelligence, battle damage assessment (BDA), and deliberate production is the all-source fusion platoon (AFP).

All-Source Fusion Platoon

The AFP, in conjunction with other elements of the intel bn and production elements of radio battalion, force reconnaissance company, Marine tactical electronic warfare squadron (VMAQ), and Marine unmanned aerial vehicle squadron (VMU), provide the capability for all-source intelligence P&A support to the full range of operations conducted by the MEF and other MAGTFs. During operations, AFP forms the core of P&A cell.

Organization for Support

Intel bn's P&A company is organized to provide intelligence support to elements of the MEF CE and MSCs. During operations, P&A company is functionally organized into teams as the P&A cell. The teams support other MAGTF staff organization cells (see table 2-1).

Table 2-1. P&A Company Organization for Support.

Intel Bn, P&A Company Team or Unit	MEF CE Supported Cell
All-source fusion platoon	
• Analysis team	G-3 current and future operations, G-5, and other MEF staff elements*
• OOB team	G-3 current and future operations, G-5, and other MEF staff elements*
• Target analysis and BDA team	G-3 targeting cell and other MEF staff elements*
• IPB team	G-3 current and future operations, G-5, and other MEF staff elements*
Topographic platoon	MEF
Imagery intelligence platoon	MEF
Direct support teams	P&A cell, G-3 current or future operations, G-5, or designated MSC G-2
*The P&A cell supports the G-4, G-1, and other MEF CE staff elements, as appropriate.	

Production and Analysis Cell

The mission of P&A cell is to plan, coordinate, and produce fused all-source tactical intelligence in support of the MEF, its MSCs, and other MAGTFs and commands as directed. A multi-disciplined group of intelligence officers and specialists, the P&A cell provides the intelligence necessary to support contingency planning and current intelligence threat requirements of the MEF, its subordinate MAGTFs, and other commanders as directed.

Tasks

During operations and exercises, the P&A cell provides the intelligence necessary to support current and future operations, future plans, targeting, and development of enemy situation and capabilities. It is responsible for processing information and intelligence from organic and external commands and intelligence organizations. The P&A cell personnel—

- Receive, process and exploit, integrate, analyze, evaluate, interpret, and synthesize intelligence and other information into comprehensive and tailored intelligence products required for the planning and execution of MAGTF operations.
- Provide intelligence support across the conflict spectrum and in support of deliberate and crisis planning, MAGTF deployments, and other operations as directed.
- Provide a dynamic, detailed OOB picture of threats within the MAGTF AO and AOI.
- Provide detailed intelligence P&A support to targeting.
- Maintain a MAGTF-wide summation of damages caused to hostile targets and augment BDA efforts of MAGTF elements as required.
- Provide MAGTF-level BDAs for forwarding to the component, joint task force (JTF), and/or theater commander in chief (CINC) as applicable.
- Provide IPB support to the MAGTF G-3/S-3 and G-5 for battle management and planning efforts and provide IPB-related support to MAGTF elements beyond their organic capabilities.
- Disseminate intelligence products and information to the MAGTF staff and MSCs in a timely, relevant manner.
- Establish and maintain intelligence data bases to support intelligence P&A.
- Coordinate with the collection management and dissemination officer to provide the SARC with collection requirements for MAGTF and external collection units.
- Coordinate with the dissemination manager to disseminate intelligence products throughout the MEF and external organizations.
- Coordinate with the MEF G-2 and intel bn commander/ISC to—
  - Ensure disseminated intelligence and products are understood.
  - Determine whether intelligence products answer commander's PIRs and users' IRs.
  - Identify new intelligence production requirements (IPRs) that result from disseminated intelligence products.
  - Assess the overall effectiveness of intelligence production operations.

Organization

The P&A cell is essentially organized in garrison as it would be organized for operations. Each team has the flexibility to add intelligence and nonintelligence specialists (e.g., G-2 operations red cell members) from other intelligence and reconnaissance organizations as required based on the specific mission and intelligence needs of the MAGTF. For sustained MEF-level operations, global sourcing from other Marine Corps organizations may be required to augment the P&A team structure and to provide sufficient personnel depth for 24-hour operations.

The following P&A cell internal organization and subordinate teams and units provide the P&A functions required to support current and future operations, future planning, targeting, and BDA.

P&A Cell Staff

Members of the staff provide leadership and support functions such as maintenance of the intelligence library. In conjunction with the intel bn's collection management and dissemination officer, P&A cell staff members are responsible for production and IPR management as well as coordination of IPRs with intel bn's overall IR collection and dissemination.

Analysis Teams

The two analysis teams are composed of all-source analysts and specialists from other disciplines (e.g., medical, weather, CI/human intelligence [HUMINT], imagery, terrain, signals intelligence [SIGINT]). With support from other elements of the P&A company, the rest of intel bn, radio battalion, force reconnaissance, VMU, VMAQ, and MSC G-2 intelligence analysts, P&A cell analysis teams produce integrated all-source intelligence products to include—

- Contingency and other focused intelligence studies.
- Intelligence estimates.
- Intelligence summaries.
- Briefings.

OOB Teams

The P&A cell has two OOB teams. These teams analyze and maintain a detailed, comprehensive, evolving picture of ground, air, naval, electronic, weapons of mass destruction, and other threats within the MAGTF AO and AOI. The OOB teams perform OOB analysis, and the primary products include—

- Graphic or electronic situation overlays.
- OOB data bases and files.
- Threat models for various threat elements.

Target Analysis and BDA Teams

The two target analysis and BDA teams focus on detailed analysis of MAGTF commander, staff, and MSC-identified targets not destined for the air tasking order (ATO). (The Marine aircraft wing [MAW] G-2 section generally manages target and BDA analysis and intelligence support for ATO-nominated targets.) These teams—

- Provide target development and analysis to support the MAGTF deliberate and reactive targeting efforts.
- Maintain the comprehensive picture of battle damages caused to targets.
- Prepare BDA reports and assessments, which support the MEF combat assessment effort.

IPB Teams

The two IPB teams focus on IPB production support to the MEF G-3 and G-5 in the areas of current battle management and future planning. They also assist subordinate unit intelligence personnel with IPB-related production when requirements are beyond the organic capabilities of that unit.

Direct Support Teams

The two P&A cell direct support teams allow enhanced IR management, intelligence P&A, and dissemination capabilities to be focused down to one or more MSCs. Direct support teams augment the supported unit's intelligence section by—

- Providing an extension of the intel bn's P&A cell or MSC G-2 intelligence operations element for the receipt, collaborative analysis, production, and dissemination of intelligence to the supported unit.
- Tailoring higher and external intelligence products to the needs of the supported unit.

- Assisting the supported unit's intelligence officer in the formulation and management of external IRs.
- Assisting the supported unit in the production of IPB and other intelligence products to support detailed mission planning and execution.
- Enhancing the intelligence dissemination efforts of the supported unit's intelligence section.

Supporting Organizations

Several organic MAGTF intelligence organizations support the P&A cell P&A effort by contributing specialized MAGTF intelligence expertise and resources. The intel bn commander, serving as the ISC, is directly responsible to MEF AC/S G-2 for exercising C2 staff cognizance of supporting intelligence and reconnaissance organizations to ensure unity of effort and production of all-source intelligence. These supporting organizations contribute to fused, all-source MAGTF intelligence products. The following supporting intelligence and reconnaissance organizations provide significant specialized support to the P&A cell P&A effort.

Imagery Intelligence Platoon

Organized under the intel bn, P&A company, imagery intelligence platoon (IIP) provides imagery interpretation support for MEF requirements and maintains the imagery data base and imagery library for the MAGTF (see fig. 2-2). The IIP is capable of providing IMINT derived from available imagery sources in support of MEF P&A cell products. This includes annotated imagery in support of MEF P&A cell production or in response to separate IRs. A key imagery exploitation resource organic to the IIP is the tactical exploitation group (TEG), which is an element of the broader Joint Services Imagery Processing System (JSIPS). The IIP normally concentrates on the exploitation of imagery and production of IMINT from MEF, JTF, and other tactical resources, such as unmanned aerial vehicles (UAVs) or the F/A-18D (RC) advanced tactical aerial reconnaissance system (ATARS).

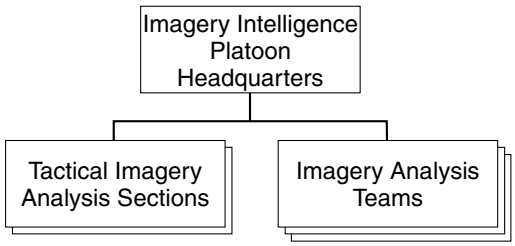


Figure 2-2. IIP Organization.

Topographic Platoon

Organized under the intel bn, P&A company, the topographic platoon provides geospatial information and GEOINT support for all MAGTF requirements (see fig. 2-3). The topographic platoon and IIP work closely as both use many of the same baseline intelligence data and sources for production.

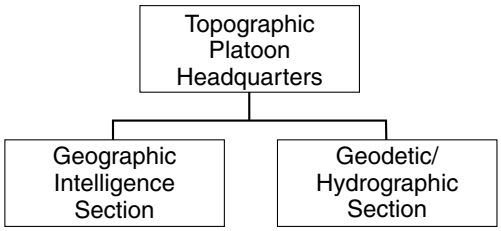


Figure 2-3. Topographic Platoon Organization.

The topographic platoon personnel—

- Integrate, deconflict, analyze, and disseminate theater, Service, and national geospatial data bases for the MAGTF.
- Provide GEOINT and specialized mapping, graphics and other geospatial information and services, and GEOINT products in support of P&A cell all-source intelligence products.
- Provide key support to the IPB process.

- Produce independent GEOINT studies in response to separate requirements.

CI/HUMINT Company

Organized under the intel bn, the CI/HUMINT company is responsible for the development and maintenance of the MEF CI estimate and reporting information (see fig. 2-4). The CI/HUMINT company produces—

- Intelligence derived from human source exploitation, to include—
  - Interrogations of enemy prisoners of war, refugees, and displaced persons.
  - Counterintelligence operations.
  - Human source operations.
- Intelligence derived from exploitation of captured documents or materiel.
- Specialized CI or force protection assessments in support of P&A cell production or in response to specific IPRs.

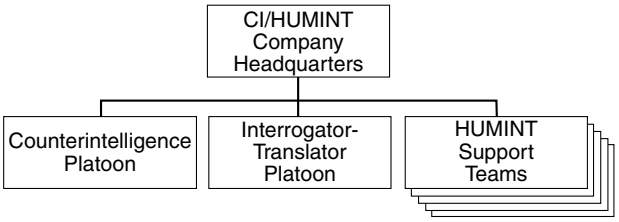


Figure 2-4. CI/HUMINT Company Organization.

Radio Battalion Operational Control and Analysis Center

The radio battalion operational control and analysis center (OCAC) provides the principal MEF SIGINT analytical and production support to MEF IRs. Under staff cognizance of the ISC, the radio battalion is tasked with the responsibility of maintaining the MAGTF electronic OOB and SIGINT data bases and of providing SIGINT analytical and production support to the P&A cell. The OCAC provides MAGTF units with time-sensitive SIGINT and product reporting based on intelligence reporting criteria and the MAGTF intelligence dissemination plan.

VMAQ

In conjunction with the MAW G-2, VMAQ is responsible for the processing, analysis, and production of routine and time-sensitive electronic intelligence reports resulting from EA-6B operations. The resulting information and intelligence is used to help update and maintain the threat electronic OOB, which is used in the planning and execution of aviation and other MAGTF operations. A threat's electronic OOB and the location of electronic emitters in the battlespace are important indicators of threat dispositions, capabilities, and intentions.

Force Reconnaissance Company

The mission of the force reconnaissance company is to conduct amphibious reconnaissance, surveillance, and limited-scale raids in support of the MEF, other MAGTFs, or JTFs as directed.

Under the staff cognizance of the ISC, force reconnaissance company conducts specialized terrain reconnaissance and prepares intelligence products to support hydrographic, beach, road, bridge, route, urban area, helicopter landing zones (HLZs), drop zones (DZs), landing craft air cushion (LCAC) landing zones (LZs), and aircraft forward operating site intelligence studies.

Principal Staff Officers

Like the commander, the other principal staff officers play an important role in intelligence P&A. Through development of focused intelligence requirements, and recommending which should be priority intelligence requirements PIRs, they assist in directing the intelligence P&A effort. They also assist the analytical effort by availing the wide range of skills and backgrounds resident within their staff sections to the intelligence section. A tremendous synergism is achieved when

task-organized teams of intelligence analysts and other occupational specialists form to analyze a specific issue. Likewise, a key component to effective wargaming is a red cell, which has experts in various warfighting functions thinking and fighting like the threat. Principal staff officers must—

- Use the intelligence products.
- Evaluate the worth and effectiveness of those products.
- Provide constructive feedback.
- Develop IRs and recommend their priority.

Unit Intelligence Officer

The intelligence officer manages the intelligence effort for the commander by implementing activities that execute the intelligence P&A function for the command. Understanding the scope and rationale behind the commander's decisionmaking process enables the intelligence officer to anticipate future requirements and properly focus the P&A effort. To execute P&A responsibilities, the intelligence officer must—

- Integrate and focus all-source intelligence on the commander's and sub-ordinate commanders' PIRs to support estimates of the situation, situation development, COA development, planning, and decisionmaking.
- Supervise the development and dissemination of all-source intelligence products that are tailored to the units' needs and concepts of operations and that are provided in time to support planning and decisionmaking.
- Provide the commander and staff with a bottom-line analysis of enemy capabilities, strengths, and vulnerabilities as well as opportunities and limitations presented by the environment.
- Request P&A support for requirements that exceed organic capabilities.
- Ensure the nature of the analytical effort and the content of the intelligence product is understood and properly used in the planning and execution of combat operations.

Organic Intelligence Sections

The unit intelligence section supports the commander, the intelligence officer, and the command through the development of mission-oriented intelligence products. The analytical and production capabilities of organic intelligence sections vary with the size of the section and level or type of command it supports. However, intelligence sections and their supporting intel bn or detachment are capable of performing the following P&A tasks:

- Conducting mission-focused IPB P&A for the unit's AO and AOI.
- Developing and maintaining a comprehensive intelligence estimate.
- Tailoring intelligence products to meet unit requirements.
- Maintaining an accurate all-source picture of the enemy situation in the AO and AOI.
- Preparing target analysis and target intelligence products.
- Providing intelligence operational linkage and communications and information system connectivity with higher, adjacent, supporting, and subordinate analytical elements.

Organization for Employment

When deployed, the P&A cell functions as part of the MEF CE combat intelligence center (CIC), IOC, under C2 of the ISC.

Combat Intelligence Center

The MEF CE CIC is the overarching IOC, which is established within the MEF main command post to conduct the primary functions of MEF intelligence section and intel bn. Key CIC elements (see table 2-2) are designed to

provide tailored, yet flexible, intelligence C2 and functional capabilities to meet MEF and subordinate commander's IRs and supporting intelligence and reconnaissance operations.

Command and Control

The MEF AC/S G-2 focuses on overall C2 and direction of MEF intelligence, CI, and reconnaissance operations by exercising staff cognizance over intel bn, radio battalion, force reconnaissance company, and other MEF intelligence and reconnaissance assets (e.g., UAV squadron). Within this C2 authority, the intel bn commander, serving as the G-2's ISC, performs MEF-wide IR management; develops, integrates, and manages supporting intelligence plans; and supervises plan execution.

These plans encompass the MEF-wide organic efforts for collection, processing, production, and dissemination activities of intelligence and reconnaissance operations. The intel bn commander/ISC is responsible for the establishment and operation of the IOC (see fig. 2-5 on page 2-10).

Table 2-2. MEF CE's CIC Key Elements.

Element	Responsibilities
G-2 Plans	Serves as the G-2 section's main element for coordinating and providing intelligence support to the MEF CE future plans team and leadership and direction of the G-2 section's imagery and mapping, SIGINT, and weather sections.
G-2 Operations	Serves as the G-2 section's main element for coordinating and providing intelligence support to the MEF CE commanding general (CG), battle staff, and current operations center elements; target intelligence support to the force fires and future operations; G-2 section intelligence requirements management activities; red cell support; and MEF intelligence liaison with external commands and organizations.
IOC	Serves as the principal MEF intelligence operations and C2 center that is established by intel bn; performs intelligence requirements management, staff cognizance of ongoing organic and supporting collection operations, intelligence P&A, and intelligence dissemination.
• Support Cell	Serves as primary element for conducting MEF-wide intelligence requirements management, weather support, collections and dissemination planning and direction, and intelligence staff cognizance of MEF organic and supporting intelligence and reconnaissance operations.
• P&A Cell	Serves as the primary P&A element of the MEF; processes and produces all-source intelligence products in response to requirements of the MEF; serves as the principal IMINT and GEOINT production element of the MEF.
• SARC	Serves as the primary element for the supervision of MEF collection operations; directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets.
CI/HUMINT Company Command Post	Serves as the primary element for conducting CI/HUMINT planning and direction, C2, and coordination of MEF CI/HUMINT operations with external CI/HUMINT organizations.
OCAC	Serves as the main node for the C2 of radio battalion SIGINT operations and the overall coordination of MEF SIGINT operations; processes, analyzes, produces, and disseminates SIGINT-derived information; and directs the ground-based electronic warfare activities of the radio battalion.
Reconnaissance Operations Center	Serves as the main node for the C2 of force reconnaissance company's operations and the overall coordination of MEF ground reconnaissance operations; processes, analyzes, produces, and disseminates ground reconnaissance-derived information in support of MEF intelligence requirements.

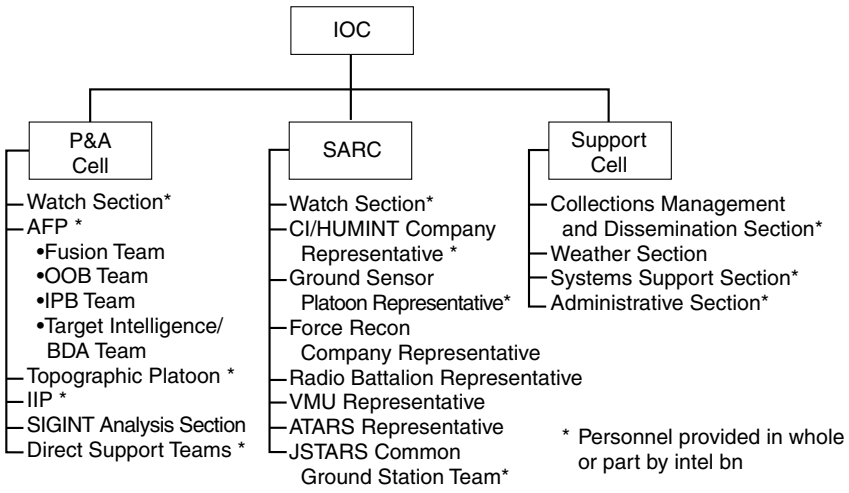


Figure 2-5. IOC Organization.

Senior Marine Expeditionary Force Intelligence Staff Officers

Table 2-3 highlights the key MEF senior intelligence staff officers and their responsibilities, roles, and tasks.

Intelligence Production Support Flow

Requests for intelligence production support from the P&A cell, or other MEF intelligence or reconnaissance elements, must be validated and forwarded via the chain of command to the MEF G-2 for validation, prioritization, and tasking. The intel bn commander, serving as ISC, performs this function for the G-2.

The ISC, upon approval by the AC/S G-2, uses the prioritized intelligence collection requirements (ICRs), IPRs, and intelligence dissemination requirements (IDRs) for planning and direction, follow-on taskings to MEF organic and supporting intelligence and reconnaissance units, C2, and execution. The ISC's overall intelligence production staff cognizance relationships and resulting P&A cell intelligence production support flow are as indicated in figure 2-6.

Organization for Combat Operations

The intel bn and P&A company tailor day-to-day garrison operations to support the IRs of the commander, staff, and MEF subordinate units. With minor adjustments, the P&A company transitions from garrison pre-hostilities organization to P&A cell crisis or combat operations functioning. In practice, the organization of the P&A cell supporting each MEF is based on prospective missions of that MEF and corresponding potential AOs.

During contingency or combat operations, the P&A cell functions as part of the MEF CE's CIC and the intel bn's IOC. The P&A cell may be tasked to provide limited personnel support to an intelligence node or cell with the MEF. In such cases, the intelligence component of these command echelons will contain a limited P&A capability (focused on providing the commander with situational awareness).

Table 2-3. Senior Intelligence Staff Officers.

ISC	G-2 Operations Officer	G-2 Plans Officer
Planning and execution of intelligence operations to support all MEF IRs.	Providing intelligence support to MEF CE battle staff and current operations center agencies.	Providing intelligence support to the plans officer's future planning team for future planning IRs.
Establishing and directing the IOC (P&A cell, SARC, and support cell).	Coordinating intelligence support to higher and adjacent headquarters and agencies.	Recommending IR validation, prioritization, and tasking to AC/S G-2.
Managing IRs (collection, production, and dissemination), validating, prioritizing, and tasking IRs, per AC/S G-2 direction.	Recommending IR validation, prioritization, and tasking to AC/S G-2.	Establishing and directing the G-2 future planning intelligence element.
Exercising C2 of intel bn and staff cognizance over SIGINT, CI, HUMINT, measurement and signature intelligence, IMINT, and air and ground reconnaissance, including staff cognizance of designated G-2 elements.	Establishing and directing intelligence elements and support to the combat operations center, future operations center, target intelligence section, force fires, red cell, and MEF intelligence liaison teams.	Establishing and operating the intelligence section's imagery and mapping, CI, HUMINT, SIGINT, and weather sections (less that under staff cognizance of the ISC).

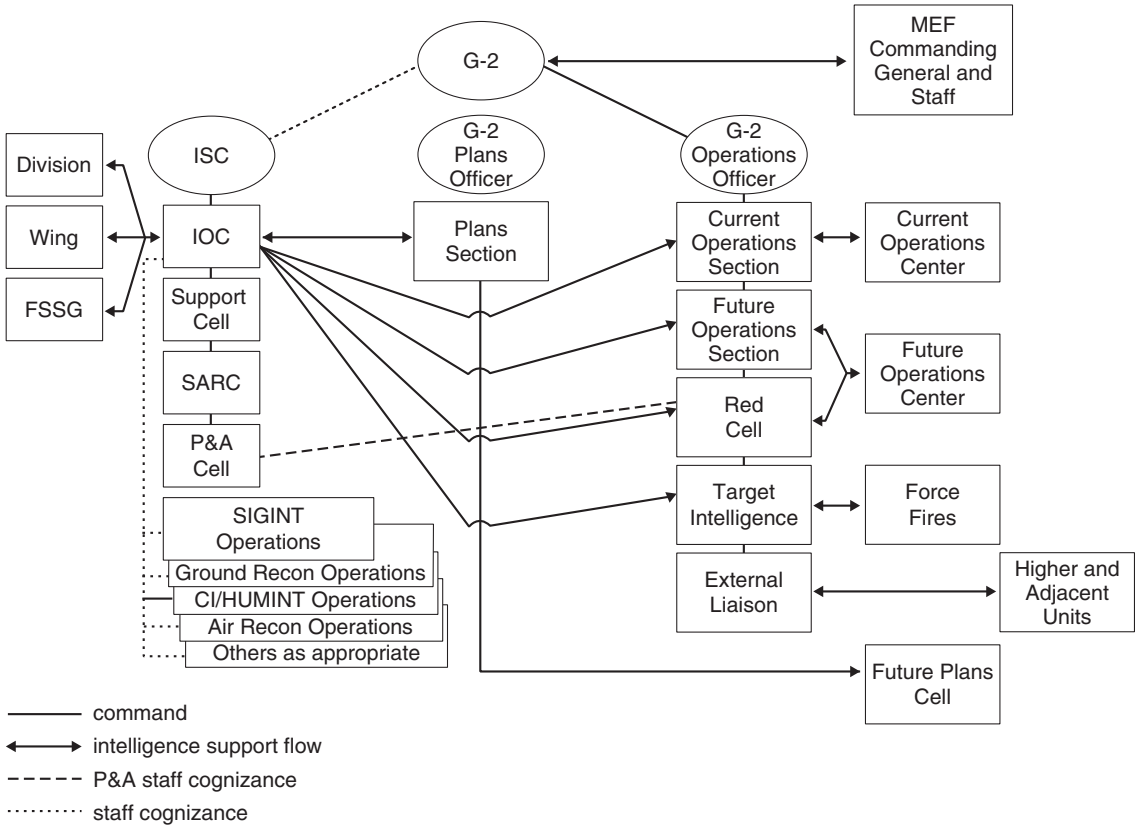


Figure 2-6. C2 and Staff Cognizance of Intelligence Production Support Flow.

The P&A cell may be tasked to provide personnel to support intel bn detachments provided to subordinate commands, MAGTFs, or separate units. Each P&A cell contains within its table of organization (T/O) two direct support teams which can be used to augment the IR management, analysis, production, and dissemination capabilities of the supported unit. Direct support teams can be employed by the MEF AC/S G-2 or ISC to focus intelligence planning, direction, analysis, production, and dissemination support to the main effort or other specified MEF priority. When not so assigned, direct support teams will be integrated within other P&A cell or intel bn operations.

When a MAGTF of less than full MEF size is deployed, the P&A cell may contribute personnel to a task-organized intel bn detachment normally attached to the MAGTF or special-purpose MAGTF (SPMAGTF) command element. A common example would be the detachments provided to Marine expeditionary unit (special operations capable) (MEU[SOC]) CEs. Standing support includes small detachments from the IIP and topographic platoon. The lead and tactical echelons' intelligence nodes and detachments rely heavily on electronic CIS connectivity to allow reach back to the more robust and capable analytical and production resources of the MEF and intel bn.

Communications and Information Systems

The intel bn, P&A cell, subordinate elements, and other key intelligence producers (e.g., radio battalion) must have sufficient communications resources to support internal C2, operations, and IR support. Communications capabilities generally consist of short- and medium-range voice communications equipment. The communications battalion or communications elements provide P&A CIS support beyond the basic requirements.

Basic Requirements

Regardless of the size of the MAGTF, the following standing CIS requirements must be satisfied to facilitate intelligence P&A operations.

Capability to Command and Control Subordinate Units

Intelligence officers and intelligence production element commanders or officers in charge must be capable of positive staff cognizance or C2 of subordinate units and integration of their operations with broader MAGTF and external intelligence and operations C2. Traditionally, single-channel radio and record message traffic have been used to support MAGTF intelligence units' C2, particularly at echelons below the MSC level. At MSC, major subordinate element (MSE), MAGTF CE, and higher command echelons, high capacity communications networks support intelligence production C2, operations, and product dissemination. In semi-static situations, secure electronic mail or telephone provide significant communications capabilities; in highly fluid or mobile scenarios, cellular, satellite communications (SATCOM), and very high frequency (VHF) and high frequency (HF) radios may be used.

Ability to Receive Collected Data, Information, and Intelligence from Organic and External Intelligence Organizations and Production Elements

The CIS architecture must provide connectivity between organic and supporting intelligence units and production elements. Principal and alternate means of CIS are dependent on mission, enemy, terrain and weather, troops and support available-time available (METT-T) factors. The commanders and users' desired product formats also influence the selection of CIS means. The means of communication must include the capability to transmit imagery, GEOINT, and other intelligence products with large data files as well as the capability to

disseminate IMINT and reports digitally via fiber optics, wire, radio, and voice formats.

Ability to Provide Intelligence to Supported Commanders

Supported commanders' intents, concepts of operations and intelligence, command relationships, and standing PIRs and IRs influence intelligence production CIS requirements. The CIS architecture must be capable of integrating production elements' C2 and supporting CIS operations, including general service (GENSER) and sensitive compartmented information (SCI) communications with the primary CIS channels used by supported commanders. The determination of principal and alternate CIS means depends on METT-T. The product format desired by commanders and intelligence users also influences the CIS means. The means of communication must include the capability to transmit imagery, GEOINT, and other intelligence products with large data files as well as the capability to disseminate SCI and GENSER all-source and intelligence discipline-unique reports digitally via fiber optics, wire, radio, and voice formats.

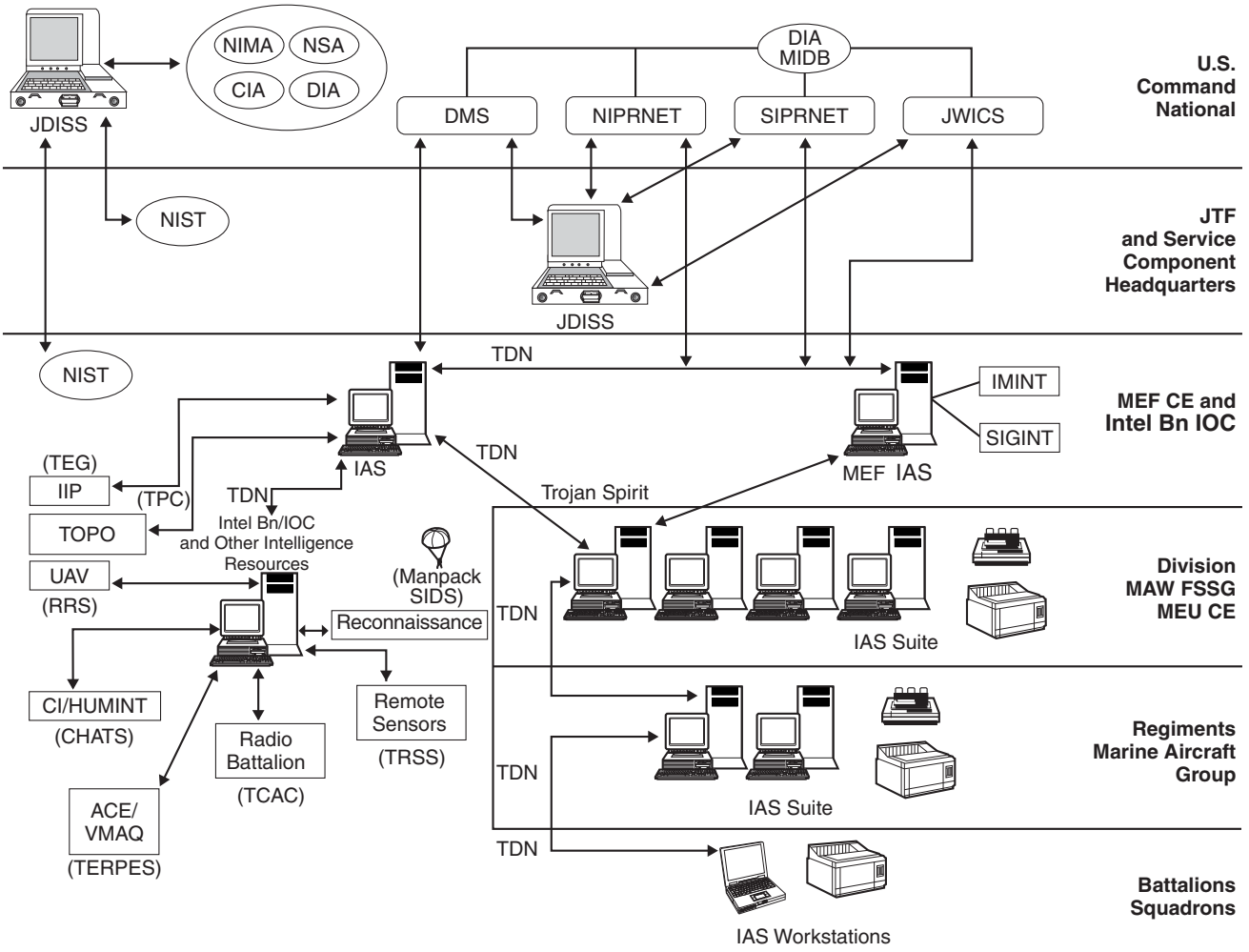
Ability to Share Intelligence Products and Reports with All-Source JTF, Other Components, Theater, National, and Multi-national Intelligence Organizations, Agencies, and Centers

Traditionally, MAGTF GENSER secure record and voice communications provide this capability. While these techniques continue to be used for MAGTF intelligence production, they are now secondary in importance to the use of Joint Worldwide Intelligence Communications System (JWICS), SECRET Internet Protocol Router Network (SIPRNET), and other CIS capabilities which allow participants to access each others' intelligence products and data bases and to immediately pull required data, intelligence, and other products. This CIS requirement includes the capability to disseminate intelligence with designated nongovernmental organizations (NGOs), private volunteer organizations (PVOs), and other U.S. and multinational governmental agencies, particularly during military operations other than war (MOOTW).

Information Systems

Information systems, such as the intelligence analysis system (IAS), and their associated networks are the lifeblood and lifelines of P&A cell and MAGTF intelligence analysis, production, and dissemination operations. Intel bn has sufficient information systems resources to satisfy internal C2, operations, and intelligence needs. Most information systems require access to SIPRNET for GENSER requirements and to JWICS for SCI requirements, which provide intelligence and data base access to MAGTF, JTF, and other components' elements, and theater and national intelligence reporting and data bases.

The nonsecure internet protocol router network (NIPRNET) is also a key resource for intelligence analyst research and access to public domain information, as well as a means to exchange unclassified information. The supporting MEF communications battalions provide the necessary network connectivity for GENSER information networks and communications pathways, and radio battalion provides SCI networks. Figure 2-7 on page 2-14 depicts a notional MEF intelligence processing, analysis, production, and dissemination CIS architecture and resources.



CHATS=CI/HUMINT automated tool set
CIA=Central Intelligence Agency
DIA=Defense Intelligence Agency
DMS=Defense Message System
FSSG=force service support group
IIP=imagery interpretation platoon
JDISS=Joint Deployable Intelligence Support System
MIDB=modernized integrated data base
NIMA=National Imagery and Mapping Agency
NIST=national intelligence support team
NSA=National Security Agency
RRS=remote receive station
SIDS=secondary imagery dissemination system
TDN=tactical data network
TERPES=tactical electronic reconnaissance processing and evaluation system
TOPO=topographic platoon
TPC=topographic production capability
TRSS=tactical remote sensor system

Figure 2-7. Notional MEF CIS Architecture.

CHAPTER 3. FILTERING, RECORDING, AND EVALUATING

When preparing information for analysis, intelligence personnel—

- Identify Information of Immediate Tactical Value. Every piece of data, information, or intelligence received must be assessed to determine its tactical value and its effect on current operations. Particular attention must be paid to possible alarms, triggers, and high-payoff targets (HPTs), which are defined by, and tied to, the PIRs, commander's decision support tools, and targeting priorities. If the information is relevant to ongoing operations, immediate production is initiated. The information is rapidly evaluated, analyzed, and disseminated for use by the commander and staff as well as subordinate and other affected units.
- Eliminate Redundant and Irrelevant Data Early in Processing. Each item received must be scrutinized to determine its pertinence to the unit's intelligence requirements. The incoming flow of data, information, and intelligence must be filtered for redundancy and relevance to the mission, AOI, and timeliness. This ensures intelligence analysts receive information and data that is useful to the analytical process while not being overwhelmed with unnecessary information or repetitive reporting.
- Identify Relevance to Ongoing Production. An important aspect of preparing an item for analysis is determining its impact on the ongoing intelligence production effort. The received data or information is evaluated to identify how it contributes to ongoing production in order to determine who should get the information, how urgent the information is, and in what format the information should be provided.
- Practice Standing Operating Procedures. The employment of information handling standing operating procedures (SOPs) saves time and effort. Standard methods of filtering, collating, recording, and evaluating speed up the preparation of incoming items for analysis, provide consistency in the way information is handled, and enhance comprehension of personnel performing the procedures and of the analysts receiving the incoming items.
- Employ Reliable and Accessible Recording Tools. Effective analysis depends in part on the ability to access, recall, and manipulate the stream of all-source data, information, and intelligence flowing into the command. Recording methods should be simple and flexible without interfering with timely analysis, production, dissemination, and use of intelligence. Analysts must be able to access information when they need it to receive the information in a form that facilitates understanding, and to rapidly integrate the data with other information or intelligence. The widespread use of automated information systems enhances the speed and utility of intelligence recording tools. However, analysts must ensure the necessary reliability and accessibility are built into the automated information systems and that associated backup procedures are established.

SECTION I. FILTERING

Filtering is the discarding of irrelevant or repetitive information prior to its entering the P&A process. Because current and emerging collection, communications, and intelligence automated information systems provide access to a vast quantity of raw data, processed information, and finished intelligence, there is significant potential for information overload of intelligence

sections and personnel. An effective filtering system is essential for managing the flow of data, information, and intelligence into the unit's intelligence processing and production system.

Filtering Criteria

Before information is entered into the production process, each item's relevance to the unit's intelligence requirements is assessed and unrelated material is discarded. The unit intelligence officer establishes basic criteria for filtering. Critical criteria drive the establishment of PIRs and IRs. The filtering criteria must be reviewed on a regular basis and updated to reflect changes in intelligence requirements, the AOI, and timeliness of information needed. Intelligence analysts use the following criteria when making assessments.

Subject Matter

The content of the data or report must be related to the unit's PIRs/IRs. Information that has no bearing on the PIRs/IRs is discarded, unless the information may impact future requirements.

Location

The event detailed in the data or report must have occurred within the unit's AO or AOI.

Time of Occurrence

The report should have continuing significance. For example, reports of future air or missile strikes may be received after the strike has begun; such reports are discarded unless they contain details of analytical importance.

Redundancy

Multiple reports relating to the same data or event are often received. Reports that repeat the initial information without adding significant data or analysis should be discarded, unless the reports provide critical confirmatory information.

Methodology

Filtering should occur as early as possible in the information processing system. Despite the fielding of automated intelligence systems, such as the Marine Corps IAS and the technical control and analysis center (TCAC), filtering is largely a manual process. A human must review voice reports, translated documents, images, and finished intelligence documents from higher echelons.

Manual Filtering

Most intelligence sections establish a central point for the receipt and distribution of incoming intelligence, counterintelligence, and reconnaissance reports. Normally, the intelligence watch within the combat operations center or the surveillance and reconnaissance cell is the receiving and distribution point. The watch examines each piece of data, information, and intelligence received; compares the content to the filtering criteria; and decides whether to discard the report. Filtering personnel must be able to rapidly identify new intelligence information of immediate tactical value and to quickly initiate the necessary actions.

Automated Filtering

For machine-readable formatted messages, automated intelligence systems are significant filtering tools. Systems such as the IAS can automatically filter incoming messages according to specified parameters such as location, time, and type of report. Use of IAS speeds the filtering process by correlating incoming information to existing units' tracks within the data base. However, the unit name or identification and location data fields in the formatted message must be filled out for this automatic function to occur, or the system will hold the message for

manual correlation. Automated systems are a tool to assist the analyst, not replace them. The system operator must continually review the filtering parameters and assess the effectiveness of the information filtering system. As with manual filtering, IAS operators must be familiar with the unit's intelligence requirements, have situational awareness, and exercise sound judgment.

SECTION II. RECORDING

Recording is the reduction of information to written or other graphical representation and the arranging of this information into groups of related items. This step is performed so items of information can be observed as an integrated picture and studied in relation to each other. Recording information makes evaluation and analysis easier and helps prepare intelligence products by drawing together available information on a specific subject. It also provides a record of events for post-operation study of the enemy and AO.

Methodology

Recording performed by intelligence sections at all levels normally involves—

- Registering all incoming information.
- Logging, map or chart marking, filing and indexing, or entering information in the data base of an automated system.
- Maintaining a system designed for rapid and efficient operations.

At lower command echelons, especially during mobile operations, recording may be no more than the maintenance of a log and marked map. At higher command echelons, recording relies heavily on automated information systems, electronic data bases, and visual display units. Both methods should make full use of graphic recording tools (i.e., maps, overlays, graphs, and charts) that make it possible to visualize and absorb the maximum amount of information in the shortest possible time. The indexing and categorizing of subject matter in a recording system must be related to the projected area, scope, and nature of the operations and must be based on the—

- Commander's PIRs.
- Other IRs.
- Anticipated information flow.

The recording means must be able to handle the volume of information and intelligence received and to serve the needs of individuals requiring access to that information. In addition, recording means and techniques must permit timely dissemination of information and intelligence.

In the past, most recording was manually generated either on a map, journal, or status board. Today, the most common recording devices are automated data processing and information systems such as IAS. Office automation software allows the rapid creation of charts and graphs, the annotation and manipulation of images, and the rapid assembly of words and text. Intelligence journals, files, records, and data bases can be updated automatically, and the data can be recalled and displayed in an overlay form.

Recording Tools

Whether operating in a manual or automated environment, the most common types of recording tools used by the intelligence analyst are the intelligence journal, enemy situation map, intelligence workbook, order of battle or analyst files, and target files.

Intelligence Journal

The intelligence journal is an official, permanent, and chronological record of reports and messages that have been received and transmitted, of important events that have occurred, and of response actions taken (see fig. 3-1). Messages are place in the journal file in the numerical order of the journal entry number. The journal, besides providing a brief chronological account of events, serves as an index to the journal file. The journal covers a stated period, normally 24 hours. Each item entered in the journal normally contains—

- An entry number, which is assigned to an incoming message and is recorded on the message.
- The time the information was sent, received, or noted.
- The message date-time group.

INTELLIGENCE SECTION JOURNAL

PAGE NO.	NO. OF PAGES
1	1

ORGANIZATION OR INSTALLATION	LOCATION	PERIOD COVERED			
		FROM		TO	
		HOUR	DATE	HOUR	DATE
1ST MARDIV	BURGEW, GE (LA567275)	0001	02 DEC 00	2400	07 DEC 00

ITEM NO.	TIME IN	TIME OUT	INCIDENTS, MESSAGES, ORDERS, ETC.	ACTION TAKEN	INL
1	0001		Journal opened 0001		BW
2	0030		5th MAR: Company team A patrol reported enemy		
			supply dump vicinity LA888912.	Map, S3, Cdr	BW
3		0055	ALL UNITS: Execute alternate challenge password,	CO, Staff, Units	DJT
			Primary compromised at 0700045.		
4	0200		5th MAR: Follow up to item 2. Search results:	CO, S3	DJT
			12XAT mines, 30,000 rounds 7.62 ammunition, 6 rolls		
			barbed wire, all destroyed in place.		
65	2400		Journal closed 2400		
			SUMMARY		
			No enemy contact during period,		
			but one enemy ammunition dump destroyed.		

TYPED NAME AND GRADE OF OFFICER OR OFFICIAL ON DUTY	SIGNATURE
SAMUEL A. MORRIS, CAPT, COC Intel Watch Off	SAM

Figure 3-1. Example of an Intelligence Journal Page.

- The originating agency or addressee.
- A brief description of the item.
- The disposition information.

Enemy Situation Map

The enemy situation map is a temporary graphic display of current enemy dispositions, major enemy activities, and other pertinent intelligence and information. By presenting that information in relation to each other, the enemy situation map also helps with interpretation, analysis, and decisionmaking. In addition, it helps dissemination by permitting the ready transfer of intelligence concerning enemy forces capable of interfering with the mission of the unit concerned. A primary analytical tool, the enemy situation map is often the only recording device used during fast-moving combat operations, particularly at lower command echelons.

Methodology

The enemy situation map should cover enough area to facilitate the conduct of current operations and the planning of future operations. A large MAGTF, such as a MEF, normally requires the following three enemy situation maps:

- Large-scale tactical map (approximately 1:50,000) for current ground operations.
- Medium-scale operational map (approximately 1:250,000) covering the AO and portions of the AOI to record deep enemy installations (e.g., airfields, missile sites) and enemy forces that can affect friendly operations.
- Small-scale strategic map (approximately 1:1,000,000 or smaller) to cover the MAGTF AOI and beyond.

At lower echelons, one map may suffice. The scale depends on the mission and threat. The map scale(s) used should be decided between the G-2/S-2 and the G-3/S-3 when the battlespace is defined (step one of the IPB process). Often, a combined G-2/G-3 map is used to conserve space in the combat operations center or other C2 cells. If separate intelligence and operations maps are maintained, overlays must be readily interchangeable between maps. Information displayed on the situation map must be tailored to the—

- Mission.
- Nature of the threat or enemy.
- Terrain.
- Command echelon being supported.
- Unit's PIRs/IRs.
- Force protection.
- Targeting priorities.

Generally, enemy maneuver units posted on the situation map are two echelons below that of the friendly unit. Enemy units, regardless of size, in friendly rear areas are always posted because of the amount of damage they can inflict on C2 and sustainment. The situation map reflects—

- Enemy unit identification, disposition, and boundaries.
- Significant terrain and infrastructure features.
- Locations of manmade and natural obstacles.

When plotting enemy activities and dispositions, intelligence personnel—

- Indicate the latest time when the activity was observed or the disposition was confirmed.
- Post information using standard military symbols and abbreviations. See Field Manual (FM) 101-5-1/Marine Corps Reference Publication (MCRP) 5-2A, *Operational Terms and Graphics*, for standard symbology.
- Explain any deviations from these symbols in the marginal data on the map or overlay.
- Mark maps and overlays clearly with the appropriate classification.

Information is posted on the situation map as it is received. Information is removed promptly when

no longer current, because omissions or outdated information may result in erroneous evaluations, interpretation, and decisions. On a hard copy situation map, separate flaps of acetate can be used to record different types of information, which reduces overcrowding. Also, to reduce overcrowding, a number or letter system can be used to record significant events or activity. The letter or number is marked at the appropriate location on the map where the activity occurred. On a board or marginal area alongside the map, the same letter or number is recorded with a notation of the activity observed. A numbering system that is easily cross-indexed to the journal or message file should be used.

Automation

Automated functions of the IAS and other intelligence information systems greatly assist the maintenance of an enemy situation map. The IAS enables the operator to—

- Zoom in and out through various maps to quickly change scale views of the battlefield, thereby enhancing the number, size, and types of enemy units displayed.
- Call up information, including last report and location, by clicking on the unit of interest.
- Forward electronic overlays to other IAS users or to systems such as tactical combat operations for display.
- Use large-screen displays to deliver information briefings.
- Share a common picture of the battlespace in near-real time with users at separate locations by using robust communications connectivity. Consideration must be given to developing manual and electronic backups in the event of catastrophic failure of the system.

Intelligence Workbook

Incoming information is recorded by subject in the intelligence workbook for ready reference and comparison. The workbook helps in determining the meaning and significance of related items of information, which facilitates further processing, production, and dissemination (i.e., preparation of intelligence summaries and reports). The workbook can be set up in any format; however, the most common format organizes the book according to topics in the intelligence summary.

As information is received, it is recorded in one or more parts of the workbook based on its content. For example, a report concerning a newly identified enemy armor unit could be recorded under the new units section as well as in the armor section. Each entry should include—

- Journal entry number for the source report.
- Time of the event or observation.
- Location.
- Brief extract of the information applicable to the workbook section.

Maintaining the workbook is a time-intensive, manpower effort, but a properly maintained workbook is a powerful analysis tool. The IAS operator has the ability to simultaneously break down portions of incoming messages into numerous sections of an electronic data base or workbook. Employed properly, this capability can significantly streamline the maintenance of an intelligence workbook.

Order of Battle Files

OOB files include information and intelligence on the identification, strength, command structure, and disposition of personnel, units, and equipment of a military force. Combined with information on the threat, terrain, and weather, OOB information is a key element in the creation of finished intelligence products (e.g., IPB, estimates, BDA).

OOB files maintained on threat, allied, and neutral or third party forces can be subdivided into—

- Ground OOB.
- Air OOB.
- Naval OOB.
- Electronic OOB.
- Weapons of mass destruction.
- Other categories tailored to the unit's needs.

The OOB subdivisions and level of detail maintained in each subdivision depends on the—

- Command level where the analysis takes place.
- Type of threat forces that can influence friendly operations.
- Mission assigned.
- Area of responsibility.

A MEF conducting an amphibious operation needs to maintain information on all types of forces, while a battalion or squadron operating as part of sustained operations ashore focuses on the ground or air OOB that most affect them. The battalion or squadron relies on higher, adjacent, supporting, or Service commands in the theater to provide other OOB (e.g., weapons of mass destruction, electronic OOB, naval OOB). Specific factors are evaluated for each type of OOB (see chapter 7 for a detailed discussion of these factors).

Lower command echelons' OOB analysis is generally more focused, less detailed, immediate in nature, and performed by the unit's intelligence personnel as part of their general duties. At higher levels, particularly at a MEF or MAGTF CE, one or more analysts are assigned to each type of OOB. At these levels, OOB information normally becomes voluminous in a short period of time. In organizing this information, OOB analysts must maintain extensive and systematic compilations and filing systems. Specific items of information and intelligence must be located on short notice and incorporated into comprehensive reports or analyses. Regardless of the level of command, analysts at the tactical intelligence level use several OOB tools.

Unit Workbook

The format for the unit workbook depends on the structure of the enemy force being monitored. It consists of a collection of unit worksheets arranged by type of unit or in numerical sequence. Analysts with OOB baseline documents at their disposal use them as unit workbooks by inserting additional pages as new information is received. Normally, the parent unit listed on the unit worksheet is equivalent in size to the level of command performing the analysis. Records are maintained on units one level above and two levels below the enemy unit being monitored; however, this can be modified based on the situation. The date and the source of information are recorded for each entry (see fig. 3-2 on page 3-8). Unit OOB details noted in the remarks column include—

- Reports of branch insignia.
- Number and types of weapons.
- Local residents' statements in abbreviated form.

OOB Situation Overlay

This is a graphic portrayal of current confirmed or unconfirmed enemy OOB. It shows identification and disposition of enemy units and other information that will assist in developing the enemy OOB. Enemy units, down to and including two echelons below the analyst's own level of command, are plotted using the standard symbols included in FM 101-5/MCRP 5-2A.

Peculiarities of enemy organizations, the tactical situation, and time and personnel available determine what to plot or omit on OOB maps. The information time and date are entered below each plotted symbol.

Parent Unit _____						
Subordinate Units	City	Coordinates	Installation	Personalities	Identification or Code No.	Remarks
Division Headquarters	Stein	PV818147	1 and 3	Commander Col Crechin		EPW no. 26, captured 2 Feb 68
96th Mechanized Rifle Regiment	Delltach	PU820934	4	Commander Col Kurshave	16181	Document captured 19 Mar 68
145th Mechanized Rifle Regiment	Ellenburg	PU852961	2	LtCol Shrenko	16182	Deserter 21 Mar 88
3d Battalion	Gladbach	PV891024	1			Gladbach residents report battalion subordinate to headquarters in Ellenburg, 3 Feb 88
43d Medical Tank Regiment	Linburg	PV863106	3	Commander Col Reshvic		Agent report 26 May 68
358th Transportation Battalion	Lehrt	PV825158	1		16195	OOB Bank

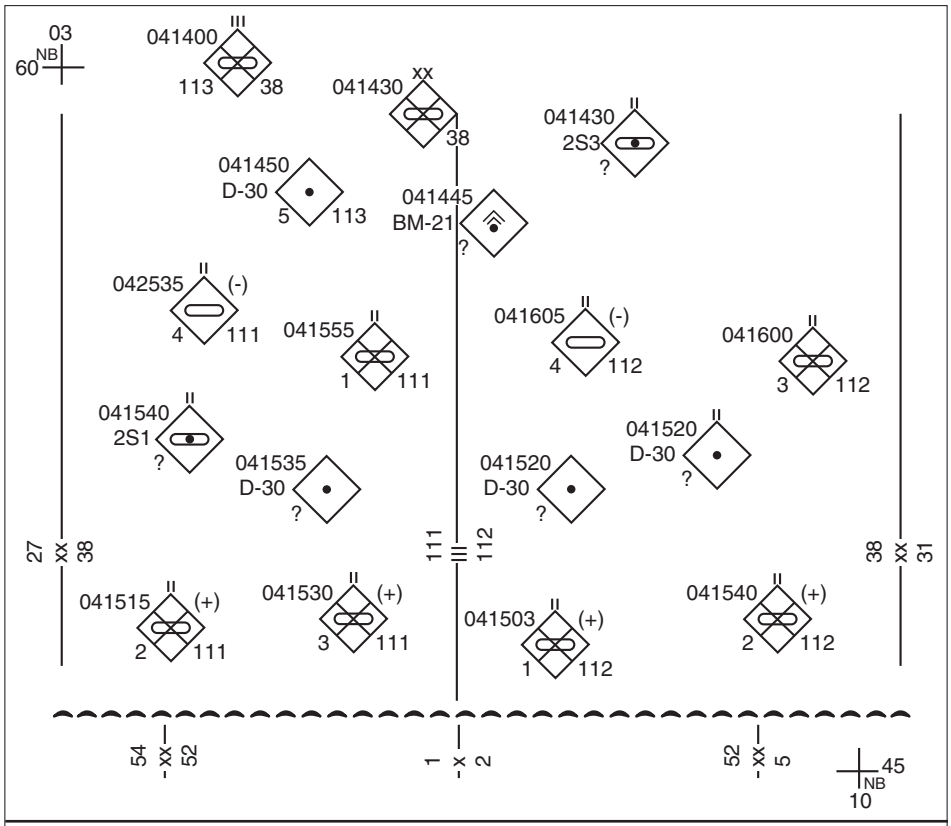
Figure 3-2. Example of a Unit Workbook Page.

An OOB situation map caption box contains annotated information that helps explain the OOB situation. Normally, the three types of caption boxes are: strength, unlocated units, and legend. At lower tactical echelons, the OOB situation overlay and the enemy situation map are combined for simplicity. At higher echelons, applicable analysts maintain separate types of OOB on overlays near their work area. A composite OOB overlay is used for the enemy situation map and for briefings (see fig. 3-3). The IAS allows the rapid generation of tailored electronic overlays based on available data base information.

OOB Record

As referenced in Standardization Agreement (North Atlantic Treaty Organization [NATO]) (STANAG) 2077, *Orders of Battle*, OOB record files are used to maintain accurate and complete data on all units. Normally, one record is maintained on each threat unit in a position to affect current or future operations (see fig. 3-4 on page 3-10). The OOB record contains the following information:

- Service (branch of armed forces to which the unit belongs, including paramilitary and insurgent).
- Formation or unit name (official title).
- Alternative name (unofficial name).
- Role (principal function of the unit, e.g., command, combat, combat service support [CSS]).
- Superior formation (immediate senior formation or unit).
- Headquarters location name (nearest identifiable town or village).
- Headquarters location coordinates (universal transverse mercator [UTM] and latitude and longitude).



Located Units (by type)			Unlocated Units
Committed Forces			
Unit	No.	Weapon	Recon Bn, 38th GMR Div 114th Tk Regt, 38th GMR Div UI Ind Tk Bn, 38th GMR Div SSM Bn, 38th GMR Div
Mech Bn	6		
Tk Bn	2	80 T-64	
Reinforcement			
Tk Regt	1	94 T-64	
Ind Tk Bn	1	51 T-64	
Fire Support			
SSM Bn	1	SS-21	
Arty Bn	8	18xBM-21 MRL 18x152mm SP How 72x122mm How 36x122mm SP How	

Arty=artillery
Bn=battalion
Div=division
GMR=guard motorized
How=howitzer
Ind=Independent
Mech=mechanized
mm=millimeter
MRL=multiple rocket launcher
Recon=reconnassiance
Regt=regiment
SP=self-propelled
SS=surface-to-surface
SSM=surface-to-surface missile
Tk=tank
UI=unidentified

Figure 3-3. Example of OOB Overlay.

PARENT FORMATION									
Service		Formation or Unit Name		Alternative Name		Role		Superior Formation	
HQ Location Name		HQ Location Coordinates		Combat Effectiveness		Allegiance		Commander's Last Name	
SUBORDINATE FORMATIONS/UNITS									
Serial Number	Subordinate Unit or Formation Name	Location Coordinates	Role	Signature Equipment	Equipment Quantity	Commander's Last Name	Personnel Strength	Combat Effectiveness	Record Date/Update
Record Evaluation and Source					Remarks				

SAMPLE

Figure 3-4. Sample OOB Record.

- Combat effectiveness assessment (ability to perform intended mission or function expressed in a percentage).
- Allegiance (entity or country to which unit owes its loyalty).
- Commander's last name.
- Subordinate formations' and units'—
  - Serial number.
  - Subordinate unit name.
  - Location coordinates (UTM and latitude and longitude).
  - Role.
  - Signature equipment (equipment that might identify the unit).
  - Equipment quantity (number of signature equipment in the unit).
  - Commander's last name.
  - Personnel strength (assessed strength).
  - Combat effectiveness.
  - Record date and update (date of information or last time record was updated whichever is later).
  - Record evaluation and source (listing of source and reliability as well as validity of the information).
  - Remarks (e.g., unit history, insignia).

Personality File

Personality data on designated categories of individuals are recorded. Information on key figures is valuable in establishing an opponent's intent.

Military Installation File

This file contains collected information on each installation, to include the—

- Number and types of buildings and their capacities.
- Personnel uniforms and insignia.
- Major items of equipment.
- Maps, town plans, or sketches that show the location of each installation within the city.

Organizational Chart

This chart depicts the organization of units, from the highest headquarters to the lowest unit. It includes personnel and major weapon strengths. Principal weapon and equipment charts may be prepared to supplement organizational charts.

Strength Worksheet

Used to maintain a running numerical tabulation of the enemy's personnel and equipment strengths, the worksheet contains information recorded on committed units, fire support units, and reinforcements. The strength worksheet may be combined with OOB cards or other unit files. See chapter 8 for a detailed discussion of combat strength assessment.

Target Files

Target files are either standard (full page) or card type files.

Target Intelligence Files

Target intelligence files are developed selectively and aggressively to include the targets which, when attacked, will have an effect on the enemy. These files contain the following information:

- Location (geographic and UTM coordinates, accurate within 10 meters).
- Altitude (target location expressed in meters or feet above sea level).
- Description (type, shape, attitude, dispersion, and composition).
- Vulnerability (assessed vulnerability of target to ordnance delivery, including construction, degree of protection, and dependence of the target on component parts).
- Recovery time (accurate assessment of the time required for the enemy to replace or return the target to active or usable status).
- Accessibility (location of a target with respect to other terrain or cultural features that may limit the direction or angle of attack).
- Importance (estimate of how the enemy would be affected by damage to that target).

Target Card Files

These files are comprised of sets of cards; each card contains a target serial number and information concerning a specific target. Target card files are prepared and maintained on current targets and serve as a basis for the preparation of the target list and target bulletins. Cards are also prepared and maintained on potential targets so that a threat unit changing status can quickly be added to the target list. Complete target card files are maintained by commands that will exercise control of the target list during some phase of the operation.

Tools Automation

The IAS provides an automated means to employ the intelligence recording tools. When attached to appropriate communications, the IAS can automatically filter, parse, collate, update, and display threat-related data received from the national and theater level's modernized integrated data base. That data can be manipulated to provide the functionality of an intelligence journal, enemy situation map, workbook, OOB overlays, OOB files, and target files. Desktop application software can be used to generate spread sheets for strength tabulations and other files.

SECTION III. EVALUATION

During evaluation, the intelligence section determines the relevance**,** the source reliability, and the accuracy of recorded information. Evaluating information in this manner also determines whether immediate or deliberate production and dissemination should be performed.

Relevance

Upon receipt, each item of information is examined for its relevance by area, time, and content. Information relevant to the AO or AOI is processed further. Urgent information is rapidly evaluated and disseminated to those who need it. Information that is not of an urgent nature is usually fully evaluated, interpreted, and disseminated later.

Reliability

The information source and the information collection agency are evaluated for reliability. The principal basis for judging the reliability of a source or agency outside the MAGTF is previous experience with the source. Normally, analysts expect a highly reliable source to provide accurate information. Analysts must consider that even highly reliable human sources have limitations and a reliable electronic source may be subject to enemy interference and deception measures. Information reported from reliable sources should be compared with other facts before being classified as fact.

The headquarters closest to the source or agency is ordinarily the best judge of its reliability. Normally, a higher headquarters accepts the reliability evaluation of the reporting headquarters. Criteria for evaluating MAGTF unit reliability include knowledge of the unit's—

- Training.
- Experience.
- Past performance.

Accuracy

Accuracy involves the probable truth of the information. The most reliable method of judging accuracy is comparison with other information obtained through other collection sources and agencies.

A marked difference in the information accuracy evaluation may occur between higher and lower echelons. Higher echelons have access to more sources of information and intelligence than lower echelons, thus they provide more opportunity to confirm, corroborate, or refute the accuracy of reported data.

Regardless of the source, the accuracy of each report or piece of information is reevaluated at each echelon. Processed, evaluated, and interpreted information received from higher headquarters may be old, or new information that was not available at the time of the higher headquarters assessment may alter the information's accuracy.

Evaluation Rating System

A technique for evaluating the reliability and accuracy of information is determined by using a standard system described in STANAG 2022, *Intelligence Reports*. This system uses code letters to indicate reliability of the source and code numerals to indicate accuracy of the information.

Evaluation ratings are most valuable when information is disseminated to higher, adjacent, or lower units. Each item of information in a report should contain an evaluation to aid the recipient in understanding its significance.

Reliability Evaluation Codes

Agencies are ordinarily rated **A, B,** or **C**; however, when the source and the collecting or reporting agency are evaluated differently, the lowest degree of reliability is indicated. Reliability of the source is rated as—

- **A**—Completely reliable (indicates the source has experience and extensive background with the type of information reported).
- **B**—Usually reliable (indicates a source of known integrity).
- **C**—Fairly reliable.
- **D**—Not usually reliable.
- **E**—Unreliable.
- **F**—Reliability cannot be judged (indicates there is no basis for estimating the reliability of the source).

Accuracy Evaluation Codes

Accurate ratings are preferred, but when the truth cannot be judged, the rating of **6** is always favored over the inaccurate of ratings **1** to **5.** The accuracy of information is rated as—

- **1**—Confirmed by other sources (indicates that the information confirms currently held information and originates from a different source).
- **2**—Probably true (indicates that the information confirms all or essential parts of currently held information and does not come from the same source, but cannot be confirmed by other sources).
- **3**—Possibly true (indicates that the reported facts, on which no further information is yet available, are compatible with the previously observed target behavior; or that the known background of a person confirms that person's reported actions).
- **4**—Doubtfully true (indicates unconfirmed information that contradicts estimates or the known behavior of the target).
- **5**—Improbable (indicates information that is not confirmed by available data and that contradicts the experience previously assumed reliable).
- **6**—Truth cannot be judged (indicates there is no basis for ratings 1 to 5 because of the complete absence of other information on the same subject).

Although both letters and numerals are used to indicate the evaluation of an item of information, they are independent of each other. A completely reliable agency may report information obtained from a completely reliable source which, on the basis of other information, is judged to be improbable and rated as **A-5**. A source known to be unreliable may provide raw information that is confirmed by reliable sources, accepted as credible information, and rated as **E-1**. A report evaluated **F-6** may be accurate and should not be arbitrarily discarded.

CHAPTER 4. ANALYTICAL THINKING

Through analysis, information is transformed into knowledge. Understanding is achieved by applying judgment to knowledge, and the future is anticipated by understanding the present. Intelligence analysts enhance the understanding of the commander and staff to reduce uncertainty, limit risk, and support planning and decisionmaking. To enhance understanding for the commander, intelligence analysts must understand how decisionmaking occurs, the forms of reasoning, and the pitfalls often associated with analysis. At a minimum, the analyst must—

- Know the commander's mission, intent, and guidance.
- Understand the battlespace framework, which includes the AO, AOI, battlefield organization, and tangible and intangible factors (e.g., culture, politics, economics, religious, ethnic).
- Understand information management.
- Understand friendly and threat doctrine and tactics.
- Develop PIRs and IRs with the commander, other staff sections, and subordinate units' intelligence officers, who are geared to answer or provide additional information on a threat's capabilities, vulnerabilities, intentions, and COAs.
- Understand how to use analytical tools (i.e., IPB, automated intelligence systems, data bases, indications and warning, situation development, targeting, and OOB factors).
- Relate information to the six intelligence functions and METT-T.

SECTION I. ANALYTICAL PROCESS

Intelligence personnel analyze, synthesize, and estimate data gathered on a specific area or subject to support the commander's decisionmaking process.

Analysis

Analysis is a process used by commanders and analysts to establish IRs, to study information and available intelligence, and to determine a threat's capabilities, vulnerabilities, intentions, and COAs against friendly operations and systems. During analysis, a commander's AO and AOI are dissected for pertinent information and intelligence. In its simplest terms, analysis breaks down a geographic region or subject into bits and pieces of information and evaluates that information for its significance. Analysis considers the battlespace and its parts in terms of depth, width, height, time, surface, subsurface, and both friendly and threat commanders' IRs and decision cycles.

The commander starts the analysis process by defining the battlespace and submitting IRs; analysts can then—

- Focus on the AO and critical aspects of the AOI.
- Prioritize all IRs.
- Query intelligence data bases.
- Determine gaps.
- Leverage collection and production assets to estimate the threat's capabilities, vulnerabilities, and intentions.

Synthesis

Synthesis is the piecing of information into a coherent, meaningful picture. It is based on the ongoing or previous analysis of separate information and events taking place within a given area. More than simply pulling together information, synthesis determines the relationships that exist among that information. It allows commanders and analysts to see the battlespace as a whole and to rapidly discern emerging patterns and indicators. Threat capabilities, vulnerabilities, and intentions are estimated based on the synthesized picture.

Estimation

Estimation is the most challenging element and the last step in the analytical process. It involves a high degree of risk because it addresses future outcomes and probabilities. Intelligence analysts must stretch their intellectual resources to the limit to provide the best estimate possible given the information at hand and the needs of the commander. Employing experience, judgment, intelligence tools, and methodologies, the intelligence analyst must base estimates on solid analysis of identified activity patterns to determine the threat's intentions and probable COAs as well as the effects of those actions on friendly forces. The following example illustrates the analysis, synthesis, and estimation process.

Example: Analysis, Synthesis, and Estimation Process.

Information from aerial reconnaissance indicates the movement of approximately 31 moving target indicators (MTIs). The MTI locations and times are annotated on a mission report. Based on this report, the analyst conducts mental functions (analysis), attempts to fuse this information into what is happening in the battlespace (synthesis), and predicts intentions (estimation). To arrive at a conclusion, the analyst—

- Plots MTI locations on a situation map and annotates the date-time group. Looks for any relationships to previously reported units in the area and—
  - If a relationship is not found, determines what must be done to answer the who, what, where, and why questions.
  - If a relationship is found, determines the type of unit (e.g., tanks, armored personnel carriers), the direction of movement, and the unit's speed as MTIs pass through named AOIs.
- Looks at the big picture to synthesize the information and to answer the following questions:
  - Does the movement indicate where the MTIs will be committed?
  - Is this part of the threat's main effort?
- Prepares to state the threat's intentions through the combination of analysis and synthesis.
  - Provides an estimate, which specifies the type of equipment, the unit designator, the speed of march, and the probable time of attack.

SECTION II. ANALYTIC PROBLEM SOLVING

Intelligence analysis involves the application of reason and logic to solve problems related to the effects of weather, terrain, and threat on current and future friendly operations. During fast-paced, tactical-level operations, the entire analyze-synthesize-estimate process may occur mentally within a matter of seconds. At higher levels, the process may be more involved, with more time available to rigorously apply the analytical techniques. This section discusses

the problem solving analytical theories, terms, and processes most commonly used by military intelligence analysts.

Analytical Theories

Most analytical theories begin with a proposition or premise, which is a statement that may or may not be true.

Proposition or Premise

A proposition or premise is a combination of evidence and assumptions, which, when combined, lay the foundation for an argument, hypothesis, or conclusion. Propositions can be detailed or abstract, observable or inferable, with varying degrees of certainty and fuzziness.

Detailed

In military intelligence, the term for a detailed proposition is a specific information requirement. An example of a detailed proposition is: "An enemy company is defending at named area of interest (NAI) 13." When creating this mental proposition, the analyst is at the "I wonder if stage" of analysis. Because the statement is not known to be true or false, the analyst rephrases the proposition as a question. For example: "Is there an enemy company defending at NAI 13?" The detailed proposition requires verification from a collection asset.

Abstract

The doctrinal term for an abstract proposition is an IR, but commanders designate critical abstract propositions as PIRs. An abstract proposition might be: "Is the enemy's main effort going to be along the landing beaches south of Church Hill?" This proposition is abstract because no one single observation will confirm or deny it. The abstract proposition requires analysis and deduction based on multiple collection asset reports of detailed propositions. These reports would allow the analyst to discern or infer the enemy's main effort.

Observable

A single collection asset can verify a detailed proposition through observation and documentation in a single report.

Inferable

Abstract propositions can only be inferred by the analysis of a set of detailed propositions from multiple reports. The intelligence staff normally generates specific information requirements to subdivide an IR or PIR into more detailed propositions that can be addressed through integrated intelligence operation (i.e., collection, production, and dissemination) planning. The relationship between two propositions allows an intelligence analyst to make inferences and analyze intelligence information or to arrive at analytical conclusions. This relationship is expressed as: "Proposition X causes proposition Y." The same relationship can also be expressed as: "From the observance of proposition Y, we can infer proposition X." The following example illustrates the relationship between two propositions.

Example: Relationship between Two Propositions.

The existence of a regimental artillery group at NAI 14 will cause the existence of certain air defense assets in and around NAI 14. This proposition is restated as: "From the observance of certain air defense assets in and around NAI 14, we can infer the existence of a regimental artillery group at NAI 14."

The probability of each relationship must be taken into account. For example, the types of air defense assets normally associated with the regimental artillery group may also protect a logistic support area or command post. It is more accurate to state: "From the observance of a certain type of air defense near NAI 14, we can infer there is a 50 percent probability of a regimental artillery group in the NAI 14, a 40 percent probability NAI 14 contains a logistic support area, and a 10 percent probability it contains a command post."

Certainty and Fuzziness

Propositions have varying degrees of both certainty and fuzziness. Certainty is the degree of belief in something. An example of certainty is: "I personally saw an enemy company at NAI 13, and we have six corroborating reports." A less certain proposition would be: "HUMINT has a semireliable source that claims there is a company at NAI 13, and we have no other reports on the subject."

Fuzziness is the measure of how well the known information matches the desired information. An example of a certain proposition is: "Our patrol reports the exact number of enemy soldiers and equipment for an enemy company." A fuzzy proposition would be: "Our patrol reports about half the number of personnel and equipment of an enemy company, so this could be an augmented platoon, two understrength platoons, an extremely weak company or an under-reported enemy company."

A Priori

Probabilities, in the absence of other information, are called *a priori*. In practice, the *a priori* is rarely assessed in isolation of other information; however, more information is possessed than the contents of a single report. This leads to the use of a conditional probability. An example of this situation states *a priori* of the enemy commander choosing to concentrate his/her main effort along avenue of approach number 1 (AA-1) may be 66 percent. However, the conditional probability of the main effort along AA-1 might be 25 percent given that an unusually large number of combat vehicles on AA-2 were observed.

Applied Logic

Typically, intelligence deals with obscure data, few facts, and severe time constraints, which can limit the analyst's ability to apply formal logic in intelligence analysis. Nevertheless, there are areas of applied logic that are most relevant to intelligence analysis.

In its most basic form, analysis involves drawing reliable conclusions based on facts, opinions, and inferences. As information is received, it is categorized as either fact or opinion. From these facts and opinions, analysts attempt to piece together a picture of the battlefield and the commander's battlespace and to make certain inferences or conclusions. When presenting the resulting conclusions, it is important to distinguish between what is fact and what is opinion.

Facts

A fact is a statement that has been demonstrated to be true. As an example, it is a fact that you are reading this statement. Given a preference, an analyst will always choose to work with facts. Unfortunately, facts are not always available. In the absence of facts, opinions may be used. Combining available facts and expert judgment, analysts attempt to piece together a picture of the battlefield and the commander's battlespace. When presenting the resulting conclusions, it is important to distinguish between what is fact and what is opinion.

Opinions

When facts are unavailable, an analyst might use opinions. An opinion is what someone believes to be true, but it may or may not be true. Sometimes opinions are uttered as statements of fact and often they reflect value judgments. A value judgment is an expression of personal taste, reference, worthiness, merit, quality, excellence, or bias. For example: "Electronic intelligence is a far more reliable source of intelligence than HUMINT." In this case, the speaker's perception is an opinion or generalization. Analysts must use extra caution when basing conclusions on opinions.

Inferences

Inferences are conclusions drawn from facts, opinions, or other inferences. Noting that one area of foliage appeared discolored in contrast

to surrounding foliage, an image interpreter concluded that the area being looked at contained a camouflaged position. Based on expert knowledge of imagery, the analyst inferred the presence of a camouflage position from the fact of discolored foliage. Such inferences may serve as input for subsequent problems; in this case, determining what is camouflaged at that particular location. Inferences are particularly important in determining a threat commander's intent. Unless the threat commander announces it, intent can only be established by inference. Such inferences are based on facts developed through the continual study of an adversary's doctrine, tactics, and capabilities. Whenever possible, inferences should be drawn from facts, or a mixture of facts and opinion. Conclusions drawn from opinions alone are prone to be wrong and should not carry the same weight as those drawn from facts.

Reasoning

Reasoning is the mental process that is brought to bear on facts, opinions, and inferences. Analysts solve problems through deductive and inductive reasoning.

Deductive

The process of reasoning from general cases to specific cases is deductive reasoning. It is the drawing of conclusions from one or more propositions or premises. For example, the statement, "Air strikes and naval bombardment always precede an amphibious landing," is a proposition based on an assumption. Propositions may or may not be true; in the case of the statement above, not all amphibious landings are preceded by preparatory fires. For deduction to be used effectively, intelligence analysts must make certain their propositions are true and their reasoning is correct or valid.

Example 1: Deductive Reasoning.

A Naval intelligence analyst is given a report about an unidentified submarine transiting the polar ice cap. The analyst deduces that—

- The ability to transit under the ice cap requires long submerged endurance.
- The only submarines with adequate endurance are nuclear-powered.
- The unidentified submarine is nuclear-powered.

In this case, the analyst reasoned from a general type (submarines) to a specific type (nuclear-powered).

In the example, the propositions are stated as facts. However, depending on the time of year, the polar ice cap can be transited on the surface. Furthermore, the second proposition, although stated as a fact, assumes that the threat has not developed high-endurance power sources other than nuclear energy. As a result, the conclusion, although valid, is unreliable. In order to be reliable, a conclusion must be drawn from valid and true propositions. If a deductive argument is valid, and if the propositions of that argument are true, then the conclusion of that argument must also be true.

Example 2: Deductive Reasoning.

During a field training exercise, reconnaissance elements are able to photograph opposing force tanks in defilade. The photograph shows a main gun tube with a 125mm bore and three track-return rollers. Four types of threat tanks are equipped with the 125mm gun (T-64, T-72, T-80, and T-90), but only two have three track-return rollers (T-72 and T-90). Since the T-90 was not replicated in this exercise, analysts conclude that friendly forces will be engaging T-72 tanks. In this case, the reasoning went from the general (125mm gun and three track-return rollers) to the specific (T-72, which was the only tank with both characteristics replicated in the exercise). The argument is valid and the propositions forming the argument are true, so the conclusion of the argument must also be true.

Inductive

The process of arriving at conclusions based on evaluating facts or inferences is inductive reasoning.

Example 1: Inductive Reasoning.

The following reports reach an intelligence agency regarding the actions of two adversarial countries—

- Country X is massing armor and artillery along the border of Country Y.
- Country X has also blockaded sea-lanes used by both countries.
- Finally, Country X has imposed wartime restrictions on its civilian population.

From these reports, the analyst uses inductive reasoning by inferring that hostilities between the two countries are imminent.

Induction goes beyond the facts or observations to a statement that has not been or cannot be verified. Since only verified data can be called reliable, conclusions drawn inductively are somewhat unreliable.

Example 2: Inductive Reasoning.

An intelligence analyst is given the following information about a coalition armored vehicle:

- Fact 1—Five road wheels and four return rollers.
- Fact 2—Armament that includes a single 73mm gun, one coaxial- and two hull-mounted 7.62mm machineguns, and a single SAGGER antitank missile mounted on the barrel of the 73mm gun.
- Fact 3—Crew of four with three passengers.
- Inference 1—A maximum speed estimated to be 80 kilometers per hour.

From these characteristics, the analyst inferred that the reported vehicle was a Russian-made BMD. Since a number of separate facts or inferences were used in the reasoning process, the analyst arrived at a conclusion through inductive reasoning.

The strength of an inductive argument depends on how probable the conclusion would be true if the premises or propositions were true. Inductive arguments are characterized as being strong or weak vice valid and invalid. Arguments are made strong by—

- The number of instances cited in the propositions.
- The number of propositions that confirm the conclusion.
- The closer in time the occurrences are to the conclusion.
- Dissimilarities in the evidence that still support the conclusion.

Very often propositions used in deduction are arrived at inductively and vice versa.

Example: Deduction and Induction.

Major proposition: The massing of troops along a border is a prelude to war.

Minor proposition: A country is known to have massed troops along the border.

Conclusion: This country is about to initiate war with its neighbor.

At first glance, the deductive argument shown above might seem acceptable. However, a closer look will show that the major proposition is not always true. In certain instances, troops could be massed for internal security, exercises, or a show of force. The major proposition, derived from inductive reasoning, by itself is an ambiguous signal. Assuming the propositions are true, and assuming the analyst reasoned validly, the conclusion the analyst reached is valid. An analyst may reason correctly, but from data that is incorrect, thus arriving at conclusions that are not true.

Tests of Truth

Both inductive and deductive reasoning involve three basic tests of truth that intelligence analysts employ to determine the truth of propositions.

Correspondence Test of Truth

The theory that truth is a statement that corresponds to reality is known as the correspondence test of truth. An analyst, who is studying an information report, notices that the presented information is the result of first-hand observation. Knowing the source to be professionally competent, the analyst assumes that every statement in the report corresponds to reality.

In the example, the statements or other evidence corresponded to reality. To test the degree of correspondence, observations are required. These observations must be tested by additional observations. The chief criterion in observations is objectivity, and using a mix of collection assets can attain greater objectivity.

Analysts naturally place more confidence in one source or system than another. In the case of the UAV report verses the pilot's report, the analyst had more confidence in the UAV's ability to observe the target from multiple aspects. The UAV-derived information had more credibility than the pilot's report, because the pilot may have only had a fleeting glimpse of the target while trying to egress. When a variety of sensors tend to corroborate each other, confidence in the conclusions increases.

The correspondence test of truth requires observations to test whether or not, and to what extent, statements correspond to reality. One problem with this theory is that the threat seldom permits direct observations and often goes to great lengths to prevent direct observations or to deceive those observations.

Example: Correspondence Test of Truth.

Pilots returning from an interdiction mission claim three tanks destroyed. The squadron chief interrogated each pilot separately and they gave substantially the same report.

Assuming the pilots' claims are accurate, then it would reflect reality. By reporting battle damage assessment of three tanks probably destroyed, the squadron chief is adhering to the correspondence test of truth.

Despite the fact that all pilots of one flight claimed three tanks destroyed, the MAGTF commander wants more supporting evidence. To provide confirmation, the MAGTF G-2 plans an UAV mission over the area where the tanks were reportedly hit. Both the commander and the G-2 are placing more credibility in visual evidence, because it is believed to be more objective and less prone to human error. This ignores the fact that video requires interpretation, and this interpretation involves a degree of subjectivity.

Humans must interpret all images. When humans interpret images, they use subjective judgment. One of the weaknesses of the correspondence test of truth is that observations are required to establish the truth. Invariably, these observations must be tested by other observations.

The UAV tape revealed three badly damaged tanks in defilade. The MAGTF battle damage assessment analyst considers the UAV report along with the pilot debriefs. Based on the combined information, the analyst reports three tanks confirmed damaged.

Coherence Test of Truth

This test of truth uses consistency with other ideas or facts to validate statements. Where direct access to the threat is denied, the coherence test of truth becomes necessary. The coherence theory refers to how consistent different pieces of information are in relation to each other. An analyst considering a new piece of information

that corroborates known information would place more credibility in the new information and the conclusions drawn from it.

In the realm of theory, intelligence usually works with some factual basis for most inferences or conclusions. The coherence test of truth supplements the correspondence test of truth.

Example: Coherence Test of Truth.

In the latter part of September, the commander in chief's intelligence staff considered the following information:

- The ACME coalition countries normally conclude a training cycle with a large-scale combined exercise (historical record).
- Visitors to Coyote Land reported being denied access to certain areas in the vicinity of Road Runner in the western Tunnel Province (confirmed report).
- Reports indicate certain infantry, armor, and engineer units from Tasmania, Elmer Land, and Chickenhawk have moved from their garrison locations (unconfirmed reports).
- All commercial air traffic to Road Runner will be restricted for a period of 2 weeks, starting 1 October (confirmed report).

The intelligence staff concluded that this year's ACME exercise will take place in or near Road Runner, Tunnel Province, during the period 1 to 14 October. Although no one piece of information pointed directly to this conclusion, all pieces of information seemed consistent with each other as well as to the conclusion.

Pragmatic Test of Truth

This test proposes that a given statement is true if it works in practice.

A practical tool, the pragmatic test of truth has some weaknesses. First, the results may only appear to justify the means used to achieve them. Second, a successful outcome may be attributed to other factors that could have produced the same outcome. In the Admiral Scott example, the use of radar-controlled guns may have produced the same result no matter what formation was used. Lastly, an unsuccessful outcome does not necessarily imply that the means used were unsound; again, other unknown factors may have contributed to the unsuccessful outcome.

Example: Pragmatic Test of Truth.

Prior to the Battle of Cape Esperance in World War II, Admiral Norman Scott organized a task force into a long, single column. Admiral Scott believed this line-ahead formation would be effective against the Japanese units' night tactics. In the ensuing battle, Scott sank two Japanese destroyers and severely damaged two cruisers. After the battle, Admiral Scott concluded the original line-ahead formation theory was indeed effective. By combining radar-controlled fire control systems with line-ahead formation, Admiral Scott believed any night battle could be mastered.

SECTION III. PITFALLS OF ANALYSIS

The application of logic and reasoning is a mental process that is subject to numerous influences. Intelligence analysts involved in discerning facts, inferences, and conclusions are prone to the influences that shape and mold their view of the world and their ability to reason. These influences are referred to as pitfalls of analysis. To minimize their impact, analysts must be able to recognize these pitfalls in their own analysis and the analysis performed by others. Logical

fallacies and biases are two general categories of analytical pitfalls.

Logical Fallacies

Logical fallacies are errors in the reasoning process caused by the failure to apply sound logic. Though usually committed accidentally, these fallacies are sometimes used deliberately to persuade, convince, or deceive. Omission and assumption are two categories of logical fallacies.

Omission

Fallacies of omission leave out something important. The argument may omit a consideration of many cases; it may omit a consideration of a hypothesis that would account for the same conclusion; or it may omit something unfavorable to the argument. Fallacies of omission can occur in many forms.

Oversimplification

Oversimplification is a generality that fails to adequately account for all the complex conditions bearing on a problem.

Example 1: Oversimplification.

"Air power and the M1A1 tank won the Gulf War." This statement ignores the fact that the attack aircraft and the M1A1 tank were only two of many weapons systems and other capabilities used to provide critical support and ultimate success during the Gulf War.

Oversimplification results when one or more of the complex conditions pertaining to a certain situation are omitted and includes—

- Ignoring facts.
- Using generalities.
- Applying an inadequately qualified generalization to a specific case.

Example 2: Oversimplification.

An ordnance specialist inspecting a captured, hand-carried, surface-to-air missile launcher concludes that the threat has no effective low-level air defense. The assessment is based on the fact that the launcher is equipped with antiquated guidance mechanisms. The ordnance specialist's conclusion omits the following considerations:

- That the launcher was planted by the threat to give a misleading picture of their true capabilities.
- That the threat abandoned the launcher because it was ineffective and more capable systems were available.
- The weapon may have been deliberately doctored to mislead weapons experts.

Other weapons (e.g., antiaircraft artillery, small arms) can be very effective in some situations.

Hasty Generalization

Conclusions drawn from samples that are too few or from samples that are not truly representative are hasty generalizations.

Example: Hasty Generalization.

After interrogating an enemy prisoner of war (EPW), the interrogation officer reports the threat's morale as extremely low and that surrender is imminent.

In this case, the interrogator is making a hasty generalization because the sample population considered (one EPW) is too small.

Composition

The fallacy of composition is erroneously reasoning from the properties of a single entity to properties of a group.

Example: Composition.

During a skirmish with a Viet Cong battalion, a single EPW was captured. This EPW was suffering from malaria, malnutrition, and low morale. It was noted that the EPW was equipped with a semiautomatic weapon of World War II vintage. After a brief interrogation, the intelligence analyst reported the enemy battalion recently engaged was starving, diseased, and poorly armed.

The intelligence analyst failed to consider that—

- The one prisoner captured was too sick to keep up with the rest of the battalion.
- The weapon of early vintage did not necessarily make it ineffective.
- Few captured prisoners have high morale; in fact, low morale could just as easily result from being captured as it could contribute to being captured.

In this example, besides falling prey to hasty generalization, the analyst also demonstrated the fallacy of composition by applying the properties of a single prisoner to an entire enemy unit.

Division

The fallacy of division erroneously assumes that the characteristics of a group exist in every member of that group.

Example: Division.

Members of the threat guard's brigade had never surrendered in previous combat. After a recent engagement, an EPW claimed membership in the guard brigade. The interrogator doubted the EPW's statement because personnel from that brigade never surrender.

In this example, the interrogator committed the error of division by assuming that since no guard brigade personnel had ever surrendered, the EPW could not be from that brigade. The analyst took the characteristics of a unit and uniformly applied them to every member of that unit.

Special Pleading

In special pleading, only one side of an argument is presented.

Example: Special Pleading.

At the conclusion of a staff study, the staff members, who are proponents of the proposed COA, are directed to list the pros and cons of the proposal.

Arguments for the proposal:

- Job requires little to no increase in staffing.
- Job can save the Government 2 million dollars.
- Risk to personnel is minimal.
- Equipment is readily available.
- Little special training is required.
- Arguments against: None.

By omitting arguments against the COA, the staff committed the fallacy of special pleading. This fallacy also arises when the many interacting forces that give rise to a situation (i.e., cause and effect) are ignored.

Post Hoc

In the fallacy of *post hoc* ergo *propter hoc* (before the event, therefore caused the event), consideration of other factors that might have accounted for the same result are omitted. Post hoc fallacies often occur when trying to establish cause and effect.

Example: Post Hoc.

An aircraft equipped with a new jamming pod was not fired on while flying over threat-controlled territory. It was concluded that, since the aircraft was not intercepted or fired upon, the jamming pod was extremely effective in suppressing threat electronic systems.

The conclusion may or may not account for the aircraft not being attacked. Other considerations include—

- The threat was obtaining electronic intelligence on this new pod.
- The threat recently relocated several surface-to-air missile units and did not want to reveal their new positions.

False Dilemma

The fallacy of the false dilemma omits consideration of more than two alternatives.

Example 1: False Dilemma.

"Either we attack at dawn or the enemy will be too strong."

The two words that generally warn of a potential false dilemma fallacy are "either" and "or." False dilemmas exclude middle alternatives and consider only options of two extreme positions.

Example 2: False Dilemma.

An intelligence staff officer reports to the commanding officer that the enemy has only the capability to either defend in place or retreat. The intelligence officer committed the fallacy of false dilemma by failing to anticipate or ignoring that the enemy could—

- Attack if they were willing to accept high casualties.
- Withdraw to an alternate defensive position.
- Conduct a delaying action.

Assumption

Fallacies of assumption relate to begging the question, stating hypotheses contrary to fact, poisoning the well, and misusing analogies. All of these fallacies implicitly or explicitly involve assumptions, which may or may not be true.

Begging the Question

This fallacy occurs when a speaker gives what is assumed to be a legitimate response to a question but it is merely a rephrase of the question.

Example 1: Begging the Question.

When asked why the enemy was not pinned down by fire, the platoon leader replied: "Our suppressive fire was inadequate."

The fallacy in this response is that by definition suppressive fire pins down or intends to pin down the enemy. Since the platoon failed to pin down the enemy, the inadequacy of this fire was self-evident.

Example 2: Begging the Question.

A pilot reporting to a debriefing officer stated: "In response to your questions about whether or not all of my bombs landed on target, I'd like to say that as soon as I completed my pass there were two large secondary explosions."

The pilot begs the question by shifting attention from the primary issue to a secondary one. The response did not address the question that was asked.

Stating Hypotheses Contrary to Fact

This fallacy occurs when someone states decisively what would have happened had circumstances been different. Such fallacies involve assumptions that are either faulty or simply cannot be proven.

Example: Hypotheses Contrary to Fact.

If we had not supported Castro in his revolutionary days, Cuba would be safe for democracy today.

Besides being a gross oversimplification, the assumption made in the statement cannot be verified.

Poisoning the Well

This fallacy seeks to discount evidence before it is presented, most often by discrediting the source.

Example 1: Poisoning the Well.

An ardent spokesperson against the value of strategic bombing states: "You can't trust that Air Force employee's testimony regarding the effectiveness of strategic bombing.

The speaker is trying to discredit contrary evidence by creating the specific impression that the testimony is biased because the testifier represents a certain organization.

Example 2: Poisoning the Well.

One intelligence analyst says to another analyst engaged in pilot debriefs: "Be careful with these pilots; it is their first mission."

This statement intends to discredit evidence before it is presented. It pleads against the subject by assuming that the pilots' lack of experience will result in bad information.

Misusing Analogies

Analogies are strong tools that can impart understanding in a complex issue. In the absence of other evidence, intelligence analysts may reason from analogy. Such reasoning assumes that the characteristics and circumstances of the object or event being looked at are similar to the object or event in the analogy. The strength of a conclusion drawn from analogy is proportional to the degree of similarity between two objects or events. The danger in reasoning from analogy is assuming that because objects, events, or situations are alike in certain aspects, they are alike in all aspects.

Conclusions drawn from analogies are inappropriately used when they are accepted as evidence of proof. Situations may often be similar in certain aspects, but not in others. When one generalizes indiscriminately from analogy to real world, this is misusing analogies. One method for weakening an analogous argument is by citing a counteranalogy. A counteranalogy weakens the original analogy by citing other comparisons that can be made on the same basis.

Biases

A subjective viewpoint, bias indicates a preconceived notion about someone or something. Although biases interfere with successful analytic thinking, they can have a positive influence on analysis. With a lack of information, a preconceived notion can give the analyst a starting point for thinking about a situation. However, biases generally have a detrimental impact because they obscure the true nature of the information. Intelligence analysts must be able to recognize cultural, organizational, personal, and cognitive biases and be aware of the potential influence they can have on judgment.

Cultural

Americans see the world in a certain way. The inability to see things through the eyes of someone from another country or culture is cultural bias. Biases interfere with the analyst's ability to think the way an enemy commander might think or to give policymakers informed advice on the likely reaction of foreign governments to American policy. Also known as mirror imaging, cultural bias attributes someone else's inten-

tions, actions, or reactions to the same kind of logic, cultural values, and thought processes as the individual analyzing the situation. Although cultural bias is difficult to avoid, the following measures can lessen its impact:

- Locate individuals who were born or raised in the analyzed country or culture and—
  - Include them in the analytical process.
  - Ask their opinion about likely responses to friendly actions.
  - Take care when using their opinions, since they may be subject to biases regarding ethnic groups or cultures in the region and their knowledge may be dated or inaccurate.
- Locate regional experts such as foreign area officers and regional area officers who have lived or traveled through the area and are somewhat conversant regarding the culture. Assess the quality of the information provided against the level of knowledge and experience the individual has for that culture or region.

Organizational

Most organizations have specific policy goals or preconceived ideas. Analyses conducted within these organizations may not be as objective as the same type of analysis done outside the organization. Groupthink and best case are organizational biases that can affect subjective internal analysis.

Groupthink

This bias occurs when a judgment is unconsciously altered because of exposure to selective information and common viewpoints held among individuals. Involving people outside the organization in the analysis can combat this bias.

Best Case

This bias occurs when an analyst presents good news or bad news in the most optimistic light. The judgment is deliberately altered to provide only the information the commander wants to hear. Analysts can avoid this bias by having the moral courage to tell the commander the whole story, good and bad.

Personal

Personal biases stem from past experiences. If a thought pattern previously led to success, the analyst tends to follow that pattern. Even if the situations have nothing in common, the tendency to follow past successful methods is very strong.

Cognitive

The all-source intelligence analyst evaluates information from a variety of sources (e.g., HUMINT, SIGINT, IMINT, open source). The degree of reliability, completeness, and consistency varies from source to source and even from report to report. This variance often creates doubt about the reliability of some sources. Cognitive biases that affect the analyst include vividness, absence of evidence, oversensitivity to consistency, persistence of impressions, dependence on memory, and acceptance of new intelligence.

Vividness

Clear and concise or vivid information has a greater impact on analytical thinking than abstract and vague information. A clear piece of information is held in higher regard than a vague piece of information that has more value as evidence. Analysts must consider that an enemy may use deception to portray vivid facts, situations, and capabilities that they want the friendly intelligence effort to believe.

Absence of Evidence

Lack of information is the analyst's most common problem, especially in the tactical environment. Analysts must do their best with limited information and avoid holding back intelligence because it is inconclusive. To avoid this bias, the analyst should—

- Realize that information will be missing.
- Identify areas where information is lacking and consider alternative hypotheses.
- Adapt or adjust judgments as more information becomes available.
- Consider whether a lack of information is normal in those areas or whether the absence of information itself is an indicator.

Oversensitivity to Consistency

Consistent evidence is a major factor for confidence in the analyst's judgment. Information may be consistent because it is appropriate, or it may be consistent because it is redundant, is from a small or biased sample, or is the result of the enemy's deception efforts. When making judgments based on consistent evidence, the analyst must—

- Consider if the evidence represents all available information and intelligence. If it does not, or if it is not known, then the confidence level will be low, regardless of the consistency.
- Be receptive to information that comes in from other sources regardless of whether it supports the hypothesis or not.
- Be alert against confirmatory circular reporting, which is intelligence already obtained by the unit that is then reformatted by other units and intelligence organizations, modified slightly, and disseminated back to the unit.
- Know, to the degree possible, the original source for all intelligence to ensure that a circular report is not used as confirmatory evidence for an intelligence estimate or conclusion.

Persistence of Impressions

When evidence is received, there is a tendency to think of connections that explain the evidence. Impressions are based on these connections. Though the evidence eventually may be discredited, the connection remains and so do the impressions.

Dependence on Memory

The ability to recall past events influences judgment concerning future events. Since memory is more readily available, it is easy to rely on memory instead of seeking a proper sample to predict events.

Acceptance of New Intelligence

Often newer intelligence reports are valued more than older intelligence reports, which can occur when the intelligence collectors or sources are different.

> **Example: New versus Old Intelligence.**
>
> A ground reconnaissance team reports at 1300 that an enemy mechanized column is moving along a line of communications (LOC) at a given speed and direction. Later, at 1325, an AV-8B in-flight report indicates that the enemy column is moving along a different LOC.
>
> In such cases, the newer intelligence report should be assessed against the full tactical context, and not simply its timeliness, to preclude incorrect intelligence interpretations.

Using the above example, follow-on coordination with the better situated ground reconnaissance team, capable of observing the same LOC and enemy targets for a greater period of time, may lead to a very different intelligence interpretation.

SECTION IV. DECISIONMAKING

One aim of intelligence analysis is to allow the commander to make timely and informed decisions by providing the right elements of available information at the right time and place. Gaining more information can reduce uncertainty, but a decrease in uncertainty occurs at the expense of time. Uncertainty and time always influence the commander's analytical and intuitive decisionmaking ability.

Analytical

In analytical decisionmaking, several options for solving the problem at hand are identified, studied, and compared to arrive at the best solution. Basically, comparing multiple options concurrently produces the optimal solution. This approach to decisionmaking tends to be methodical and time-consuming.

Intuitive

In intuitive decisionmaking, the commander assesses the situation in an effort to recognize a pattern; once a pattern is identified, experience and judgment guide the commander in evaluating the key elements of the problem and rapidly determining a satisfactory solution. The intuitive approach focuses on situation assessment instead of on the comparison of multiple options. Generally much faster than analytical decisionmaking, intuitive decisionmaking aims at finding the first solution that will satisfactorily solve the problem.

Comparison

Each analytical and intuitive decisionmaking approach has strengths and weaknesses. Although conceptually distinct, the two are rarely mutually exclusive. Intelligence supports analytical decisionmaking by helping to identify available options and by providing the estimates and studies for comparisons of those options.

Intelligence supports intuitive decisionmaking by providing the knowledge that helps the commander recognize emerging patterns. The process of intelligence analysis employs both analytical and intuitive decisionmaking to arrive at the conclusions presented to the commander. The IPB process, particularly if the various types of products are prepared in detail, is a distinctly analytical process. The decision support template derived from the IPB process, however, is a tool that facilitates intuitive decisionmaking. Generally, the analytical approach conforms well to the prehostility or contingency planning phase, while the intuitive model is usually more appropriate during execution of tactical operations.

The challenge for the intelligence analyst is knowing how much and what kinds of information the commander requires. Too much information may only confuse an intuitive decisionmaker and information requirements will change continually. Too little information for an analytical decisionmaker may result in procrastination and the continual demand for more information. The key to overcoming these challenges is a solid understanding of the commander, constant interaction through training and exercises, and a well developed process for identifying information requirements.

CHAPTER 5. INTELLIGENCE PREPARATION OF THE BATTLESPACE

An analytical methodology, IPB is employed during operations to identify, assess, and reduce the effects of enemy, environment, and terrain uncertainties on friendly and threat forces. The IPB process analyzes the threat and environment in a specific geographic area to determine and evaluate the threat's capabilities, vulnerabilities, and probable COAs. Designed to support staff estimates, planning, and decisionmaking, IPB results are incorporated into the intelligence estimate, which provides knowledge-based intelligence that can be visualized and absorbed by decisionmakers. See appendix A for a detailed outline of the intelligence estimate format. The formatted graphics and images provided through the IPB process help the commander to rapidly visualize, assimilate, and apply intelligence in the decisionmaking process. This enhances the commander's ability to discern patterns as they emerge and to conduct recognitive or intuitive decisionmaking, thereby increasing operational tempo.

Operations and intelligence must have a common focus to successfully apply the interactive IPB process. See FM 34-130/Fleet Marine Force Reference Publication (FMFRP) 3-23-2, *Intelligence Preparation of the Battlefield*, for a detailed discussion of the IPB process.

The IPB requirements for a humanitarian assistance operation differ significantly from a combat operation against a conventional armed force. In a given situation, a unit or staff section may prepare some or all IPB products. Determining which products to prepare and identifying their relative priority depends on the factors of METT-T and command guidance.

The IPB process develops tailored, mission-focused, knowledge-based intelligence that is incorporated into a variety of intelligence products. Intelligence preparation of the battlespace provides intelligence in graphic and image formats that help the commander rapidly visualize, absorb, and apply the intelligence in the decisionmaking process. Numerous standard overlays and graphics are associated with the IPB process; however, each situation is unique. A modified combined obstacle overlay and threat doctrinal template that support conventional operations may be of limited use in military operations other than war (MOOTW). The type of products generated as a result of IPB vary based on the—

- Size of the unit.
- Time available.
- IRs.
- Characteristics of the mission and AO.

The IPB process defines the battlespace environment, describes the battlespace effects, evaluates the threat, and determines threat COAs. These steps are discussed in this chapter and remain constant regardless of the type of mission or size of the staff section; however, the application of the steps varies with each situation. This chapter also goes into detail about the decision support template and discusses the abbreviated IPB process.

SECTION I. STEP 1—DEFINE THE BATTLESPACE ENVIRONMENT

The first step of the IPB process identifies the physical space and specific features of the environment or activities that may influence friendly and enemy COAs and commander's decisions. When defining the battlespace environment, intelligence analysts conduct the following procedures.

Identify Significant Characteristics of the Environment

Characteristics of the battlespace environment that will influence the commander's decisions or affect the COAs available to friendly forces or the threat are of special significance. During a humanitarian assistance operation, for example, the location and activities of civilian relief organizations might be a significant characteristic of the battlespace. During support to counterdrug operations, significant characteristics might include narcotics production or weapons trading. During a conventional war, typical characteristics may include location and activities of enemy reserves, reinforcements, and long-range fire support. When identifying significant characteristics of the battlespace, intelligence personnel consider threat forces and other aspects of the environment that may have an effect on accomplishing the unit's mission. Depending on the situation, these environmental aspects may include—

- Geography (e.g., area terrain and weather).
- Population demographics (e.g., ethnic groups, religious groups, age distribution, income groups).
- Political or socioeconomic factors (e.g., the role of clans, tribes, gangs).
- Infrastructures (e.g., transportation, telecommunications).
- Rules of engagement or legal restrictions (e.g., international treaties, agreements).
- Threat forces and their capabilities (e.g., paramilitary and unconventional forces).

Initially, each environmental characteristic is examined in general terms to identify its significance to the command and its mission. Identifying the significant characteristics of the battlespace environment helps establish the geographical limits of the AOI and directs analytical efforts in steps 2 and 3 of the IPB process. It also helps identify uncertainties or gaps in the type of information and intelligence required to complete the IPB process and answer the PIRs and IRs (see fig. 5-1).

Identify the Command's Area of Operations and Battlespace Limits

The AO represents an area assigned to a commander with authority and responsibility for the conduct of operations (see fig. 5-2). The limits of the AO are normally the boundaries specified in the OPORD or higher headquarters execute order that defines the command's mission.

Area of Influence

This is the geographical area where a commander is able to influence operations through C2 of maneuver or fire support systems. Based on the range of organic or supporting weapon systems, the area of influence may extend beyond the AO.

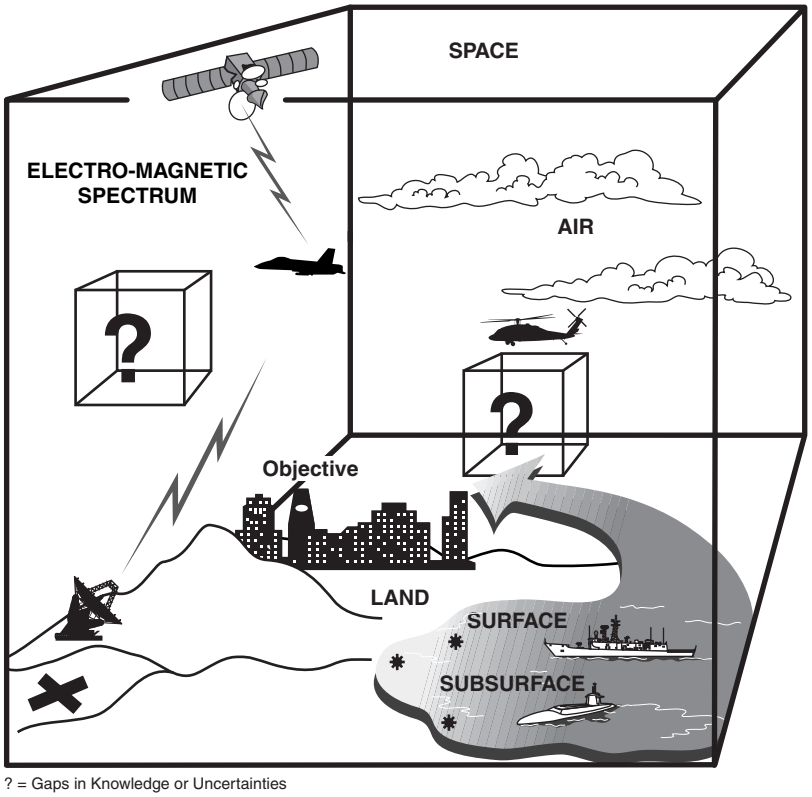


Figure 5-1. Battlespace Examination.

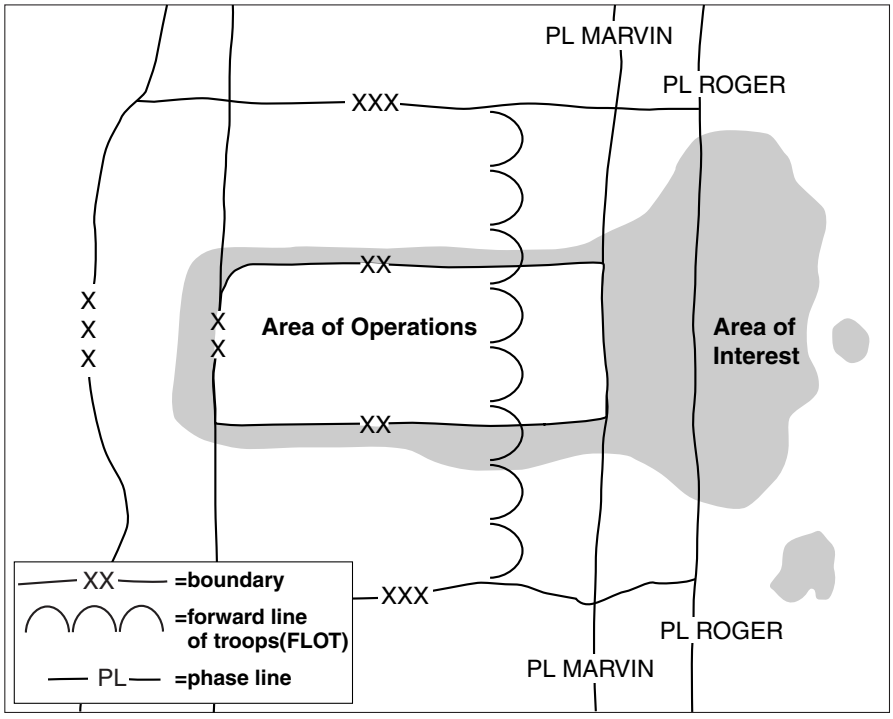


Figure 5-2. AO and AOI.

Area of Interest

The commander selects the AOI based on the estimate of the situation. The dimensions are not constrained by the organic ability to acquire information on that area. The AOI must extend, in as irregular a shape and as far as needed, in all directions to safeguard the command from surprise (see fig. 5-2). The AOI must be viewed in terms of width, depth, height or airspace, and time.

Battlespace

The battlespace is all aspects of air, surface, subsurface, land, and space, as well as the electromagnetic spectrum, the information environment, and other dimensions which encompass the AO, the area of influence, and the AOI. Figure 5-3 depicts many of these battlespace dimensions and factors.

Establish the Area of Interest Limits

The AOI is the geographical area from which information and intelligence are required to permit planning or successful conduct of the command's operation. The command's AOI is generally larger than its AO. The limits of the AOI include each of the characteristics of the battlespace environment identified as exerting an influence on potential COAs or command decisions.

The limits of the AOI are based on the ability of the threat to influence the accomplishment of the command's mission. The geographical locations of other activities or characteristics of the environment that might influence COAs or the commander's decision and the resulting changes in the command's battlespace must be considered when establishing AOI limits.

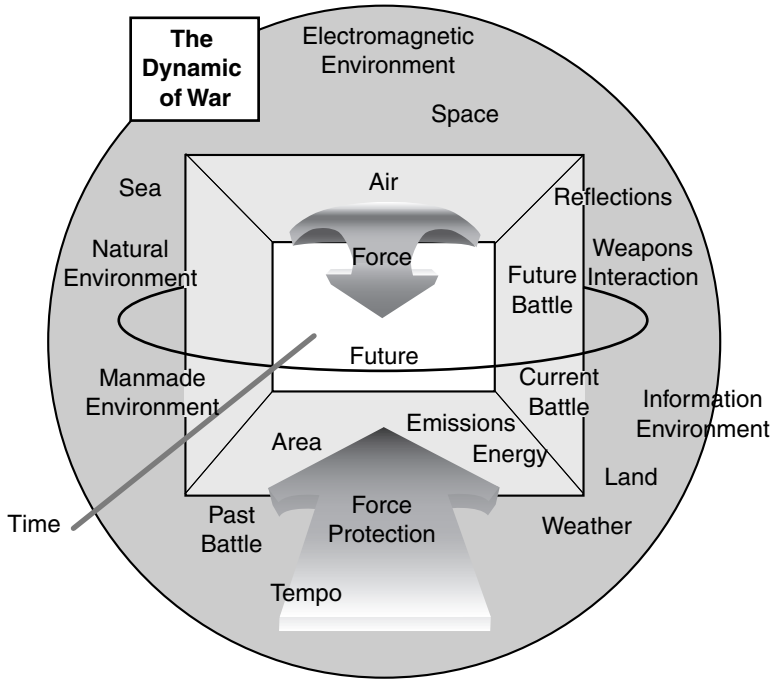


Figure 5-3. Battlespace Dimensions and Factors.

Areas of interest can be divided into several components (e.g., ground, air, political). Altitude must be considered in the air AOI when the projection of air power is of interest. When an air defense-related IPB is conducted, the AOI should extend upwards to the maximum service ceiling of the threat's aircraft. When an aviation-related IPB is conducted, the AOI should extend to the maximum service ceiling of friendly aircraft or the maximum effective altitude of threat air defense systems, whichever is greater. When space-based IPB is conducted, the AOI must extend to the maximum effective altitude of relevant space-based systems. Although AOIs may be developed separately, at some point they must be considered as an integrated whole.

One of the primary considerations in establishing the limits of the AOI is time. The time limit is based on the threat's ground and air mobility and the amount of time needed to accomplish the friendly mission. For missions of relatively short duration, such as the evacuation of noncombatants or raids, the AOI may be relatively small and usually includes only immediate, direct threats to mission accomplishment. A helicopter raid where the MAGTF has air superiority might have an AOI that includes only air defense systems within the range of the engagement area and the air routes. Some long-term missions, such as peacekeeping, will result in an extensive AOI that considers political, economic, and conventional military factors.

Since the limits of the AOI are based on threats to mission accomplishment rather than strictly terrain considerations, the limits may cross into neutral countries. If developments in a neutral country might influence accomplishment of the unit's mission, that country must be included in the AOI.

Identify the Detail Required for the Time Available

The time available for completion of the IPB process may not permit the luxury of conducting each step in detail. The focus must be on the parts of IPB that are most important to the commander in planning and executing the mission. Identifying the amount of detail required avoids wasting time on developing more detail than necessary in each step of the process. For example, the situation may require detailed threat analysis only on selected areas within the command's AO based on the assigned mission or other METT-T factors. Some geographical areas or threat forces within the AO may require only a summary type evaluation of their effects or capabilities.

Evaluate Existing Intelligence Data Bases and Identify Intelligence Gaps

Data bases may only contain some of the intelligence and information required to evaluate the effects of each battlespace characteristic and each threat force. This is especially true of the majority of countries where the MAGTF may conduct operations in the future. Identifying the intelligence gaps early allows the intelligence analysts to initiate action required for collecting intelligence and filling the gaps, to perform the necessary production, and to disseminate the intelligence products in a timely manner. When evaluating existing data bases, intelligence analysts must—

- Identify and prioritize the intelligence gaps in current holdings, using the commander's PIRs and intent to set the priorities.
- Identify any gaps that cannot be filled within the time allowed for IPB.
- Inform the commander and operators of unfilled gaps so that reasonable assumptions can be formulated.

Collect the Required Intelligence and Materials

Ideally, intelligence operations enable the analyst to develop estimates of the battlespace and the threat that match the actual situation. In reality, intelligence will never eliminate the unknown aspects or uncertainties that concern a commander and staff. Intelligence analysts must be prepared to fill in the gaps with reasonable assumptions and estimates. When collecting the required intelligence and materials, intelligence analysts must—

- Initiate collection or requests for intelligence to fill the gaps and to conduct IPB.
- Prioritize collection against all identified significant characteristics of the battlespace.
- Initiate action on identified IPRs and continuously update the IPB products as additional intelligence is received.
- Inform the commander as assumptions are confirmed during the initial mission analysis and IPB process.
- Re-examine the evaluations and decisions on which proven invalid assumptions were based.

SECTION II. STEP 2—DESCRIBE THE BATTLESPACE EFFECTS

The second step in the IPB process is to determine how the battlespace environment affects both threat and friendly operations. This evaluation step begins with an analysis of existing and projected conditions of the battlespace environment and determines how those conditions will affect friendly and threat operations and broad COAs. Intelligence analysts describe the battlespace effects by analyzing the battlespace environment, such as terrain, weather, and other battlespace characteristics, and by describing the battlespace effects on threat and friendly capabilities and broad COAs.

Analyze the Battlespace Environment

The degree of detail in the analysis varies depending on the area of the battlespace environment being evaluated. Generally, the AO is evaluated in more detail than the AOI. Additionally, the focus varies throughout each area. For example, rear areas within the AO may require a different focus than areas near the main battle area. Certain areas or subsectors affect various types of operations to varying degrees. During the evaluation, intelligence analysts must identify areas that favor each type of operation (e.g., offensive, defensive, force protection, peace enforcement). Terrain, weather, and other characteristics of the battlespace are analyzed as part of the IPB process.

Terrain

Terrain analysis is the means to determine which friendly COAs can best exploit the opportunities the terrain provides and how the terrain affects the threat's available COAs. The best terrain analysis is based on a reconnaissance of the AO and AOI. Analysts must identify gaps in knowledge of the terrain that a map analysis cannot satisfy and use the identified gaps to guide reconnaissance planning and to focus on areas most important to the commander and the mission.

The members of intel bn's topographic platoon usually conduct the major portion of the terrain and hydrographic analysis and development of supporting GEOINT products. They also receive

support from Army topographic units operating as part of or in support of the joint force. Topographic personnel work closely with weather personnel and weather analysts to ensure that terrain analysis incorporates the effects of current and projected weather events.

The National Imagery and Mapping Agency (NIMA) produces specialized maps, overlays, and automated data bases for specified areas of the world to aid in map-based evaluations. The tactical terrain analysis data base consists of selected terrain information that is limited to natural and manmade features of tactical military significance, which can be exploited by terrain analysts to satisfy military requirements. Specialized NIMA products address—

- Cross-country mobility.
- Transportation systems (road and bridge information).
- Vegetation type and distribution.
- Surface drainage and configuration.
- Surface materials (soils).
- Ground water.
- Obstacles.

Terrain analysts must ensure that the analysis includes the effects of existing and forecasted weather on the military aspects of the terrain, because changes to the battlespace environment may change the terrain analysis evaluation results. Analysts express the results of evaluating the terrain's effects by identifying areas of the battlespace that favor, disfavor, or do not affect each broad COA. These conclusions are reached through analysis of the military aspects of the terrain and evaluation of the terrain's effects on military operations.

Analyze the Military Aspects of the Terrain

Terrain analysts evaluate the following military aspects of terrain to determine the effects on military capabilities:

- Key Terrain—Any locality or area (natural or manmade) that the seizure, retention, or control of will afford a marked advantage to either combatant.
- Observation and Fields of Fire—Observation is the ability to see the threat either visually or through the use of surveillance devices. Fields of fire are areas that a weapon may effectively cover with fire from a given position.
- Cover and Concealment—Cover is protection from the effects of direct and indirect fires. Concealment is protection from observation. Ditches, caves, river banks, folds in the ground, shell craters, buildings, walls, embankments, woods, underbrush, and other natural or manmade features can provide cover and/or concealment.
- Obstacles—Any natural or manmade feature that stops, impedes, slows, or diverts military movement.
- Avenues of Approach and Mobility Corridors—Avenues of approach (AAs) are air, sea or ground routes of an attacking friendly or threat force of a given size leading to its objectives or to key terrain in its path (see figs. 5-4 below and 5-5 on page 5-8). Mobility corridors are areas where a force will be

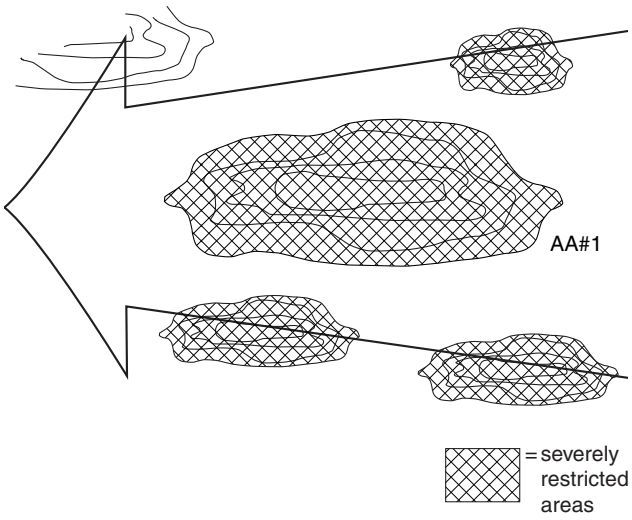


Figure 5-4. Regimental Ground AA.

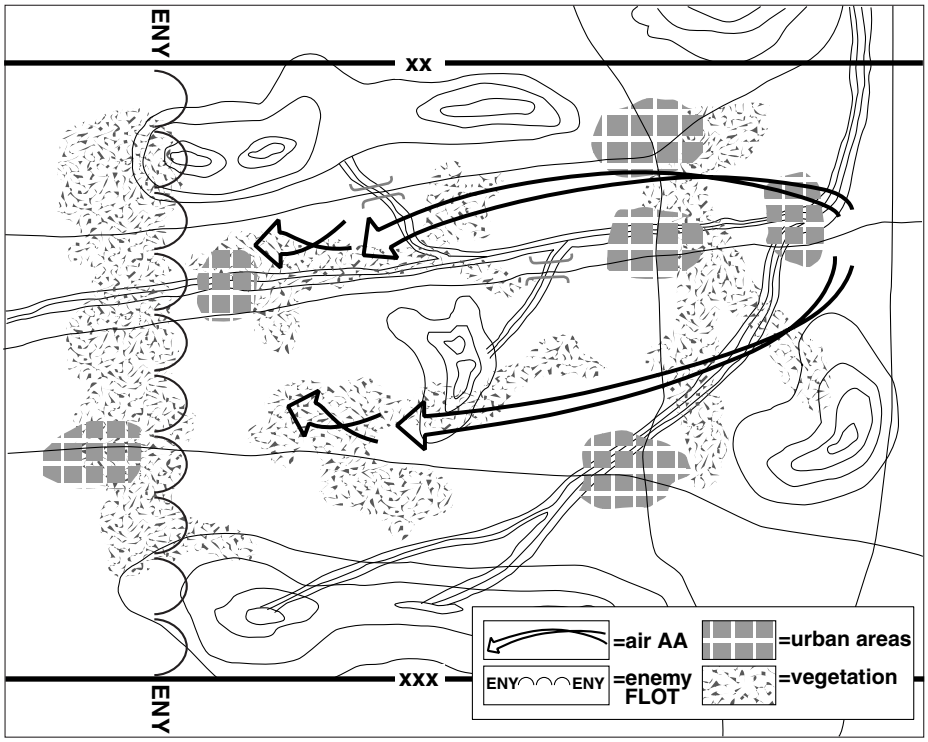


Figure 5-5. Air AAs Overlay.

canalized due to terrain restrictions. A mobility corridor is relatively free of obstacles and wide enough for maneuver of tactical formations, which allows military forces to capitalize on the principles of mass and speed. When grouped together, mobility corridors constitute an AA (see fig. 5-6). Based on previous terrain analyses, the analyst determines how the terrain will allow maneuver to objectives. Analysts must consider littorals/waterways (e.g., beaches, rivers) as possible mobility corridors and AAs.

Evaluate the Terrain's Effects on Military Operations

Terrain analysts evaluate the terrain's effects on friendly and threat offensive and defensive COAs by identifying the areas along each AA best suited for use as potential—

- Engagement areas and ambush sites—Using results of concealment and cover evaluation, terrain analysts identify areas where maneuvering forces are vulnerable to fires. They consider ranges of weapons, flight times of missiles, and the likely speed of maneuvering forces. If the unit is attacking, analysts identify areas where the unit will be vulnerable to threat fires. If the unit is defending, analysts identify potential engagement areas (see fig. 5-7).
- Battle positions—These positions may be used by friendly attacking forces to block enemy counterattacks. Terrain analysts identify concealed and covered positions that offer observation and fields of fire into potential engagement areas. If a command is defending, these positions are potential defensive positions; if a command is attacking, the positions provide a start point for determining possible threat COAs.

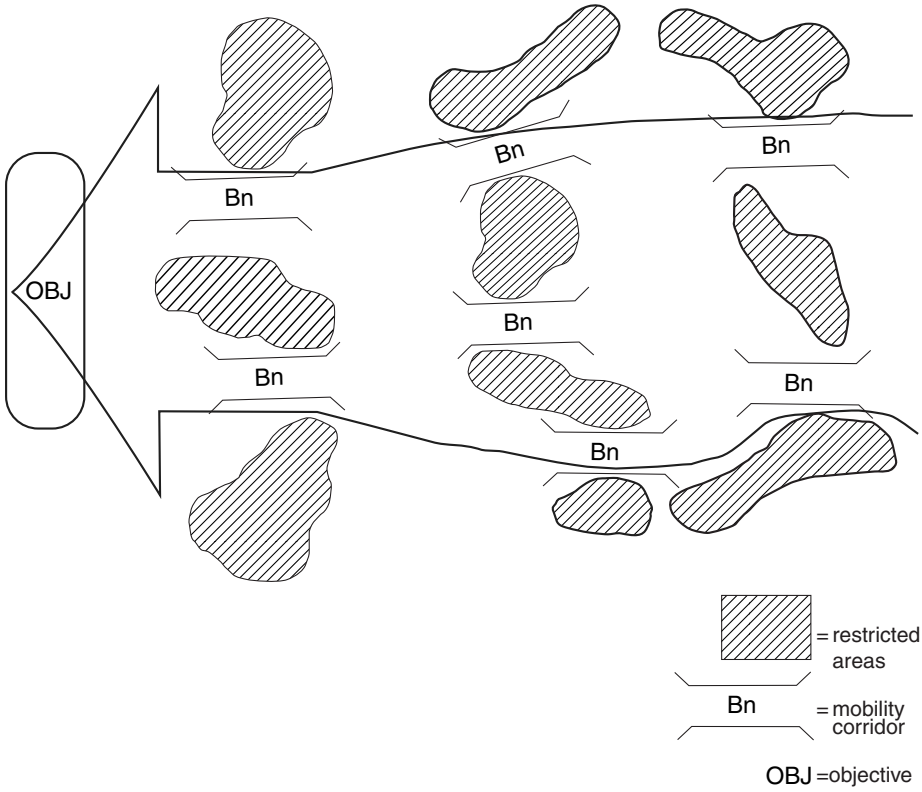


Figure 5-6. Mobility Corridors Grouped to Form an AA.

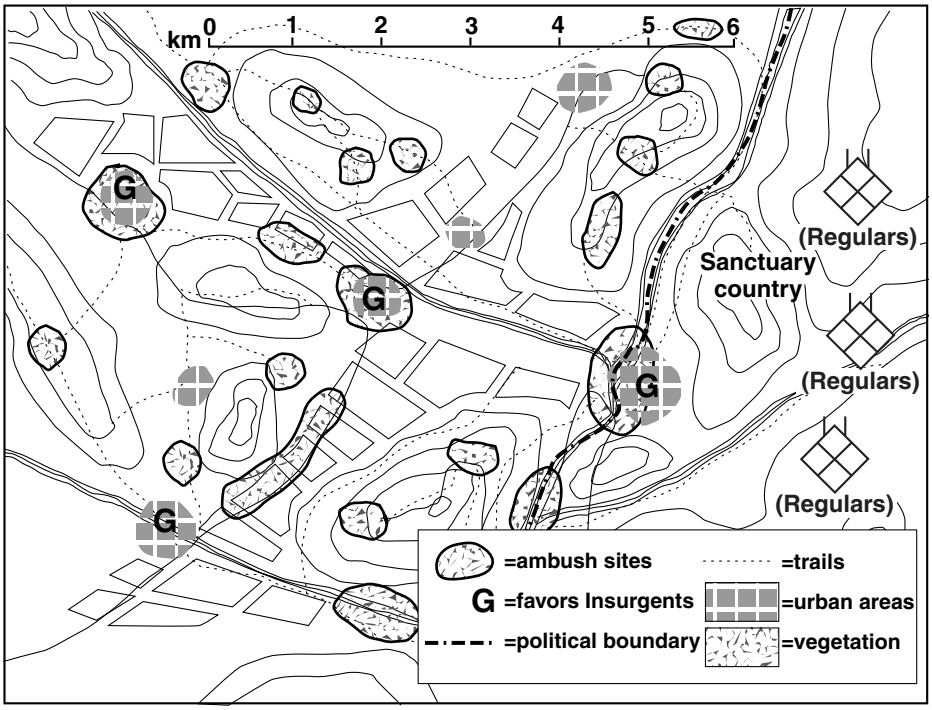


Figure 5-7. Lines of Communications and Likely Ambush Sites.

- Immediate or intermediate objectives—Terrain analysts identify any areas or terrain features that dominate AAs or assigned objective areas. These areas usually correspond to areas already identified as key terrain. As time permits, or situation requires, analysts also identify potential assembly and dispersal areas, observation posts, artillery and air defense positions, LZs, and DZs.

The terrain rarely favors one type of operation throughout the width, depth, and height of the battlespace. Based on the location and nature of the potential engagement areas and battle positions, analysts determine which areas of the battlespace favor attack or defend COAs.

Analysts consider all terrain factors in any order that best supports their analysis, but must focus on the factors most relevant to the specific situation and needs of the commander. To aid the commander's staff in the completion of their estimates and plans, analysts construct a combined obstacle overlay (COO) or a modified combined obstacle overlay (MCOO), which are graphic products that depict battlespace effects on military operations (see fig. 5-8).

Weather

Commanders can take advantage of the weather or minimize its effects through planning based on a weather analysis. During the weather analysis step, weather is studied to determine how it affects friendly and enemy capabilities to move, shoot, and communicate. Terrain and weather are inseparable factors of tactical intelligence and must be integrated. Weather forecasts and assessments contribute to intelligence and must be considered when commanders develop their COAs. The type and amount of weather support needed for a particular mission depends on the mission, the forces, the terrain, and the enemy.

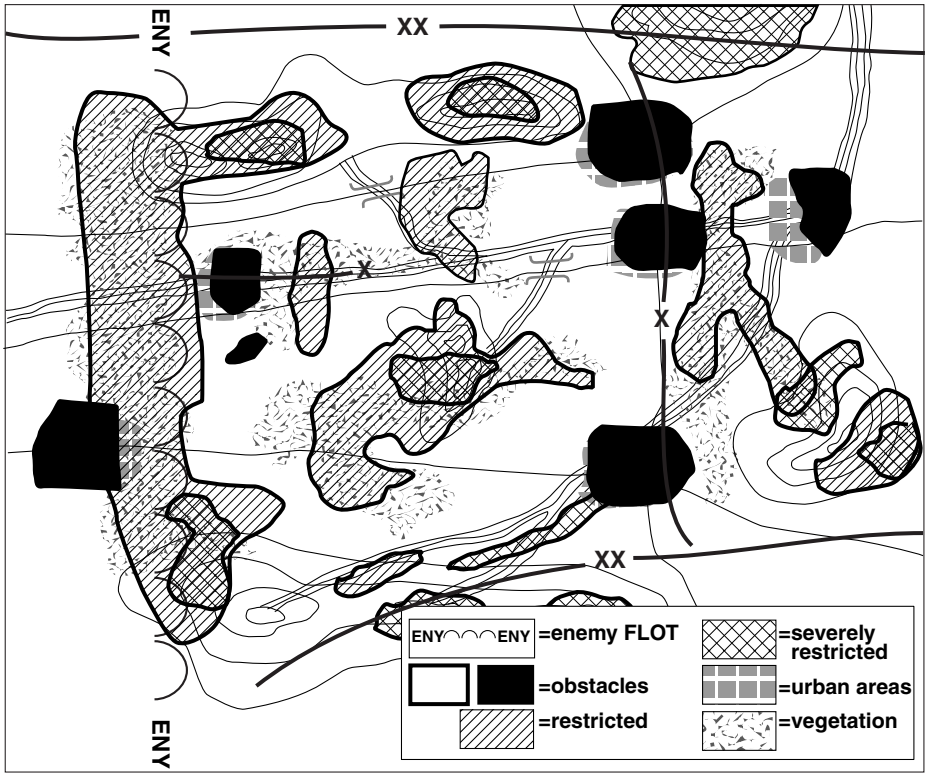


Figure 5-8. Combined Obstacle Overlay.

Evaluation of the direct effects of weather begins by establishing critical values for each aspect of the weather's effects on personnel, equipment (to include all sensors), and military operations the command may be required to perform. Unit intelligence officers and operations personnel develop detailed critical value tables for their units as part of the IPB process. These critical values are used to measure the effects of local weather on both friendly and enemy military operations. See appendix B for an example of a weather critical values table. Weather analysis is covered in more detail in chapter 6 and in Marine Corps Warfighting Publication (MCWP) 3-35.7, *MAGTF Meteorological and Oceanographic Support*. Weather analysis is accomplished by analyzing the military aspects of weather and evaluating the weather's effects on military operations.

Analyze the Military Aspects of Weather

Analysts consider the following five military aspects of weather:

- Temperature and humidity.
- Precipitation.
- Wind.
- Visibility.
- Clouds.

Evaluate the Weather's Effects on Military Operations

Weather has both direct and indirect effects on military operations. Examples of indirect effects include—

- Temperature inversions that might cause some battle positions to be at risk to the effects of chemical warfare.
- Local conditions of visibility, such as fog, that might make some potential engagement areas attractive.
- Hot, dry weather that might force a unit to consider water sources as key terrain.

Other Characteristics of the Battlespace

These characteristics include all aspects of the battlespace environment that affect friendly and threat COAs not incorporated into terrain and weather analysis. For example, an intelligence officer may report that religious considerations will make cordon and search operations on Wednesdays difficult to execute since the local population will be praying at the time of the scheduled search. Examples of other characteristics include—

- Logistic infrastructure (e.g., land use patterns, sources of potable water, bulk fuel storage, natural resources, industries and technologies, chemical and nuclear facilities).
- Population demographics (e.g., living conditions, cultural distinctions, religious beliefs, political grievances, political affiliation, education levels).
- Naval approaches.
- Economics.
- Local, regional, and international politics (e.g., treaties, agreements, legal restrictions, unofficial systems, gangs).

Although effects of other characteristics are usually discussed in text or matrix form, analysts should use graphics wherever possible. Examples of graphic depictions include an overlay showing areas most vulnerable to insurgent activity based on demographic distribution or an overlay showing high-value targets (HVTs) in the logistic infrastructure.

Describe the Battlespace Effects on Threat and Friendly Capabilities and Broad Courses of Action

Intelligence analysts combine the evaluation of the effects of terrain, weather, and other characteristics of the battlespace into one integrated product. They focus on the total environment's effects on COAs available to both friendly and threat forces.

Prior to development of friendly COAs, intelligence analysts provide the operations officer or planning staff with the following IPB products:

- An evaluated and prioritized set of AAs to assist in the designation of axis of advance, direction of attack, or zone of attack for each subordinate unit in offensive operations.
- Sets of defensible terrain along threat AAs to assist in the development of strongpoints, battle positions, or sectors for each subordinate unit in defensive and retrograde operations.
- Periods when weather conditions will optimize the use of friendly target acquisition and aviation operations to help time operations.

After the development of friendly COAs, intelligence analysts provide an evaluation of how each COA does or does not use the opportunities the battlespace provides. When addressing effects on threat COAs, intelligence analysts should view capabilities from the perspective of the enemy. The evaluation of the battlespace effects on the threat must be tailored to include weather and terrain that may affect threat weapon systems, vehicles, and personnel differently than friendly personnel. Operations and planning staffs must understand these battlespace effects on the threat to avoid assumptions that the battlespace will affect both forces equally. Other characteristics may influence threat actions more than weather and terrain, and cultural biases may cause threat personnel to view legal, political, economic, and demographic issues in an entirely different manner than friendly personnel would.

When describing the battlespace effects on threat and friendly capabilities and broad courses of action, intelligence analysts must—

- Evaluate the battlespace from the perspective of the threat.
- Express the evaluation in terms of COAs, not detailed descriptions of the analytical factors that led to the conclusions.
- Focus the commander by relating specific threat activities in both time and space.
- Back their conclusions with the detailed analysis performed.
- Communicate final conclusions in written reports such as the analysis of the AO or intelligence estimate.
- Disseminate graphic products developed during the analysis and evaluation to the staff and other commands for use in their own IPB and planning efforts.

SECTION III. STEP 3—EVALUATE THE THREAT

The third step in the IPB process is to determine the threat force capabilities and the doctrinal principles, tactics, techniques, and procedures it has historically used. This involves a detailed study of the threat's composition, tactical doctrine, procedures, weapons and equipment, and supporting systems. The intelligence section determines threat capabilities and how the threat operates by updating or creating threat models and identifying threat capabilities.

Update or Create Threat Models

Threat models depict how threat forces prefer to conduct operations under ideal conditions. They are based on the threat's normal or doctrinal organization, equipment, tactics, techniques, and procedures. Threat models result from a detailed study of the threat force. Ideally, threat models are constructed prior to deployment. Threat models consist of doctrinal templates, a description of preferred tactics and options, and identification of HVTs.

Doctrinal Templates

Doctrinal templates illustrate the deployment pattern and disposition preferred by the threat's normal tactics when not constrained by the effects of the battlespace environment. They are usually scaled graphic depictions of threat dispositions for a particular type of standard operation, such as a battalion moving to contact or an insurgent ambush (see fig. 5-9).

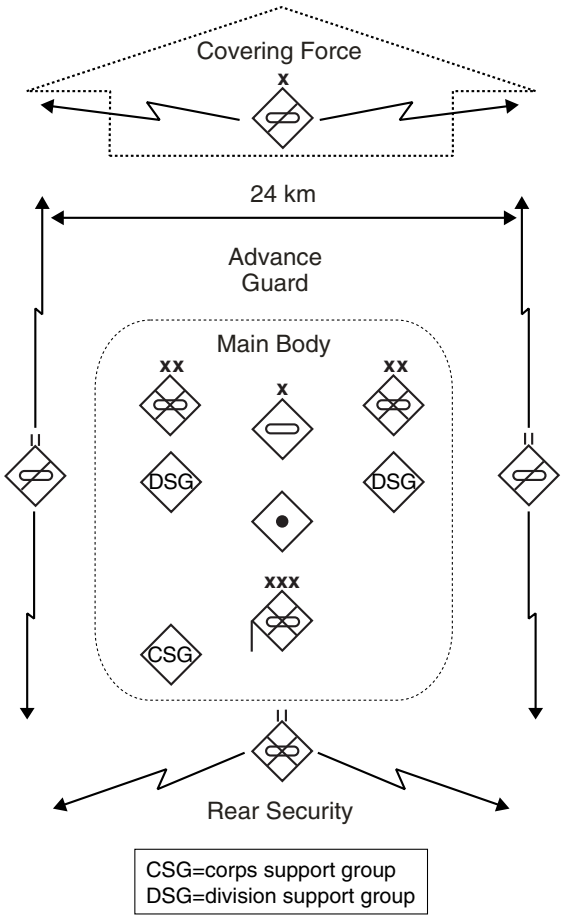


Figure 5-9. Doctrinal Template.

Doctrinal templates must be tailored to the needs of the unit or staff section creating them. Templates are constructed through an analysis of intelligence data bases and an evaluation of the threat's past operations. The analysis should focus on patterns in task organization, timing, distances, relative locations, groupings, and the use of terrain and weather. Some doctrinal templates consider the threat force as a whole, while others focus on a single battlefield function like intelligence or fires.

Description of Tactics and Options

The threat model includes a description of the threat's preferred tactics. It addresses the operations of the major units or elements portrayed on the template and the activities of different battlefield functions. It also contains a listing or description of the options (branches) available to the threat should the operation fail, or subsequent operations (sequels) if it succeeds. Even if the threat's preferred tactics can be depicted graphically, the threat model includes a description.

The description aids in mentally wargaming the operation over its duration during the development of threat COAs and situation templates. It should address typical time lines and phases of the operation, points where units transition from one formation to another, decision criteria, and each battlefield function's contribution to the operation's success. This analysis of the individual role of battlefield functions, related in time and space, will aid in the later identification of HVTs and HPTs.

Identification of Center(s) of Gravity

Marine Corps Doctrinal Publication (MCDP) 1, *Warfighting*, defines a center of gravity (COG) as any important source of strength. It may be mental, moral or physical strength, power or will. COGs may exist at each level of war: strategic, operational, and tactical. It may be tangible or intangible, and there may be multiple COGs. While knowledge of a threat's COGs at all levels is useful, the analyst should focus on the COGs appropriate to the level of operations that concern their friendly force. At this stage of the IPB process, the identification of COGs is an initial assessment.

Critical Vulnerabilities

Aspects of a COG that, if exploited, will do the most significant damage to an adversary's ability to resist are critical vulnerabilities. Vulnerability cannot be critical unless it undermines a key strength. Some vulnerabilities may contribute significantly to the enemy's downfall while others may lead only to minimal gains. Therefore, analysts must focus on a vulnerability that will do the most damage to the enemy's ability to resist.

Identification of Type High-Value Targets

Assets that the threat commander requires for the successful completion of the mission depicted and described on the template are HVTs. Examples of type HVTs include C2, intelligence, fire support, communications and information systems, air defenses, engineers, and logistics and CSS. When evaluating the threat, intelligence analysts must—

- Identify HVTs from an evaluation of the data base, the doctrinal template, the template's supporting narrative, and the use of tactical judgment.
- Develop the initial list of HVTs by mentally wargaming and thinking through the operation to identify assets that are critical to the operation's success, particularly at critical junctures or phases.
- Identify assets, which are key to executing the primary operation, particularly those that are key to satisfying decision criteria.
- Group the identified key assets into one of 13 categories used to develop target sets, thus assisting in the development of targeting strategies.
- Determine how the threat might react to the loss of an HVT; consider his/her ability to substitute other assets or modify his/her plan to compensate.
- Rank the identified HVTs with regard to their worth to the threat's operation.
- Identify HVT value changes by phase because that value usually varies over the course of an operation.
- Tailor IPB products to the command's needs by concentrating on HVTs that are important to the mission.

Identify Threat Capabilities

Threat capabilities are the broad COAs and supporting operations that the threat can take to influence the accomplishment of the friendly mission. The following four tactical or broad COAs are generally open to military forces in conventional operations:

- Attack.
- Defend.
- Reinforce.
- Retrograde.

Each of these broad COAs can be divided into more specific COAs. An attack may be envelopment, penetration, or other variations of an attack. A retrograde movement may be a delaying action, a withdrawal, or a retirement. Other threat capabilities include support to

broad COAs or specific types of operations, including—

- Deception operations.
- Riverine operations.
- Psychological operations.
- Intelligence operations.
- Nuclear, biological, and chemical weapons employment.
- Espionage, sabotage, subversive, and terrorist operations.

Threat capabilities take the form of statements, such as—

- The enemy has the ability to insert up to two infantry battalions in a single lift operation.
- The enemy can establish a prepared defense by 14 May.
- The demonstrators can effectively block traffic at up to seven intersections in our zone.

When identifying threat capabilities, intelligence analysts—

- Start with developed threat models.
- Consider other types of operations and broad COAs at other levels of war and during operations other than war.
- Consider the threat's ability to conduct each operation based on all factors related to the current situation. (The threat may be understrength in equipment or personnel, short of logistic support, lacking air support, or his/her troops may be inexperienced or poorly trained.)

SECTION IV. STEP 4—DETERMINE THREAT COURSES OF ACTION

This step of the IPB process is the identification and development of likely threat COAs that will influence the accomplishment of the friendly mission.

Identify the Threat's Likely Objectives and Desired End State

Depending on METT-T, intelligence analysts generally start identifying threat objectives and desired end state of the threat command at least one level above their own command. Analysts repeat the process for the next subordinate level to at least two levels below their own command, ensuring that each threat level's objective will accomplish the likely objectives and desired end state of its parent command. In operations other than war, analysts may be required to start more than one level above their command (e.g., the government or major clan leadership level). Usually, analysts state the threat's objectives and desired end state as assumptions. The analysts must make sure the assumptions are clearly identified as such and ensure the assumptions are discussed with the commander and staff. During operations other than war, analysts must consider more than the conventional objectives of terrain or friendly forces. This is also true at higher levels of command where the threat's political and economic objectives have a direct influence on his/her COAs.

Identify the Full Set of Courses of Action Available to the Threat

When identifying the COAs available to the threat, analysts must—

- Consider the COAs that the threat historical doctrine and tactics, techniques, and procedures (TTP) indicate are appropriate to the current situation and the likely objectives identified. This requires an understanding of the threat's decisionmaking process as well as

an appreciation for how he/she perceives the current situation.

- Consider the threat COAs that could significantly influence the command's mission, even if the threat's doctrine and TTP indicate these as infeasible under current conditions; and consider any indirect COAs that the threat is capable of executing.
- Consider the threat COAs indicated by recent activities and events. To avoid surprise from an unanticipated COA, consider all possible explanations for the threat's activity in terms of possible COAs.
- Consider each COA's subset independently to avoid forming biases that restrict the analysis and evaluation.
- Combine the subsets to eliminate redundancy and minor variations.
- Compare the consolidated list of COAs to threat capabilities identified in step 3 of the IPB process and eliminate any COAs that the threat is incapable of executing.
- Select threat models that will accomplish the threat's likely objectives based on the evaluation of the threat's capabilities.
- Examine how the effects of the battlespace described in step 2 of the IPB process influence the application of COAs (see fig. 5-10).
- Define COAs open to the threat, such as deliberate attack, hasty attack, defend, and delay.
- Define each general COA as a set of specific COAs by integrating the threat models with a description of the battlespace effects.

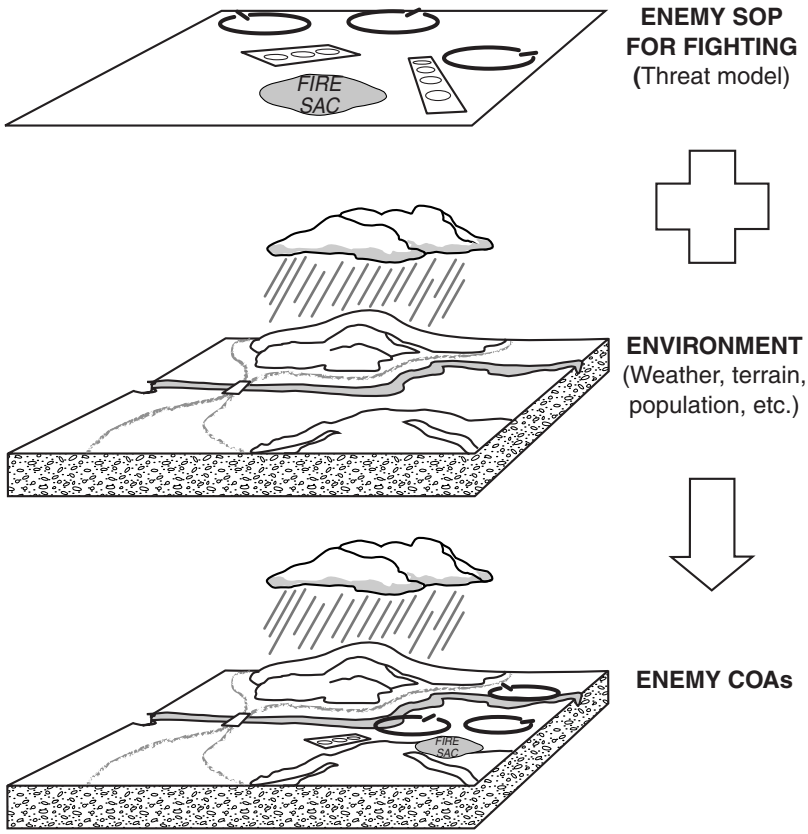


Figure 5-10. Combining Doctrine and Battlespace Effects to Develop Threat COAs.

- Ensure each COA identified is suitable, feasible, acceptable, unique, and consistent with threat doctrine or TTP and recently observed activities and patterns (see figs. 5-11 and 5-12).

Evaluate and Prioritize Each Course of Action

Analysts must evaluate each identified threat COA and prioritize it according to an estimate

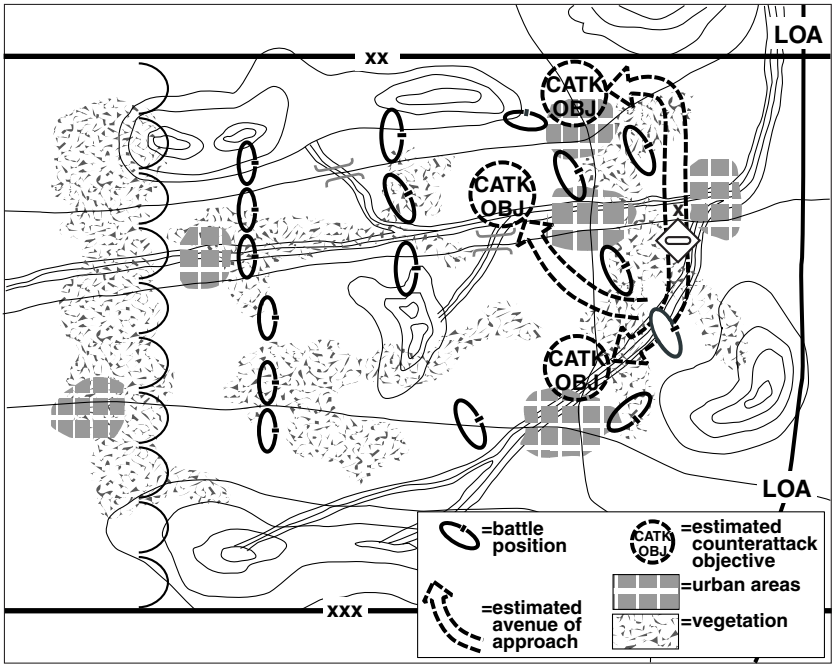


Figure 5-11. Enemy COA 1—Counterattack.

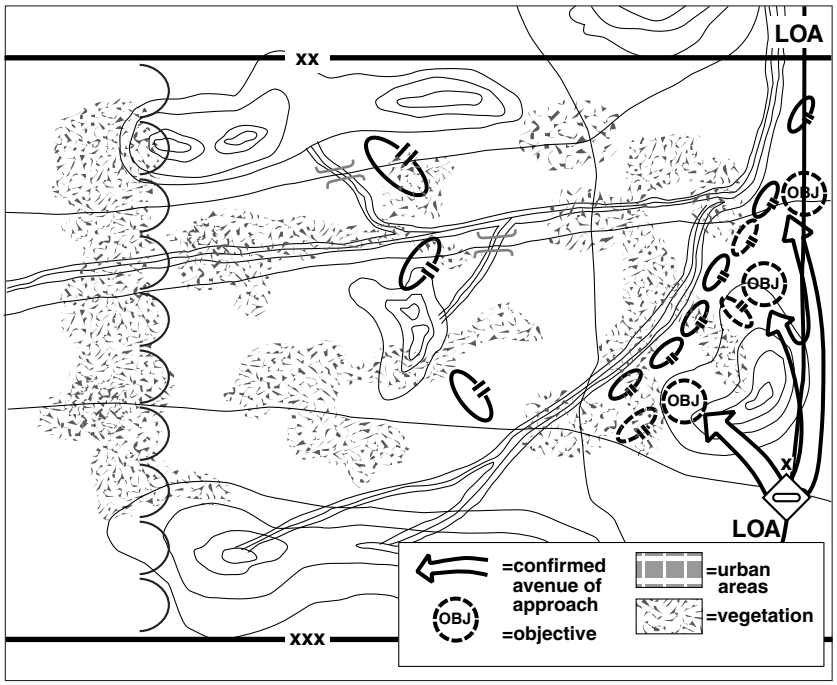


Figure 5-12. Enemy COA 2—Withdrawal from Current Position and Set Up Defense on Eastern Shore of River.

of likely adoption by the threat. The priority list allows the commander and staff to develop a plan for friendly COAs that is based on assumptions about the threat. Once the commander selects a friendly COA, the list may need to be reprioritized to reflect possible reactions to friendly dispositions and activities.

Develop Each Threat Course of Action in the Amount of Detail Time Allows

Once the complete set of threat COAs has been identified, analysts develop each COA in as much detail as the situation requires and time allows. The order in which each COA is developed is based on its probability of adoption and the commander's guidance. To ensure completeness, each COA must answer the following five questions:

- What (type of operation)?
- When (time the action will begin)?
- Where (sectors, zones, axis of attack)?
- How (method by which the threat will employ his/her assets)?
- Why (objective or end state of the threat)?

When developing each COA, analysts must consider threat forces at least one level above their own command level. For example, a battalion S-2 would consider the COAs available to threat regiments and brigades. This helps account for possible reinforcing forces and the higher threat command's objectives and intent. Generally, analysts consider threat COAs two levels of command below their own command when the MAGTF is in the offense and at least one level below their command when the MAGTF is in the defense. Thus the previously discussed battalion S-2 would depict missions and actions down to the platoon level.

Each developed threat COA has a situation template; a COA description, COGs, critical vulnerabilities, and options; and a listing of HVTs.

Situation Template

Situation templates are graphic depictions of expected threat COAs (see fig. 5-13). Templates usually depict the most critical point in the operation as agreed upon by the G-2/S-2 and G-3/S-3. An analyst may prepare several templates to illustrate different points of time in an operation, starting with the threat's initial array of forces. These templates are useful in depicting points where the threat may adopt branches or sequels to the main COA, places where the threat is especially vulnerable, or other key points in the battle such as initial contact with friendly forces. Situation templates are used to support staff wargaming and to develop event templates. Analysts construct a situation template by—

- Beginning with the threat model representing the operation under consideration.
- Overlaying the doctrinal template on the products (generally, COO or MCOO) that depict the battlespace environment's effects on operations.
- Adjusting the dispositions portrayed on the doctrinal template based on the battlespace environment's effects.
- Viewing the situation from the threat commander's point of view when selecting from among available options.
- Checking the situation template to ensure that all the threat's major assets have been accounted for, particularly the locations and activities of the HVTs listed in the threat model.
- Evaluating time and space factors to develop time phase lines (TPLs) to depict threat movement. The TPLs can be refined during wargaming (see fig. 5-13).

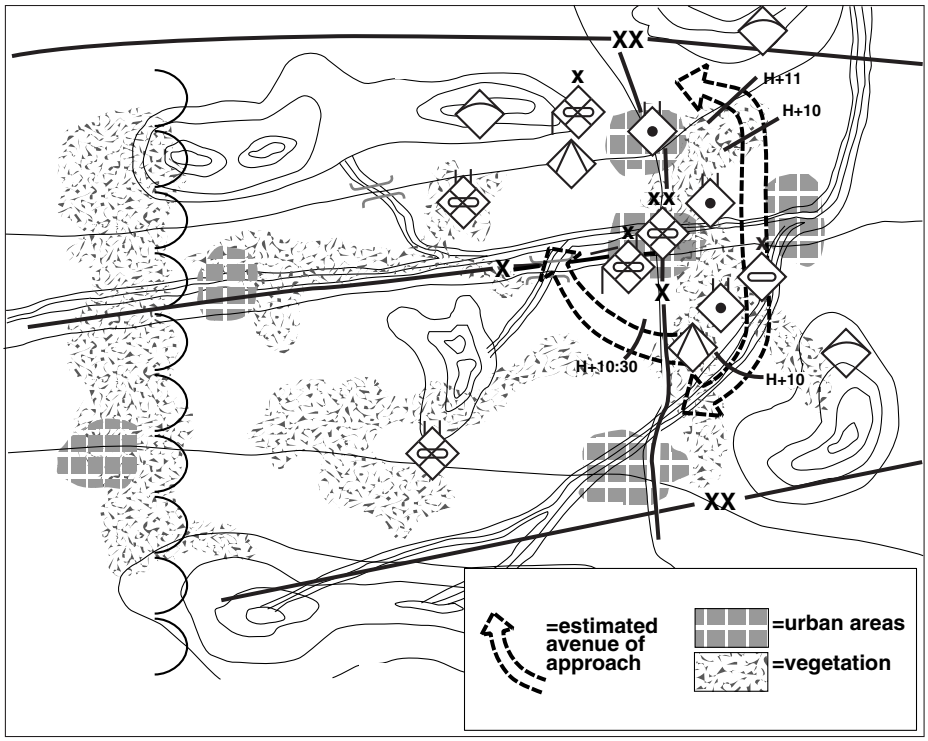


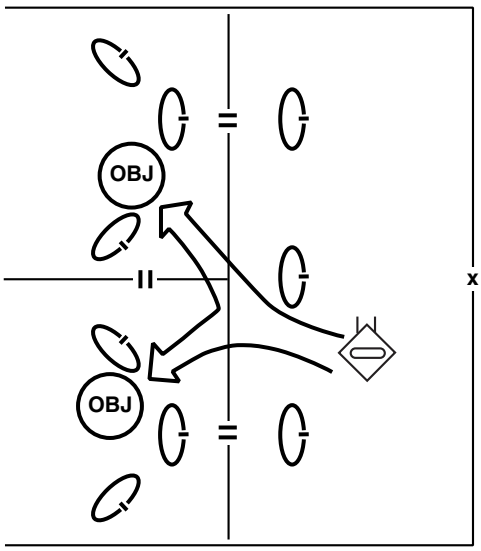
Figure 5-13. Counterattack Situation Template with TPLs and HVTs.

Description of the Threat's Courses of Action and Options

This is a description of the forces' activities depicted on the situation template. It can range from a narrative description or a combined graphics overlay or text matrix (see fig. 5-14 on page 5-20) to a detailed intelligence synchronization matrix depicting the activities of each threat unit and battlespace function in detail (see fig. 5-15 on page 5-20). The COA description supports staff wargaming and the development of the event template and supporting indicators. When preparing the description, analysts mentally war game the COA and attempt to tie threat actions and decisions to both time and space. The description should address the—

- Earliest time the COA can be executed.
- Threat COGs.
- Time lines and phases associated with the COA.
- Decisions the threat commander will make during and after execution of the COA.

Intelligence synchronization is more than simply ensuring that collection systems are operating 24 hours a day. The G-2/S-2 must plan and direct the intelligence system, receive the information it produces, process it, and then produce and disseminate intelligence of value to commanders and planners in time to support their decisions. The coordination of this entire cycle is intelligence synchronization. The IPB process provides the products and tools the G-2/S-2 needs to quickly evaluate incoming information and intelligence as it relates to the command's IPRs and IRs, intelligence synchronization matrix, and the decision support template (DST). These products and tools support the commander's decisions during COA execution and help the commander to quickly confirm or deny the assumptions used during COA wargaming. During operations, the commander and staff track the DST and the intelligence synchronization matrix against incoming intelligence and other tactical reports. As the commander and staff near each decision point, they look to the G-2/S-2 for the intelligence that supports that decision.



Description:

- Defense in two echelons with a reserve.
- Local counterattacks to restore defensive positions.
- Tank battalion counterattacks if defense compromised.
- Detailed and coordinated fire support plan supporting defense and counterattack.
- They prefer obstacle systems (usually minefields) that turn enemy forces into their engagement areas. They seldom employ fixing, blocking, or disrupting obstacles.
- Surface-to-air missiles usually deploy forward with companies. Antiaircraft artillery usually protects battalion assets.

Failure Options:

- Local counterattacks.
- Counterattack by division reserve.
- Withdraw.

Figure 5-14. Threat COA Overlay with Text Description.

TIME	T + 10	T + 24	T + 36	T + 48
Friendly Event	penetrate 80th Corps	shape 90th Corps	shape 90th Corps	shape reserve
Threat Event		reserve departs assembly areas	reserve deploys combat formation	Corps artillery forward deploys
Decision Points	shift main effort to aviation combat element		shift shaping actions	
Intelligence Event (PIR)	NAI 24-will the reserve reinforce 90th Corps	NAI 1-identify reserve HVT AA	NAI 2-identify reserve HVT locations	NAI 3-identify Corps artillery refueler locations
Intel and Recon Collectors	JSTARS Force Recon Rivet Joint UAV/ATARS Radio Battalion Ground Sensors	JSTARS	Force Recon Senior Scout UAV/ATARS	JSTARS Force Recon

Figure 5-15. Intelligence Synchronization Matrix.

Sometimes a battle progresses in a direction unanticipated during the initial IPB and wargaming, because the enemy follows his/her own plans and time lines. As the operation unfolds and the enemy's intentions become clearer, key staff members reinitiate the IPB and decision-making processes and conduct a modified war game as needed. During these sessions, the G-2/S-2 reviews and modifies the initial IPB. The battle staff then war games the best friendly response or preemptive action based on the updated set of IPB predictions. New decisions and COAs lead to updating and refining the collection plan, intelligence synchronization, and new decision support tools.

The intelligence synchronization matrix and other intelligence tools are consolidated and displayed within the current operations center to provide all watch leaders and personnel with critical current intelligence operations information. This tool is called the intelligence synchronization sheet, which is tailored to the command echelon or C2 node being supported (see fig. 5-16). Generally, the intelligence synchronization sheet includes lists of—

- Threat objectives and battlespace conditions.
- Current PIRs.
- Anticipated critical threat events, critical intelligence actions, and likely threat activities.
- Targeting priorities.
- Intelligence support priorities.
- Key intelligence collections, production, and dissemination activities.

High-Value Targets

While preparing and mentally wargaming the situation template, the analyst notes how enemy systems provide critical support to the COA. This

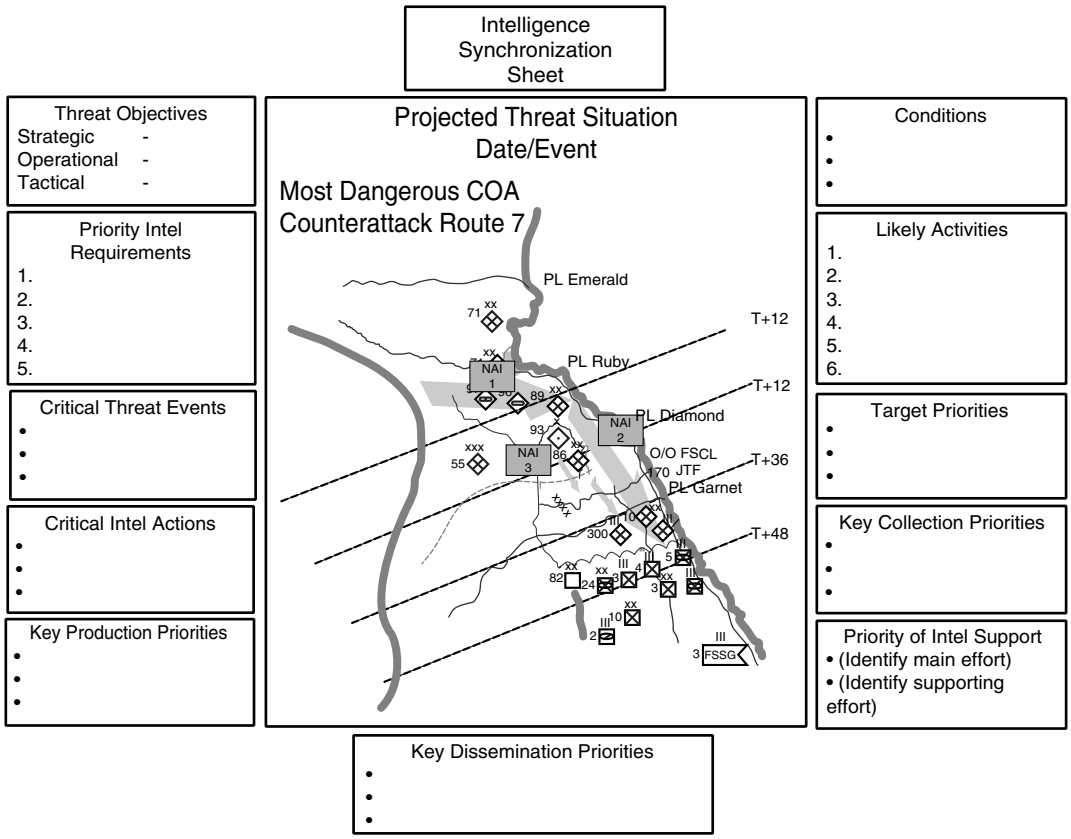


Figure 5-16. Intelligence Synchronization Sheet.

exercise leads to identification of HVTs that may be COGs, critical vulnerabilities, or assets, which if destroyed or neutralized may allow friendly forces to attack a COG or critical vulnerability. Once the HVTs list is compiled, analysts—

- Use the list in the threat model as a guide.
- Determine the effect on the COA of losing each HVT and identify likely threat responses.
- Identify the times or phases in the COA when the target is most valuable to the threat commander and make the appropriate notations on the list of HVTs.
- Transfer the refined and updated list of HVTs to the situation template (see fig. 5-17). The list will support staff wargaming and the targeting process.
- Note on the situation template any areas where HVTs must appear or be employed to make the operation successful.
- Focus on HVT locations at the times they are most valuable or just before. These are potential targeted areas of interest (TAI) and engagement areas that will be refined and used by the G-3/S-3.

Identify Initial Intelligence Collection, Production, and Dissemination Requirements

After identifying potential threat COAs, the analyst must determine which one the enemy will adopt. Initial collection requirements are designed to help answer the challenge. The identification of initial ICRs revolves around predicting specific areas and activities, which, when observed, will reveal which COAs the threat has chosen. The area where the analyst expects key events to occur is designated an NAI. The activities that reveal the selected COA are called indicators. Identified IPRs support prioritization and planning of necessary intelligence products, and identified IDRs support prioritization and planning for the eventual

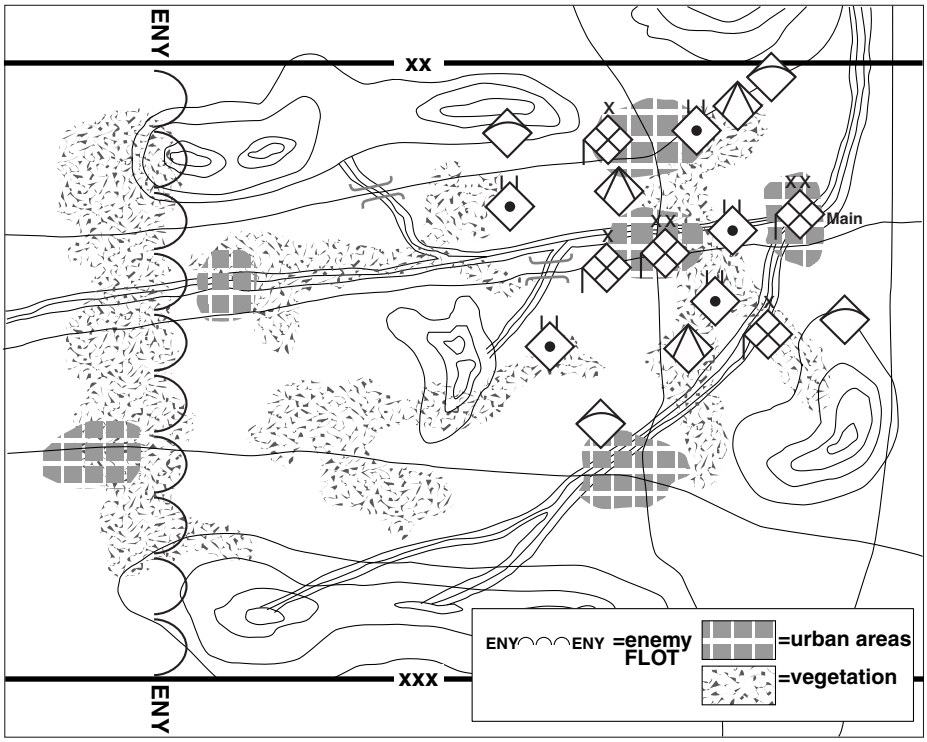


Figure 5-17. Templated Locations of HVTs for Enemy COA 1.

dissemination of intelligence products, such as the event template and event matrix, to commanders and staff sections needing them.

The event template and matrix form the basis for planning integrated collection, production, and dissemination strategies, and synchronize friendly intelligence operations. They enable the G-2/S-2 to develop precise ICRs, IPRs, and IDRs by maximizing the effectiveness of limited resources over extended areas against a vast array of threat targets.

Event Template

The differences between the NAIs, indicators, and TPLs associated with each threat COA form the basis of the event template (see fig. 5-18). The event template is a guide for collection, reconnaissance, and surveillance planning. It depicts where to collect information that will indicate which COA the threat has adopted.

Analysts evaluate each threat COA to identify its associated NAIs. They mentally war game execution of the COA and note places where activity must occur if that COA is adopted. Intelligence analysts must pay particular attention to times and places where the threat's HVTs are employed or areas where HVTs can be easily acquired and engaged. Analysts must also consider places where the threat is expected to take actions or make decisions, such as adoption of a branch plan or execution of a counterattack. These areas will evolve into NAIs in support of targeting.

An NAI can be a specific point, a route, or an area. They can match obvious natural terrain features or arbitrary features, such as TPLs or engagement areas. Analysts must make the NAIs large enough to encompass the activity that serves as the indicator of the threat's COA.

Intelligence analysts compare, contrast, and identify the differences between each COA's NAIs

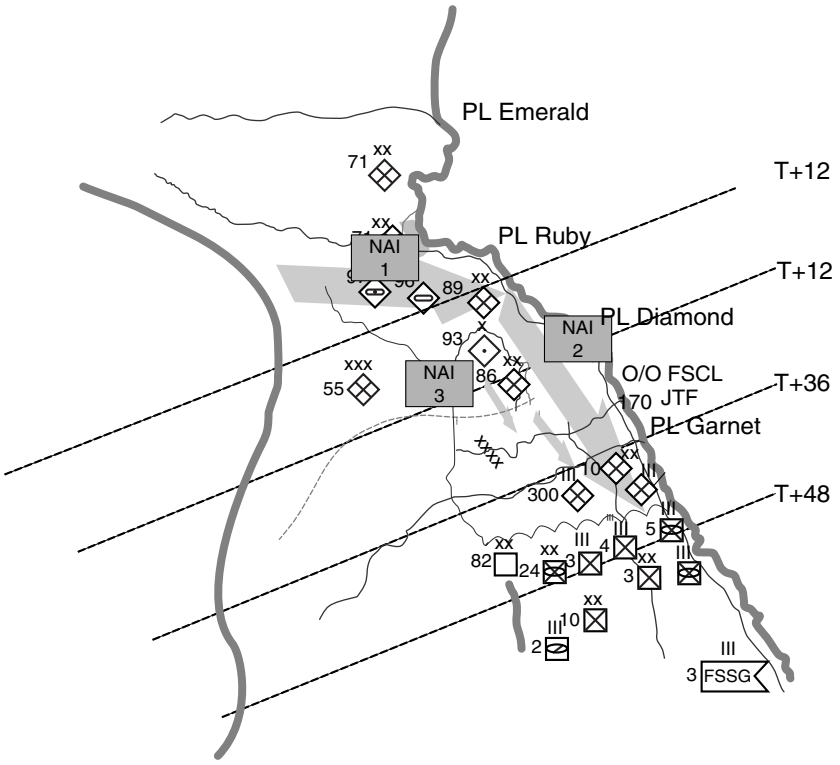


Figure 5-18. Event Template.

and indicators, concentrating on the differences that will provide the reliable indications of COA adoption. Selected NAIs are marked on the event template. The initial event template focuses on identifying which of the predicted COAs the threat has adopted. Analysts update and refine the event template and its supporting matrix to support friendly decisions identified during staff wargaming (see fig. 5-19).

Event Matrix

The event matrix supports the event template by providing details on the type of activity expected in each NAI, the times the NAI is expected to be active, and the relationship of the activity to other events on the battlefield. Primarily used in planning intelligence collection, the event matrix also serves as an aid to situation development (see fig. 5-20).

When preparing the event matrix, intelligence analysts—

- Examine the events associated with each NAI on the event template and restate them in the form of indicators.
- Enter the indicators along with the times the indicators are most likely to occur by using TPLs from the situation template or the description of the COA to establish the expected times.
- Record the latest-time-information-of-value time line, if available, based on the expected flow of events, as a guide for the collection manager.

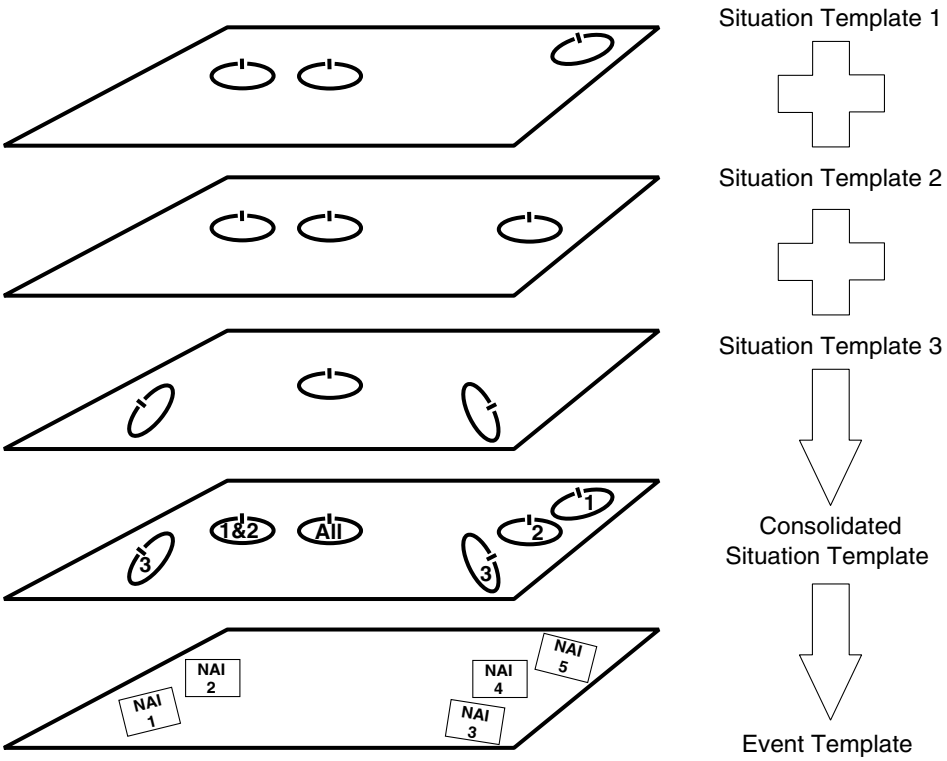


Figure 5-19. Event Template Development by Comparing and Contrasting Each COA's NAIs and Indicators.

NAI	Estimated Time	COA Indicators	COA 2 Indicators	COA 3 Indicators	Other COA Indicators
1	H-15		air assault forces		
2	H-15		air assault forces		
3	H-15	air assault forces		air assault forces	
4	H-15		infiltration of light infantry		
5	H-4		light infantry attack		
6	H-4	light infantry attack NAI 7	light infantry attack		
7	H-4	light infantry attack NAI 8		light infantry attack	
8	H-4	poised to attack		light infantry attack	
9	H-4	poised to attack	poised to attack		tank division attacks
10	H-4		poised to attack	poised to attack abreast	tank division attacks
11	H-6			shifts north	
12	H-18				
13	H-18				1 or 2 brigades attack south

Figure 5-20. Detailed Event Matrix for a Specific NAI.

SECTION V. DECISION SUPPORT TEMPLATE

The DST is the capstone product in the staff planning process and the logical conclusion to IPB, although it is not part of the formal IPB process. The DST relates time, space, and threat actions to assist the commander in determining when decisions need to be made, either to employ fires or maneuver forces (see fig. 5-21 on page 5-26). This template helps the commander think ahead in the battle to reduce uncertainty and aids in recognitive or intuitive decisionmaking.

The DST is normally developed during COA wargaming as threat and friendly actions are compared in time and space. Unlike the previous products, the DST is a staff product prepared under the staff cognizance of the G-3/S-3. It reflects the judgment and expertise of the intelligence, maneuver, fires, CIS, and logistic support staffs. The threat COA models, the event template, and event matrix developed during IPB form the basis for and drive wargaming and development of the DST.

Targeted Areas of Interest

Through event templating, identification is made of those areas on the battlefield where significant events and activities will likely occur and where targets will likely appear. As the wargaming process proceeds, the staff identifies areas where the commander can influence the action through fire and maneuver. These areas are designated TAIs. A TAI is an engagement point or area, usually along a mobility corridor, where the interdiction of threat forces by fires, maneuver, or jamming will deprive or reduce a threat capability. It can also cause the threat commander to abandon a particular COA or require the use of unusual support to continue operations. Times and

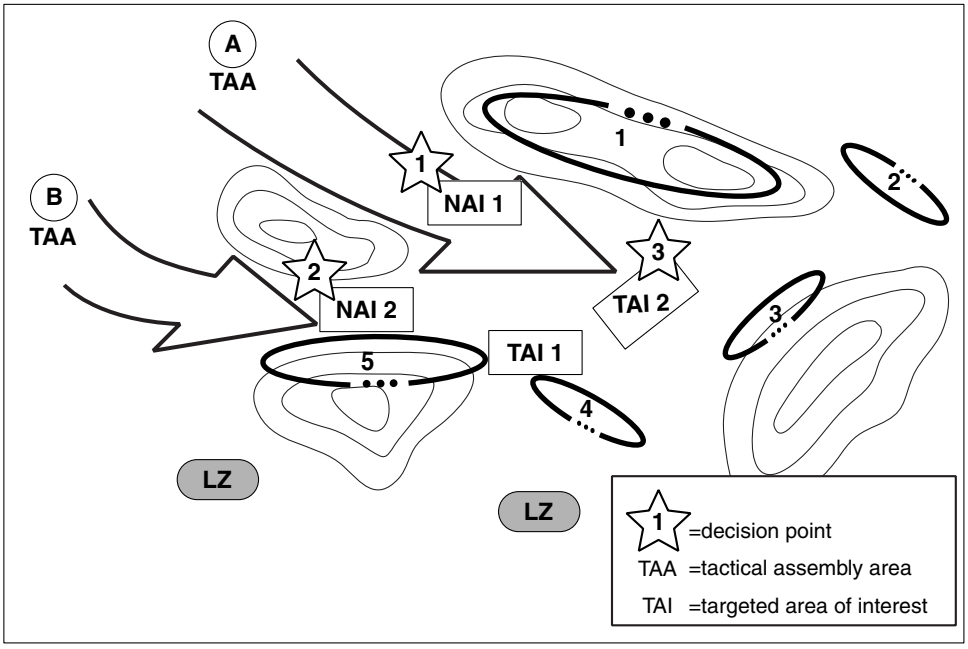


Figure 5-21. Decision Support Template.

locations where HVTs will appear are particularly suited to become TAIs.

The identification of TAIs is a joint effort between the intelligence, operations, and fire support staffs. The intelligence staff identifies the times and places where opportunities present themselves and the effect of interdiction on threat capabilities. The operations and fire support staffs consider the availability of interdiction resources, the effects of interdiction on the accomplishment of the friendly mission, and the priorities for the use of available resources.

Decision Points

Following the selection of TAIs, analysts identify decision points. The location of decision points is largely influenced by the availability and capability of friendly fire and maneuver systems; therefore, decision point selection is primarily a G-3/S-3 function, with support from the fire support coordinator and other key participants in the planning staff.

Types

Decision points identify battlefield events that may require tactical decisions. These points also identify when the tactical decisions must be made for the commander to retain available options. Examples of the types of decisions include—

- Commit the reserve.
- Surge friendly air support.
- Concentrate artillery on TAIs, perhaps in conjunction with electronic attack (EA) operations.
- Deliver scatterable mines.
- Shift the main effort.
- Commence the next phase of an operation.
- Change subordinate unit's overall mission.
- Request assistance from higher headquarters.

Considerations

Decisions must be made early enough to ensure that they can be coordinated across all command echelons and implemented in time to achieve the desired results. The developed NAIs must

provide the required indicators in sufficient time and preciseness to ensure timely decisions.

When identifying decision points, the G-3/S-3 must consider the—

- Time required for intelligence collection, processing, analysis, production, and dissemination to take place.
- Time required to prepare and/or move friendly assets that will execute the mission.
- Activities and movements of the target or threat during the time elapsed between decision and execution.

As the wargaming progresses, a recorder tracks decision points, both by time and location, and develops the synchronization matrix to ensure all battlespace functions are working in harmony toward the same goals. After the commander selects a friendly COA, the intelligence staff develops detailed collection and dissemination plans to support the decision points, NAIs, and TAIs.

SECTION VI. ABBREVIATED INTELLIGENCE PREPARATION OF THE BATTLESPACE PROCESS

Many of the steps involved in IPB are time, labor, and resource intensive, especially at lower tactical echelons where automated systems and personnel support for terrain analysis and other intelligence production functions are usually not available. Those same echelons generally have less time available for the IPB process. Besides the available time, intelligence personnel and resource constraints affect the scope and depth of IPB activities. Consequently, most Marine Corps units use the abbreviated IPB process.

The intelligence product that results from the abbreviated approach is far less than the comprehensive set of previously discussed products. The one-overlay product, when developed to a quality standard and focused on the unit's mission, PIRs, and IRs, has repeatedly proven to be effective on the battlefield. In its most elementary form, the IPB process can be abbreviated by working ahead, focusing on essentials, staying objective oriented, and minimizing essentials.

Work Ahead

When conducting an abbreviated IPB, intelligence personnel should complete as much work ahead of time as possible by—

- Establishing a series of base products, particularly those that deal with the battlespace environment's effects on operations.
- Keeping the products updated by periodic review instead of waiting until receipt of a new mission.
- Updating data bases on potential threats and changing the threat models as intelligence is received that indicates changes or evolution in threat doctrine.
- Conducting periodic reviews to ensure that the base IPB products, such as descriptions of the battlespace environment and the threat, are updated regularly.

- Becoming familiar with the support available from higher headquarters, theater intelligence centers, and Service agencies; knowing how to get needed information and products.
- Submitting PRs for information and intelligence products on areas where the unit is most likely to be employed.
- Developing checklists on how to get support, before, during, and after deployment.
- Maintaining an awareness of plans and priorities for all ICRs, IPRs, and IDRs submitted to higher headquarters.

Focus on Essentials

When starting the IPB effort, intelligence personnel should focus on essentials by—

- Considering the METT-T factors, particularly the factor of time.
- Determining how much time can be devoted to each step of the IPB process, and ensuring that the time line allows for the proper support of the planning and decisionmaking process.
- Deciding which products will be developed and to what degree of detail, and focusing on products most important to the mission.
- Identifying the full range of available threat COAs, rather than fully developing one threat COA at the expense of the others; determining the degree of detail required; and then developing all threat COAs to that level of detail.
- Working in a priority order established by the commander's intent and needs, and developing in detail only those COAs the commander has specified.

Stay Objective Oriented

The objective of IPB is to help the commander and staff make decisions and develop the best possible plans in the time available. This requires models of viable threat COAs that will influence mission accomplishment. Supporting the finished plan with intelligence requires a good event template and matrix.

Minimize Essentials

When minimizing essentials, intelligence personnel can get by with a good set of threat models and a good event template and matrix. They can also save time and materials by—

- Combining threat COA model templates and the event template on a single map overlay or using cartoons and sketches as a map substitute.
- Working directly from the map or sketch of major terrain features if the battlespace environment's effects have not been described.
- Identifying the set of threat COAs and briefly comparing them to determine which is most likely and which is most dangerous based on the current situation and the command's mission; and ranking the remaining threat COAs in order of likely adoption.
- Developing the most dangerous and most likely threat COA, and in the absence of guidance from the commander or G-3/S-3, using judgment in deciding which COA to develop first.
- Constructing an event template that focuses on identifying which of the two COAs the threat adopted, developing the remaining COAs, and working each COA in priority order.
- Incorporating each COA's NAIs in the event template as each threat COA is finished.
- Developing the second most likely or second most dangerous threat COA if the most likely COA is also the most dangerous COA, and ensuring at least two COAs are war gamed.
- Waiting until the staff conducts wargaming before structuring the ICRs.

Output

Throughout the IPB process, various products such as the threat models, threat COA graphics, and the event template are produced to support staff planning. The graphics developed, particularly the weather and terrain effects graphics, the situational templates, and the event template, can be disseminated to assist subordinate units in their own planning. Done correctly, these graphics can provide tremendous volumes of understanding and knowledge in concise and easily usable forms. At other times, however, additional written products can and should be prepared. The two products discussed below are the most commonly used, and both are directly derived from the IPB process.

Intelligence Estimate

In order to facilitate staff planning, the G-2/S-2 prepares the intelligence estimate before the remainder of the staff complete their own estimates. The intelligence estimate is the standard means of conveying key basic and current intelligence and relating it to the operational mission. It is a snapshot in time and forms the basis for the facts and assumptions of the decision-making process, driving the other staff estimates and the remaining steps of the Marine Corps Planning Process.

At higher command levels, the intelligence estimate provides major portions of the commander's written estimate. The products of IPB are the basis for the intelligence estimate. If the G-2/S-2 lacks the time required to prepare a written estimate, usually graphics that depict the results of the IPB evaluations and analysis are used as a substitute. A detailed outline for the intelligence estimate format is provided in appendix A.

Target and Objective Studies

The IPB impacts development through the evaluation of terrain and weather and the association of threat forces at specific times and locations within the battlespace. Situation, event, and decision support templates identify NAIs. Once identified, NAIs can then confirm or deny a threat's activities or adoption of a particular COA. Decision points and TAIs are also identified, requiring key intelligence that supports either fire or maneuver. From the IPB and wargaming processes, HVTs and HPTs are derived. Target and objective studies are focused, detailed intelligence products that aid in the application of fires or the maneuver of forces against a specific target set or area. Small units, such as MEU(SOC)s, can also use these studies for mission preparation and execution. See chapter 8 for a detailed discussion of target development.

CHAPTER 6. ANALYSIS OF THE BATTLESPACE

Analysis of the battlespace is a comprehensive study to determine the characteristics and effects of weather, oceanographic, and terrain environmental factors on enemy and friendly operations throughout the commander's AO and AOI. The battlespace analysis serves as a basis for developing specific friendly COAs and for determining enemy capabilities and COAs. This analysis allows the commander and staff to—

- See the battlespace in both spatial (width, depth, height or airspace) and temporal (time) dimensions.
- Appreciate fully the opportunities and limitations afforded by major terrain and oceanographic features, zones of entry, transportation networks, obstacles, and built-up areas within the AO and AOI.
- Fit an operational concept to that battlespace environment.

The limits of the battlespace are determined for all aspects of air, surface, subsurface, land, space, and the electromagnetic spectrum that can impact friendly forces. Defining the limits of the battlespace is a joint effort between the operations and intelligence staffs based on the commander's guidance.

SECTION I. RESPONSIBILITIES

When time permits, the intelligence officer coordinates the development of a battlespace analysis based on anticipated missions. On receipt of the warning or execute order, the intelligence officer reevaluates the analysis in terms of the commander's assigned AO and potential AOI. Changes in the mission and the commander's AO and AOI, or receipt of additional or more accurate information, necessitate revision of the analysis as the operation progresses. Normally, MEF and higher headquarters staff prepare a detailed written analysis when planning anticipated missions. In MSCs, the G-2s may prepare a written analysis tailored to the unit's specific mission and intelligence needs. However, in most operations, the geospatial information and services officer, the intel bn commander or intelligence support coordinator, and the P&A cell officer in charge use the MEF's analysis supplemented by graphic representations of weather and terrain data covering the MAGTF's AO and AOI.

The intelligence officer is responsible for initiating, coordinating, and ensuring that the analysis of the MAGTF's AO and AOI is completed and disseminated. The final analysis represents a coordinated effort of the intelligence officer, the operations officer, and other staff personnel who contribute within their respective warfighting functional areas. At the MEF or MAGTF level, the following organizations and personnel contribute to the final analysis:

- Topographic platoon, P&A company, intel bn—
  - Provides tailored terrain, littoral, and infrastructure studies and factor overlays.
  - Supports integration of weather factors into terrain studies portraying environmental effects.
  - Disseminates products such as graphic tactical decision aids to support IPB and COA development.
- Staff weather officer, intelligence section, MEF CE provides operational weather forecasts and environmental impact graphics as well as other weather and climatic data (e.g., light and tidal information).

- All-source fusion platoon, P&A company, intel bn—
  - Develops information on sociological, political, economic, technological, and related conditions covering countries of interest.
  - Provides fused, all-source IPB and other intelligence products to support MEF staff planning and decisionmaking.
- Civil affairs officer provides information on civilian personnel, local labor conditions, and capabilities.
- Engineer officer assists in the analysis of routes, potential obstacles and barriers, and other information related to mobility and countermobility.
- Psychological operations officer assists in the assessment of local conditions for psychological operations.

SECTION II. CHARACTERISTICS OF THE BATTLESPACE

The limits of the battlespace are determined for aspects of air, surface, subsurface, land, space, and the electromagnetic spectrum, which can directly or indirectly impact friendly forces. The battlespace generally includes all or most of the AO as well as the AOI. The AOI encompasses that area beyond the AO from which intelligence and information are required to permit planning, decisionmaking, and the successful conduct of operations. Defining the limits of the AO, the AOI, and the battlespace is a joint effort between the operations and intelligence staffs based on the commander's guidance. The AO and AOI are dynamic in nature and include interrelated factors capable of affecting a unit's operation.

The battlespace is measured in four dimensions: depth, width, height, and time. A battlespace analysis of the AO and AOI evaluates and integrates four environmental dimensions: terrain analysis (land), hydrographic analysis (sea), airspace analysis (air), and climatological analysis (weather). The battlespace analysis study allows the operational commander and staff to fully appreciate the opportunities and limitations afforded by major terrain and oceanographic features, zones of entry, transportation networks, obstacles, and built-up areas within the AO and AOI and fit an operational concept to that environment.

SECTION III. TERRAIN ANALYSIS

Terrain analysis is the evaluation of natural and manmade geographic features. This evaluation provides the planning headquarters with information on AAs (location and trafficability), zones of entry (deep, close, and rear areas), and key or decisive terrain.

Responsibilities

Much of the detailed terrain analysis work is done by P&A company GEOINT support teams attached to or in direct support of the MSCs or by GEOINT teams attached to a MEU(SOC) CE. The P&A company's topographic platoon and imagery intelligence platoon personnel conduct the major portion of the terrain analysis production by—

- Using data bases as a guide for collection, production, and dissemination planning and operations while focusing on the areas of most importance to the commander and the mission.
- Combining data base information with the results of tactical, aerial, and ground reconnaissance.
- Working closely with staff weather officers to ensure terrain analysis products incorporate the effects of current and projected weather phenomena.

- Using AO and AOI reconnaissance analysis results to focus on areas of most importance to the commander and the mission.
- Analyzing terrain continuously to evaluate the effects of changes in the battlespace environment.
- Forming conclusions regarding the effects of terrain through analysis of the military aspects of the terrain, and evaluation of the terrain's effects on military operations.

Sources of Information

National Imagery and Mapping Agency produces numerous digital data bases that support the development of geospatial factors and geographic classification. Topographic and geodetic maps, aerial charts, and facility maps are basic sources of information used by terrain analysts. Topographic publications can also be obtained from—

- Geographic societies.
- Engineering and scientific firms.
- Government intelligence agencies.
- Libraries.
- Bookstores.
- Universities.

Geospatial Factors

Terrain analysts need data on the trafficability of soils, the presence of bedrock, as well as the type and density of vegetation when developing cover and concealment, cross-country movement, or other geographic data bases.

Surface Configuration

Surface configuration refers to the shape of the earth's land surface. Terrain analysts study surface features such as mountains, slopes, ravines, embankments, ditches, plowed fields, and rice field dikes, because they can profoundly influence military operations. This factor is limited only by physical shape, size, and arrangement; it is not concerned with whether the feature is manmade or of natural origin.

Analysts categorize surface features or landforms by size and shape. The principal groups of landforms are plains, hills, and mountains; within each of these groups are smaller surface features, such as flat lowlands, and valleys. For geospatial analysis and GEOINT production purposes, major landforms are defined on the basis of local relief. Local relief represents the differences in the elevation of each landform group and subgroup (see table 6-1).

Table 6-1. Landform Elevations.

Landform	Elevation
Plains	less than 150 meters
Flat	less than 15 meters
Undulating	15 to 50 meters
Gently rolling	50 to 100 meters
Rolling	100 to 150 meters
Hills	150 to 600 meters
Low	less than 300 meters
High	300 to 600 meters
Mountains	more than 600 meters
Low	600 to 1500 meters
High	more than 1500 meters

Hydrologic Features

Hydrology is the science of surface and subsurface waters. Terrain analysts are concerned with the shape, size, distribution, and temporal variance of water bodies. Analysts classify hydrologic features as surface water, subsurface water, and wet areas.

Surface Water

This hydrologic feature encompasses inland waters, which are classified as watercourse (e.g., streams, rivers, canals) and standing bodies of water (e.g., lakes, ponds, glaciers). Terrain analysts evaluate watercourses because drainage conditions vary from place to place and from time to time. Military planners are concerned with the flow and channel characteristics of these watercourses and their effect on military operations. Water bodies affect the characteristics of surface drainage by storing precipitation and runoff and by retarding or augmenting flood flows. These water bodies can obstruct cross-country movement or provide AAs when sufficiently frozen.

Subsurface Water

Groundwater or subsurface water is located beneath the surface of the earth. Groundwater is less susceptible to contamination and may be the only source of water in arid regions.

Wet Areas

These tracts of ground are covered with water seasonally or perennially (e.g., swamps and marshes). These areas are treated separately in the collection of data because information requirements differ from other water bodies, especially in evaluation for cross-country movement.

Vegetation Features

Vegetation includes plant life growing on the surface of the earth or other flora in or on the water. Terrain analysts evaluate area vegetation to determine the potential effect on vehicular and foot movement, concealment, cover, observation, airdrops, and construction. The vegetation present indicates the climatic conditions, soil, drainage, and water supply. Vegetation is grouped by type (e.g., trees, scrub and shrubs, grasses, crops).

Trees

This group of vegetation includes perennial woody plants at least 10 feet in height, with single stems and defined crown shapes. An area extensively covered by trees is classified as a forest. Smaller areas covered by trees are classified as woods, groves, or woodlots. On military maps, any perennial vegetation high enough to conceal troops or thick enough to be a serious obstacle to free passage is classified as woods or brushwood.

Scrub and Shrubs

Either deciduous or coniferous, scrubs include a variety of trees that have had their growth stunted because of soil or climatic conditions. Scrub growth includes cactus, stunted shrubs, sagebrush, mesquite, and similar plants found in arid or semiarid areas.

Shrubs, like trees, are either deciduous or coniferous. Shrubs comprise the undergrowth in open forests; in arid and semiarid areas they are the dominant vegetation. Shrubs normally offer no serious obstacle to movement and provide good concealment from ground observation; however, they may restrict fields of fire.

Grasses

This vegetation group includes nonwoody plants. A grassland is an extensive area where the natural vegetation consists primarily of grasses and herbaceous plants, the dominant type in alpine and certain semidesert areas. In low latitudes, grasslands often are termed savannas; in middle latitudes, they are called prairies (tall grass) and steppes (short grass). Grasslands in wet or poorly drained areas are commonly called meadows. For geospatial analysis purposes, grass more than 1 meter (3 feet) high is considered tall, and below that height, grass is considered short. Grass often improves the trafficability of some soils; very tall grass may also provide concealment for foot troops.

Field Crops

The predominant class of cultivated vegetation is field crops. Vine crops and orchards are common but not widespread, and tree plantations are found in relatively few areas. Sizes of cultivated areas range from paddy fields covering a quarter of an acre to vast wheat fields extending for thousands of acres. In a densely populated agricultural area where all arable land is used for the crop that brings the highest yield, it may be possible to predict the nature of the soils from information about the predominant crops.

For example, rice requires fine-textured soils. Other crops generally must have firm, well-drained land. An area of orchards or plantations usually consists of rows of evenly spaced trees, which shows evidence of planned planting that can be distinguished on aerial photographs. Usually such an area is free from underbrush and vines. Rice fields are flooded areas surrounded by low dikes or walls. Some crops, such as grain, improve the trafficability of soils, while other crops, such as vineyards, present a tangled maze of poles and wires that are definite obstacles to vehicles and dismounted troops. Wheeled vehicles and some tracked vehicles are unable to cross-flooded paddy fields, although they can negotiate them when the fields are drained or frozen.

Surface Materials

Terrain analysts evaluate the composition and physical properties of the earth's surface materials, which are classified as soil and rock, to determine their effects on military operations and construction.

Soil

This unconsolidated material is an accumulation of disintegrated and decayed rock and vegetation that overlies bedrock. This accumulation can be hundreds of feet thick or it may be absent in given areas. Soils between 15 centimeters (6 inches) and 2 meters (6 feet) in depth are the most important. Next in importance are the soils from 2 to 6 meters (6 to 20 feet). Soil depth can be measured directly from borrow pits, road cuts, building excavations, and stream banks. For field identification, analysts classify soils as gravel, sand, silt, clay, and organic matter.

Rock

Rock is the firm or consolidated mineral matter of the earth's crust. Bedrock is solid undisturbed rock either exposed at the surface or underlying the soil. Terrain analysts evaluate the physical and engineering characteristics of bedrock for use in construction and in locating ground water.

Military Aspects of Terrain Evaluation

Using portions of the IPB process, the intelligence officer evaluates the battlespace in terms of **K**ey terrain, **O**bservation and fields of fire, **C**over and concealment, **O**bstacles, and **A**As and mobility corridors (KOCOA). The KOCOA analysis is appropriate at the battalion, squadron, regimental, Marine aircraft group, and CSS detachment levels. At division, Marine aircraft wing, force service support group (FSSG), and higher levels, KOCOA is absorbed into the terrain analysis process. Analysts use KOCOA to determine which friendly COAs can best exploit the opportunities the terrain provides and how the terrain affects the threat's available COAs.

Key Terrain

Key terrain is any location or area that the seizure, retention, or control of affords a marked advantage to either combatant. Terrain analysts depict key terrain on overlays with a large "K" in a circle that encloses and follows the contours of the designated terrain.

Observation and Fields of Fire

Cover and concealment factors can limit or deny observation. Observation analysis is useful in—

- Selecting LZs and DZs.
- Planning helicopter forward arming and refueling point (FARP) locations.
- Identifying areas vulnerable to aerial intelligence collection systems.
- Selecting low-level flight routes and aerial battle positions.

An ideal field of fire for flat trajectory weapons is an open area in which the threat can be seen and on which he/she has no protection from the fire of those weapons, out to the weapon's maximum effective range.

Geographic factors that offer good observation and fields of fire generally favor defensive COAs. Analysts represent areas of poor observation and fields of fire on an overlay with marked parallel diagonal lines or crosshatching. Observation and fields of fire evaluations identify—

- Potential engagement areas (often referred to as fire sacks or kill zones).
- Defensible terrain and system or equipment positions.
- Locations where maneuvering forces are most vulnerable to observation and fires.

Cover and Concealment

Analysts can combine the cover and concealment evaluation with the overlay developed during the observation and fields of fire evaluation (see fig. 6-1). When preparing the overlay, analysts identify factors that provide cover and concealment. Commanders and staffs use the results of the evaluation to—

- Identify and evaluate AAs.
- Identify defensible terrain and potential battle positions.
- Identify potential assembly and dispersal areas.

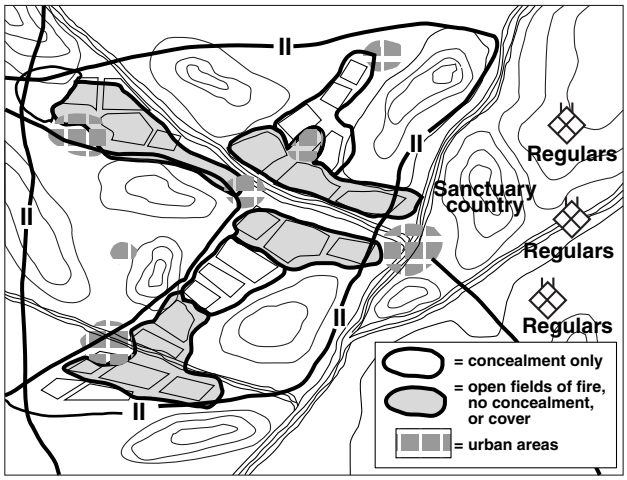


Figure 6-1. Concealment and Cover Overlay.

Cover that provides protection from the effects of direct and indirect fires can be provided by—

- Ditches.
- Caves.
- Riverbanks.
- Folds in the ground.
- Shell craters.
- Buildings.
- Walls.
- Embankments.

Concealment that provides protection from observation can be provided by—

- Woods.
- Underbrush.
- Snowdrifts.
- Tall grass.
- Cultivated vegetation.

Obstacles

Analysts identify natural and manmade obstacles that stop, impede, or divert military movement. Obstacles to air mobility include features that exceed the aircraft's service ceiling, restrict nap-of-the-earth (NOE) flight, or force the aircraft to employ a particular flight profile. An evaluation of obstacles leads to the identification of mobility corridors. This in turn helps identify defensible terrain and AAs.

Evaluation

When evaluating obstacles, analysts—

- Identify pertinent obstacles in the AO by considering—
  - Vegetation.
  - Surface drainage.
  - Surface materials.
  - Surface configuration.
  - Transportation systems (e.g., bridge classifications, road conditions).
  - Weather effects (actual or projected).
- Determine the effect of each obstacle on the mobility of the evaluated force by preparing a separate overlay for each factor, or combine the effects of individual obstacles into an integrated product or COO, which depicts the battlespace effects on mobility.

Classification

Analysts graphically depict and classify the cumulative effects of obstacles as unrestricted, restricted, and severely restricted areas, which are defined below:

- Unrestricted. Indicates terrain free of any restrictions to movement. Nothing needs to be done to enhance mobility. Typically this terrain is flat to moderately sloping terrain with scattered or widely spaced obstacles such as trees or rocks, which allows for armored or mechanized forces and wide maneuvers.
- Restricted. Indicates terrain that hinders movement to some degree. Units may have difficulty maintaining preferred speeds, moving in combat formations, or transitioning from one formation to another. This terrain slows movement by requiring zigzagging or frequent detours. Moderate to steep slopes or moderate to densely spaced obstacles such as trees, rocks, or buildings may restrict armored or mechanized forces. Swamps or rugged terrain may restrict dismounted infantry forces. Poorly developed road systems may restrict logistical and rear area movement. Analysts depict restricted terrain on overlays and sketches by marking the areas with parallel diagonal lines.
- Severely restricted. Indicates terrain that severely hinders or slows movement in combat formations unless some effort is made to enhance mobility. The mobility enhancement efforts could include committing engineer assets to improve mobility, moving in column instead of line formations, or moving at slower than preferred speeds. Steep slopes and large or densely spaced obstacles with little or no supporting roads typically characterize severely restricted terrain for armored and mechanized forces. Analysts depict this type of terrain on overlays and sketches by marking the areas with crosshatched diagonal lines.

Avenues of Approach and Mobility Corridors

To develop the air or ground routes of an attacking force, analysts must identify and categorize mobility corridors. Mobility corridors are areas where a force is channeled around obstacles. The best mobility corridors use unrestricted terrain with enough space for a force to move in its preferred doctrinal formations while avoiding major obstacles. These corridors usually follow the direction of roads and trails.

Considerations

Analysts use the COO to identify mobility corridors wide enough to permit maneuver in tactical formations. If friendly and threat forces require

mobility corridors of different widths as a result of organizational or equipment differences, analysts may conduct two separate evaluations. Identification of mobility corridors requires some knowledge of friendly and threat organizations for combat and preferred tactics. When identifying mobility corridors, analysts must evaluate obstacles and force mobility. The analyst should also consider that—

- Mechanized and armored units generally require large open areas to move.
- Dismounted infantry, most insurgents, and terrorists are less restricted by the presence of obstacles or hindering terrain and prefer areas that provide concealment and cover.
- The mobility corridor used by a jet aircraft with a minimum operating altitude of 1,000 feet is quite different from that considered by a helicopter with a maximum service ceiling of 10,000 feet.

Categories

Once identified, mobility corridors are categorized according to the size or type of force they will accommodate. Mobility corridors are normally identified for forces two echelons below the friendly command. In addition, where terrain is restrictive, the evaluation may need to look several echelons below the friendly command.

Analysts group mobility corridors together to form AAs. Avenues of approach may include areas of severely restricted terrain since they show only the general area through which a force can move. Analysts depict AAs on an overlay using an outline arrow that encompasses the mobility corridors. Threat AAs are generally depicted in red, friendly AAs are depicted in blue.

Evaluation

During offensive operations, analysts evaluate AAs to recommend the best route to the command's objective and to identify avenues available to the enemy for force withdrawal or movement of reserves. During the defense, analysts identify AAs that support the threat's offensive capabilities and avenues that support the movement and commitment of friendly reserves.

An evaluation of AAs identifies those that best support maneuver capabilities. This evaluation should be a combined effort performed by the intelligence section, the imagery and mapping officer or GEOINT support team, and the operations section. These AAs are evaluated for—

- Access to key terrain and adjacent avenues.
- Degree of channelization and ease of movement.
- Use of cover and concealment.
- Use of observation and fields of fire.
- Sustainability.
- Directness to the objective.

SECTION IV. HYDROGRAPHIC ANALYSIS

Sea or hydrographic analysis is the study of areas containing shorelines. Intelligence of coasts and landing beaches is important to military planners because the coast is a country's first line of defense. The hydrographic analysis is subdivided into the offshore, nearshore, and foreshore environments. The land analysis is subdivided into the beach and inland environments. Intelligence personnel conduct hydrographic P&A to evaluate coastal conditions that support amphibious operations. Amphibious operations require detailed oceanography studies that are discussed in Joint Publication (JP) 3-02, *Joint Doctrine for Amphibious Operations,* and FM 34-81, *Weather Support for Army Tactical Operations*.

Sources of Information

The Naval Oceanographic Office (Major Shared Resource Center, John C. Stennis Space Center, National Aeronautics and Space Administration, MS), conducts comprehensive analysis of littoral and hydrographic factors worldwide. Joint Intelligence Center, Pacific; Joint Forces Intelligence Command; and Marine Corps Intelligence Activity (MCIA) produce detailed imagery-based beach studies. Graphic and text-based analysis are available both online via intelligence link (INTELINK) or intelligence link-SECRET (INTELINK-S) and via request for production validated through the operational chain.

Hydrographic Conditions

Analysts evaluating the hydrographic conditions of a coastal region study seas and surf, tides, and currents that can affect amphibious landings.

Seas, Swells, and Surf

Seas are waves that originated in local storms. Swells are waves that have traveled hundreds to several thousands of miles from a distant storm before arriving at the landing site. Breaking waves or surf 4 feet in height normally are considered too high for amphibious assault operations or for logistics over the shore. By identifying the following types of breakers, analysts can determine the trafficability of the nearshore bottom:

- Spilling breakers indicate a gentle sloping bottom. The waves lose energy gradually as they approach shore by breaking only at the crest, and it is common to see a number of such breakers existing simultaneously.
- Plunging breakers indicate an unstable nearshore bottom. These waves break in a rollover, plunging action that causes abrupt changes in the form of a longshore bar or degree of steepness at the shore.
- Surging breakers indicate a steep nearshore gradient and are the least common of all types of breakers. This type of wave peaks near the shoreline, but instead of breaking or spilling, it actually surges up the face of the beach.

Tides

Tides are the alternate rising and falling of the sea caused by the gravitational attraction of the moon and sun. The tidal range is the complicated product of various forces, including local bottom configuration and the size and configuration of oceanic basins that can alter the height and time of the tides. When identifying beach widths, hazards, and depths, analysts must specify the time of day observations were made to permit tidal computations. Tidal information for most places on the coasts of the world can be obtained from tide tables published by the U.S. Department of Commerce.

Currents

Currents in the nearshore zone which influence amphibious landing operations are generally classified as wave-generated, tidal, or river currents.

Wave-Generated Currents

These currents are caused by the angular breaking of waves on the beach slope and the resultant back rush normal to the beach, which results in a littoral current (longshore current) in the nearshore zone, flowing generally parallel with the shoreline. It is found shoreward of the outermost edge of the breaker zone and varies in velocity or force with the force of the waves, their angle of impingement upon the shore, and the steepness of the foreshore. Littoral currents may be insignificant in terms of amphibious operations, or they may be strong enough to cause personnel to lose their footing, to make maneuvering of craft difficult, and to throw landing or assault craft out of control and expose them to broadside attack by the surf. Littoral currents are particularly significant where depths

shoreward of the breaker zone are such as to make wading hazardous.

Tidal Currents

These currents affect amphibious landings in the proximity of tidal inlets, estuaries, river mouths, and similar restricted channels. With large tidal ranges these currents may make the maneuver of landing craft on beaches adjacent to the tidal inlet extremely hazardous.

River Currents

Currents that extend from rivers into the open sea are frequently of such strength that they affect the maneuver of landing craft near the river's mouth.

Beach Selection Considerations

Beaches are the most prevalent natural features of the coastal region. They are accumulations of loose sand, gravel, or boulders that are shaped by waves and currents acting on the shore. Along many lowland coasts, beaches occur as barrier islands that parallel the coast and are separated by a lagoon or bay. Along other stretches of coast, beaches are backed by eroding cliffs, or the beach may be absent with high rocky cliffs facing the waves.

Hydrographic conditions shoreward of the 30-meter depth curve should be thoroughly investigated and surveyed. Shallower depths of the surf zone from 0 to 30 meters are of primary concern in amphibious operations because crafts ground and troops and vehicles disembark in this area. When preparing hydrographic beach surveys, analysts must—

- Record accurate locations of obstructions.
- Determine clear boat passages to the beach.
- Determine trafficability of bottom materials.
- Select suitable beaching locations for amphibious vehicles.
- Determine maneuver areas for crafts.

From a tactical perspective, the ideal sea approaches to the beach should have—

- No obstructions.
- Deep water close inshore.
- Nearshore gradients deep enough for dry-ramp beaching of landing craft and ships.
- Soil composed of firm sand with gentle gradients.
- Small tides.
- No currents or surf.

The ideal beach terrain should be—

- Flat or gently rising.
- Backed by a coastal range high enough to mask the landing area.
- Relatively clear.
- Firm with adequate drainage.

Analysts evaluate the following beach features to determine those areas that come nearest to the optimum landing requirements.

Size

Analysts measure the beach to determine the force size that can be supported. The beach size also defines requirements for follow-on logistical forces and establishment of logistical base sites or dumps. Analysts determine the usable beach length by measuring, in kilometers, the gross length minus unsuitable landing features, such as rivers and rock outcroppings. When preparing the overlay, analysts describe and plot—

- Unsuitable beach sections.
- Features that might affect movement along the beach.
- Beach widths available at the low-water tide stage (maximum width) and at the high-water tide stage (minimum width), noting each stage of the tide.
- Locations of major changes in width.

Approaches

Analysts identify major obstructions and obstacles in the offshore approaches for an area seaward of the 30-meter depth curve. More detailed analysis and information are provided shoreward from the 30-meter depth curve giving distances and azimuths of obstructions and obstacles from the centerline of the beach. When describing general approach conditions, analysts note the presence of—

- Shoals.
- Bars.
- Kelp beds.
- Island groups.
- Exposed rocks.

Gradient

The foreshore gradient may be so steep as to prohibit the landing of vehicles from beached craft without use of matting, or it may be so flat as to cause personnel and vehicles to move great distances from boats over exposed areas to cover. Analysts express the gradient as one unit of vertical rise in relation to horizontal distance (e.g., 1 foot vertical height over 20 feet of horizontal distance = 1:20). Gradient may also be given in percent of slope or degree of angle. Analysts record gradients when—

- High-water zone of the foreshore is much steeper than the foreshore.
- Seasonal gradient changes information is available.
- Backshores are not level.

Composition

A description of the characteristics of the beach material gives a valuable clue to the slope or gradient of a beach when other information is lacking. Analysts can determine the gradient by the size of the beach material and the character of wave action. The depth of beach materials and the nature of subsurface materials are also indications of beach firmness and trafficability.

Trafficability

The beach's ability to sustain troop and vehicle traffic depends on factors such as moisture content, slope, grain size, and compacting. When evaluating beach trafficability, analysts must consider the following general rules:

- Changes in beach firmness may occur in short periods of time.
- Sandy beaches are more firm when damp.
- Beach backshores are frequently dry and therefore soft.
- Pebbles and cobbles are firm for bearing capacity but are loose for vehicle traction.
- Clay is soft when wet, but combinations of clay and sand may be firm.
- Fine to coarse sand mixtures tend to be firm.
- Soft zones are common near the upper level of wave wash at high tide because air pockets are trapped under the wet sand.
- Sand beaches exposed to wave action are generally firmer than beaches of similar material in sheltered locations.

Vegetation

Beach vegetation rarely affects military operations except for mangrove. These tropical trees and shrubs normally grow in sheltered tidal areas that have a soft, fine bottom material, but they may exist on foreshores that do not experience heavy wave action. Analysts identify the mangrove's interlaced roots, which constitute a barrier to movement.

Natural Obstacles

Analysts evaluate cusps, beach ridges, scarp, and berm to identify areas that could impede movement.

Natural Cusps

These are more or less evenly spaced ridges or horns of beach material and intervening crescent shaped troughs. The horns trend at right angles to the shoreline and taper to their point seaward. Cusps present on beaches should be noted. There are several characteristics of this beach feature that may be significant in amphibious landings. Along gravel beaches, the cusps may develop very large proportions, rising several feet above adjacent troughs and becoming a serious hindrance to traffic. Cusps are soft, whereas the troughs are usually of the same firmness as the normal beach face.

Beach Ridges

These continuous mounds or ridges are created by wave action along the upper limits of the beach. They may occur as single ridges or as a series of parallel ridges extending some distance inland. Commonly 3 to 8 feet in height above mean high tide, beach ridges can attain a height of 30 feet on pebble beaches. Ridges may consist of sand, pebbles, or gravel. Gravel or shingle ridges are high and loose and are very difficult to traverse.

Scarp

This near-vertical face cut into beach materials is caused by erosive wave action and may be a formidable barrier to movement across the beach. Scarps cut into the backshore have permanence, but normal wave action will eliminate foreshore scarps.

Beach Berm

A horizontal formation of material deposited by wave action, beach berm begins at the limit of normal-wave up rush and extends landward. Where more than one berm exists, they are separated by beach scarps in various stages of deterioration. The seaward margin of a berm is know as the berm crest. Berms are usually dry and soft but may be firm for a short time when damp.

Manmade Obstacles

Groins, jetties, bulkheads, and sea walls are manmade structures that could hinder beach operations.

Groins

These structures are used to stabilize a beach. They are long, low, narrow structures extending seaward from the backshore that are built to trap water-suspended sand on shore. Because groins are usually built as a system of structures spaced at regular intervals along the beach, analysts identify them as obstacles to the lateral movement of vehicles.

Jetties

Used to improve and stabilize inlets and river mouths, jetties project seaward from the shoreline through the normal surf zone. They are larger and more massive than groins. They prevent sand deposits in the channel, regulate the inflow and outflow of tides and river discharge, and protect vessels entering the inlet or river. Analysts evaluate jetties to determine if they are high enough to protect vessels against storm wave action and to prevent sand movement in the channel.

Bulkheads and Sea Walls

These structures protect areas of the coast against heavy storm wave action. They limit the shoreward movement of destructive waves, but under severe wave action they may cause the removal of sand from the beach. Analysts evaluate bulkheads and sea walls because they are normally strongly built and difficult to break through, which can prevent troop and vehicular movement from the beach to inland areas.

Exits

Uninterrupted movement inland from a beach is necessary to provide direct, rapid support and supply of combat forces and to avoid the creation of lucrative targets of accumulated material

and personnel on beaches. However, movement off a beach inland onto favorable terrain in many localities is one of the most difficult aspects of a landing because of the prevalence of bluffs, dunes, swamp, or lagoons close behind the beach. Existing exits require little or no preparation. They may be manmade or natural, such as roads, ramps, stairs, paths, gullies, dry stream beds, and gaps between dunes. Another characteristic of an exit requiring evaluation is the width. An exit should have a minimum width of 8 feet to permit the passage of vehicles.

SECTION V. AIRSPACE ANALYSIS

The addition of the airplane and helicopter to the arsenal of war requires that the battlespace be viewed in terms of width, depth, and a third dimension, height or airspace (measured in cubic kilometers). Because airspace has no reference points to guide the analyst and evidence of air activity is erased seconds after the activity occurs, it is often difficult to establish NAIs, TAIs, and air operations decision points. Airspace analysts are required to tie air events to time and the ground and to integrate the terrain analysis with analysis of—

- Aircraft maximum service ceilings.
- Minimum operating altitudes for fixed- and rotary-wing aircraft.
- Maximum effective ranges of air defense weapons systems.

Geospatial Analysis Support

The intelligence staff receives support from the terrain team during airspace analysis. However, this support must be augmented by personnel from other functional areas with an understanding of the air threat, air defense systems and operations, and close air support techniques.

Geospatial analysis and GEOINT production in support of air defense, counter air, and air-associated operations deal with an environment that extends several thousand meters above ground level and with forces whose mobility is limited only by the ability of their equipment. Terrain analysis is required because aircraft and air defense elements use the terrain to their best advantage.

Standard military topographic maps are not normally considered suitable for other than the most basic airspace analysis. Standard 1:50,000-scale topographic maps are most useful when analyzing the ability of an aircraft to approach, acquire, and engage a target. The analysis of an aircraft's approach (from air base to target vicinity) or of enemy air corridors should be conducted using standard 1:250,000-scale joint operations graphic-air (JOG-A) specifically designed for this purpose.

Airspace Evaluation

The third dimension of the battlespace includes the air AO and the air AOI. The air AO is the area where the commander is assigned responsibility and authority for military operations. The air AOI includes airspace adjacent to the air AO and extends into enemy airspace upward to the maximum service ceiling of enemy aircraft and the maximum effective altitude of enemy air defense weapons systems. It takes into consideration any space-capable system, i.e., satellites. In addition, the air AOI may extend as far as enemy airfields and to the maximum range of enemy surface-to-surface missile systems. During the airspace evaluation of the battlespace, analysts identify potential locations of LZs, DZs, FARPs,

and forward assembly or expeditionary airfields to pinpoint requirements for further analysis.

Military Aspects of Terrain Evaluation

Terrain analysis for air operations focuses on the same military aspects of terrain as ground operations. However, the analysis of these aspects is directed first at their effects on airspace operations and then on their resultant effects on the overall operation.

Key Terrain

Key terrain in airspace analysis is any terrain feature that allows air defense weapons to engage channeled or constrained air or airborne forces. Analysts should identify—

- Areas that limit aircraft lateral movement.
- Areas that restrict air maneuver.
- Elevations higher than maximum aircraft service ceilings.
- Airfields.
- LZs and DZs.
- Fixed or surveyed air defense weapons and radar sites.
- FARPs.

Observation and Fields of Fire

As with ground operations, observation involves the effects of the terrain on reconnaissance and surveillance as well as target acquisition. Fields of fire involve the effects of terrain on weapon's effectiveness. In air defense, both counterair and other air operations are closely related to line of sight (LOS). Ground operations are concerned primarily with horizontal LOS; air and air-associated operations are primarily concerned with air and ground oblique and vertical LOS.

Attack aircraft and air defense assets want as much protection as possible from enemy observation, and both require direct LOS to the target. It is, therefore, necessary to analyze airspace regarding the routes which provide the best protection for aircraft entering the target area and those which provide the best fields of fire for the aircraft once it reaches the target area. Similarly, the analysts must consider where air defense assets can best be hidden from observation and retain good fields of fire against the primary air AAs and mobility corridors.

Cover and Concealment

Friendly force operations require cover from aerial direct fires and concealment from aerial reconnaissance and surveillance. The enemy also uses terrain to provide cover from direct fires and to conceal their operations from friendly detection. Analysts evaluate airspace routes that provide the best protection for aircraft entering the target area and identify locations where air defense assets can best be hidden from observation.

While not considered as either concealment or cover in the strictest sense, NOE flight enhances both fixed- and rotary-wing aircraft survivability. An NOE flight makes the optimum use of available terrain for concealment and cover and hinders quick countering responses by ground forces and air defense assets.

Obstacles

When evaluating terrain, analysts identify the following types of obstacles, which channel aircraft movement and restrict evasive' actions:

- Obstacles to the effective employment of air defense target acquisition or weapon systems (e.g., terrain that masks LOS, built-up areas, tall buildings, vegetation).
- Obstacles that restrict NOE flights, which are below 22.8 meters or 75 feet in height (e.g., tall trees; radio, television, and microwave relay towers; power transmission lines; support towers; smoke and obscurants; tall buildings).

- Obstacles that force aircraft to employ a particular profile or attack route or to gain excessive altitude that is above 22.8 meters in height (e.g., mountains, large hill masses, built-up areas, excessively tall trees).
- Obstacles that restrict lateral movement within the air AA or mobility corridor. These obstacles have the same effect on aircraft as ground obstacles, that is, channeling movement and restricting evasive action. They often become key terrain for the employment of air defense weapons systems.

Avenues of Approach

A good air AA permits maneuver while providing terrain masking from air defense weapons systems. In addition to the criteria evaluated for ground AAs, analysts consider the following variables when analyzing air AAs:

- Type of aircraft.
- Maximum service ceiling of the aircraft.
- Attack profile being employed.
- Weapon system or expected ordnance.
- Type of target to be attacked.

Weather

Aviation operations are especially susceptible to weather effects, because temperature, humidity, and cloud cover can have a significant impact on an aircraft's ability to use a particular AA. Analysts must evaluate the effects of visibility, wind speed and direction, precipitation, cloud cover, temperature, and humidity when conducting analysis for airspace operations.

SECTION VI. WEATHER ANALYSIS

Commanders and their staffs must acquire weather information about the entire battlespace area and know how to exploit the opportunities the weather offers while minimizing its adverse effects on personnel, equipment, and mission accomplishment.

Responsibilities

The following units and personnel are responsible for determining weather effects on the battlespace environment:

- MEF topographic platoon.
- MSC supporting GEOINT support teams.
- MEU(SOC) CE GEOINT teams.
- Staff engineer officer.
- Staff weather officer.
- Weather team.

Weather Effects

Weather, climate, and terrain are so interrelated they must be considered together when planning MAGTF operations. Weather elements are capable of drastically altering terrain features and trafficability. Conversely, terrain features exert some influence on local weather. This relationship of weather and terrain must be carefully correlated in terrain studies to produce accurate geospatial analysis. Terrain features are affected by such elements as visibility, temperature, humidity, precipitation, winds, clouds, and electrical phenomena. The specific factors described vary with the geographic area, time, and season. Terrain features also influence the climate of an area. The effects of temperature, humidity, precipitation, visibility, wind speed and direction, clouds, and atmospheric pressure can affect the battlespace environment, which can enhance or limit military operations.

Temperature and Humidity

Temperature is the value of heat or cold recorded by a thermometer, which is normally placed 6 feet above the ground. Temperatures are recorded in Fahrenheit and Celsius values.

Humidity is the water vapor content in the atmosphere. It is expressed as relative or absolute humidity.

When evaluating temperature and humidity, analysts must consider the following effects on operations:

- Aircraft efficiency is reduced in areas of high temperature and high humidity, because when temperature and humidity are high, the air is denser.
- Extreme temperature and humidity will reduce personnel capabilities and may necessitate a reduction of aircraft payloads.
- Tactics devised for one climatic zone may require considerable revision if used in another zone.
- High temperature and humidity conditions found in the tropics are conducive to growth of dense foliage and jungles, which affects trafficability and cross-country mobility.
- Cold weather periods—
  - Create a need for heated shelters.
  - Make the construction of fortifications difficult.
  - Increase the amount of dependence upon logistical support.
  - Necessitate special clothing, equipment, and combat skills.
- Periods of freezing temperatures—
  - Increase the trafficability of some soils.
  - Create ice sheets on roads, making movement more difficult.
  - Decrease a projectile's ability to penetrate the earth.
  - Increase the casualty effect of contact-fuzed shells.
- Melting snows may cause floods and avalanches.
- Temperature inversions (air nearest ground is colder than overlying air) cause the air to remain stable and to hold dust and smoke near the ground, which reduces both visibility and air purity.
- The amount of water vapor in the air affects the trajectory of projectiles.
- Humidity affects the distance sounds travel, thus affecting listening posts and sound-ranging operations.

Precipitation

Precipitation is any moisture falling from a cloud in frozen or liquid form. Common types of precipitation are rain, snow, hail, drizzle, sleet, and freezing rain. The intensity of precipitation is described as light, moderate, or heavy.

The primary significance of precipitation is its effect on the state of the ground and trafficability, on the efficiency of personnel, and on visibility. The effects of restricted visibility caused by precipitation are just as important as those caused by airborne particles such as dust or smoke. When evaluating precipitation, analysts must consider the following effects on operations:

- Rain, snow, and fog mask patrol and guerrilla activities by decreasing the enemy's surveillance and detection capability.
- Precipitation severely reduces trafficability by altering the surface condition of different soils to varying extents.
- Heavy rain may make some types of unsurfaced roads impassable.
- Heavy or prolonged precipitation usually aids the protected defense by limiting the mobility of an offensive force.
- Precipitation can drastically reduce the efficiency and effectiveness of exposed personnel.

- Precipitation may aid offensive operations by degrading the surveillance capabilities of radar, electro-optical, and infrared devices.
- Seasonal precipitation may change soil trafficability and affect cross-country movement.
- Seasonal floods or swelling streams may make fording and bridging operations difficult or impossible.
- Snow and sleet hamper movement on roads, often making them impassable in mountainous areas.
- Snow accumulations in mountains afford lower, drier regions with a water supply throughout the year.
- Precipitation usually has an adverse effect on visibility and observation.
- Rain may wash excessive impurities from the air.
- Rain and snow aid concealment, which may facilitate surprise attacks.
- Precipitation often limits operations of listening posts and many electro-optical systems.

Visibility

Weather personnel determine visibility by measuring the horizontal distance that the unaided eye can discern a large object or terrain feature. Visibility is reported in meters or fractions of a mile for the prevailing value of the visibility in all directions. Diminishing visibility measurements are noted in the remarks section of the weather observation report.

When evaluating the weather effects on military operations, analysts must consider that poor visibility—

- Aids ground offense and withdrawal.
- Restricts visual reconnaissance and surveillance.
- Tends to conceal concentrations and maneuver of friendly forces from the enemy, which enhances the possibility of achieving surprise.
- Hinders the defense because defensive cohesion and control are difficult.
- Decreases the ability to place aimed fire on the advancing force, making target acquisition less accurate.
- Enhances patrol activities and guerrilla operations by masking and screening movement.

Wind Speed and Direction

When weather personnel determine wind speed or velocity and direction, they measure the air movement rate past a given point and the direction from which the wind is blowing. A gust is a rapid fluctuation in wind speed with a variation of 10 knots or more between peak and lull.

When evaluating wind speed effects on the environment, analysts must consider the following effects on operations:

- Wind velocity on the surface and aloft favors the upwind force in any type of operation.
- Chemical and biological weapons will saturate the low-level, downwind atmosphere with contaminating aerosols.
- An upwind force, with the wind at its back, has better forward visibility and can advance easier and faster.
- Strong winds in arid or semiarid areas frequently raise large clouds of dust and sand, which greatly reduce observation.
- Blowing snow may reduce visibility over wide areas, which may ground observation aircraft and sensors.
- Winds tend to deflect projectiles from their normal paths, particularly when they are fired at long ranges. The effect that wind will have on a projectile increases with an increase in the wind velocity and the projectile size. The wind direction and velocity must be known to apply compensating corrections to firing data.

- Strong winds hinder amphibious operations by creating high seas, which can prevent landing craft from landing or retracting and restrict helicopterborne operations during the ship-to-shore movement.

Cloud Conditions

Cloud conditions are described by the amount and height of the cloud cover. Weather personnel measure the height of the cloud base from ground level and report that measurement in feet. A cloud base is the height of the lowest broken or overcast layer, while a cloud ceiling is the height of the highest layer of several scattered cloud layers. The types of clouds help determine the intensity and amounts of precipitation.

The type and amount of cloud cover, as well as the height of cloud bases and tops, influence ground tactics because they affect the entire range of both friendly and enemy aviation. Analysts should consider the following effects on operations when evaluating cloud conditions:

- Extensive cloud cover reduces the effectiveness of air support but provides a tactical advantage as cloud cover increases, as cloud bases lower, and as associated conditions increase (e.g., icing, turbulence, poor visibility).
- Clouds affect ground operations because they may limit illumination and visibility.
- As solar radiation interceptors, clouds tend to reduce extremes of surface temperature.
- Daytime cloudiness reduces the amount of heat received from the sun at the earth's surface, slowing down the drying of roads and affecting the trafficability of soils.
- Extensive night cloudiness prevents the loss of heat from the earth's surface, resulting in higher nighttime temperatures.
- Cloudiness affects air operations by limiting aerial observation and reconnaissance.

Atmospheric Pressure

The pressure exerted by the atmosphere at a given point is atmospheric pressure, which is measured by a barometer in millibars or in inches of mercury. The air density is measured at high and low altitudes and is reported as high pressure and low pressure. High pressure is critical to air operations because it affects the lift capability of helicopter and fixed-wing aircraft.

Weather Forecast and Weather Effects Products

While planners cannot control the weather, they should be able to exploit the opportunities offered by weather effects while reducing or minimizing its adverse effects on battlespace operations. Analysts provide planners with weather forecasts that cover the geographical layout of the battlespace and meet or exceed the duration of the planning and execution cycles. Using weather critical values tables created during IPB and weather forecast graphics (see fig. 6-2), analysts can quickly identify and determine the impact of weather effects on personnel, equipment, and planned operations. These impacts are displayed in the weather effects matrix (see fig. 6-3).

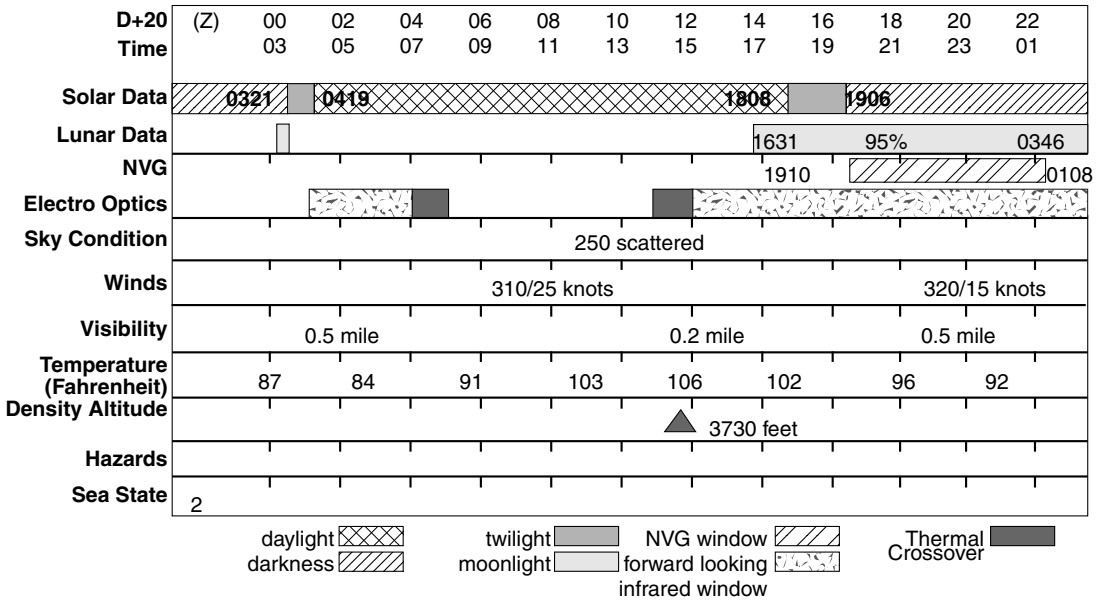


Figure 6-2. Weather Forecast Graphic.

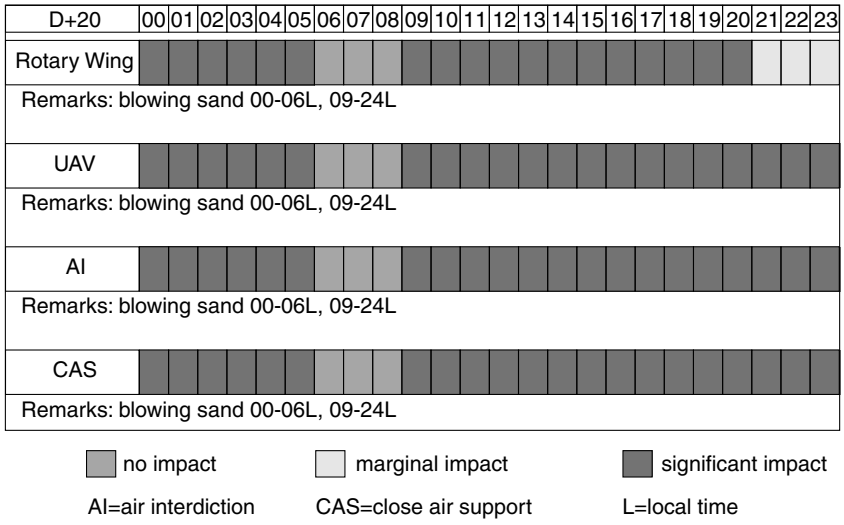


Figure 6-3. Weather Effects Matrix.

SECTION VII. INFRASTRUCTURE ANALYSIS

The infrastructure of a potential AO is a key element of information in an expeditionary environment. Points of entry, transportation systems, economic infrastructure, and social infrastructure, impact how friendly forces enter into, move through, and sustain themselves in the

AO. Infrastructure also impacts a potential threat's ability to conduct operations. The importance of particular facilities depends on the units involved and the type of operations envisioned. The study of a target area's infrastructure must focus on factors that are crucial to mission accomplishment. Most commands, particularly lower level tactical commands, must rely on other organizations and agencies to conduct infrastructure analysis and to provide accessible information.

Sources of Information

Detailed infrastructure analysis can be resource and time intensive, thus identification of analytical requirements prior to conflict or crisis helps ensure the availability of the information when needed. The intelligence staff must be familiar with all sources of infrastructure information that can be rapidly accessed when needed. Infrastructure analyses are performed by—

- Theater joint intelligence centers (JICs).
- U.S. Transportation Command.
- NIMA.
- Defense Intelligence Agency (DIA).
- Service intelligence centers (e.g., National Ground Intelligence Center, MCIA).
- Nonintelligence organizations (e.g., Marine Corps and Army civil affairs units).

Transportation System

In preparing intelligence studies, all transportation facilities must be carefully evaluated to determine their effect on the proposed operations. At higher levels of command, each major facility may be the subject of a detailed study by unit intelligence analysts or by external agencies such as theater JICs, U.S. Transportation Command JIC, or DIA.

Highway or Road Network

For intelligence purposes, a highway means roads, trails, multilane super highways, pack trails, and footpaths. Associated structures and facilities necessary for movement and for protection of routes, such as bridges, ferries, snowsheds, tunnels, and fords are integral parts of the highway system. An adequate highway system is required to conduct a major military operation. Military interest in highways of a given area or country covers physical characteristics of the existing system and various administrative and operational aspects pertaining to construction and maintenance.

Transportation studies should provide information on existing routes, major repair or rehabilitation requirements, and locations of new routes needed to support planned operations. The terrain study should indicate the minimum maintenance and construction requirements that may be anticipated during a planned operation. When evaluating the road network, analysts should consider—

- Routes in the combat zone should meet minimum standards.
- Roads in rear areas near water terminals, airfields, and supply installations must be well surfaced and capable of carrying heavy traffic without excessive maintenance.
- Operations on a wide front require a large number of secondary routes in forward and rear areas. The information presented in a terrain study should indicate the minimum maintenance and construction requirements that may be anticipated during a planned operation.
- Large volumes of heavy traffic severely abuse roads.
- Important bridges, intersections, and narrow passes are primary targets for enemy fires or unconventional operations.

- Maintenance should be conducted only on necessary routes.
- Construction of new routes must be held to a minimum.

Railroad Network

A railway includes fixed property belonging to the line. The fixed property includes land, facilities, bridges, tunnels, snowsheds, galleries, ferries, and other structures necessary for the movement of traffic. Railroad studies cover information pertaining to the development, construction, maintenance, and physical characteristics of the existing system. The network's physical characteristics information is necessary for determining capacities and maintenance requirements. Physical characteristics include the railroad's critical features, component parts (e.g., roadbed, ballast, track, rails/gauge), and horizontal and vertical alignment.

When evaluating railroad networks, analysts must consider the following factors:

- Railways are often the main transportation system in countries without an extensively developed road system.
- Suitability for mass movement and low susceptibility to weather effects make railroads useful for logistic support.
- Secondary and feeder railway lines are important to maneuver warfare with its emphasis on dispersal and the requirement for more and smaller rear installations.
- Railways and their associated facilities are highly vulnerable to enemy attack (e.g., sabotage, guerrilla operations).
- Keeping a railroad operational requires trained security forces and extensive protective measures.

Port and Harbor Facilities

Information and intelligence on ports, naval bases, and shipyard facilities is essential for estimating their capacities, capabilities, vulnerability, and other items of military significance. In wartime, principal and secondary ports and bases are prime targets for destruction. A port normally consists of a harbor plus terminal facilities. When natural, improved, or artificial harbors are developed for transactions between ship and shore, they become part of a port. Analysts classify these harbors as coastal, bay and estuary, and river. When evaluating port and harbor facilities, analysts are interested in harbor works, depths, navigable fairways, and anchorage.

Harbor Works

Structures designed to provide shelter, to control water flow, and to regulate erosion for the improvement of the navigability of a harbor are protective or harbor works. Harbor works do not include port facilities that are designed specifically for the transfer of cargo and the servicing of ships. The principal types of structures are—

- Breakwaters.
- Jetties.
- Groins.
- Sea walls.
- Bulkheads.
- Dikes.
- Locks.
- Moles.

Depths

Analysts compute depths of harbors, entrances, anchorages, wharves, and dry docks in reference planes based on tidal levels. When reporting depth, analysts must clearly indicate the reference plane or chart datum on the hydrographic chart. Datum established for ports is the basis for soundings.

Navigable Fairways

The approach, entrance, and the harbor itself frequently determine the size of ships that can

be accommodated in the port. Analysts must evaluate these fairway dimensions and describe any limitations on a ship's navigation (e.g., draft, length, beam, height above water). In addition, analysts should report ships' experiences entering the fairway.

Anchorage

Analysts show anchorage data on large scale charts and plans. Operational information reported includes—

- Anchorage designations.
- Berth assignments.
- Anchoring practices.
- Ships' experiences.

Airfields

Whether military or civilian, airfields are of vital importance to military combat situations. The size and features of an airfield determine its combat and reconnaissance capabilities.

Types

Installations termed airfields include—

- Air bases.
- Airports.
- Airstrips.
- Landing strips.
- Air depots.
- Heliports.
- Helipads.
- Seaplane stations.

Characteristics

Analysts conduct geographic studies to identify the airfield's—

- Type.
- Physical dimensions.
- Construction materials.
- Field condition.
- Support facilities.

Considerations

When evaluating the airfield, analysts report answers to the following questions:

- Is it serviceable?
- Is it occupied?
- Is it under construction?
- Is it in full or partial operations?

Structures and Crossings

Structures and crossings on highways or railways may reduce or interrupt the flow of traffic on a transportation route. Detailed information on structures and crossings is essential to a battlespace analyst and to an engineer, who may be required to repair or restore a structure. These structures and crossings include bridges, culverts, tunnels, galleries, snowsheds, retaining walls, ferries, fords, cableways, and tramways.

Bridges

Highway and railway bridges are vulnerable points on a LOC. Timely preservation, destruction, or repair of a bridge may be the key to an effective defense or to the successful penetration of an enemy area. A bridge seized intact has great value in offensive operations; even a small bridge facilitates the movement of forces over a river or stream.

Analysts obtain bridge information from reconnaissance or from the NIMA-produced planning terrain tactical data base. Using aerial photographs, analysts can determine bridge length, width, clearance, and height above water. Basic information requirements reported on a bridge include—

- Summary of its structural characteristics.
- Critical dimensions (length, usable width, overhead clearance).

- Capacity estimation.
- General conditions.

Tunnels, Galleries, and Snowsheds

Features on a transportation route where it would be relatively easy to block traffic or that affect the traffic capacity of the road, are considered to be critical features of the road. Such features include tunnels, snowsheds, galleries, mountain passes, terrain gaps, gorges and defiles, deep cuts, steep grades, and sharp curves. Any obstructions to traffic flow, which limit the physical dimensions of vehicles utilizing a specific route, are important aspects of route studies. Reductions in traveled way widths, such as narrow streets in built-up areas, drainage ditches, embankments, and war damage limit vehicular movement. Underpasses and other covered traveled ways may restrict traffic flow not only as to width but also as to height.

A tunnel is an underground section of the route that has been made by cut-and-cover or bored for the passage of a route. It consists of the bore(s), a liner (optional), and portals. Common shapes of tunnel bores are semicircular, elliptical, horseshoe, and square with arched ceiling. Bores may be unlined or lined with brick, masonry or concrete. Some long tunnels are artificially ventilated by blowers at the portals or in ventilating shafts above the bore. Alignment of tunnels may be straight or curved.

Snowsheds and galleries are protective structures built in rugged mountainous terrain. These are not as common as bridges or tunnels. Snowsheds offer protection against snow accumulations as well as drifts and slides on exposed sections of the permanent way. Galleries offer protection against snow and rock avalanches. They may be cut into the side of a cliff and have a natural overhang, or the cover may be a concrete slab, either of which guides the avalanche across the track or road. One side of a gallery is usually open.

Retaining walls are built to support embankments, either on the uphill or downhill side of the roadway. Retaining walls also are necessary where an embankment requires support against the pressure of water.

Ferries

A ferry site is that place where traffic and cargo are conveyed across a river or other water barriers by a vessel called a ferry or ferryboat. Ferryboats or vessels vary widely in physical appearance and capacity depending on the depth, width, and current of the stream and the characteristics of traffic to be moved. Propulsion of ferries may be by oars, cable and pulleys, poles, stream current (trail and flying ferries), or by steam, gasoline, and diesel engines. Analysts report the capacity of a civil ferryboat in tons and total number of passengers. In addition, it is often assigned a military load classification number. Ferry slips or piers are generally provided on the shore to permit easy loading of passengers, cargo, and vehicles. The slips may vary from simple log piers to elaborate terminal buildings. A distinguishing characteristic of a ferry slip is often the floating or adjustable approach ramp, which accommodates variations in the ferry deck level.

The limiting characteristics of ferry sites includes the width of the water barrier from bank to bank, the distance and time traveled by the ferryboat from one side to the other side, and the depths of the water at each ferry slip. Climatic conditions have a marked effect on ferry operations. Fog and ice substantially reduce the total traffic moving capacity and increase the hazard of the water route. Therefore, data on tide fluctuations, freezing periods, floods, excessive dry spells, and their effects on ferry operation are important considerations. Ferry slips are often optimal places for grounding displacement landing craft or as exit points for amphibious vehicles.

Fords

A ford is a location in a water barrier where the physical characteristics of the current, bottom, and approaches permit the passage of personnel or vehicles and other equipment under their own propulsion. Analysts assess a ford site for use as a bridge bypass.

Ford approaches may be paved with concrete or bituminous surface material but are usually unimproved. The composition of the stream bottom determines its trafficability. In some cases, the natural river bottom of a ford may have been improved to increase load-bearing capacity and to reduce the water depth. Improved fords may have gravel or concrete surfacing, layers of sandbags, metal screening or matting, timber or wooden planking. Bottom conditions are determined by checking the stability and composition of the bed. Known and suspected ford sites are key information when assessing the ability of a bridge to be bypassed.

Basic information requirements reported on a ford include—

- Trafficability.
- Approaches.
- Bottom composition.
- Current.

Cableways and Tramways

Cableways and tramways may be encountered in rugged mountainous regions and beach areas or used as connections between two primary supply routes. Cableways and tramways are considered obstacles to low flying aircraft.

Inland Waterways

The term inland waterways is applied to rivers, streams, canals, lakes, and inland seas which are used as avenues of transport. It also includes the intercoastal waterways, usually running parallel to the coastline of a landmass and sheltered to permit the navigation of small vessels. When evaluating inland waterways, analysts must consider the following factors:

- Inland waterways provide an economical form of transportation for bulk supplies, freeing faster modes for shipments of a higher priority.
- Depths of rivers and streams fluctuate with maximum and minimum rainfall.
- Falls and rapids commonly interrupt streams with fairly direct courses.
- Streams of low and uniform gradients are usually slow moving and their channels shift constantly, creating sandbars, which are a menace to navigation.
- Traffic is halted completely during a freezing period unless ice-breaking operations can be conducted.
- Thaw following a freeze may cause floods.
- Periods of drought may result in insufficient water for the movement of vessels.
- Waterway locks, bridges, cuts, dams, and other fixed facilities are vulnerable to enemy action.

Supply Systems

Utilities, services, facilities, and construction resources comprise the essential internal supply systems and installations used to protect and maintain the life of a region or city. Military interest in this field is primarily logistical, although these facilities take on greater importance during urban operations, particularly operations other than war. Analysts must report the adequacy and quality of the petroleum and natural gas facilities, as well as power, water, and telecommunications systems, to ensure their maximum use by military forces.

Power System or Grid

Electricity is essential to the life of modern regions and cities. Destruction of electrical generation and distribution facilities in most

cities would bring industrial production and most utilities and services to a halt.

Petroleum, Oils, and Lubricants Facilities

Information on a nation's petroleum and natural gas resources provides a means for evaluating the capacity of a nation to produce, process, and supply fluid or gaseous hydrocarbons for military purposes. Analysts also evaluate the petroleum supply system's vulnerability to attack.

Water

Water is the most extensively used commodity in both urban and rural habitats. Water supply systems maintain and control the quality and quantity of water in urban areas. Analysts evaluate an area's water supply system to ensure there is an adequate supply of quality water for military purposes.

Telecommunications

Analysts evaluate an area's civil and military telecommunications systems, services, facilities, and equipment for use by military forces. Governmental and commercial organizations that regulate and operate the area's systems are also evaluated. Telecommunications services evaluated include—

- Telephone.
- Telegraph.
- Teleprinter.
- Facsimile.
- Data transmission.
- Radio broadcast.
- Television broadcast.

Urban Areas

The ever-increasing urbanization of the world's population dictates that urban areas will increasingly be the AO for war and operations other than war. Urban area geospatial studies are important in the planning of operations, targeting, and logistical support for operations.

Characteristics

Knowledge of the characteristics of urban areas is essential to the conduct of civil affairs and counterintelligence operations. Urban areas are significant as military objectives, targets, and bases of operations. Often they will be the focal point for internal ethnic, class, religious, or cultural conflict. Urban areas may be one or a combination of—

- Power centers (e.g., political, economic, military).
- Industrial production centers.
- Population centers.
- Transportation centers.
- Service centers (e.g., distribution points for fuels, power, water, raw materials, food, manufactured goods).
- Cultural and scientific centers (e.g., seats of learning, modern technological developments).

Urban Area Classification

An important aspect in the classification of cities is the determination of construction type. Rarely is a city of one type of construction; instead there will be a mixture of everything from shantytowns to skyscrapers. The analyst should attempt to determine what the predominant construction type is as well as what percentages of the city are composed of varying types. Urban areas or cities are classified according to their—

- Population size and density.
- Position in the country's society, economy, and defense establishment (strategic, secondary, or minor).
- Function.
- Construction type (e.g., shantytowns, skyscrapers).

Evaluation Factors

Line of sight considerations in cities are crucial, thus the urban area must be assessed in ground-level, above-ground, and below-ground dimensions. Since urban operations are manpower intensive and generally conducted at low unit levels, the information required is usually very detailed. The MCIA-1586-005-99, *Urban Generic Information Requirements Handbook*, discusses the components of urban area analysis. The primary factors evaluated in urban area GEOINT studies include—

- Physical characteristics.
- Building construction type.
- Accessibility.
- Utilities.
- Civil facilities.
- Industrial facilities.
- Military and other important installations.
- Underground facilities (e.g., subways, sewers, underground rivers, utility tunnels).

Construction Resources

Analysts conduct construction resource studies to evaluate a foreign area's capability to support friendly military operations. To determine construction capabilities, analysts compare area construction types to the work carried out by the U.S. Army Corps of Engineers. These studies include data on—

- Available construction materials.
- Construction industry organization.
- Major construction firms, including data on the firm's—
  - Size.
  - Capital assets.
  - Organization.
  - Amount of equipment.
  - Personnel skills.
  - Experience.
  - Specialization.

SECTION VIII. POLITICAL, ECONOMIC, AND SOCIOLOGICAL ANALYSIS

The current and historical setting of a country is an important and integral part of intelligence analysis. Most of the analysis effort is expended on armed forces and GEOINT, but the factors that can make a difference in many operations, especially operations other than war, involve political, economic, and sociological aspects of the target area.

Political Intelligence

Political intelligence begins with an assessment of the internal political dynamics of a country to include its leadership, internal political stability, economic position, labor supply, physical resources, and relative military power. The first consideration is the distribution of political power—is it a democracy, an oligarchy, a dictatorship, or has political power devolved to multiple interest groups such as tribes, clans, or gangs?

Consideration must be given to the sources of political power: authority based on a legitimate constitution and the will of the people, political magnetism, skill and competence of the leaders, or brute force. It is particularly important for western-trained analysts to understand nonwestern political institutions. In other countries, institutions that on the surface are western in nature may in fact operate quite differently. For example, civil and military bureaucracies may not be neutral agents of policy but may operate almost entirely in their own self interest. Armies

may function as political parties or administrators rather than as guardians of the national security. Parliaments may have a developmental or honorary role rather than a legislative role.

The analyst must evaluate the political system as it really operates, not the way it is supposed to operate. Political analysis of a foreign country begins with an assessment of the basic principles of government, governmental operations, foreign policy, political parties, pressure groups, electoral procedures, subversive movements, as well as criminal and terrorist organizations.

Basic Governmental Principles

The starting point of political analysis is the formal political structure and procedure of a foreign nation. Analysts must evaluate—

- Constitutional and legal system.
- Legal position of the legislative, judicial, and executive branches.
- Civil and religious rights of the people.
- People's national devotion to constitutional and legal procedures.

Governmental Operations

Governments are evaluated to determine their efficiency, integrity, and stability. Information about how the government actually operates and changes in the method of operation give the intelligence user clues about the probable future of a political system. When assessing governmental operations, analysts should consider the following:

- Marked inefficiency and corruption, which differs from past patterns, may indicate an impending change in government.
- Continued inefficiency and corruption may indicate popular apathy or a populace unable to effect change.
- Increased restrictions on the electoral process and on the basic social and political rights of the people may mean the government is growing less sure of its position and survivability.

Foreign Policy

Analysis of a target country's foreign policy addresses the country's public and private stance toward the United States, foreign policy goals and objectives, regional role, and alliances. Analysts gather foreign policy data from various sources, to include—

- Diplomatic and military personnel.
- Technical collection systems.
- Official foreign government statements.
- Press releases.
- Public opinion polls.
- International businessmen.
- Academic analyses.

Political Parties

Analysts study special interest parties and groups, (e.g., labor, religious, ethnic, industry) to evaluate their—

- Aims.
- Programs.
- Degree of popular support.
- Financial backing.
- Leadership.
- Electoral procedures.

Pressure Groups

With few exceptions, most states have some type of formal or informal pressure groups. Examples include political parties, associations, religious or ethnic organizations, labor unions, even illegal organizations (e.g., banned political party). The analyst must identify these pressure groups and their aims, methods, relative power,

sources of support, and leadership. Pressure groups may have international connections, and in some cases, may be almost entirely controlled from outside the country.

Electoral Procedures

Elections range from stage shows of limited intelligence significance to a means of peaceful, organized, and scheduled revolution. In addition to the parties, personalities, and policies, the intelligence analyst must consider the circumstances surrounding the actual balloting process and changes from the historical norm.

Subversive Movements

In many countries there are clandestine organizations or guerrilla groups whose intention is to overthrow or destroy the existing government. When analysts report on subversive movements, they should include the organization's—

- Size.
- Character of membership.
- Power base within the society.
- Doctrine or beliefs system.
- Affiliated organizations.
- Key figures.
- Funding.
- Methods of operation.

Criminal and Terrorist Organizations

Criminal organizations in some countries are so powerful that they influence or dominate national governments. Analysts must examine the organization's influence or forceful methods of control. Most terrorist organizations are small, short-lived, and not attached to any government. Analysts should determine if external factors or even the area's government assists the terrorist group.

Economic Intelligence

The study of economics involves the production, distribution, and use of wealth. It analyzes the factors of production and how those factors are used to produce the things that people need and want. Economics focuses on production within nations and on relations between nations, especially on the competition for the world's scarce resources. That competition continues to be a major cause of international conflict.

Economic intelligence focuses on the use of natural and human resources, and especially on the functioning of national economies and economic relations between countries. Economic intelligence is vital to estimating the magnitude of military or other threats to ourselves and our allies. A nation can undertake and carry out only those operations, military or economic, that its economy is able to mount or sustain. In the short run, national strength consists of staffing that can be mobilized and weapons and supplies that have been manufactured or purchased.

The extraordinary expense of modern warfare means that anything beyond the briefest of campaigns will require the total economic resources of a nation. Despite the simplicity of the concept, this task is elusive and difficult.

A large nation's economic resources offer a wide range of possible actions. For example, efforts to increase military preparedness do not necessarily foretell military aggression. While it is possible to develop probability estimates based on key indicators, it would be unwise to think that analysis of economic information alone will yield completely dependable results.

Economic intelligence provides indications and warning of potential crisis or conflict. Economic failure often generates social unrest or disputes with neighboring nations. The resulting instability

may require United States or other national force intervention.

Sources of Economic Intelligence

Because nations and businesses often hide information to limit competition or to prevent the discovery of sensitive military-related technologies, the most reliable information may have to be obtained from more traditional intelligence methods such as informed reporting by attaches and officers on the scene. The most comprehensive and reliable sources of economic intelligence are printed and electronic trade and business publications. These open sources should be supplemented with reports from—

- Attaches and officers on the scene.
- Foreign broadcasts.
- Defectors.
- Commercial contacts.
- Clandestine sources.

Evaluation Factors

Analysts gather the following information for economic studies:

- Size of the area's economy.
- Sources of raw materials (e.g., minerals crucial to production of military weaponry).
- Products of the area manufacturers.
- Methods of production (e.g., advanced technologies).
- Profits from narcotics trafficking.
- Funds transfers by terrorist organizations.

Narcotics and Terrorism

Tracking profits from narcotics trafficking has been one of the most useful forms of intelligence activity against these organizations. Drugs enter the United States via a huge number of routes, but the profits exit by a more limited, and potentially traceable, number of routes. In some cases, narcotics are a country's prime resource and export. Terrorist organizations can also be tracked and studied using information on funds transfers, although the amounts tend to be smaller than those of narcotics traffickers.

Sociological Analysis

Analysts must study the way people organize their day-to-day living, including the study of groups within society, their composition, organization, purposes and habits, and the role of the individual in society. For intelligence purposes, analysts study seven sociological factors.

Population

Intelligence data derived from censuses and sample surveys describe the size, distribution, and characteristics of the population, including rate of change. Most countries now conduct censuses and publish detailed data. The U.S. Census Bureau and the United Nations are prime sources for detailed data on foreign populations. Analysts use censuses and surveys to evaluate an area's population in terms of—

- Location.
- Growth rates.
- Age and sex structure.
- Labor force.
- Military staffing.
- Migration.

Characteristics of the People

Analysts study social characteristics to determine their contribution to national cohesion or national disintegration. Social characteristics evaluated by analysts include—

- Social stratification.
- Number and distribution of languages.

- Prejudices.
- Formal and informal organizations.
- Traditions.
- Taboos.
- Nonpolitical or religious groupings and tribal or clan organizations.
- Idiosyncrasies.
- Social mobility.

Public Opinion

Key indicators of a society's goals may be found in the attitudes expressed by significant segments of the population on questions of national interest. Opinions may vary from near unanimity to a nearly uniform scattering of opinion over a wide spectrum. Analysts should sample minority opinions, especially of groups capable of pressuring the government.

Education

Analysts concentrate on the general character of education and on the quality of elementary through graduate and professional schools. Data collected for these studies include—

- Education expenditures.
- Relationship between education and other social and political characteristics.
- Education levels among the various components of society.
- Number of students studying abroad.
- Extent to which foreign languages are taught.
- Subjects taught in schools.

Religion

Religious beliefs may be a potentially dangerous friction factor for deployed U.S. personnel; this was experienced in the Middle East with fundamentalist Islamic sects. Understanding those friction factors is essential to mission accomplishment and the protection of friendly forces. Analysts evaluate data collected on an area's religions, which includes—

- Types.
- Size of denominations.
- Growth or decline rates.
- Cooperative or confrontational relationships between religions, the people they represent, and the government.
- Ways the government deals with religious organizations.
- Roles religious groups play in the national decisionmaking process.
- Religious traditions and taboos.

Public Welfare

To evaluate the general health of a population, analysts must identify—

- Health delivery systems.
- Governmental and informal welfare systems.
- Social services provided.
- Living conditions.
- Social insurance.
- Social problems that affect national strength and stability (e.g., divorce rate, slums, drug use, crime) and methods of coping with these problems.

Narcotics and Terrorism Tolerance

A population's level of tolerance for narcotics and terrorist activities depends on the relations between these organizations and the population as a whole. Analysts should determine if the tolerance is a result of the huge sums of money traffickers pump into the economy or a result of trafficker's use of force. Terrorists may be accepted and even supported by the local populace if they are perceived to be working for the good of the local people. The intelligence analyst must evaluate the way these organizations operate.

CHAPTER 7. THREAT ANALYSIS TECHNIQUES

Intelligence analysts make the greatest impact on plans and operations by conducting threat analysis. Using the IPB threat analysis techniques, analysts provide commanders and planners with paragraphs 3 through 5 of the intelligence estimate (see appendix A). To enhance the intelligence estimate, analysts use specialized analytical techniques. This chapter provides a detailed view of the knowledge essential in conducting threat analysis.

SECTION I. INTELLIGENCE PREPARATION OF THE BATTLESPACE TECHNIQUES

When conducting threat IPB, intelligence analysts evaluate the threat OOB, develop a threat model, and determine, evaluate, prioritize, and develop threat COAs.

Threat Order of Battle

An integral part of intelligence analysis, OOB is the identification, strength, command structure, and disposition of units, personnel, and equipment of foreign military forces, including irregular force units, auxiliary, insurgent, and criminal elements. The analyst must consider and integrate OOB intelligence with other METT-T factors to determine threat capabilities, vulnerabilities, intentions, and COAs.

Order of Battle Factors

The OOB analysis involves evaluating a threat force's composition, disposition, strength, tactics, training, logistics, combat effectiveness, electronic technical data, command and control warfare (C2W) data, and other supporting data.

Composition

The identification and organization of specific threat units or commands are keys to OOB intelligence. Through identification, the analyst develops a history of the threat unit's composition, tactics, training, and combat effectiveness. To determine a unit's composition, analysts identify the threat unit by—

- Name.
- Number.
- Type.
- Size or strength.
- Subordination.

Organization is the physical structure of a unit and the relationship of the various elements within that structure. The threat unit's identification within an organization alerts the analyst to the possible presence of other units in the same organization. With knowledge of the threat's organization, analysts can develop accurate intelligence on current strength and combat efficiency.

When analyzing composition, intelligence personnel should consider the unit's self-sufficiency. Units subordinate to a self-sufficient tactical unit, although capable of limited independent action, cannot sustain themselves over relatively long periods of time. These subordinate units are seldom employed independently or separately from the basic self-sufficient tactical unit. For example, a new threat battalion is reported to be operating in the AO. Knowing that the threat normally organizes and operates in brigades composed of three

to five battalions and that those battalions are normally not employed independently, analysts determine it is probable that the remaining elements of the threat brigade are in or near the AO.

Disposition

The threat unit's disposition consists of the unit's location and tactical or administrative deployment method. When evaluating a threat unit's disposition, analysts include the unit's current and projected movements to determine the capabilities of the enemy force and its effect on friendly mission accomplishment. A threat that has moved, is moving, or is planning to move may become capable of a number of actions (e.g., attacking, reinforcing, replacing, withdrawing). Analysts must continually monitor threat movements to integrate the threat unit's disposition with terrain analysis into doctrine and situation templates. When assessing a threat unit's disposition, analysts should consider—

- Predetermined doctrinal deployment, which may lead to an accurate appraisal of probable threat COAs.
- Knowledge of the threat's echelon arrangement may indicate which units will be employed in supporting and reserve roles.
- Patrol activity may indicate planned movement (but in itself is not movement).

Strength

A threat unit's strength is described in terms of personnel, weapons, and equipment. Information concerning enemy strength provides the commander with an indication of threat capabilities and helps determine the threat commander's probable COA. When assessing a threat's strength, analysts should consider—

- Lack of strength lowers the threat force's capabilities estimate, while superiority of strength raises the force's capabilities estimate.
- Marked concentration or buildup of units in an area may indicate a probable COA and threat objectives.
- Changes in strength of potential threat forces during peacetime may indicate the threat's intention to wage conflict.

Tactics

In OOB intelligence, tactics include tactical doctrine as well as tactics employed by specific units. While tactical doctrine refers to the threat's accepted organization and employment principles, tactics refer to the threat's conduct of operations. From tactical doctrine knowledge, the analyst can determine how the threat may employ his/her infantry, mechanized, armor, and artillery units in the offense and defense under various conditions. Analysts integrate tactics in doctrinal templates and other intelligence products.

Training

Individual and unit training can significantly contribute to the combat effectiveness of any military organization. Analysts assess the thoroughness, degree, and quality of individual training received by the threat's recruit, specialist, noncommissioned officer, and officer to determine the overall efficiency of its armed force. When evaluating the threat's training, analysts should consider—

- Small unit exercises to large scale training maneuvers conducted in seasonal cycles are an essential part of the training necessary for a unit to operate at its full potential.
- Each type or phase of training accomplished by a unit adds to its capabilities and effectiveness.
- Crew training for weapons systems (e.g., tanks, artillery, and aircraft) increases weapons systems effectiveness.

Logistics

The threat's adoption of a COA depends on the ability of the logistical system to support that action. With knowledge of the threat's logistic capabilities, analysts can accurately evaluate the threat's capabilities, strength, and combat effectiveness. The location of a threat unit's logistical support structure elements aids analysts in determining the disposition of maneuver formations. Logistic information critical for effective intelligence analysis includes—

- Classes and types of supply.
- Lines of communication.
- Logistical requirements.
- Procurement methods.
- Distribution priorities and procedures.
- Transportation networks and modes.
- Installations and terminals.
- Evacuation and salvage procedures.
- Maintenance.

Combat Effectiveness

The abilities and fighting qualities of a unit are affected by numerous tangible and intangible factors. Analysts are expected to rate threat combat effectiveness by analyzing the following factors:

- Personnel strength, including estimated losses.
- Conditions and amounts of weapons and equipment.
- Status of training.
- Quality of leadership.
- Individuals' combat experience.
- Length of time a unit has been exposed to combat.
- Efficiency and training of the officer and noncommissioned corps.
- Past performance and traditions.
- Commander's personality traits.
- Morale, esprit, health, discipline, and political reliability (belief in the cause).
- Status of technical and logistical support of the unit.
- Adequacy of military schooling.
- Socioethnic characteristics of the people.
- Geographic area in which committed.

For each unit of interest, analysts must define, evaluate, and assign a color value to each applicable factor. This assessment is highly subjective; the experience and knowledge of the analyst and the scope of available intelligence will determine its validity.

Example: Assessment Values

When evaluating the length of time a unit has been exposed to combat, analysts use the following values:

- *Green*—Sporadic to intermittent limited combat (small arms fire, fire fights).
- *Amber*—Constant limited combat to sporadic intense combat (artillery barrage, heavy weapons).
- *Red*—Sustained intense combat (deliberate attack or defense).

Where a factor has elements, analysts assign a value to each element and then synthesize an overall value for that factor. After assigning a value to each factor, analysts assign an overall combat effectiveness rating to the unit. This process is highly subjective, and allowances can be made for prioritizing or weighting the individual factors. The values assigned to factors and the definitions of the effectiveness rating may be adjusted as the situation dictates.

The values and definitions should be understood by personnel using the information and should be marked on summaries or reports disseminated outside the command.

Example: Combat Effectiveness Values

Threat unit combat effectiveness can be expressed as a color corresponding to the following example definitions. The following associated percentages are not indicators of T/O and table of equipment (T/E) strength, but are shown to indicate a relative range for each definition:

- *Green:* Combat Effective (80-100%)—The unit possesses the required resources to undertake the wartime mission for which it is organized or designed. Few, if any, negative factors exist. The unit does not require any compensation for deficiencies.
- *Amber:* Marginally Combat Effective (60-79%)—The unit possesses the required resources to undertake most of the wartime missions for which it is organized or designed. Some negative factors are present. The unit would require little, if any, compensation for deficiencies.
- *Red:* Limited Combat Effectiveness (40-59%)—The unit possesses the required resources to undertake some, but not all, of the wartime mission for which it is organized or designed. Significant negative factors are present. The unit would require significant compensation for deficiencies.
- *Black:* Combat Ineffective (less than 40%)—The unit is not prepared to undertake its wartime mission. Numerous debilitating negative factors are present.

Electronic OOB and Technical Data

Electronic OOB and other electronic technical data are required to plan and execute SIGINT, electronic warfare, CIS, C2W, and other operations against the threat. This data includes threat communications and noncommunications equipment parameters, modulation, multiplex capability, pulse duration, pulse repetition, frequency, bandwidth, associated weapons systems, and other technical characteristics of electronic emissions. The data also includes critical threat C2 nodes such as command posts, air defense operations centers, and communications relay sites.

With sufficient data, analysts can template threat emitters, which can be used to locate and develop the disposition of forces based on the forces' electronic emission assets. With electronic technical data, a more accurate evaluation of the threat's vulnerabilities to friendly EA and deception can be determined. Additionally, signals intercept and direction finding for SIGINT production are made easier and enhance support to electronic protection.

C2W Data

Analysis of C2W provides the commander with an assessment of the threat's ability to interfere with the friendly force's C2. The C2W data includes threat assets and capabilities to conduct electronic warfare, deception operations, psychological operations, and information warfare. Of increasing importance is the ability of any enemy to penetrate and disrupt friendly C2 and information systems or to deceive or jam friendly position locating devices (e.g., the global positioning system). This requires knowledge of a threat's deception capabilities, EA systems and protection measures, and monitoring capabilities.

Supporting Data

Analysts need supporting information to develop other OOB elements and comprehensive intelligence estimates. Basic intelligence describes the enemy and includes personalities' biographic data, unit history, uniforms and insignia, vehicle numbers, and other information important to mission accomplishment. Biographic data contains information on characteristics and attributes of a threat force's members. Knowledge of personalities is important in identifying units and, in some

cases, predicting a unit's COA. Personality data is valuable because the tactics and combat efficiency of particular units are closely tied to the commander's character, schooling, and personality traits. In MOOTW, supporting data may include tribal, clan, or ethnic group traits and their effects on the combat capabilities or limitations of the threat force.

Analytical Considerations

When assessing OOB factors, analysts should consider that—

- OOB factors must be analyzed as a whole.
- Changes in training status, command personality, strength, or any other OOB factors may affect a unit's tactics.
- The OOB factors form a framework for evaluation of any force.
- Extended family ties of suspected traffickers should be included when evaluating composition during a counternarcotics operation.
- The insurgent political structure and its relationship to the military elements should be included when evaluating an insurgent force.
- Composition analysis of a local terrorist organization would identify the support infrastructure among the local population.
- The OOB evaluation framework should be adapted to the mission and a unit's needs.
- An aviation unit's evaluation of composition would focus more on threat units that contain air defense assets; the equipment evaluation would focus on vulnerabilities of threat targets and technical characteristics of threat air defense systems.
- Properly maintained OOB files are sources of information on the threat's operations, capabilities, and weaknesses. See chapter 2 for a discussion of OOB files.

Threat Model Development

The threat model is a method of synthesizing information into a coherent evaluation of threat intentions and capabilities and predicting COAs. See chapter 5 for a discussion of doctrinal templates, description of preferred tactics and options, and identification of type HVTs.

Doctrinal Templates

When evaluating doctrinal templates, analysts must—

- Determine how the threat normally organizes for combat and how he/she deploys and employs his/her maneuver units and various supporting assets.
- Look for patterns in task organization of forces, timing, distances, relative locations, groupings, or use of terrain and weather.

Doctrinal templates can also portray the threat's normal organization for combat, typical supporting elements available from higher commands, frontages, depths, boundaries, engagement areas, objective depths, and other control measures. The amount of this detail available will vary from situation to situation or may not exist at all. In the latter case, the analyst will need to rely on basic principles of war and tactics to develop an initial doctrinal template. Doctrinal templates are tailored to the needs of the unit creating them.

Description of Tactics and Options

Like the template, the description of the threat's tactics and options is developed from an evaluation of his/her doctrine and previous and current operations. Analysts include a description of the branches and sequels available to or preferred by the threat should the depicted operation succeed or fail. For example, the threat might prefer to follow successful attacks with pursuit. Should an attack begin to fail, his/her preferred branches might

include committing reserves, reinforcement, or shifting the main effort. Should the attack fail, his/her preferred sequel might be a hasty defense.

Analysts include decision criteria revealed in the data base that cause the threat to prefer one option over another. This intelligence will aid in wargaming threat and friendly COAs, targeting, and deception planning. When developing a threat model, analysts use the following techniques to describe tactics and options:

- Start with the scheme of maneuver and examine how each battlespace function provides support.
- Use time-event charts to describe how the threat normally conducts operations. These are particularly useful for describing large-scale air operations, which are difficult to depict graphically. With a time-event chart the time relationship between various echelons and their normal composition can be described easily.
- Make marginal notations on the graphic template and combine words with pictures to enhance understanding. Marginal notes are particularly effective when tagged to key events or positions on the template.
- Use a battlespace or warfighting function synchronization matrix (see fig. 7-1) to dissect threat operations and relate particular actions to time for threats with well-developed tactics and complex combined-arms organizations.

Time	H-10	H-1	H	H+4	H+7	H+8.5	H+10
Friendly Action	Begin move to attack position	Prepare fires	Cross line of departure	Engage 1st echelon	Defeat 1st echelon		
Enemy Decision Point							
Enemy Maneuver				Local counterattack	Close air support and attack helicopters to counterattack objective	Reserves begin move	Reserves pass NAI 9
Enemy Fire Support		Counterbattery	Engage HPTs	Defensive fires	Countermobility fires	Support reserve in engagement areas 7, 8, and 9	
Enemy Intelligence	Locate main effort	Locate artillery, identify main effort	Locate reserve, HPTs				
Enemy C2					Commit reserve to counterattack option 1 or block options 2 and 3		
Enemy Engineers	Continue countermobility in main battle area						

Figure 7-1. Threat Synchronization Matrix.

Identification of Type High-Value Targets

Analysts use the following techniques to identify type (e.g., air defense, engineer) HVTs for the threat model:

- Use tactical judgment when evaluating the data base, the doctrinal template, and its supporting narrative to identify HVTs.
- Mentally war game the threat operation under consideration to determine how the threat will use battlespace assets and to identify those assets critical to the operation's success.
- Identify assets necessary to satisfy decision criteria or initial adoption of the branches and sequels listed in the description and option statements.
- Determine the threat's reaction to the loss of each identified HVT. Consider his/her ability to substitute other assets and to adopt branches to the operation.
- Rank the set of HVTs in order of their relative value to the threat's operation, record sets as part of the threat model, and note value changes by phase of operation.
- Use a target value matrix to annotate identified HVTs in the margins of the doctrinal template. Figure 7-2 is a threat model depicting a doctrinal template, tactics and options description, and target value matrix.

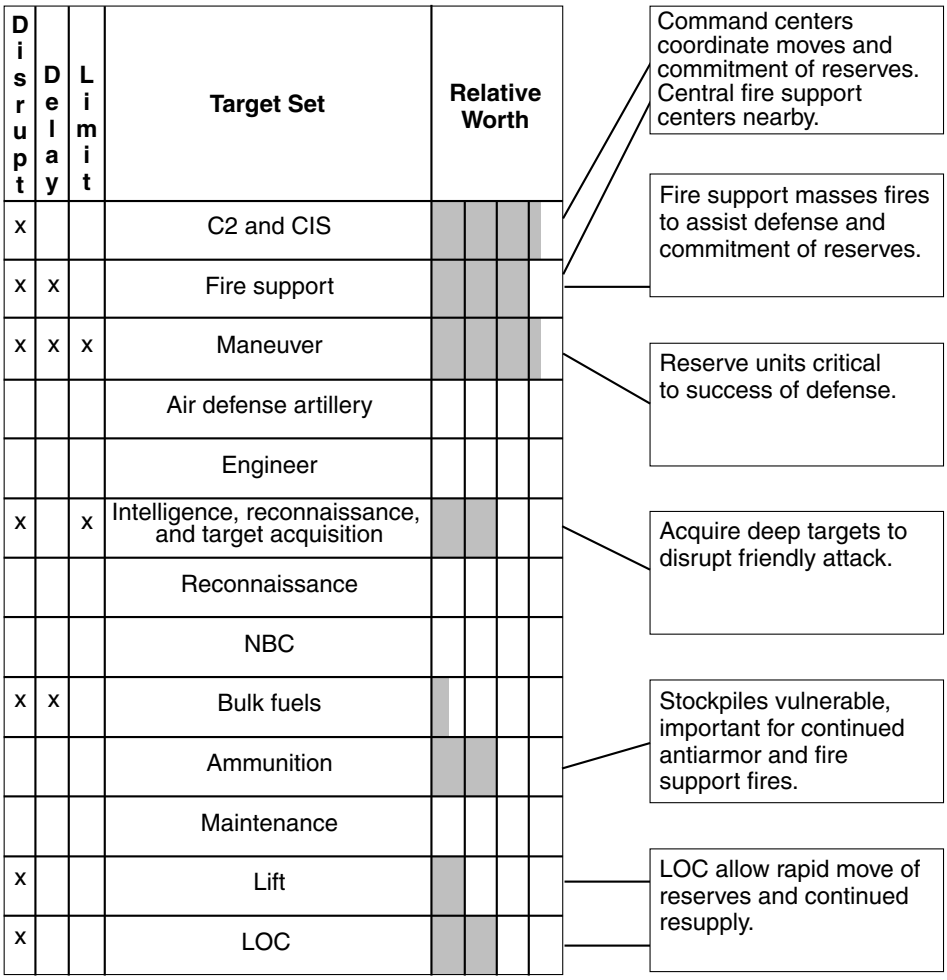


Figure 7-2. Threat Model with Target Value Matrix.

Threat Courses of Action Determination

To determine threat COAs, analysts start with general COAs open to the threat, such as deliberate attack, defend, and delay. They further define each general COA as a set of specific COAs by integrating the threat models developed in IPB process step 3 with the description of the battlespace effects from IPB process step 2.

Criteria for Testing Threat Courses of Action

Analysts must test each enemy COA using the criteria of suitability, feasibility, acceptability, uniqueness, and consistency with doctrine.

Suitability

When determining the suitability of a threat COA, analysts must evaluate the COA's potential for accomplishing the threat's objective.

Feasibility

Analysts evaluating the feasibility of a threat COA must answer the following questions:

- Are the time and space required to execute the COA available?
- Does the threat have the physical means required to make the COA a success?
- What radical measures can he/she take to create the conditions for success?

Acceptability

In determining the acceptability of a threat COA, analysts must consider the amount of risk involved by answering the following questions:

- Will threat forces accept the amount of risk entailed in adopting the COA?
- Can they afford the expenditure of resources for an uncertain chance at success? (This is a subjective judgment based on knowledge of the threat and his/her doctrine. In some instances, the threat might undertake otherwise unfavorable COAs, particularly if they are the only means to accomplishing his/her objective.)

Uniqueness

To determine the uniqueness of each threat COA, analysts must use their experience and training to answer the following questions:

- How will the COA affect the friendly mission?
- Will the threat use reserves or a second echelon?
- Where is the threat's main effort?
- What is the threat's scheme of maneuver?
- How is the threat task-organized?

Consistency with Doctrine and Recent Activities

When evaluating a threat COA's consistency with doctrine and recent activities, analysts must answer the following questions to be consistent with the threat's doctrine and recently observed activities, practices, and patterns.

- Is the COA consistent with the threat's written doctrine and past application of doctrine observation, as revealed in the intelligence data base?
- Will the threat achieve surprise by deviating from its known doctrine?

Considerations

To determine the COAs the threat believes are available, analysts should—

- Consider the effect of friendly dispositions or the threat's perception of friendly dispositions on the threat's COA.
- Conduct reverse IPB or replicate the process the threat is employing to discern friendly COAs.
- Consider the intelligence and reconnaissance assets available to the threat, their ability to collect information and produce intelligence, and the picture that intelligence will give threat commanders.

- Focus on threat COAs that will affect accomplishment of the friendly mission and include those indications that the threat might adopt a COA that favors accomplishment of the friendly mission. This prepares the commander to take advantage of opportunities that might arise.

> **Example: Threat COA That Favors Friendly Mission Accomplishmentp**
>
> If the friendly mission is to attack to destroy the threat, interfering threat COAs could be defend (including counterattacks), reinforce, and withdraw. If the friendly mission is to seize a terrain objective, interfering threat COAs could be defend (including counterattacks) and reinforce. Threat withdrawal would favor the accomplishment of this friendly mission and should also be included in the set of COAs if there are indications the threat might actually withdraw.

- Identify less likely but viable threat COAs by considering the threat's—
  - Superior understanding of the political, cultural, or information characteristics of the battlespace.
  - Ignorance of the military arts and sciences.
  - Immature decisionmaking.
  - Uncertainty as to friendly dispositions or intent.
  - Unexpected objectives or desired end states.
  - Cultural definitions of defeat and victory.
  - Willingness to sustain defeat at the tactical or operational level to achieve victory at the strategic or political level.
  - Desperation.
  - Bureaucratic inefficiency.
  - Audacity.

Course of Action Evaluation and Prioritization

The resulting set of COAs developed should depict the full set of options available to the threat. At this point the analyst should remember that the threat COAs identified are assumptions about the threat, not facts. For this reason, the analyst cannot predict with complete accuracy which of the COAs the threat will employ. However, the commander and staff still need to develop a plan that is optimized to one of the COAs, while allowing for contingency options if the threat chooses another COA. Therefore, the analyst must evaluate, analyze, and form an estimate for each COA and prioritize it according to how likely it is that the threat will adopt that option. The analysts must establish an initial priority list to allow the staff to plan for friendly COAs. Once the commander selects a friendly COA, the analyst may need to reorder the list of threat COAs and consider changes in the threat's perception of friendly forces.

Course of Action Development

Once the complete set of threat COAs has been identified, analysts develop each COA into as much detail as the situation requires and time allows. Analysts base the order in which each COA is developed on its probability of adoption and the commander's guidance. Each COA must answer the following five questions:

- **What**—The type of operation (e.g., attack, defend, reinforce, conduct retrograde).
- **When**—The time the action will begin is usually stated in terms of the earliest time that

the threat can adopt the COA under consideration.

- **Where**—The sectors, zones, axis of attack, AAs, and objectives that make up the COA.
- **How**—The method by which the threat will employ his/her assets (e.g., dispositions, location of main effort, the scheme of maneuver, and support required).
- **Why**—The objective or end state the threat intends to accomplish.

Course of Action Parts

Analysts consider threat forces available to at least one level of command above their own command when developing each COA. This helps to ensure accountability for possible reinforcing forces and the higher command's own objectives and intent. Each developed threat COA should contain a—

- Situation template.
- Description of the COA and options.
- Listing of HVTs.

Considerations

When considering an attacking threat, less detail is required. For example, depending on the situation, a friendly battalion might need only to work to a level of detail of threat companies. Considering the possible variations in the threat's COA based on the details of employment of individual platoons adds a tremendous amount of effort to the process, perhaps for little gain.

When considering a defending threat, a greater level of detail generally is required. For example, an attacking friendly battalion might be concerned with individual crew-served weapons positions given their relative contribution to the threat's defense.

Operations other than war will generally require a greater level of detail. The situation template may address such things as locations and movements of potential evacuees, displaced persons, or protesters as well as threats such as individual air defense systems and irregular forces. Analysts must focus on what is essential to accomplishing the friendly mission.

Course of Action Key Elements

The key elements of each COA are indicators, NAIs, and HVTs. These key elements will drive the collection and production efforts to determine which COA the threat will actually adopt. The art of identifying initial ICRs and IPRs revolves around—

- Predicting specific areas and activities which, when observed, will reveal the COA the threat has chosen.
- Determining the type intelligence products, formats, and who needs them.

As a threat force is visualized executing a COA during situation templating, analysts identify places where activity must occur if that COA is adopted. The NAIs facilitate intelligence collection, reconnaissance and surveillance, and analysis because—

- Attention is focused on areas where the enemy force must appear if the enemy has selected a particular mobility corridor or AA.
- Military significant events can be framed by time and location within the NAI.
- Events in one NAI can be compared to events occurring in the NAI of other mobility corridors as the basis for determining enemy intentions.
- Events within NAIs can be analyzed for indicators and HVTs against which intelligence and target acquisition resources can be directed.

SECTION II. SPECIALIZED ANALYTICAL TECHNIQUES

While IPB provides the overall framework and techniques for analyzing the threat, situations may dictate the use of more specialized techniques to enhance the overall product. Discussed below are a few of the more common techniques used by intelligence analysts.

Subsystem Threat Analysis

Subsystem analysis plays a major role in determining the overall posture of a threat force. Most of the products prepared during the IPB process will only partially satisfy the requirements of other staff sections and subordinate units. The targeting process may require focus on a particular aspect of the threat force. The intelligence analyst must be aware of the important threat analysis factors that specialized staff sections and units use in their IPB responsibilities. Intelligence analysts serve as the focal point for supplying information and data on a specific subsystem to other staff sections and units. Intelligence personnel assigned to specialized units discussed below will tailor their IPB efforts to the needs of their unit.

Air Defense

Evaluation

When air defense units and staffs evaluate the threat, they focus on threats posed by UAVs, cruise and ballistic missiles, fixed- and rotary-wing aircraft, and airborne and air assault forces. In addition to the broad range of OOB factors and threat capabilities, air defense staffs and units must evaluate—

- Flight operations tactics.
- Ordnance types and availability.
- Ordnance delivery techniques (e.g., standoff ranges, release speeds and altitudes, guidance systems).
- Technical capabilities of aircraft (e.g., all-weather or night, maximum and minimum speeds, ceilings, range, payloads, aerial refueling).
- Target selection priorities for air strikes or attack by air assaults.
- Air strike allocation procedures.
- C2 and supporting CIS procedures and techniques.
- Navigation capabilities.
- Threats to friendly air defense artillery (ADA) assets, including threat ground forces and electronic warfare assets.

COA Determination

The threat's air activities will be a part of his/her overall operation. Intelligence personnel begin determining the threat's air COAs by acquiring the supported command's basic IPB products, to include situation templates. Analysts evaluate the general COAs that situation templates portray and determine how the threat might support COAs with air power. When determining air COAs, analysts must consider the maneuver forces the COAs support. The employment flexibility of modern aircraft makes the determination of specific threat COAs extremely difficult. When determining the threat's air COAs, analysts should answer the following questions:

- Where will the threat locate FARPs?
- When will the threat's air strikes or air assault operations occur?
- What are the threat's targets and objectives?
- What are the threat's likely air corridors and air AAs?
- What are the threat's strike package composition, flight profiles, and spacing in time and space, including altitudes?

- Where do friendly air defense assets fit into the threat COA?
- Will the threat ground COAs require movement of friendly ADA assets?

Artillery

Evaluation

When evaluating the threat, the artillery unit personnel or staff should—

- Refine standard threat models to focus on HVTs.
- Evaluate the threat's ability to fight the counterfire battle by—
  - Identifying the threat's target acquisition assets and describing their normal deployment patterns and tactics.
  - Describing the accuracy and timeliness of each threat target acquisition system.
  - Identifying CIS that moves target acquisition information to decision-makers or weapons systems, and describing the system in terms of efficiency and timeliness.
- Describe the threat's ability to locate and destroy friendly target acquisition assets.
- Use techniques associated with the rear battle to evaluate rear area threat to artillery units.

COA Determination

When determining threat COAs, analysts—

- Refine the threat COA models to reflect—
  - HVTs.
  - Dispositions and activity of threat fire support.
  - Dispositions of threat target acquisition assets.
  - Rear area threats to friendly units.
- Focus on COAs that primarily deal with counterfire against friendly assets, other aspects of force protection, and threat activities that will require friendly units to displace.

Aviation

Evaluation

When evaluating the threat, aviation unit personnel identify—

- Units supported by ADA assets.
- Types of ADA systems and their capabilities, such as—
  - Ranges.
  - Altitudes.
  - Engagement times.
  - Fusing systems.
  - Radars.
  - Countermeasures.
  - Range capabilities.
  - Altitude restrictions.
- Other threats such as lasers or artillery fire zones.
- Artificial illumination effects on target acquisition and night vision devices.
- Target characteristics, such as—
  - Normal deployment patterns.
  - Capability to detect attacking aircraft.
  - Typical reactions.
  - HVTs within each formation.

COA Determination

When refining the higher command's threat COA model, analysts—

- Include air defense system range fans.
- Determine where radars and weapons systems are masked by terrain.
- Identify areas with the least amount of air defense coverage.
- Identify likely threat air approaches to friendly engagement areas and battle positions.
- Develop situation templates for threat actions within the engagement area and include reactions to aviation attack.

- Identify threat units along flight paths, consider threat units' reactions, and develop appropriate situation templates.
- Consider threat reactions to downed pilots.

Counterintelligence

Evaluation

When assessing the threat, counterintelligence personnel—

- Describe the threat decisionmaking process and include descriptions of the threat's—
  - IPB process.
  - Command estimate and wargaming methods.
  - Techniques for selecting intelligence requirements.
  - Collection planning and collection management.
  - Asset reporting system.
  - Intelligence processing architecture.
  - Dissemination procedures.
- Estimate the standard lengths of the threat decision cycle for both anticipated and unanticipated decisions by answering the following questions:
  - How long does it take the threat staff to plan and execute a new mission?
  - How long does it take the threat staff to plan and execute changes to the current mission?
  - What is the length of time between acquisition of key indicators by collection assets and execution of that decision?
- Identify the collection systems available to each threat unit, develop doctrinal templates and descriptions for the standard employment of these systems, and rank each collection system in relative order of importance to standard threat operations.

COA Determination

When formulating threat COAs, the analyst should—

- Determine threat intelligence requirements by using the basic maneuver COA model and by answering the following questions:
  - What does the threat need to know to make operations successful?
  - Where are the decision points?
  - When does the threat need to know?
- Estimate the threat's intelligence requirements and attempt to recreate his/her version of the event template, matrix (NAIs and indicators), and collection plan.
- Develop products that show the employment of each collection system and the ensuing coverage by—
  - Depicting range fans for each system.
  - Describing the type of activity that can be collected within each range fan.
  - Highlighting the strengths and weaknesses of the threat collection plan.
- Develop a friendly event template to support counterintelligence and counterreconnaissance.
- Identify locations (NAIs) and activities (indicators) that confirm or deny key elements of the threat collection assumptions.

Command and Control Warfare

Threat analysis in support of C2W can be divided into areas of threat capabilities to conduct C2W and threat vulnerabilities to C2W.

Evaluation of Capabilities

When evaluating threat C2W capabilities, the analyst should consider the threat's—

- Ability to locate and intercept our C2 centers and agencies and supporting CIS.
- Targeting speed and accuracies of threat intelligence collection systems and capabilities of its production elements.

- EA equipment and techniques effectiveness, to include capabilities against space-based systems and computer networks.
- Ability to link collection systems to indirect fire systems.
- Range capabilities of supporting indirect fire systems.
- Ability to conduct deep strikes or special operation forces operations.
- Deception doctrine, tactics, techniques, procedures, and effectiveness.
- Psychological operation capabilities and effectiveness.
- Deployment patterns and tactics of SIGINT collection systems and EA assets, as depicted on the threat model.
- Deployment patterns, tactics, and range capabilities of long-range indirect fire systems, as depicted on the threat model.
- Techniques of intrusion or electronic deception, as depicted on the threat model.

Evaluation of Vulnerabilities

When evaluating threat vulnerabilities to C2W, analysts consider the threat's—

- C2 structure and CIS, with emphasis on locating key C2 nodes.
- Decisionmaking process and speed.
- Command personalities.
- Intelligence, reconnaissance, and target acquisition assets and their vulnerability to jamming or deception.
- Communications security procedures and their ability to work through or around EA.
- Counterintelligence effectiveness.
- Operations security procedures and effectiveness.
- Effectiveness of electronic protective measures and computer network protection.
- Susceptibility to psychological operations and ability to conduct counterpsychological operations.

COA Determination

When developing threat COAs, analysts consider threat C2W capabilities and how those capabilities will be used to support specific operations. The threat command, control, and communications posture and associated vulnerabilities are considered during the identification of COGs and HVTs and contribute to development of HPTs and targeting strategies.

Engineer

Evaluation

Analysts conducting threat analysis in support of engineer planning should evaluate the threat's—

- Engineer units' organization, standard operations, equipment, and employed tactics for conducting mobility, countermobility, survivability, obstacle placement, and breaching operations.
- Engineering capabilities required to lay each type of obstacle system, to breach obstacles, to entrench a type unit, and to bridge different size rivers and streams.
- Logistical system ability to sustain engineer operations.
- Weapons capabilities to penetrate friendly survivability measures and systems.
- Survivability techniques (e.g., use of chain-link fence to defeat antitank rounds and missiles).
- Engineer capabilities of threat infantry, armor, and other nonengineer units.

COA Determination

When determining threat COAs, analysts should include engineering factors in threat models and templates. To develop situation templates for engineers, analysts use the maneuver situation

template of the supported unit and develop multiple threat engineer COAs that include—

- An engineer status estimate, which includes the percentage of combat vehicles with entrenched primary, alternate, supplementary, and deception positions and the extent of likely obstacle system measures.
- Likely locations and obstacle systems required to support, disrupt, turn, fix, or block defensive measures.
- A mobility support estimate, which includes the maneuver and supporting engineer detachments' breaching and fording capabilities.

Combat Service Support

Evaluation

When conducting threat analysis in support of CSS staffs and units, analysts should include—

- Regular threat formations, particularly reserves or second echelon units, that might penetrate main defenses or conduct counterattacks through CSS areas.
- Details on air assault, airborne, unconventional warfare, and light infantry forces and their means of infiltration (e.g., air, ground, and sea).
- Insurgent and partisan forces.
- Terrorist organizations.
- Criminal organizations.

COA Determination

When preparing threat models in support of CSS units, analysts include—

- Air assault, airborne, and light infantry techniques for deep attack.
- Unconventional warfare techniques for deep operations.
- Standard procedures for insurgent raids and ambushes.
- Typical procedures for terrorist attacks.
- Targets and methods of operations for criminal organizations.

COA Development

When evaluating threat COAs, the analyst should consider each maneuver COA available to the threat and develop multiple CSS COAs that include—

- Likely areas of penetration for ground forces.
- Likely objectives in the rear area that will facilitate the threat's main attack or defense.
- The HVTs and HPTs (e.g., key terrain, specified CSS activities) that the threat will identify to support their concepts of operations.
- Situation templates for air assault and airborne operations (e.g., air avenues to LZs and DZs, infiltration lanes, exfiltration lanes).
- Insurgent or partisan activities (e.g., assembly and hide areas, infiltration routes, objective actions, exfiltration).
- Terrorist and sabotage activities.

Pattern Analysis

Pattern analysis is the process of careful observation and evaluation of threat activities to deduce the doctrinal principals and techniques, tactics, and procedures that threat forces or groups prefer to employ. When faced by an opponent whose doctrine is unknown or undeveloped, the intelligence analyst must use pattern analysis to create or update threat models and doctrinal templates. This form of analysis is used in operations other than war, such as counterinsurgency, peacekeeping, or even humanitarian assistance operations. The coordinates register and pattern analysis plot sheet are used to develop threat models when it is necessary to determine threat operational patterns.

Coordinates Register

Sometimes referred to as an incident map, a coordinates register illustrates cumulative events that have occurred within the AO (see fig. 7-3). Coordinates registers focus on where an event occurred, but it can contain additional information as the situation dictates. The date and time of the incident are recorded next to the location. As reports of individual events or sightings are recorded, the analyst attempts to identify links between the location and time of those events. What may appear to be random events will often develop into coordinated actions. When time lined and illustrated, these events form patterns that provide the basis for developing threat models and doctrinal templates. Although the time of the event is normally recorded on the coordinates register, it should always be used with the pattern analysis plot sheet and the doctrinal template, if developed.

Pattern Analysis Plot Sheet

The pattern analysis plot sheet focuses on the time and date each incident occurs in the AO. In figure 7-4, the rings depict the days of the month and the radial segments depict the hours of the day. Events are recorded using the same alphanumeric designator as was used on the coordinates register to allow easy cross-referencing. Along the right side of the plot sheet, the events are recorded by the day and date they occurred. By organizing the events in this manner, it is possible to identify the times of the day and days of the

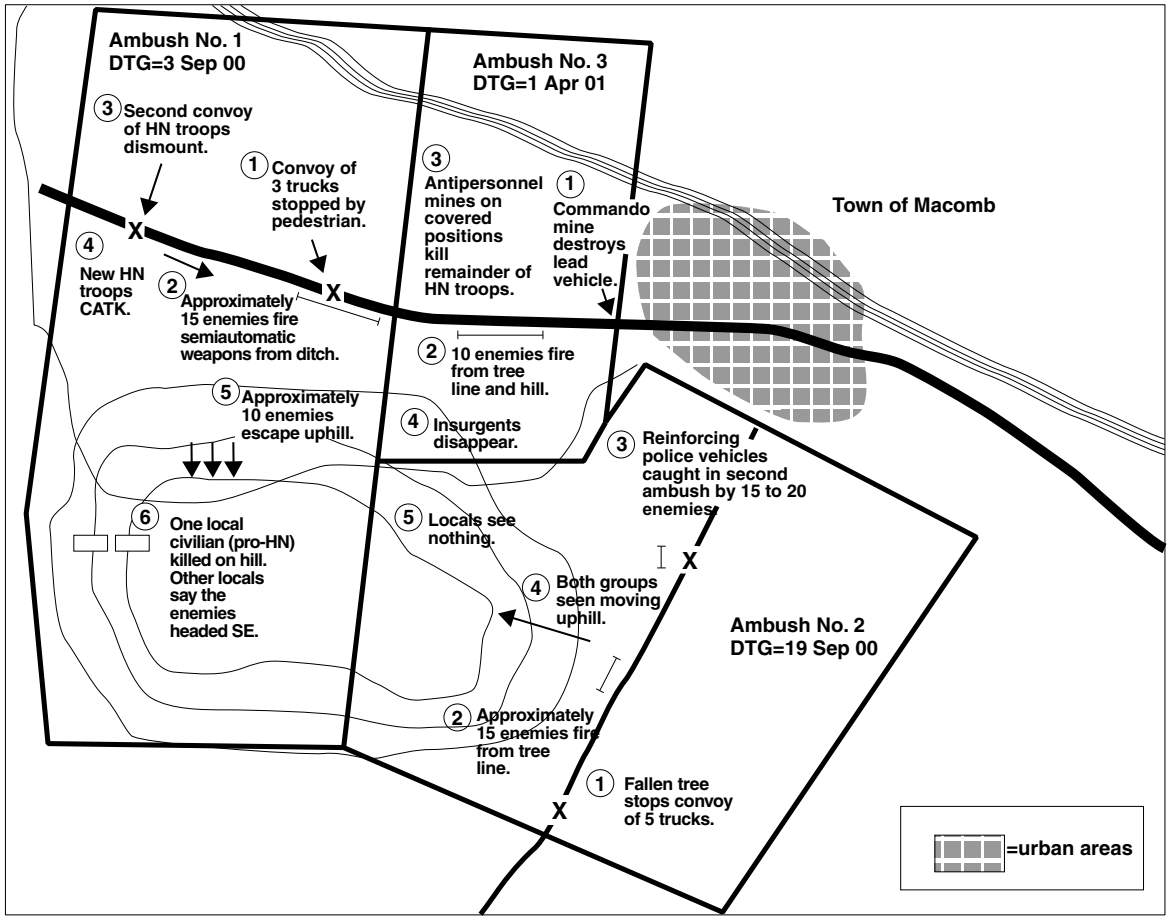


Figure 7-3. Coordinates Register.

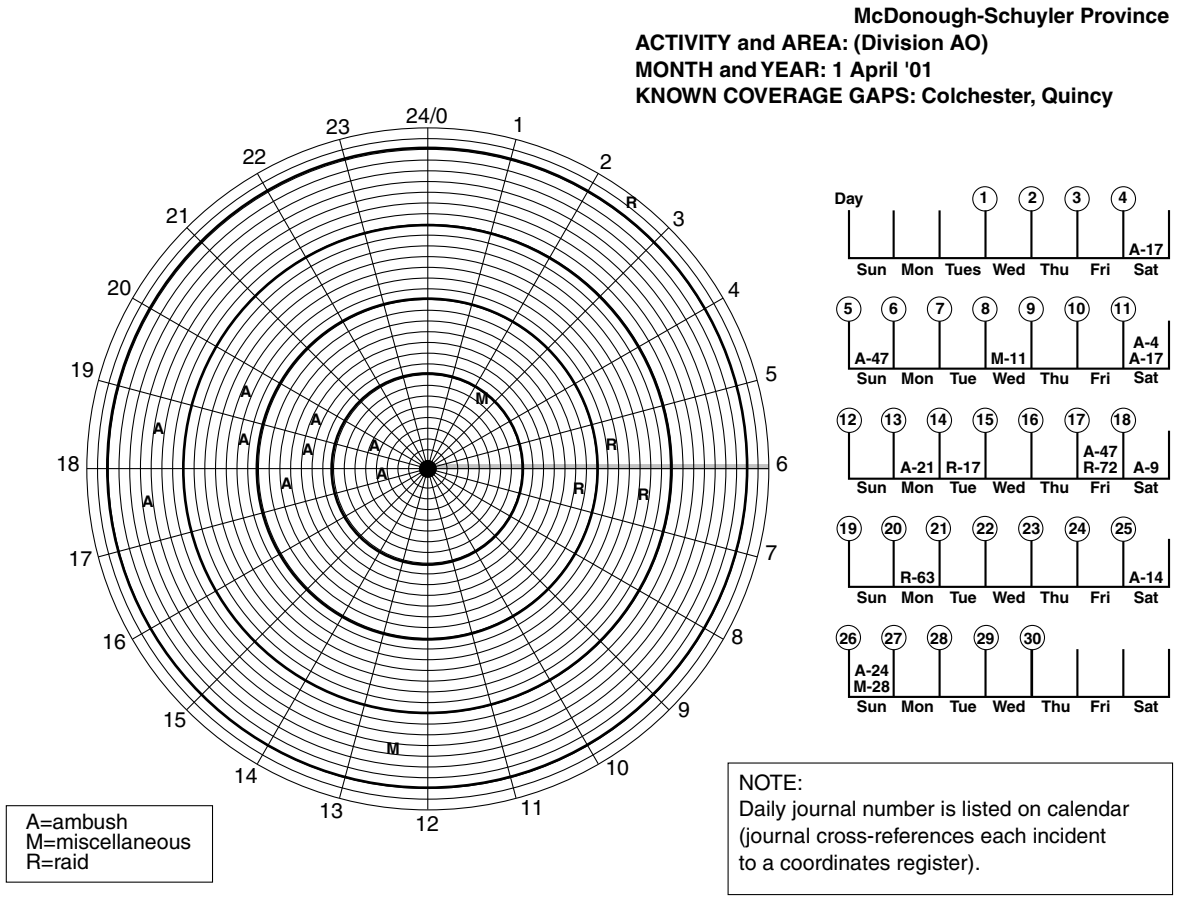


Figure 7-4. Pattern Analysis Plot Sheet.

week or month when threat activities occur. Used in conjunction with the coordinates register, the pattern analysis plot sheet identifies where, when, and how past actions occurred. This allows the analyst to use information derived from the coordinates register and pattern analysis plot sheet, to develop threat models and doctrinal templates, and to predict potential threat activity.

Matrix Analysis

Constructing a matrix is a simple, graphical way to organize a large volume of complex data. Matrices are used to show relationships between numbers of entities, such as people, incidents, organizations, weapons, locations, functions, and actions. Analysts use activities and association matrices to organize a large volume of complex data, particularly in cases where the tracking of individuals and organizations is emphasized. Activities and association matrices are useful in analyzing insurgent, terrorist, criminal or drug trafficking activity.

Activities Matrix

Analysts use the activities matrix to link people to events or organizations. An activities matrix quickly displays which notable personnel within the AO are related to a particular organization or type of activity. This matrix can also link certain activities or incidents within the AO with organizations or units.

In figure 7-5, individuals are listed down one side, with organizations listed across the top. Reported relationships are noted on an individual's row that intersects the appropriate organization's column. This example demonstrates the use of dots to signify the confirmed, possible, or probable certainty of the relationship. The absence of a dot indicates either no relationship or a lack of information. The system used must be explained in a legend. To complete this particular example, the analyst created a remarks column to record significant information regarding each individual.

● – confirmed ◌ – probable
○ – possible

Remarks		Christian Reform Party (good people)	Society for the Preservation of Order (SPO) (right wingers)	Farmer's Alliance (unknown peasant group)	People's Democratic Society (peaceful moderate)	Insurgent Company	New Liberation Movement (political front for New Metropolitan Edict [NME])	NME	Name of Individual	
Warrant Outstanding	Leader in the insurgent company. Possible platoon commander or company commander.					●	●	●	Johnston, S. D. alias "The Red"	Bandolph
	Possibly linked to death squad activities.	●	◌						Garra, N. A.	
	Mayor, ineffective due to war-torn town.	●							Mulvhill, P.	
	Possible platoon leader.	○		●	◌	○	○		Daniels, P.	
	Regional governor.	◌	○	◌	●				Jenkins, T. L.	Malcolm
Warrant Outstanding	Tactical genius, principal trainer of insurgent company.					●	●	◌	Corrnier, J.	
				○		◌	◌	◌	Webb, C.	
					◌	○	○		Seipel, B.	
	Leader in the insurgent company. Platoon leader or executive officer.			○		◌	◌	◌	Trollinger, L.	Beards town
	Possible head of intelligence.					○	●	●	Ahearn, E.	
	Probable platoon leader.					◌	○		Timoney, J.	
Warrant						●	●		Thompson, J.	
Warrant	Probable heavy weapons platoon leader.					●	○	●	Bridgeford, R.	
	Possible liaison between insurgent company and the NME			◌	○	○		○	Halbleib, M.	Bushnell
	"Doctor of Death" leads the SPO.	●	●	○	○				Mueller, H.	
Warrant						●	◌	◌	Martinez, E.	

Figure 7-5. Activities Matrix.

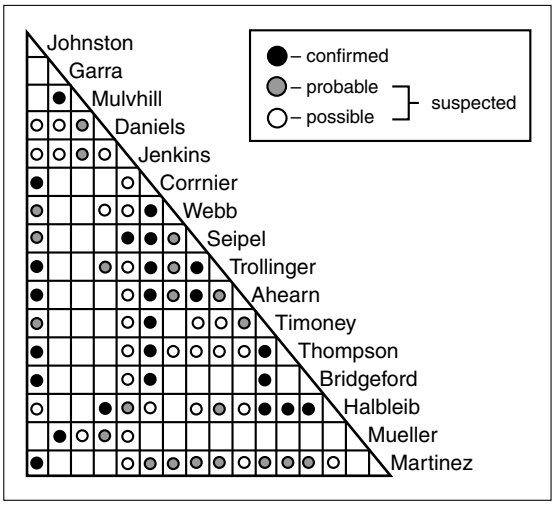


Figure 7-6. Association Matrix.

Association Matrix

The association matrix is used to show relationships between individuals. In figure 7-6, the individual names constitute both a column and a row. A dot indicates that a relationship exists. Through the use of the activities matrix, analysts note individuals that are members of the same organization and indicate the relationship on the association matrix.

Link Analysis

Link analysis is a method of evaluating and displaying relationships and activities information that has been organized into matrices. In link analysis, pictures or symbols are used to display intelligence data that depicts relationships between people or entities. Analysts assess the reliability and validity of the intelligence data and assemble a link diagram to gain greater insight into the construction of a relationship network.

In figure 7-7, the link analysis diagram uses circles to represent people, squares or rectangles to represent organizations, and lines to represent their connections. Solid lines represent confirmed or strong relationships, while dashed lines indicate suspected or weak relationships. When

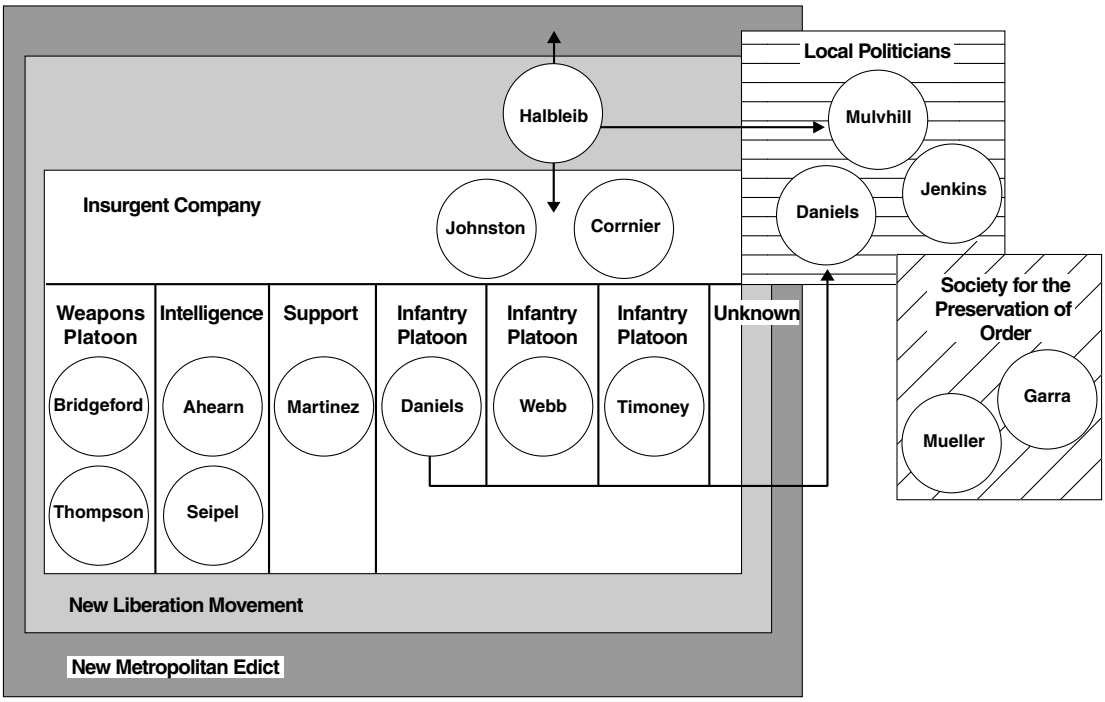


Figure 7-7. Link Diagram.

the analyst suspects that two people are actually the same person, the circles are overlapped. Circles and lines should be arranged so that their relationship lines do not cross. In complex cases, such as large groups, the circles should be arranged to keep the number of relationship-line intersections to a minimum.

The relationship of an individual to an organization can be shown a number of ways. When an individual is confirmed to belong to an organization, that individual's circle is placed within the organization's rectangle. By overlapping organizations, the analyst shows that an individual belongs to more than one organization and that there is a connection between the two organizations.

In cases where an individual is connected to but not a member of an organization, a line is drawn from the individual outside the organization to the rectangle representing the organization. If an individual's contact within the organization has been confirmed, the relationship line would be drawn between the circles representing the individuals.

Indicator List

The activities that reveal a COA are called indicators. Indicators are essential to discerning threat intentions. The analyst uses indicators to cross-reference specific events and activities with probable threat COAs and intentions. When used with other analytical tools (e.g., threat models, event templates, pattern analysis, matrices, and link diagrams), indicators are the key to estimative intelligence. During IPB, indicators are developed for each NAI to focus collection and analysis efforts. This list of indicators is constructed to satisfy the commander and staff's PIRs and IRs.

Indicator lists are formed by asking questions. Intelligence analysts develop a list of threat indicators by focusing on METT-T questions. Using METT-T, analysts determine what the threat must do and define the threat's probable activities (see the example below). These determinations become indications and warning.

Example: Forming an Indicator List Using METT-T

PIR: Will the threat defend objective C using a reverse-slope defense between 230600 to 270800 hours?

Mission: What does the threat commander accomplish by forming a reverse-slope defense?

Enemy: What types of units are available to conduct the defense? What units are necessary to construct and aid in the defense?

Troops and Support: Are threat troops experienced in reverse-slope techniques? What is their SOP for reverse-slope defense?

Terrain and Weather: Is objective C suitable terrain for a reverse-slope defense? If so, where is the most suitable terrain?

Time Available: How long will it take to develop a prepared defense versus a hasty defense? Will threat forces be able to prepare or assume a defense in the specified time period?

To further develop the indicator list, analysts can refine the questions developed using METT-T by breaking them down by battlespace functions. Information based on IPB, OOB factors, and experience aids intelligence analysts in deriving lists of activities that answer the commander's PIRs. These questions serve to narrow and focus on certain activities, equipment, troops, and training which an adversary must possess or do to accomplish their mission. For a representative listing of common tactical level indicators, see appendix C.

CHAPTER 8. TARGET DEVELOPMENT AND COMBAT ASSESSMENT

Successful MAGTF operations depend on an efficient, organized targeting effort to affect those enemy capabilities that could interfere with achievement of the friendly mission and objectives. The targeting process of detecting, selecting, and prioritizing targets requires coordinated interaction between intelligence, maneuver, fires, and planning elements of the MAGTF, joint force commander (JFC), Service components, and supporting agencies. This chapter introduces the targeting cycle, intelligence targeting support, the analyst's role in target development, and combat assessment.

SECTION I. TARGETING

Based on the friendly scheme of maneuver and tactical plans, targeting includes an assessment of the weather, terrain, and enemy to identify those enemy formations, equipment, facilities, and terrain which when attacked or controlled will ensure success. Through the targeting process, analysts develop a prioritized list of targets to be attacked and determine the weapons required to achieve the desired effects.

Targeting Cycle

Defined as deliberate or reactive, targeting is an integral part of the planning process that begins with receipt of the mission and continues through the development of the approved plan. Deliberate targeting is associated with fixed or semi-fixed targets, while reactive targeting is associated with mobile targets. Whether deliberate or reactive, the targeting cycle integrates intelligence, maneuver, fires, and C2 processes to assist the commander in deciding which targets to engage when, where, and to what effect.

Through the targeting cycle, fires planners and targeteers derive nomination lists of forces, installations, or locations that if attacked will promote the commander's warfighting objectives. The higher the command level performing the targeting process, the more formal it becomes and the more the process focuses on events well in the future. At the MAGTF or joint force level, the targeting cycle tends to be deliberate, encompasses greater resources, and involves—

- Establishment of commander's objectives, guidance, and intent.
- Target development, nomination, validation, and prioritization.
- Capabilities analysis.
- Commander's decision and force assignment.
- Mission planning execution.
- Combat assessment.

At lower tactical levels, the same process tends to be reactive, occurs in a shorter time span with less formality, and focuses on events of an immediate nature. The tactical-level targeting cycle is simplified to decide, detect, deliver, and assess

(D3A). Figure 8-1 depicts the joint targeting cycle and its relationship to D3A. Although intelligence is an integral part of each targeting cycle phase, intelligence P&A directly affects target development (decide) and effects assessment (assess).

Target Development

Target development is the analysis of potential enemy military, political, or economic systems to determine their significance and relevance to the commander's objectives, guidance, and intent. The analysis proceeds from broad systems to specific components and finally to individual elements or aim points. Analysts evaluate system components and interrelationships to establish their criticality to the threat's operation and their vulnerability to attack. Through this systematic evaluation, analysts develop targeting strategies to select potential targets and to determine the type of damage that will accomplish the friendly commander's defined objective. Objective definition and target development must comply with the commander's guidance, law of armed conflict, and rules of engagement.

Analysts evaluate each target's lethal and nonlethal capabilities to develop a prioritized list of targets and the intelligence requirements that support target acquisition and combat assessment. The scope, level of detail, and time involved depend on the situation and the level of command conducting targeting. Common processes and procedures employed in target development include IPB, target value analysis, HPT identification, and use of the high-payoff target list (HPTL).

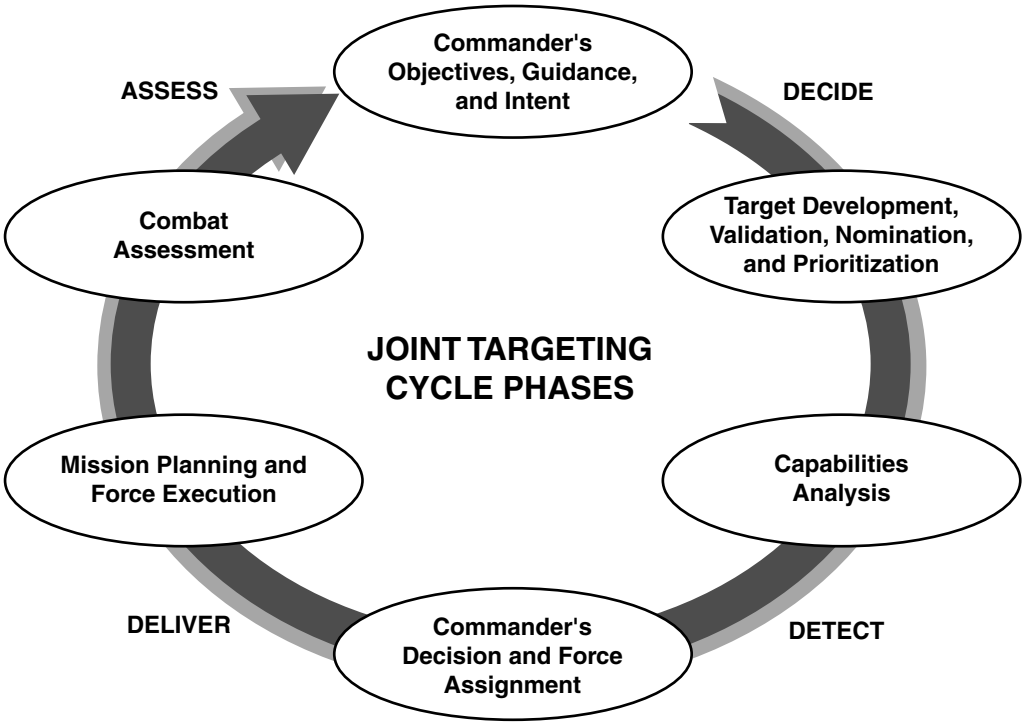


Figure 8-1. Joint Targeting Cycle and D3A.

Intelligence Preparation of the Battlespace

Through the IPB process, intelligence analysts contribute to target development by—

- Determining the threat commander's COAs through systematic analysis of the region, weather, terrain, and doctrine.
- Evaluating doctrinal templates to identify a threat's COGs, critical vulnerabilities, and HVTs.
- Constructing situation templates and examining the threat commander's decision cycle and each potential COA's decision points to refine HVTs.
- Wargaming, mentally, each COA and the threat commander's decisions to identify his/her key assets as HVTs.
- Developing event and decision support templates to help identify NAIs, decision points, decision phase lines, TAIs, and HPTs.
- Analyzing the threat's target systems, complexes, and components to develop their relevance and importance.

Target Value Analysis

Target value analysis is a method of identifying and ranking potential HVT sets in a COA. The target analyst, in coordination with the G-3/S-3, G-2/S-2, fire support coordinator, and other staff members, war game the COAs to—

- Finalize individual staff estimates.
- Develop a fire support plan, a scheme of maneuver, as well as friendly and threat decision support templates.
- Determine critical assets required by the threat commander to accomplish his/her mission.

High-Value and High-Payoff Target Identification

An HVT is an asset that the threat commander requires for the successful completion of a mission. Its loss to the threat can be expected to contribute to substantial degradation of an important battlespace function. Contributing to the targeting development process, G-2/S-2 section personnel, the fire support coordinator, and other staff members identify key threat assets that must be dealt with and nominate HVTs to be HPTs. The key to HPTs is that they are based on the friendly commander's scheme of maneuver.

The HPTs are developed during the wargaming process. As the staff fights the different options, the G-2/S-2 identifies specific HVTs. The HPTs for a specific phase of the battle are recorded on the decision support template and synchronization matrix. Those locations where HPTs are expected to appear become TAIs.

The G-2/S-2 and/or collection manager evaluate HVTs at different points in the battle to determine required collection asset capabilities and to provide the necessary target resolution. This evaluation becomes the basis for the collection plan for intelligence support to targeting. Because of their importance, HPTs receive priority in the allocation of detection systems. The G-2/S-2 and the commander must consider the impact the priority will have on maintaining situational awareness, because the same collection assets are used for targeting and battlespace awareness.

The fire support coordinator, air officer, electronic warfare officer, C2W and other representatives use their knowledge of friendly lethal and nonlethal means to determine if a capability exists to attack the HVT and the expected effects of the attack. The G-2/S-2 then assesses the threat response. This effects-based targeting assessment sequence helps determine if attacking the HVT is necessary to ensure the success of the friendly force. If the HVT is acquirable, attackable, and capable of ensuring friendly success, it becomes an HPT. The HPTL identifies prioritized HPTs for a specific battle point.

High-Payoff Target List

The commander-approved HPTL is a tool in determining attack guidance and in developing targeting intelligence collection, production, and dissemination plans.

Collection

Collection efforts focus on NAIs and TAIs that the IPB process identifies during the decide phase. Knowledge of target type and its associated signatures (electronic, visual, thermal) enables friendly forces to direct the most capable collection asset to be tasked against the target. The asset is positioned in the best location based on friendly estimates of when and where the threat target is located.

The decision to destroy, degrade, disrupt, or delay a given HPT results in a requirement to detect that target. Intelligence needs to support the detection of the target are expressed as PIRs and IRs. The PIRs and IRs that support detection of a target are incorporated into the collection plan. The collection manager translates the PIRs and IRs into ICRs and supporting specific IRs. The collection manager considers the availability and capability of MAGTF and external collection assets.

Production

Production efforts focus on developing timely, tailored intelligence products to meet maneuver and fires needs.

Dissemination

Dissemination efforts focus on ensuring CIS readiness to support both routine and time-sensitive intelligence reporting in support of MAGTF targeting needs.

Target Analysis

Target analysis helps to determine the military importance, priority of attack, scale of effort, and weapons required to obtain a desired level of damage or casualties. Other considerations for analysis include target criticality, accessibility, and recognizability. While target analysis helps to determine which targets to hit, operations planning determines how to do it. At strategic and operational levels of war, targeting is more deliberate and focuses on fixed installations or large arrays of targets.

At the tactical level, the MAGTF commander has capabilities to strike deep targets that support threat maneuver or ground forces. These targets are often complex groupings of installations, units, and defenses that may require a methodical approach to ensure success. This methodology is referred to as target system analysis.

Target System Analysis

A target system includes installations, facilities, or forces that are functionally related and situated in the same geographical area. A target system comprised of components and elements can be either fixed installations or mobile target sets. While an individual target may be significant based on its characteristics, its worth is usually derived from its relative importance within the target system. Target system elements are smaller, more intricate parts of the target system than the component and are necessary to the operation of the component. Figure 8-2 depicts the relationship of a target system, its components, and its elements.

Components

A target system's components can also be targets, such as airfields, which are a component of an air defense system. Within industrial or economic systems, a system component belongs to one or more groups of industries or basic utilities

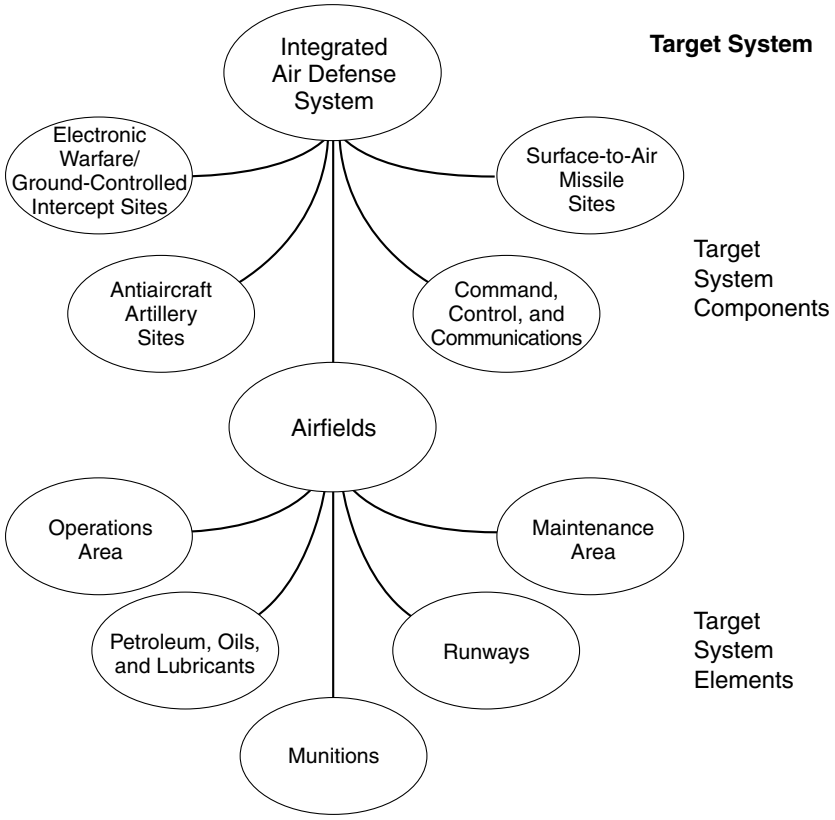


Figure 8-2. Target System, Components, and Elements.

required to produce individual parts of an end product. Target system components can also refer to component services. For example, an air defense system may include C2, early warning and target acquisition radars, antiaircraft artillery and surface-to-air missile batteries, support facilities, and other components that are neither industries nor utilities.

Activity

Target system activities encompass those actions or functions performed by the target system components in pursuit of system goals. By this definition, a combined-arms maneuver division could be viewed as a target system, with components that include air defense units, artillery, armor, mechanized infantry, and engineers. The target development process should focus on the activity of the system or its components. Analysts conduct a comprehensive evaluation of target system components and elements to understand the activities of the total system.

Once analysts have identified the enemy activity that must be affected or defeated, they can determine the key target systems, components, or elements that should be attacked, degraded, or exploited to produce the desired effects. For example, enemy air attacks against friendly ports and LOCs may seriously threaten resupply of friendly forces. To modify or defeat this enemy activity, targeteers analyze the enemy's air force system and identify threat system components and elements. They target the enemy aircraft home bases and identify runways; petroleum, oils, and lubricants storage; and maintenance facilities as potential target elements, which

friendly forces should modify to defeat the enemy's air attack activities.

Linkage

Analysts must understand the linkage or connection between installations performing identical, similar, related, or complementary activities or functions. To develop targets, analysts identify critical nodes or points where target system components and elements are linked and dependent upon each other. These key nodes also exist where target systems interact with other target systems. Matrix and link analysis, as discussed in chapter 7, are highly effective tools for determining linkages and critical nodes.

Target development focuses on identifying the critical nodes within target systems that will satisfy objectives. For example, an enemy's air defense system consists of a number of components, such as surface-to-air missile sites, early warning and ground-controlled intercept sites, antiaircraft artillery sites, and airfields. To function effectively, the elements are linked at a sector headquarters, which exercises responsibility for a specific geographic area. Analysts would target these sector headquarters to sever the critical node within the air defense system.

Target Complex Analysis

A complex is a group of physical elements in close proximity containing multiple target elements that are integrated to contribute to some function of military or civilian value. For example, a system of military airfields distributed throughout the country is made up of individual airfields (e.g., target complexes), containing multiple elements (e.g., individual aircraft, runways, hangars) in close proximity.

After target system analysis identifies a critical target complex, target complex analysis identifies the target environment and defenses associated with the complex. Target complex analysis is used to determine specific targets within the complex as well as supporting actions (e.g., defense, suppression, deception, tactics) that may be necessary to attack the target.

Target Element Analysis

A target element is the smallest identifiable activity of a target component (e.g., sheltered aircraft, control tower, defensive radar site). Based on the targeting objectives, target elements are evaluated as targets for attack. Detailed analysis must be conducted on the individual target element. When conducting target element analysis, the target intelligence officer is responsible for evaluating the element's—

- **Location**—Exact location expressed in geographic or UTM coordinates.
- **Elevation**—Altitude above sea level of the element's ground location expressed in feet or meters.
- **Identification**—Accurate determination of—
  - **Type**—Brief description of the target's military functions.
  - **Size**—Length, width, and height dimensions.
  - **Shape**—Definition of the spatial form.
  - **Attitude**—Azimuth of the element's long axis expressed in degrees (090-270) or descriptive words (east-west).
  - **Dispersion**—Pattern of individual elements in the target area expressed as a short word-picture description.
- **Vulnerability**—Susceptibility to fire.
- **Recuperability**—Time required for enemy to reactivate the target or reconstitute it in another location.
- **Importance**—Value within the enemy's operation and degree to which destruction of the potential target would reduce the enemy's capability.

Role of the Target Analyst

Target analysts should complete the following steps when conducting target P&A:

- Collect target information and intelligence.
- Collate data.
- Evaluate potential list of targets.
- Construct flow of threat target component, complex, and system.
- Determine most suitable targets.
- List targets and priorities.
- Present recommendation.
- Refine data and develop required intelligence products.

Target Analysis Products

Analysis products used in target development include a target list, no-strike target list, restricted target list, target files, and collection requirements.

List of Targets

Target intelligence analysts conduct a thorough analysis of targets and coordinate with the other P&A personnel and the G-3/S-3 maneuver and fires targeting team to provide required intelligence supporting the list of targets for the commander's consideration. The fire support coordinator maintains and prioritizes the list of targets in order of relative importance to the commander's objectives. The operations section and ultimately the commander are responsible for validation of targets and formulation of the commander's target list, which is derived from the HPTL developed during IPB and COA wargaming.

No-Strike Target List

During the target validation process that occurs during target development, some potential targets are placed on a no-strike list. Commanders designate no-strike targets, which are prohibited from attack, to avoid—

- Interference with military operations.
- Damage to relations with indigenous personnel or governments.
- Violation of international law, conventions, or agreements.

No-strike lists are nominated by elements of the joint force and approved by the JFC. This list also includes no-strike targets directed by higher authorities. Examples of no-strike targets include—

- Hospitals.
- Schools.
- Places of worship.
- Cultural shrines.

Restricted Target List

This list is composed of targets with specific restrictions. Actions exceeding those restrictions must be coordinated with the establishing headquarters. Restricted targets are nominated by elements of the joint force and approved by the JFC. This list also contains restricted targets directed by higher authorities. The decision to restrict a target centers on the importance of the target to the threat and the plans and intentions of the friendly commander. The following are examples of restricted targets:

- An area in which a friendly reconnaissance team is operating. To avoid fratricide, fires may be placed into the area, but only upon coordination with the establishing headquarters.

- A bridge identified by a commander as critical to future operations. To ensure the bridge is available to friendly forces, this target may be restricted as to the type of ordnance that can be used against it or the level of damage that may be inflicted on it.

Target File

A target file contains pertinent target system, complex, or component information collected during the target development process. Information in the target file is used to build target studies once HPTs are approved or validated. Generally, target files deal with fixed or semi-fixed targets. This information may be in the form of—

- Data bases.
- Selected imagery.
- Graphics.

Collection Requirements

Throughout the target analysis process, analysts identify targeting intelligence gaps and develop ICRs to obtain needed data. The ICRs must be stated early and clearly in the form of PIRs, IRs, and specific IRs. Analysts and planners have to think beyond the traditional picture (i.e., imagery) and use intelligence sources such as SIGINT, HUMINT (i.e., defectors, refugees, prisoners of war, travelers, aircrew debriefs, and special forces), and other sensor data that can provide indications of a target's status. Gaining a familiarity with collection system capabilities is critical. Requesters should recognize the various intelligence sources' strengths and limitations and understand how to best exploit them.

Target or Objective Studies

Once the commander approves a target, intelligence sections develop target or objective studies to support mission planning. These studies are focused, detailed intelligence products that aid in the application of fires or the maneuver of forces against a specific target set or area. Smaller MAGTFs and units use these studies for mission preparation and execution.

Target or objective studies are graphically oriented and may use many of the graphics derived during the IPB process, such as a target folder. Depending on the specific mission, the study may contain the following information:

- Orientation graphic.
- Time-distance graphic.
- Weather forecast.
- Hydrographic forecast and astronomical data.
- Intelligence briefing notes for mission.
- Graphic intelligence summary.
- Objective area graphic enhancements, such as—
  - Orientation graphic (10–20 km around objective).
  - Mission planning graphic (5 km around objective).
- Objective area imagery.
- Imagery and graphics of insertion points.
- Survival, evasion, resistance, escape plan.
- Challenge and reply passwords.
- Mission-specific data as required.

SECTION II. COMBAT ASSESSMENT

The final step of the targeting cycle, combat assessment is the determination of force and weapons system employment effectiveness during military operations. The combat assessment objective is to identify recommendations for the course of military operations. A G-3/S-3 responsibility, combat

assessment is performed as a coordinated effort by the operations, intelligence, and fires staffs. Conducted at strategic, operational, and tactical levels of war and MOOTW, the combat assessment process is used by analysts to—

- Provide the commander with information on the status of an operation.
- Help formulate subsequent battle plans.
- Serve as a benchmark for validating objectives.
- Collect data on weapons and weapons system performance.

The three components of combat assessment are BDA, munitions effects assessment (MEA), and reattack recommendations (RR). Intelligence analysis has a major role in determining BDA, which includes physical damage, functional damage, and target assessment (see fig. 8-3).

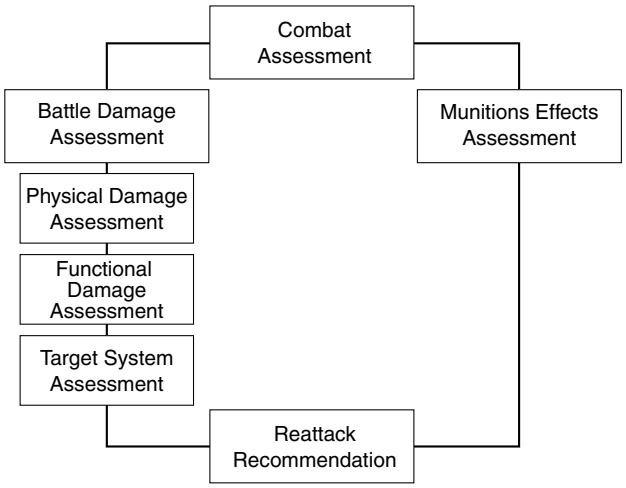


Figure 8-3. Combat Assessment Process.

Battle Damage Assessment

A key component of the combat assessment process, BDA is the timely and accurate estimate of damage resulting from the application of military force, either lethal or nonlethal, against an objective or target. Primarily an intelligence responsibility, BDA requires extensive coordination with operations and fires elements. The BDA is munitions-independent (air, ground, naval, and special forces weapon systems) and is target-independent (fixed strategic and mobile or movable tactical targets).

Munitions Effects Assessment

Munitions effects assessment is analysis of the friendly military force in terms of the weapons system, munitions, and weapon delivery parameters to increase force effectiveness. While the operations and fires staffs are responsible for MEA, the MEA is conducted concurrently and interactively with BDA, which is conducted by the intelligence staff.

Reattack Recommendations

Based on results of BDA and MEA, the operations and intelligence team make RRs for the target nomination and development process. The RRs should address operational objectives relative to the target, target critical elements, and enemy combat forces. When making RRs, the operations and intelligence team considers the—

- Current level of achieved operational and tactical objectives.
- Weapons systems and munitions.
- Target and aimpoint selection.
- Attack timing.

Battle Damage Assessment Components

Physical damage assessment (PDA), functional damage assessment (FDA), and target system assessment (TSA) are three subcomponents of BDA.

Physical Damage Assessment

Referred to as Phase I BDA, the PDA is a quantitative estimate of physical damage that occurs to a target through munitions blast, fragmentation, and fires. This assessment is based on observed or interpreted damage.

The unit controlling the weapons system and the intelligence collection observers develop Phase I BDA reports. Figure 8-4 illustrates the flow of Phase I BDA.

For example, visual observation of an enemy artillery battery (the target) verifies four self-propelled howitzers with shattered and dislodged tubes, recoil mechanisms, and turrets. Track damage to one howitzer is noted. Another

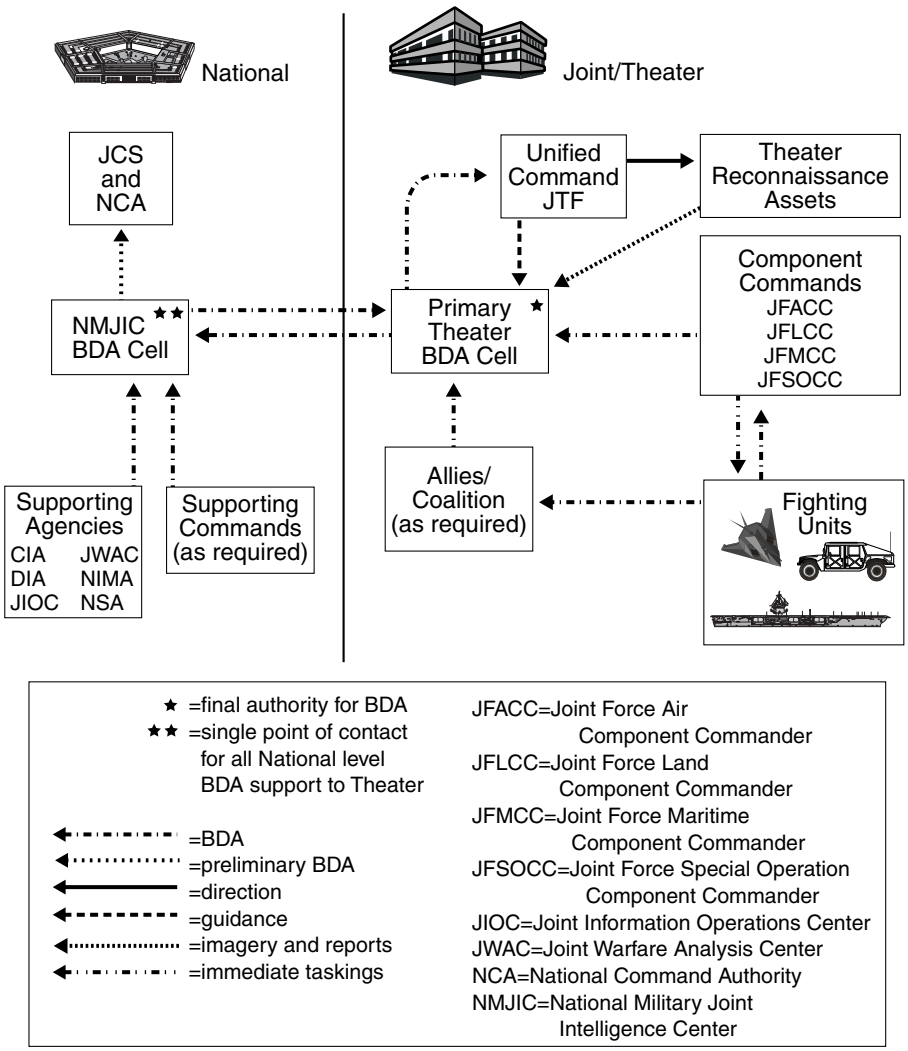


Figure 8-4. Phase I BDA or PDA Information Flow.

howitzer has no visible damage. The PDA of the battery is 65 percent destroyed. The PDA for large, complex targets is keyed to specific aimpoints and critical elements.

Combat Strength Assessment

When dealing with threat ground combat units, the more common term for Phase I BDA or PDA is combat strength assessment. Combat strength is the actual strength on hand of a ground unit in terms of operational tanks, armored vehicles, and artillery. This strength is expressed as either a count of generic type equipment or as a percentage of the T/O and T/E. Threat combat strength is a critical factor to commanders preparing for combat. During operations, commanders rely on combat strength assessment to account for enemy losses and to assess remaining enemy strength.

Combat Strength Baseline

Prior to operations, analysts establish the combat strength baseline of beginning strength numbers. These numbers remain constant for the duration of combat and serve as a benchmark against which losses or gains are measured (see table 8-1). The baseline combat strength represents the maximum amount of equipment possible for a unit, while combat losses represent verified losses.

Table 8-1. Example of Combat Strength Assessment.

105th Mechanized Infantry Division	Tanks	Armored Vehicles	Artillery
T/E	102	135	45
Beginning Strength	98	135	42
Combat Losses	17	22	4
Replacements	6	3	0
Combat Strength	87	116	38
Percent of T/E	85	85	84
Current Combat Strength = 85%			

Combat Strength Computation

Combat strength for each type of equipment is computed by subtracting the confirmed losses from the beginning strength and adding the replacements to that total. The percent of T/O and T/E is calculated by dividing the combat strength by T/O and T/E numbers. The T/O and T/E percentages are totaled and divided by the number of equipment types to determine the current combat strength for the assessed system. Note that while the baseline combat strength represents the maximum amount of equipment possible for a unit, combat losses represent only verifiable losses. Current combat strength can be viewed as a worst-case estimate since it only takes into account confirmed losses. Replacements are included when known. Equipment categories are limited to generic types.

Personnel Losses

Personnel are not normally included in determining combat strength. Acquiring accurate casualty figures and accounting for replacements is extremely difficult, and past experience has shown that body counts are often misleading. A more appropriate and meaningful assessment of the impact of personnel losses can be made as part of combat effectiveness assessment. In MOOTW, however, where personnel may be the threat's principal strength, personnel losses may have to be tracked and combat strength assessed accordingly.

Functional Damage Assessment

The FDA is an estimate of the friendly military force's effect on degrading or destroying the functional or operational capability of the target and an evaluation of the friendly force's operational objective success level. This assessment is based on all-source intelligence and includes an estimate of the time required for reconstitution or replacement of the target function. The FDA is also referred

to as Phase II BDA. Figure 8-5 illustrates the Phase II BDA information flow.

Target System Assessment

The TSA is a broad assessment of the friendly military operations impact and effectiveness against a target system capability. This assessment may be used to measure the threat's combat effectiveness. Based on the commander's operational objectives, a TSA may address significant target system subdivisions.

Analysts compile individual target FDAs to produce TSAs, which are applied to the current system analysis or OOB. For example, the threat's fire support system is known to have 21 artillery battalions. Partial destruction of one battery has minor impact on the effectiveness and capability of the threat's overall fire support system. A complex and resource intensive process, TSA is generally performed at the theater level. The TSA is also referred to as Phase III BDA. Figure 8-6 illustrates the Phase III BDA information flow.

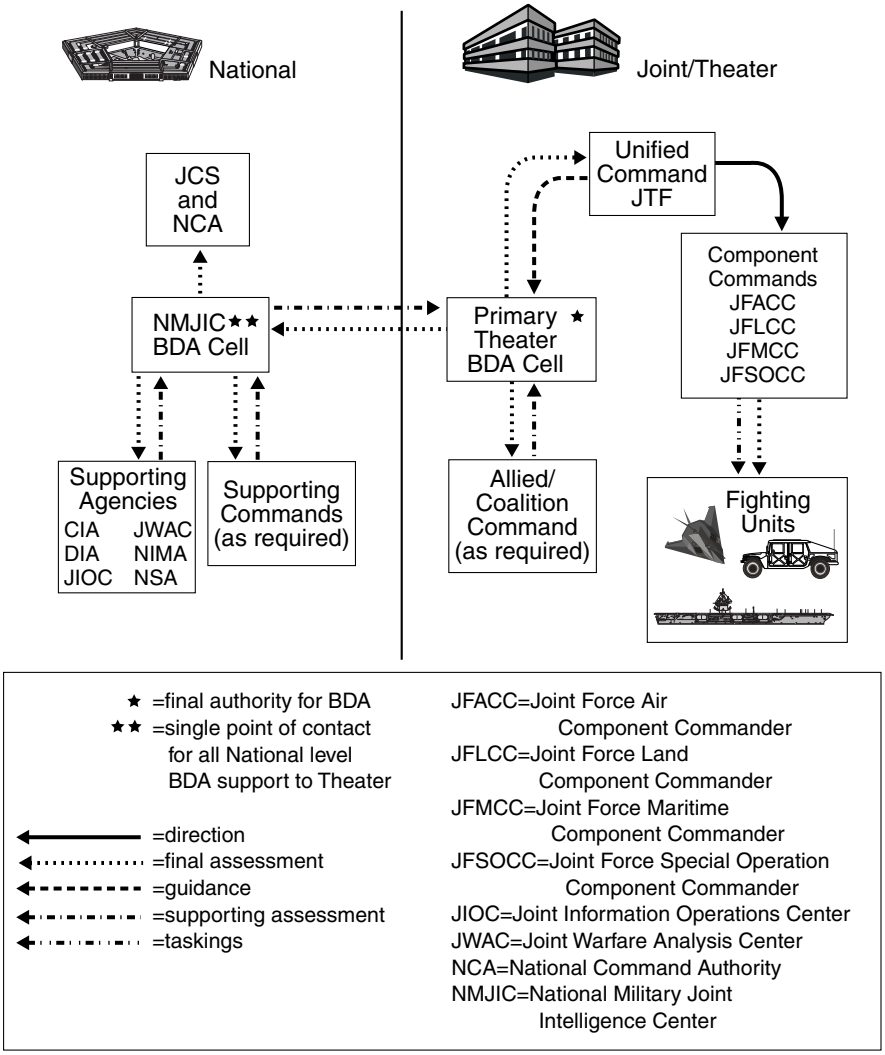


Figure 8-5. Phase II BDA or FDA Information Flow.

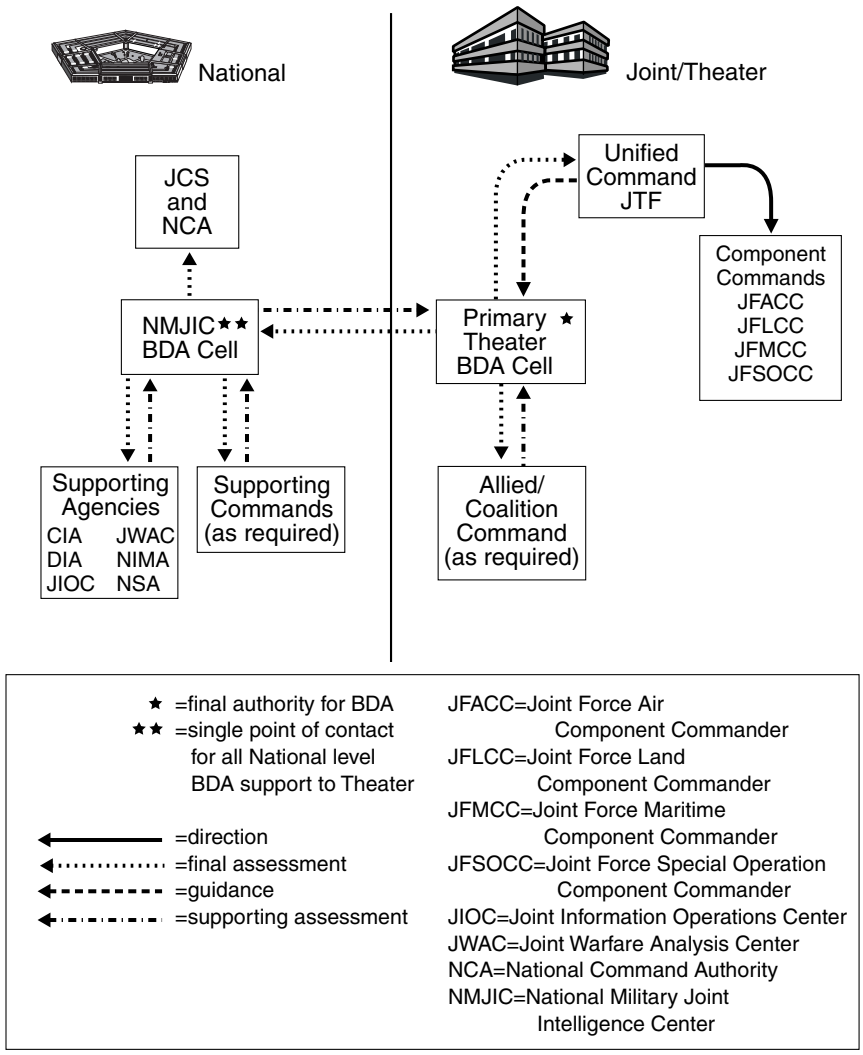


Figure 8-6. Phase III BDA or TSA Information Flow.

Responsibilities

The intelligence officer and the MEF ISC integrate intelligence and operational weapons system and munitions effects data provided by the G-3/S-3 to determine the effects of an executed COA on threat strength and combat effectiveness. In coordination with the G-3/S-3, the intelligence officer or ISC—

- Recommends HVTs.
- Develops and recommends IRs to include those for targeting and BDA.
- Coordinates with the G-3/S-3, air officer, and fire support coordinator to develop coordinated targeting, intelligence, BDA, MEA, and RR plans.
- Develops integrated collections, production, and dissemination plans to answer the commander's IRs.
- Requests collection and production support for intelligence required to satisfy targeting objectives and BDA.
- Establishes procedures to ensure observation reports from forward observers, reconnaissance, pilots, etc., are readily available to BDA analysts.

- Matches BDA against the commanders objectives to determine targeting success and refines intelligence estimates of the threat's situation and capabilities, recommends target reattack, develops and maintains historical BDA data bases, and disseminates hard and soft copy intelligence and BDA products.
- Uses the results of BDA and combat assessment in determining the need to further develop enemy COAs.

Battle Damage Assessment Methodology

After the commander identifies PIRs, IRs, and targeting priorities, the intelligence officer or MEF ISC tasks intelligence collection assets to locate, identify, and track designated targets and directs production assets to plan and prepare needed intelligence products. The ISC, fire support coordinator, and air officer coordinate to identify the appropriate attack system to capture, destroy, degrade, suppress, or neutralize the target.

Based on targets and conditions set by the commander, the ISC refines the commander's BDA-related requirements and integrates them into the intelligence operation plan. These BDA requirements are answered through execution of the intelligence cycle.

As targets are attacked, the ISC coordinates P&A cell's BDA through execution of the intelligence cycle. The commander uses BDA to decide if the target should be reattacked or if the objectives have been met. Once a BDA-related PIR is satisfied, the commander decides if there is a need to establish a new BDA-related PIR or if limited intelligence assets will be used to support another aspect of the mission. The BDA-related PIRs should only address the commander's most critical requirements.

Tactical-level BDA provides a series of timely and accurate snapshots of the effect operations are having on the threat. The BDA helps commanders determine when or if their targeting effort is accomplishing goals and objectives and provides commanders the information needed to quickly allocate or redirect forces.

Battle Damage Assessment Principles

The intelligence officer must work closely with the commander and staff to ensure they know the characteristics and limitations of BDA, which is viewed in terms of objectivity, reliability, and accuracy.

Objectivity

The BDA must be objective and supported by the most reliable data available. Generally, data collected through objective means (imagery) are more reliable than data collected through subjective means (pilot reports). The intelligence officer and ISC should strive to verify conclusions and resolve discrepancies in BDA reporting. It is particularly important to maintain BDA objectivity when BDA becomes the deciding factor for determining and executing a specific COA or decision. When disseminating intelligence, the ISC must make a distinction between facts and estimates.

Reliability

The quantity and quality of available collection and production assets impact BDA reliability. The degree of reliability and credibility of the assessment relies on the resources employed for BDA collection. Collection and production assets must be properly balanced, managed, and supervised to produce reliable reports that are concrete, quantifiable, and precise.

Accuracy

To obtain accurate BDA information, the AO must be frequently and adequately covered by a combination of national, theater, and tactical collection and production assets. Frequent coverage is necessary to accurately determine pre- and post-strike damage.

Battle Damage Assessment Reporting

The intelligence officer or ISC ensures BDA reports conform to the operational plan, reports target damage and destruction, and assesses the degree of mission success. When possible, BDA reporting includes the visual verification of physical damage and an analysis of the damage effects on the threat unit. The MAGTF and subordinate elements are primarily concerned with reporting Phase I BDA or PDA.

Reports

Reports used in BDA include—

- Mission reports and in-flight reports.
- Aircraft cockpit video or weapons system video.
- Imagery and IMINT (e.g., national, theater, and tactical imaging systems, UAVs).
- SIGINT.
- HUMINT.
- Open source intelligence (e.g., television broadcasts, radio broadcasts, newspapers).
- Visual reports from combat units, air controllers, or forward observers.

Reporting Methods

The intelligence officer compiles, refines, and validates the various sources of BDA and develops consolidated PDA or combat strength assessments. The MSCs and major subordinate elements forward consolidated BDA reports to the MEF, usually covering set time periods. See appendix D for an example of a consolidated BDA report format.

At the MEF level, P&A company, intel bn, is responsible for compiling MEF Phase I BDAs or PDAs and for adjusting master OOB data bases to reflect threat combat losses. The BDA cell also prepares and disseminates formal Phase I BDA reports according to theater and national policies and procedures. Defense Intelligence Report, DI-2820-2-99, *Battle Damage Assessment (BDA) Reference Handbook (U)*, provides detailed joint procedures and formats regarding BDA analysis, reporting formats, standard terminology, and resources. This final draft document is available on-line via INTELINK and INTELINK-S.

CHAPTER 9. INTELLIGENCE PRODUCTION

Intelligence production is the conversion of information into intelligence through the integration, analysis, evaluation, interpretation, and synthesis of all-source data and the preparation of intelligence products in support of known or anticipated user requirements. Production involves translating the results of analysis into usable intelligence products that are timely and tailored to the unit, subordinate units, and other supported commands' missions and IRs. The analyst must strive to provide knowledge and understanding that the decisionmaker can visualize and absorb. If possible, that knowledge and understanding should be presented in the form of coherent, meaningful images rather than in the form of accumulated lists, texts, or data fields. During the production phase of the intelligence cycle, information is—

- Evaluated to determine pertinence, reliability, and accuracy.
- Analyzed to isolate significant elements.
- Integrated with other relevant information and previously developed intelligence.
- Interpreted to form logical conclusions, which bear on the situation and support the commander's decisionmaking process.
- Applied to estimate possible outcomes.
- Placed in a product format that will be most useful to the user.

During MAGTF CE deliberate planning, production normally entails the development of detailed, all-source intelligence estimates and studies through the combined efforts of several intelligence and reconnaissance operation elements. During tactical execution, time constraints and ongoing battle demands require rapid processing and production with an emphasis on development of simple, mission-focused intelligence products (e.g., annotated image, target description, overlay depicting current and future threat dispositions). The value of intelligence production is measured in terms of time or resources expended and how well it places information into context, converts it into knowledge and understanding through analysis and synthesis, answers the PIRs and IRs, and applies that knowledge to the decisionmaking process.

There is an inherent friction between the desire to provide as complete and accurate an intelligence product as possible and the continuous requirement to support the time-sensitive urgency of tactical decisionmaking. In practice, these conflicting demands must be balanced by using both stated direction, such as the commander's intent and PIRs, and knowledge of the operational situation to determine when to finish and disseminate a product. To provide a framework to make these determinations, intelligence production is viewed as occurring on deliberate and immediate levels.

Production Categories

In the MAGTF, the primary categories of production are deliberate and immediate.

Deliberate Production

Deliberate production is employed when there is sufficient time to thoroughly evaluate, analyze, and synthesize available information and intelligence. The results of deliberate production efforts are formal, comprehensive intelligence products. Intelligence products that fit into this category include—

- Contingency intelligence studies.
- Detailed, fully developed IPB studies.
- Intelligence estimates.
- Target or objective studies.

Immediate Production

Immediate production is a time-limited, highly focused effort that satisfies an immediate tactical requirement. This type of production involves the rapid processing, analysis, production, and dissemination of intelligence to influence tactical decisionmaking. Often, immediate production is facilitated by, and builds on, a previously completed deliberate production effort.

Elements of data are subjected to a compressed version of the production cycle, and the resulting product is rapidly disseminated to those who are affected. Immediate production is normally conducted during execution and results in simple, mission-specific intelligence products (e.g., situational assessments or answers to specific, individual intelligence requirements).

The nature of the situation and pertinent intelligence requirements dictate the amount of time available to complete each production effort. Intelligence products that fit into this category include—

- Intelligence reports that provide alarm or warning information.
- Reconnaissance and surveillance data related to decision points for branches or sequels.
- Reactive targeting intelligence or hastily prepared intelligence briefings for initiation of small unit action.

Principles

Whether deliberate or immediate, intelligence production is guided by the following principles.

Purpose and Use of Intelligence

To understand the needs of the consumer and to answer the IRs, the producer must know the user's command level, mission, IRs, time sensitivity, responsibilities, and purpose of the intelligence products.

Objectivity

Producers must be objective and unbiased to avoid any tendency toward preconceived ideas. When conflicting information exists, efforts should be made to resolve the difference. If time and resources are inadequate to provide explicit intelligence, the commander must be made aware of the uncertainty. Commanders need pertinent intelligence, including conflicting or contradictory information and opinions.

Provision of Integrated and Tailored Products

Intelligence analysts integrate and tailor information from multiple sources to provide decisionmakers with a clear picture of the battlespace.

Coordination Among Echelons

Intelligence production should be coordinated between national, theater/operational, and tactical-level echelons. The JTF intelligence officer directs and coordinates production activities to ensure they are mutually supporting and not duplicative. Forces at every echelon accomplish joint and combined operations intelligence production, which includes Service-unique products at component commands and operating forces. Higher echelons use organic collection assets and production capabilities to produce intelligence and to refine and compile intelligence received from subordinate units and external organizations. Subordinate units use intelligence products sent to them by the senior command to determine or adjust their mission and operations.

Responsibilities

Higher echelons are responsible for ensuring subordinates are provided the required intelligence exceeding the subordinate's organic capabilities. To provide subordinate commands with required intelligence products and services, higher echelon commanders and intelligence officers identify and task organizations

that can contribute to resolution of subordinate commanders' IRs.

Management

Production management ensures effective and efficient intelligence production in support of operations. Intelligence personnel must receive, review, validate, prioritize, and coordinate production requirements to determine the task, producer, forms, and production schedule.

Production Cycle

The goal of the intelligence cycle is to produce timely, usable intelligence. The production cycle is in essence the intelligence cycle, with the constituent parts of directing, collecting, processing and exploiting, analyzing, and finally producing, disseminating, and using the intelligence. The production cycle spans months or minutes, depending on the level of command conducting production and the nature of the IRs. During the production cycle process, intelligence section personnel must focus on delivering the product in a timely, tailored, complete, and usable manner.

Define Intelligence Requirements

Properly articulated, mission-oriented requirements focus the intelligence effort and define IPRs. The commander, staff, and subordinate commanders play a role in developing the command's IRs. The intelligence officer formulates most of the initial requirements during IPB step 1 by identifying gaps in current intelligence holdings and by defining the scope and detail of production required for IPB support.

As IPB and staff planning progresses, analysts identify additional IRs, which are generally linked to proposed COAs, potential decisions, and targeting. Analysts working to satisfy the command and supported units' IRs also generate new IRs.

Based on the commander's intent and the current phase of the PDE&A cycle, the intelligence officer validates, refines, and prioritizes these additional requirements and converts them into integrated ICRs, IPRs, and IDRs. This is not a one-time effort, but instead a dynamic process of new, existing, and satisfied or no longer relevant requirements. The relative importance of each requirement changes as the PDE&A cycle progresses and as phases of the operation are executed. The intelligence officer must periodically confirm the assignment of priorities with the commander to ensure the intelligence effort is focused on the commander's desires.

Define and Prioritize Intelligence Production Requirements and Tasks

Once IRs have been clearly stated and properly defined, analysts define and prioritize IPRs and tasks by answering the following questions:

- What do I need and where can I obtain the information? The analysts must determine research needs and information sources. The tactical intelligence analyst may have access to a wide range of information and intelligence sources and documents. The product required may have been produced by another source or agency. This requirement may generate ICRs to provide the necessary information.
- When is the product required and in what form? Determination of production assets is based on time and final product requirements (e.g., document, report, supporting study, briefing).
- Who can produce the intelligence product? A small intelligence section does not have the assets to complete a large, detailed study in a short period of time.
- Who will get the product?

- Is this a product that can or must be shared with multinational allies? The intelligence product's classification and releasability must be considered.
- Does this product require supporting work? The analyst must determine the need for supporting requirements (e.g., imagery exploitation, topographic analysis).

Develop Intelligence Production Plan and Schedule

When dealing with large or complex IRs and IPRs, development of an intelligence production plan and a supporting schedule aids in effectively applying resources to accomplish the task. Production plans and schedules are particularly important at higher echelon commands and intelligence centers where numerous long-term projects are managed and coordinated. At lower echelons, production plans and schedules may consist of the intelligence officer conducting a quick mental assessment of the task and developing a time line for its completion.

Considerations

When developing a production plan and schedule, the first consideration is always priority. The requester's needs drive the due date. Once priority and time available are established, factors to be considered include—

- Research required.
- Time available to collect new information and data.
- Coordination needs.
- Review and quality control procedures.
- User's format requirements.
- Graphic preparation.
- Reproduction or conversion requirements.
- Dissemination requirements.

Preparation Methods

For large, long-term products, the production schedule is time lined with various milestones, due dates, and completion projections annotated. In large organizations with distinct collection, exploitation, editing, graphics, and dissemination assets, this time line synchronizes those assets to ensure efficient and timely project completion.

Plans and Tools

The principal planning vehicle for a MAGTF is tab B, (Intelligence Production Plan), to appendix 16 (Intelligence Operations Plan), to annex B (Intelligence), to an OPLAN or OPORD. Other tools that may be used by intelligence officers and their production leaders are the intelligence production matrix and the periodic intelligence production status report. Appendix E to this publication provides guidance and suggested formats for use of these plans and tools within a MAGTF. Specific instructions and formats are specified in unit SOPs.

Allocate Resources

The availability of the following organic and external resources required to produce the intelligence product must be determined:

- Intelligence production personnel.
- Time.
- Ongoing analysis.
- Preprocessed information sources.
- Collection assets.
- Automated information systems.
- CIS.

Assign Tasks

Specific tasks are assigned to the various collection and production resources that assist in the production process. The priority of tasks is

based on the priority of the IR, the time available, and the production schedule.

Prepare the Product(s)

During this step, existing information, data, and intelligence is researched and integrated with new information derived from collection operations and other all-source intelligence reporting. The resulting information set is analyzed and synthesized to develop conclusions and estimates. A final intelligence product(s) draft is produced based on the analysis performed.

Review and Quality Control

Procedures must be established for product review and quality control before final product approval and dissemination. A balance must be achieved between timely delivery and proper review.

Approve and Distribute the Product(s)

Responsibility for final approval of the intelligence product normally rests with the producing unit intelligence officer. At the MEF level, product approval responsibility is generally delegated to the ISC; however, time and the situation may dictate delegating this authority to lower levels. The intelligence product is only of value if it is distributed to the requester in time for proper use.

Follow Up

The final and most critical step in the production cycle is to follow up with commanders and other intelligence product users to—

- Ensure the product is understood.
- Determine whether PIRs and IRs are satisfied.
- Determine if the intelligence product generated new PIRs or IRs.

Production Management

Efficient management of the production cycle ensures effective military intelligence production in support of MAGTF and joint operations. Production management satisfies established PIRs and IRs in a complete, timely, and efficient manner; helps prioritize competing requirements to ensure timely response; and ensures the most effective use of limited intelligence resources.

Functions

Management of the production cycle encompasses the following functions:

- Determining the scope, content, and format of each product.
- Developing a plan and schedule for the development of each product.
- Assigning priorities among the various IPRs.
- Allocating processing, exploitation, and production resources.
- Integrating production efforts with collection and dissemination.

Production Managers

While intelligence production centers and agencies have separate production managers, management of the production cycle at other command levels is conducted by—

- Intelligence battalion commanding officer, serving as ISC under the staff cognizance of the MEF AC/S G-2, at the MEF CE level.
- Intelligence operations officer or air combat intelligence officer at the MSC level.
- Intelligence staff officer at lower tactical echelons.
- Officer in charge of an intelligence direct support team supporting a lower unit.

Production Management Elements

The following elements are essential for production management:

Production Requirements Development

Each IR must be validated through the chain of command and examined to determine scope, form, and content of the request. These validated and examined IRs are IPRs. A well-developed IPR includes—

- Point of contact and best way to communicate.
- Priority of the requirement.
- Date required and latest time the intelligence is of value.
- Classification, releasability, and format desired.
- Mission background.
- Brief description of the desired requirement.
- Justification for the requirement.
- Sources and documents previously consulted.
- Dissemination instructions (e.g., primary and alternate communications means or channels, designated recipients, quantities required).

Prioritization of Requirements

Production requirements are prioritized for limited intelligence resource use.

Asset Allocation

The intelligence officer and intel bn production manager consider internal or organic and external resources (e.g., JTF, theater, and national) for intelligence production tasking. Although internal resources should be considered first, production managers forward requirements for large, complex products to higher command levels. For example, IPB is an inherent function of staffs at every level; however, the production of detailed terrain analysis products may be more appropriately performed by the MEF intel bn or other supporting agencies.

Scheduling

Production managers must schedule and synchronize task elements in the time allotted to successfully complete intelligence production.

Integration with Collection and Dissemination

Production management starts in the planning and direction phase of the intelligence cycle where IRs are determined. The PIRs and IRs are either answered by intelligence products that are readily available or they become a collection or production requirement. Ultimately, products are disseminated to individuals and organizations that need them. Although collection, production, and dissemination involve their own unique internal procedures and cycles, they must be synchronized to provide a timely, pertinent, and usable intelligence product.

Intelligence Products

Intelligence products may be in graphic, written, or oral form and may be as simple as an answer to a question or as complex as a contingency intelligence study. Although they may be used to produce warnings or to identify opportunities, intelligence products are intended to facilitate planning and decisionmaking.

Graphics are the preferred product form because intelligence products should convey an accurate image of the battlespace or threat to the decisionmaker in a form that facilitates rapid understanding. The use of automated information systems is increasing the capability to develop graphic products that can be disseminated and displayed over web-based systems. Graphics developed by the MEF P&A cell may be pulled via the MAGTF tactical data network from the MEF SIPRNET web site or shared via IAS. Use of these graphics reduces or eliminates MSC production.

In time-sensitive situations, the verbal report or short text message may be the most expeditious and useful intelligence product form. For more complex or precise planning needs, graphics reinforced with detailed supporting text is usually required.

Whether oral, text, or graphic, intelligence products should use standard formats. Baseline formats may be modified to suit unit needs, but format modifications may impact interoperability so they must be thoroughly coordinated with all users. The following intelligence products are the principal intelligence products developed and used in the MAGTF.

MAGTF Contingency Intelligence Study

This baseline intelligence study is prepared in advance for standing OPLANs and likely contingencies. In written form, this study is based on the intelligence estimate format and can be converted to an intelligence estimate when a contingency becomes a reality. Many of the products created in steps 1 through 4 of the IPB process (e.g., MCOO, weather effects charts, threat models, doctrinal templates) can be prepared either as supporting graphics or as standalone products.

Intelligence Estimate and Supporting Studies

The intelligence estimate provides basic and current intelligence and mission-specific IPB results. Normally prepared by echelons of battalion or squadron size and larger during the planning phase, estimates are frequently disseminated to other units to keep them current on intelligence. Supporting studies may cover particular aspects of the enemy situation or the AO. See appendix A for the intelligence estimate format and discussion of the relationship between IPB and the intelligence estimate.

Target or Objective Study

This intelligence product provides mission-specific intelligence in support of small unit execution. There is one basic form, but many variations can be used. The study is used to support attack aviation as well as MEU(SOC) and regular combat operations. See chapter 8 for a discussion of the basic target or objective study.

Intelligence Summary

The intelligence summary (INTSUM) provides a synopsis of the intelligence situation covering a specified period prescribed by the unit intelligence SOP or annex B (Intelligence) to the OPORD. Used to report threat activities, threat capabilities changes, and P&A results, the summary is designed to update original and subsequent intelligence estimates.

At lower tactical echelons, INTSUMs are prepared according to the unit SOP or annex B to the OPORD. At higher commands, a daily INTSUM (DISUM) is published every 24 hours. Using the basic format, units tailor the INTSUM to fit the situation. Automated information systems facilitate graphic production of INTSUMs and DISUMs, which are posted on networks with links to detailed supporting intelligence products, reports, and data bases. See appendix F for the INTSUM format.

Intelligence Report

The intelligence report (INTREP) is a standardized report that is disseminated as rapidly as possible based on its importance to the current situation. This report is the primary means for transmitting new and significant information and intelligence when facts influencing threat capabilities have been observed or when a change in threat capabilities has taken place. Generally, a separate report is prepared for a single item of information by the first intelligence element acquiring the information. When time permits, the INTREP should include the

originator's interpretation of the information or intelligence being reported. See appendix G for the INTREP format.

Briefings

Intelligence briefings should always convey mission-essential intelligence and other pertinent information tailored to the audience and current IRs. Intelligence personnel must be able to prepare and orally convey relevant intelligence in a clear, concise manner to brief commanders, staffs, and subordinate units.

Briefings should be supported with graphics to enhance understanding in the least amount of time. Graphics may be as simple as a sketch or acetate overlay or as complex as a multimedia presentation delivered via video teleconferencing. Intelligence personnel must ensure graphics are clear, legible, simple, visible, and focused on relevant information.

At lower tactical levels, briefings are generally informal and often called on short notice. At higher levels, briefings may be structured and scheduled on a recurring basis. The intelligence brief is usually part of a staff briefing coordinated by the chief of staff, executive officer, or the operations officer. Intelligence briefings can be in the form of an information, decision, or confirmation brief.

Information Brief

This is the most common form of brief intended to enhance situational awareness and understanding. The commander's morning update is an example of an information brief. See appendix H.

Decision Brief

The second type of brief is for the purpose of obtaining a decision from the commander. A briefing conducted to convey wargaming results and to gain the commander's preferred COA is an example of a decision brief.

Confirmation Brief

This brief is a final review of a planned action to ensure participants are certain of the objectives and are synchronized with each other.

Organic MAGTF Intelligence Production

In the MAGTF, deliberate production of detailed, all-source intelligence products supports planning. While deliberate production draws heavily on external national, theater, and Service-level production sources, organic MAGTF intelligence sections tailor products to the MAGTF mission and needs. Small unit intelligence sections, intelligence watches at the regiment or Marine aircraft group and battalion or squadron levels, and intelligence direct support teams conduct primarily immediate production.

Unit Intelligence Sections

The MAGTF CE and MSC intelligence sections primarily conduct deliberate production to satisfy planning requirements. They produce the contingency intelligence studies that lower-level commands tailor to their needs.

Units conduct IPB and prepare estimates and target or objective studies that are tailored and focused on their mission and level of command. The IRs that are beyond a unit's production capability are normally forwarded via the chain of command to the MEF G-2 or intel bn. A well-prepared IPB is the basis for rapid and effective immediate intelligence production.

Small unit intelligence sections (e.g., regiment or battalion and Marine aircraft group or squadron) primarily conduct immediate production to satisfy tactical decisionmaking and operations. Immediate production conducted at higher echelons focuses on alarms or triggers associated with the commander's decision points or reactive targeting against identified HPTs. As units

and sensors collect data related to NAIs, TAIs, decision points, and HPTs, this information is rapidly assessed, placed in context, and disseminated as intelligence to the commander and appropriate agencies for immediate action. Often the product is a verbal report or short INTREP sent via electronic means.

Intelligence Direct Support Teams

Two direct support teams are organic to the P&A company, intel bn, and one each for the division, MAW, and FSSG headquarters. They are designed to allow the MEF or MSC commander and their G-2s to focus intelligence support to designated subordinate units. These teams tailor higher and external intelligence products to the needs of the supported unit and assist the supported unit in the production of IPB and other intelligence products to support detailed mission planning and execution.

Production and Analysis Company, Intelligence Battalion

The P&A company produces and disseminates all-source fused tactical intelligence, IMINT, and GEOINT products in support of the MAGTF, MSCs, and other commands as directed. As the focus of the deliberate production effort, P&A company satisfies IPRs for the entire MAGTF. The P&A company has the personnel and equipment resources and CIS connectivity to national, theater, and Service-level organizations' intelligence products and production resources for augmenting organic capabilities. See chapter 9 for additional information.

External Production Support

Marine Corps intelligence assets are optimized for the production of tactical intelligence in support of MAGTF operations. While organic assets are generally sufficient to meet MAGTF requirements, national, theater, and Service intelligence agencies and centers provide unique intelligence production capabilities. The MAGTF has the ability to exploit external intelligence assets to enhance its organic capabilities. The following key external capabilities are employed to support MAGTF operations:

- National, theater, and Service-level intelligence P&A.
- Geospatial information and services.
- P&A of target intelligence and target materials.
- National imagery collection, exploitation, and production.
- Collection and production support from the U.S. SIGINT System.
- National and theater-level CI and HUMINT collection and production.
- Liaison elements from national and theater intelligence agencies.

To exploit external intelligence support resources, the MAGTF must have—

- Trained personnel experienced with external intelligence assets.
- Sufficient, reliable, CIS connectivity and interoperability with national, theater, and Service intelligence architectures to receive, process, and disseminate information.
- Integration of Marine intelligence specialists into national, theater, and Service intelligence organizations to articulate Marine Corps capabilities and requirements, to influence decisions, and to optimize intelligence support to expeditionary forces.
- Established liaison between the MAGTF and supporting intelligence agencies through dedicated communications and exchange of officers.

Department of Defense Support

Within the Department of Defense (DOD) intelligence production community, the DOD Intelligence Production Program (DODIPP) provides the analytical and production resources to support

operational forces. The DODIPP incorporates basic principles that minimize duplication of effort and make the specialized expertise of its analytical personnel available to support DOD customers. The DOD intelligence production community is comprised of the following agencies, centers, and activities:

- DIA.
- Service production centers (e.g., MCIA).
- Unified command JICs or joint analysis centers, components, and Reserves.
- Allied production activities participating in the shared production program (SPP) or during crisis surge situations.
- National Security Agency, which produces SIGINT.
- National Imagery and Mapping Agency, which produces geospatial information and GEOINT.

National Production Support

The DIA and its supporting agencies (Armed Forces Medical Intelligence Center and Missile and Space Intelligence Center) are responsible for intelligence production in the following areas:

- Foreign national military policy, doctrine, strategy, and planning, including—
  - National military leadership.
  - Mobilization process and potential.
  - Strategic or large scale military operations.
  - Integrated, combined, or joint forces on military net assessments and assessments or estimates focusing on military issues at the national, regional, and global levels.
- Current indications and warning intelligence and strategic targeting and planning by the joint staff.
- Integrated force trends and projection assessments.
- Nuclear weapon programs and doctrine.
- Intelligence on proliferation and technology transfer.
- Technological capabilities of antitank guided missiles, surface-to-air missiles, short-range ballistic missiles, and antiballistic and antitactical ballistic missiles.
- Medical and biological warfare intelligence.
- Global topics, such as military geography, industrial resources, transportation systems, demographics, military industrial and resource bases, and military economics.
- Intelligence production programs on counterterrorism, counterdrug intelligence support to law enforcement agencies, foreign intelligence and security forces, and deception analysis.
- Intelligence programs fulfilling DOD-wide responsibilities of common concern, such as targeting and foreign materiel.
- OOBs and associated facilities and installations assigned under the SPP, to include assessing the general military capabilities of those forces.

Unified Command Production Support

A unified command's intelligence production is performed by a production center or JIC, which is assigned to the unified command in support of theater or specialized forces. The JICs fulfill intelligence requirements of unified command CINCs and subordinate commanders by providing tailored, finished intelligence products to support theater mission planning and execution. Regional and functional unified command JICs' production responsibilities vary.

Centers

Unified command intelligence production JICs include—

- U.S. Joint Forces Command's Joint Forces Intelligence Command.
- U.S. Central Command's JIC.

- U.S. European Command's Joint Analysis Center (JAC).
- U.S. Pacific Command's JIC.
- U.S. Special Operations Command's JIC.
- U.S. Southern Command's JIC.
- U.S. Space Command's Combined Intelligence Center.
- U.S. Strategic Command's JIC.
- U.S. Transportation Command's JIC.

Responsibilities

The JICs' intelligence production responsibilities include—

- Operational intelligence, current intelligence, and indications and warning for forces deployed within the command's area of responsibility.
- OOBs and associated facilities and installations assigned under the SPP, to include assessing the general military capabilities of those forces.
- Foreign military forces unit-level training and/or operational readiness.
- Physical environment of deployed or committed forces, including terrain analysis and IPB.
- Targeting support, including target materials, bomb damage assessments, tactical BDAs, and special operations forces targeting support.
- Support to command-sponsored joint planning and exercises.
- Tailored and focused intelligence produced elsewhere to meet the specific requirements of command customers.
- Background and tactical intelligence to customers within the theater, including operational and allied forces.

Services Production Support

The Service production centers are responsible for Service-specific intelligence production and for production relative to U.S. Military Forces assigned for the SPP.

Centers

The Service production centers are—

- Army—National Ground Intelligence Center (NGIC).
- Navy—National Maritime Intelligence Center (NMIC).
- Marine Corps—Marine Corps Intelligence Activity (MCIA).
- Air Force—National Air Intelligence Center (NAIC).

Responsibilities

The centers' intelligence production responsibilities include—

- Weapon system technical data, characteristics, performance, system vulnerabilities, and capabilities to support Service and defense acquisition activities and force developers and to support Service operational training and preparation for contingencies or conflicts.
- Basic ground, naval, and aerospace intelligence and foreign intentions and capabilities.
- Service-unique doctrine, force structure, force modernization, training and education, and acquisition.
- Support to Service schools and commands relative to training, exercises, predeployment, or crisis responsibilities or activities.
- OOB and associated facilities and installations assigned under the SPP, to include assessing the general military capabilities of Services.

Service-Unique Responsibilities

The following Service production centers have unique intelligence production responsibilities:

- NGIC produces ground-related systems and develops intelligence on—
  - Armor.
  - Infantry.
  - Field artillery.
  - Air defense guns.
  - Landmines.
  - Chemical warfare.
  - Helicopters.
  - Munitions.
  - Engineering and transport or logistic equipment.
  - Associated technologies.
- NMIC, Office of Naval Intelligence, produces naval-related systems and develops intelligence on—
  - Surface and subsurface combatants.
  - Antisubmarine or surface auxiliary and support naval ships and programs.
  - Weapons, merchant shipping, and ocean science information.
  - Associated technologies.
- NAIC produces aerospace-related systems and develops intelligence on—
  - Intercontinental ballistic missiles.
  - Intermediate-range ballistic missiles.
  - Medium-range ballistic missiles.
  - Bombers.
  - Fighters.
  - Special mission aircraft.
  - Munitions.
  - Space launch systems and satellites.
  - Associated technologies.
- MCIA produces amphibious and expeditionary warfare intelligence on—
  - Shallow water mines.
  - Coastal artillery.
  - Foreign marine and naval infantry forces.
  - Antilanding capabilities.
  - Expeditionary studies.

Non-Department of Defense Intelligence Production Support

Intelligence production in support of military forces is available from agencies outside DOD (e.g., Central Intelligence Agency). Generally, DIA serves as the focal point for tasking these agencies; however, theater and JTF intelligence staffs can access support through their national agency's liaison office or an assigned national intelligence support team (NIST).

A NIST is a nationally sourced, task-organized team composed of intelligence and communications experts from DIA, Central Intelligence Agency, National Security Agency, NIMA, or any combination of these. A NIST provides the supported command with increased IR management, production and dissemination capabilities, and a direct conduit to national agencies. The size and composition of the NIST varies according to the size and nature of the crisis and the mission and intelligence needs of the supported command.

Production Support Requests

A PR begins as an IR levied on the unit intelligence section. Before requesting production support, the unit intelligence officer must determine if the—

- Intelligence request or request for intelligence (RFI) is most appropriately answered by intelligence resources.
- Information or intelligence is already available in unit intelligence files, data bases, or information resources.
- Intelligence can be obtained by organic collection assets and developed into intelligence by its production assets.
- Intelligence request can be answered from other unit or component intelligence elements.

Once the unit intelligence officer determines that the requirement cannot be met with local resources, the requirement is forwarded up the chain of command for satisfaction. The intelligence officer determines whether to submit the requirement as RFIs, ICRs, IPRs, or PRs. (The acronym IPR is currently unique to the Marine Corps, while the acronym PR, established in joint doctrine, is chiefly applicable to intelligence operations at the MEF CE level and above.)

Generally, an RFI is submitted if the requirement is a fairly straightforward question. In a noncombatant evacuation operation, a RFI may be, "How many personnel require evacuation?" In this case, no extensive collection or production is required because the intelligence is generally available.

A PR is more appropriate when the IR is complex or substantial, for example, "What is the capability of country X to defend its coastline against an amphibious assault?" This requirement may result in an IPR for the MEF CE or a PR to the JTF headquarters because the answer will require the collection and analysis of a large amount of information ranging from hydrographic conditions to available threat weapon systems. Such analysis may be beyond the capabilities of a small unit intelligence section and more appropriately performed at the theater or Service level where access to information and ability to task collection resources are greater.

A PR is also appropriate to satisfy a requirement that may be recurring in nature or in a denied area, for example, "How many aircraft are maintained on alert status at airfield Y?" The unit intelligence officer submits a request for theater and national production assets, because the airfield will need to be monitored for a period of time to determine the answer and the requesting unit probably does not have the collection resources to monitor the airfield.

As an RFI travels up the chain of command, it is satisfied (from available information or intelligence or by collecting new data), converted into a PR, or forwarded to the next higher level for satisfaction. Each unit in the chain of command validates the PR and either satisfies it from within or passes the requirement to the next higher authority for action. Figure 9-1 illustrates the generic flow of PRs.

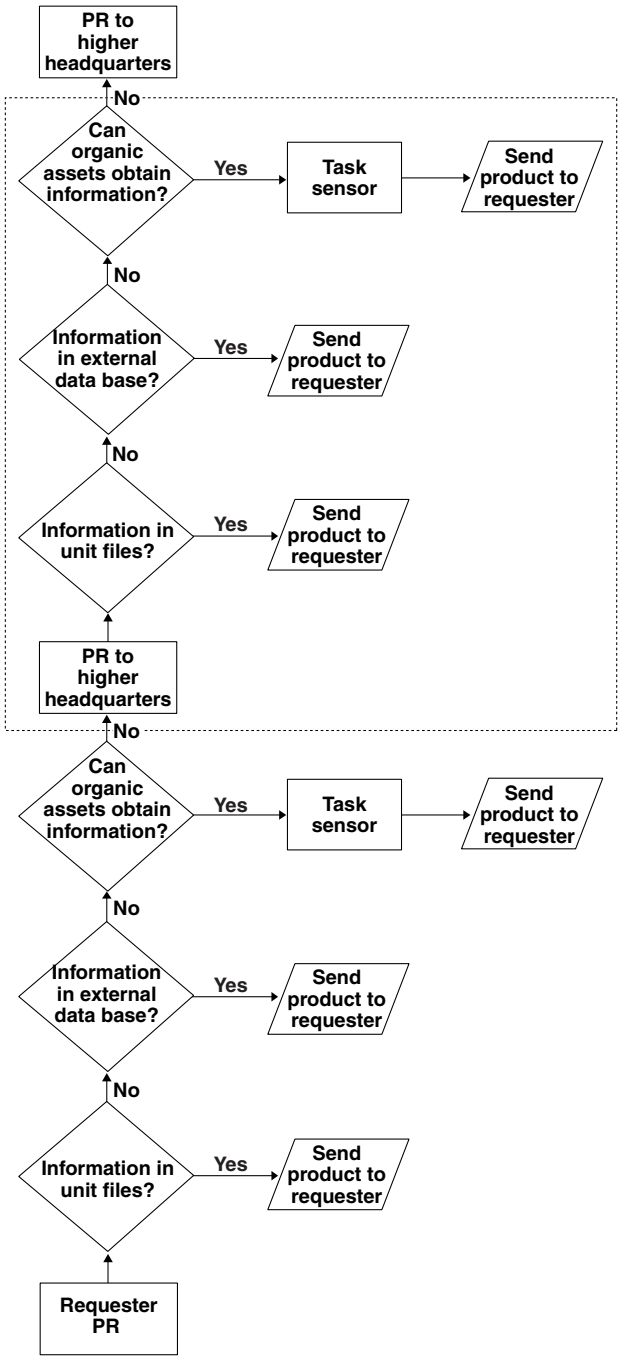


Figure 9-1. IPR Flow.

Request Process

Most IPRs are levied on the intel bn, P&A company's P&A cell, which is the MAGTF's principal deliberate production asset. Based on the commander's guidance and the G-2/S-2's direction, the intel bn commander or ISC—

- Plans, manages, and conducts MAGTF IPR management.
- Exercises staff cognizance over MEF collection and production elements to fulfill PRs.
- Determines which PRs are produced locally and which PRs are forwarded to the appropriate theater, Service, or national DODIPP production center validation office (VO).

The VO reviews the PR, determining whether to accept and satisfy the PR, forward the PR to another production center, or invalidate the PR. The combatant commander, the JFC, or the MAGTF commander directs PR and RFI procedures, which vary from theater to theater. For example, a MAGTF preparing to deploy submits PRs through the normal Service chain of command to the MCIA VO. However, a MAGTF operationally assigned to a combatant commander submits PRs through the established operational chain of command to the VO supporting that theater. A theater intelligence directorate (J-2) may delegate validation authority to a JTF J-2 during a crisis, providing the JTF J-2 a streamlined path for JIC production support and priority over other non-crisis production requirements. For most crises and contingencies, annex B to the joint force commander's OPLAN or OPORD specifies policies and procedures for requesting intelligence production support.

Request Format

The same basic format is generally used for RFIs and PRs. This facilitates conversion of an RFI into a PR at a later time. A basic level production request must include—

- Organization(s) and specific office(s) or individual(s) requesting the product.
- Statement describing the—
  - Required information and intelligence.
  - Sources consulted by the requester and source shortcomings relative to the request.
- Latest time information of value.
- Product form (e.g., hard copy text, electronic file on disk) and total quantity of each.
- Requirements prioritization for multiple elements.

The basic format provided above is sufficient at lower tactical levels; however, at higher levels the format becomes more structured. Defense Intelligence Management Document 0000-151C-95, *Department of Defense Intelligence Production Program (DODIPP): Production Procedures (U),* stipulates the format for PRs, which ultimately will be forwarded to a DODIPP VO and production center. See appendix I for PR format. Each combatant command defines formats and procedures in their applicable intelligence TTP documents. The MEF CE and MSC headquarters SOPs defines formats for their headquarters subordinate elements.

Automated Production Request Procedures

Community On-line Intelligence System for End Users and Managers (COLISEUM) provides an automated capability for the preparation, submission, validation, and assignment of PRs within the DOD intelligence production community. With this system, the requester researches existing requirements and responses to reduce the submission of duplicate requirements. Commands and production centers with access to COLISEUM have immediate visibility of existing and new requirements validation and production status and product completion notification.

Designed to function as an application under the Joint Deployable Intelligence Support System (JDISS) program, COLISEUM is currently available on JDISS 1.01 and JDISS 2.0. The IAS also provides access through JDISS. In addition, the COLISEUM is available on INTELINK sensitive compartmented information (SCI) under

DIA, Directorate of Intelligence Production. The principal inject sites for Marine Corps operating forces PRs are the MEF and Marine Corps forces (MARFOR) G-2s. The MEF, MARFOR, CINC, and DOD policy documents govern procedures for submitting PRs via COLISEUM.

CHAPTER 10. OPERATIONS

Intelligence enables the planning and execution of successful operations. Unity of effort, high tempo, timely decisionmaking, rapid execution, and the relentless exploitation of decisive opportunities characterize MAGTF operations. Intelligence P&A must have the flexibility, agility, and sustainability to support MAGTF operations. This chapter discusses intelligence P&A planning and execution considerations for various MAGTF operations and phases.

Expeditionary in nature, MAGTF operations are conducted according to the following Marine Corps maneuver warfare and emerging operational concepts, which present unique challenges and considerations for intelligence support:

- Operational Maneuver From The Sea—The maneuver of operational-level naval forces projects sea-based power ashore to deal a decisive blow at a place and time of our choosing. Operational maneuver from the sea (OMFTS) focuses on operational objectives and embodies the application of the principles of maneuver warfare to a maritime campaign.
- Sustained Operations Ashore—Those campaigns in which MAGTFs fight as sea-based operational maneuver elements. Embracing the tenets of OMFTS, sustained operations ashore (SOA) envisions a series of operational-level missions designed to enhance the joint force campaign and exploit weaknesses exposed in the opposing force. Normally, SOA involve a MEF assigned to a larger joint or combined force.
- Military Operations Other Than War—The conduct of Marine and naval expeditionary operations across the range of military operations short of war. MOOTW encompass a wide variety of activities intended to deter war, resolve conflict, promote peace, and support civil authorities.

SECTION I. OPERATIONAL MANEUVER FROM THE SEA

Success in OMFTS depends on the ability to seize fleeting opportunities and quickly take advantage of enemy vulnerabilities. Emphasis is placed on deception, surprise, speed, and battlespace preparation to create delay, uncertainty, and ineffectiveness in enemy actions. Intelligence provides the knowledge and understanding that enables the effective conduct of OMFTS. Operational maneuver from the sea relies on intelligence to drive planning, COA development, wargaming and selection, and execution by—

- Identifying the enemy's COG(s), strengths, and weaknesses.
- Exposing critical vulnerabilities to be exploited by naval forces operating from the sea.
- Assessing the potential for maneuver offered by the battlespace, to include identifying entry points where the force can establish ashore.
- Providing the foundation for effective force protection and C2W efforts, which facilitate the preservation of surprise and the employment of deception to disrupt and disorient the enemy during OMFTS.

Requirements

Key OMFTS intelligence P&A support requirements include—

- IPB and situation development covering a broad air, sea, and land maneuver space.

- Threat analysis focused on determining COGs and critical vulnerabilities.
- Detailed terrain and hydrographic analysis, which identify suitable entry points and support maneuver of widely dispersed combat and CSS elements.
- Responsive processing, analysis, and production capabilities that can rapidly develop the critical intelligence required to shape operational and tactical decisionmaking and to provide the intelligence segment of the common operational or tactical picture.
- Indepth intelligence support of force protection and C2W activities.
- Detailed information regarding local resources (e.g., petroleum, oils, lubricants, water) to reduce MAGTF ashore sustainment requirements.

Considerations

Although the requirements appear similar to the traditional amphibious operations intelligence support requirements, OMFTS presents the following unique considerations:

- The large potential AO may extend 200 nautical miles or more from the sea base.
- Points of entry may be widely dispersed instead of being grouped into a single force beachhead.
- The sea space becomes a maneuver area for LCACs and advanced amphibious assault vehicles transiting to the shore from over the horizon, requiring extensive and detailed hydrographic analysis over a larger area.
- The OMFTS forces rely on rapid maneuver for maximum effectiveness and survivability, necessitating detailed and accurate terrain analysis.
- The vision of dynamic, precision fires at maximum engagement ranges requires precise targeting data and BDA.
- Analysis must occur in real or near-real time and must be available simultaneously to every MAGTF unit and element.
- Intelligence products must be in a format that can be rapidly updated and displayed in graphic form on automated information systems to be used by units, staffs, and decisionmakers.

Support During Planning

Initial production efforts are directed at providing an extensive description of the battlespace and threat required to focus the planning effort. Under the direction of senior Navy and Marine intelligence officers, the MAGTF, MSC, naval expeditionary force, amphibious staff, and ship's intelligence sections engage in a collaborative effort to plan and execute intelligence and reconnaissance operations necessary to support development of intelligence products that support the force.

Individual intelligence sections normally concentrate on their particular areas of expertise, satisfying their units' requirements while contributing a broad-scope product to the general production effort. The MAGTF G-2 CIC or P&A cell may focus on describing the battlespace and enemy C2, logistics, and reserves; while the ground combat element's intelligence section studies the enemy ground forces. The amphibious force and the aviation combat element's intelligence sections both look at air and air defense threats, and the amphibious task force (ATF) intelligence staffs concentrate on the naval, sea mine, and coastal defense threat.

Intelligence personnel access national, theater, and adjacent component resources via reach back to augment organic resources of the force. The integrated Navy and Marine amphibious force intelligence center provides a comprehensive IPB analysis, intelligence estimate, HVT list, and supporting intelligence studies by coordinating amphibious force efforts. As the

planning phase continues, production efforts are concentrated on identifying enemy vulnerabilities to be exploited, providing IPB products, HPTs, and intelligence estimates to support specific COAs under consideration.

In the final stages of the planning process, the production effort shifts to development of mission-specific intelligence products focused on the selected COA(s). These products include IPB graphics, point of entry studies, and target or objective studies. In addition, an extensive all-source intelligence effort supports deception, operations security, psychological operations, and electronic warfare planning according to the commander's information operations or C2W strategy. The production effort becomes increasingly decentralized as MSC and subordinate element intelligence sections focus on their units' specific requirements. The MAGTF CE intelligence section continues to provide products to support the entire force, concentrating on elements designated as the main effort.

Support During Execution

During the execution phase, emphasis is placed on rapid processing and production of intelligence that supports timely decisionmaking, enhanced situational awareness, and engagement of HPTs. Because OMFTS depends on decisive action and operational tempo to break the enemy's cohesion and ability to resist, intelligence personnel must be able to—

- Demonstrate flexibility, agility, and responsiveness to recognize threat vulnerabilities and identify opportunities as they develop during battle.
- Demonstrate an awareness of ongoing operational and tactical activities and potential threat actions or reactions.
- Integrate rapidly all-source intelligence information with sensor data and combat reporting to develop a coherent, timely, and tailored picture of enemy dispositions and an assessment of its intentions and capabilities.
- Convey rapidly the developed picture and assessment to commanders in time to exploit identified opportunities.
- Engage fully in planning for future operations by continuing IPB analysis, delivering BDA results, satisfying new intelligence requirements, and participating in the decisionmaking process.

SECTION II. SUSTAINED OPERATIONS ASHORE

Sustained operations ashore require broad-based intelligence support that bridges the operational and tactical levels. Tactical plans are based on operational-level intelligence assessments, which identify the enemy's COG(s) and critical vulnerabilities across the entire theater.

In SOA, MAGTF intelligence operations contribute to the operational level assessments while translating the conclusions from those assessments into relevant tactical intelligence.

While OMFTS focuses on operations from a sea base, SOA entails large-scale, potentially long-term, land operations supported from the sea. Critical aspects of SOA include a large AO and rapid operational tempo. While P&A in OMFTS is heavily tasked with identifying points of entry, SOA focus on infrastructure related to sustaining a large force. Analysis of threat COGs and vulnerabilities, detailed terrain studies, precise targeting data, and BDA remain requirements under SOA.

Considerations

Considerations for the development of intelligence in support of SOA are similar to those for OMFTS. Intelligence support during the execution of SOA requires the same agility and responsiveness as in OMFTS, with the focus on providing critical intelligence to support tactical decisionmaking. However, SOA are normally conducted over a greater area and with a larger size force than in OMFTS, creating the requirement for a larger and more widely distributed intelligence operation support structure. The potential for integration with theater, allied, and other Service intelligence assets are also greater than in OMFTS.

Support During Planning

P&A efforts in support of SOA parallel those for OMFTS. Initial production is broad in scope, with the focus narrowing as particular COAs are selected and a concept of operations is developed. In SOA, GEOINT production takes on added importance; opportunities for ground and air maneuver as well as LOS profiles for observation, weapons employment, and communications-electronic equipment operations are major considerations. Mapping enhancements, LOC studies, and IPB graphics (e.g., cross-country mobility, weather effects, and COOs) are key products.

Threat analysis must be comprehensive and generally deals with large ground and air formations. This analysis covers reserves as well as committed forces and must take into account factors that impact the enemy's ability to fight at the operational and tactical levels (e.g., leadership, doctrine, training, readiness, and sustainability).

An extensive production effort is devoted to supporting logistic operations. The main components of this effort are studies of the local climate, infrastructure, and resources as well as the rear area threat. Products from national, theater, and joint force intelligence agencies contribute to the production effort, but many of these products will be tailored by the intel bn's P&A company, other intelligence producers, and the MSCs' intelligence sections to satisfy particular MAGTF requirements.

Support During Execution

During execution, emphasis is placed on rapid processing and production of tactical intelligence to support operational decisionmaking in the current battle, while at the same time providing detailed intelligence to shape plans for future operations.

SECTION III. MILITARY OPERATIONS OTHER THAN WAR

Military operations other than war include the following missions and tasks, which present unique intelligence requirements:

- Humanitarian assistance and disaster relief.
- Noncombatant evacuation operations.
- Maritime intercept operations.
- Show of force.
- Strikes and raids.
- Peace operations, including peace enforcement and peacekeeping.
- Support to counternarcotics operations.
- Recovery operations.

Requirements

Intelligence shapes operations during MOOTW as it does during other types of MAGTF operations. However, in addition to understanding the physical environment and the threat, the commander must have intelligence on political, economic, and sociological conditions to develop sound military plans that will accomplish the assigned mission. To support MOOTW, MAGTF intelligence personnel must be able to—

- Focus on areas with the greatest potential for the execution of contingency operations.
- Respond with minimal warning and preparation.
- Adapt to a wide variety of potential missions and possess expertise and specialized capabilities to provide MOOTW intelligence.

Considerations

Intelligence P&A activities in MOOTW are generally characterized by—

- The initial lack of detailed data bases on the AO and threat forces.
- An extensive list of nonstandard intelligence requirements that must be satisfied to support planning and execution (e.g., uncertain force protection requirements).
- Analysis of nonmilitary related data.
- A rapidly changing situation resulting from crisis conditions in the AO.
- Compressed timeframe for intelligence development.
- Restrictions on collection operations and the dissemination of intelligence, particularly with multinational military forces, NGOs, and PVOs.
- Increased likelihood of participation by coalition partners.

Support During Planning

Intelligence P&A requirements in MOOTW are normally focused on nontraditional subject areas and IRs. For example, more detailed knowledge of the host nation's economic, transportation, medical, and public works infrastructure will be required to develop plans for humanitarian assistance operations. A threat study to support a peacekeeping mission must encompass an extensive treatment of political, cultural, and sociological factors related to various insurgent or paramilitary factions in addition to the conventional military capabilities of the opposing sides.

Collaboration and coordination with area specialists and expertise from external intelligence organizations, non-DOD agencies (e.g., State Department, Office of Foreign Disaster Assistance, U.S. Agency for International Development) and NGOs or PVOs are crucial to satisfying MOOTW requirements. In turn, the requirement to share information and intelligence with those same agencies, as well as host-nation and allied forces, has a significant impact on analysis, production, and dissemination. While the goal is to provide necessary information and intelligence to participants in the operation, some information must remain releasable only to U.S. forces or allies with long-standing intelligence exchange agreements.

Production formats generally must be adapted to the requirements of a particular situation (e.g., normal IPB products must be modified to highlight factors critical to the specific MOOTW mission). In addition, P&A in MOOTW must be responsive to the unique needs of a large number of small elements conducting independent activities throughout the AO. Production in support of these elements must be tailored to specific mission requirements and provide details pertinent to the small unit level. Intelligence that increases the situational awareness of individual Marines (e.g., information on local customs,

language, health and sanitation) is an important part of this effort.

MOOTW IPB Requirements

The principal difference between IPB for conventional war and MOOTW activities is the focus and the degree of detail required to support the commander's decisionmaking process. Another major difference is the enormous demand for demographic analysis, since the population often is the focus in MOOTW. Typically force protection IRs take on greater priority. The four steps of the IPB process and sample aspects and considerations for various MOOTW activities, are discussed below. (See FM 34-130/FMFRP 3-23.2 for a discussion of each type of operation.)

Define the Battlespace Environment

Intelligence personnel define the MOOTW battlespace environment by expanding the AOI, assembling data on terrain and infrastructure, and compiling data on the host nation.

Expand the AOI

To expand the MOOTW AOI, intelligence personnel must—

- Identify potential sources of assistance to friendly force operations from outside the country or AO.
- Identify military, paramilitary, governmental, nongovernmental, and private volunteer organizations that may interact with the friendly force.
- Identify and locate external influences on the operation.
- Consider media, political, and third nation support or interference.
- Identify the geographic boundaries of the operation, applicable legal mandates or terms of reference, and other limitations or constraints that may impact on the operation.

Assemble Data on Terrain and Infrastructure

To assemble data on MOOTW terrain and infrastructure, analysts must—

- Identify existing infrastructures that have the potential for use by either threat or friendly forces in the operational area.
- Include sources of basic sustenance and energy, as well as transportation and communication networks.
- Identify facilities in adjacent or intermediate countries that could support the introduction of friendly forces or the delivery of necessary materials.
- Compile data on the geography and climate of the area, to include unusual or violent weather patterns or natural disturbances.

Assemble Data on the Host Nation

To assemble data on a MOOTW host nation, intelligence personnel must—

- Identify the existing government and military infrastructure.
- Pay particular attention to their capabilities and limitations with regard to support for or interference in the operation.
- Begin compiling demographic data on the population, to include age, education, religious beliefs, cultural distinctions, ethnic makeup, allocation of wealth, political affiliations and grievances, languages, values, and practices.

Describe the Battlespace Effects

Intelligence personnel describe MOOTW battlespace effects by identifying legal aspects, conducting terrain and weather analysis, evaluating the threat, and determining threat COAs.

Identify Legal Aspects

The MAGTF staff judge advocate should fully explain the impact of legal mandates, terms of references, or other diplomatic agreements. Intelligence personnel should include legal mandates in place that will have a major effect on friendly COAs, particularly rules of engagement and use of force.

Conduct Terrain Analysis

To conduct terrain analysis for MOOTW, intelligence personnel must—

- Use military aspects of terrain or KOCOA.
- Pay attention to routes and areas that offer good observation for friendly security forces.
- Depict potential obstacles, choke points, and ambush sites.
- Ensure that air and ground AAs are included.
- Include analysis of the urban terrain.

Conduct Weather Analysis

To conduct a standard weather analysis for the MOOTW AO, intelligence personnel must consider the effects of weather on—

- Displaced persons or refugees.
- Hostile groups.
- Trafficability.
- Air operations.
- Seaborne operations.
- Night operations.
- Communications.
- Threat tactics and civil disturbances (e.g., rallies and demonstrations).

Evaluate the Threat

Doctrinal templates for typical types of threats faced in the MOOTW environment are rare because there are many threats. Intelligence personnel must evaluate the threat according to the specific mission.

Weather

In missions involving humanitarian assistance and disaster relief, where the environment is the threat, intelligence personnel should—

- Evaluate the environmental impact on the population and friendly operations by determining, for example, if continued rains and flooding could trigger mudslides isolating portions of the population and inhibiting relief operations.
- Prepare climatic studies showing historical paths and frequencies of destructive weather (e.g., hurricanes or typhoons), which can serve as a sort of doctrinal template to determine if earthquake aftershocks could collapse fragile water and sewage treatment facilities leading to an increase in waterborne diseases and environmental hazards.

Competing Factions

In missions involving competing factions, some critical information and intelligence may exist in coalition, host nation, or U.S. data bases, which could be used to begin building a threat model for the operation. Intelligence personnel should recognize differences in threats, strategy, procedures and tactics, as well as weapons, equipment, material, and personnel.

Environment

When evaluating the threat, intelligence personnel must—

- Determine if the environment is permissive, uncertain, or hostile to U.S. forces entering with or without host nation approval.
- Determine if the population supports U.S. forces and if that support is contingent on some type or form of material compensation from U.S. forces (e.g., food, water, shelter, weapons).
- Determine if the population is organized to oppose U.S. forces and if the people are

armed and at what level (e.g., weapons, mines, vehicles).

- Identify dissident groups among the population that may publicly support but clandestinely oppose U.S. forces.
- Identify which terrorist groups are present, thought to be present, or have access to the AO, and if they are supported or directed.
- Identify leaders, trainers, and key staff members and develop psychological profiles on key personnel.

Determine Threat Courses of Action

This step in the IPB process is the culmination of battlespace environment analysis and threat evaluation. The success of U.S. operations in MOOTW depends on the combined efforts of state department officials, numerous government agencies, a unified command and its component Services, special operations forces, and the National Security Council. These organizations work together to accomplish foreign policy objectives of the United States and foreign allies. To determine threat COAs, intelligence personnel must—

- Template or describe the actions of the threat that would interfere with friendly operations (e.g., in peacekeeping operations any violations of the existing legal mandates by either belligerent could adversely effect friendly operations and security).
- Develop COA models depicting the reactions of the threat to friendly operations within the AO and AOI.
- War game each COA.
- Analyze reactions of local populace, multinational partners, NGOs, PVOs, and other key third or neutral parties to friendly COAs.
- War game terrorist and sabotage actions and other activities where the threat could reasonably avoid claiming responsibility, which could jeopardize friendly operations or security.

MOOTW IPB Products

The IPB products that may be useful in the MOOTW environment include (but are not limited to) population status, logistics sustainability, LOC, and key facilities and target overlays, as well as coordinates registers and pattern analysis plot sheets.

Population Status Overlay

To construct a population status overlay encompassing areas in the operation, intelligence personnel should, at a minimum, depict the population by political affinity or regional majority sentiment (e.g., progovernment, anti-American, neutral). If unable to ascertain some root causes of regional unrest (e.g., religious, ethnic, racial, or economic differences), intelligence personnel may display the population in terms of demographic differences. Points where demographic differences intersect often pose the greatest potential for conflict and possible disruption of friendly operations. See figure 10-1.

Logistics Sustainability Overlay

To construct a MOOTW logistics sustainability overlay, intelligence personnel should identify sources of food, potable water, fuel, etc. that could be used by the population, threat, or friendly forces. See figure 10-2.

Lines of Communications Overlay

To construct a MOOTW LOC overlay, intelligence personnel should—

- Identify routes into and out of the operational area.
- Include major streets, highways, railways, subways, waterways, etc.
- Analyze and depict the communication systems in place that could be used to support the operation (e.g., telephones, radio, television, satellite, and microwave systems). See figure 10-3 on page 10-10.

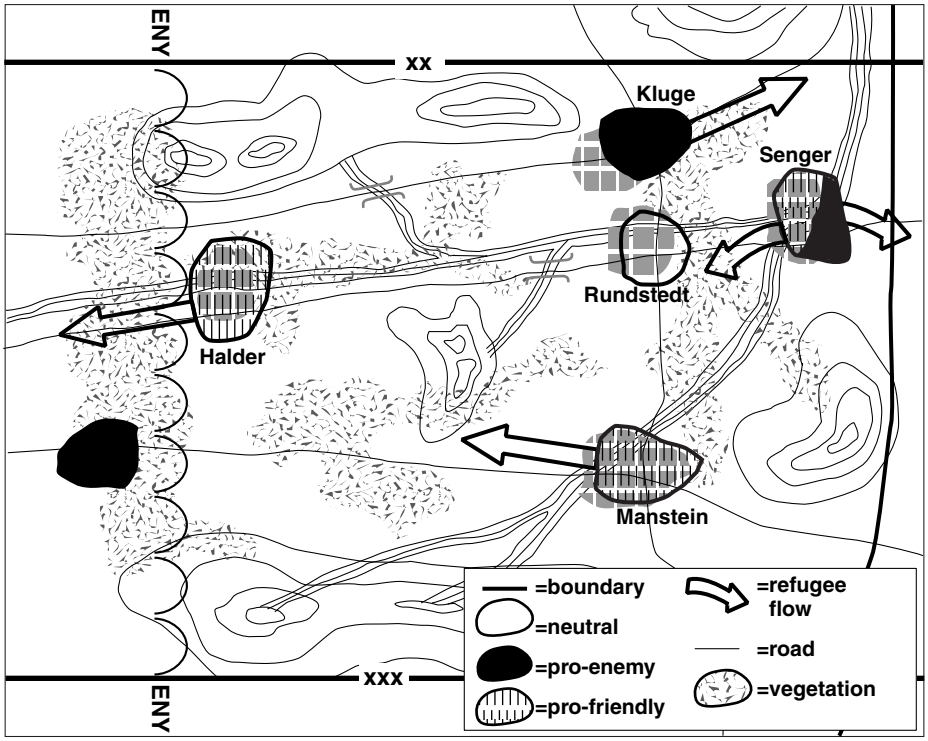


Figure 10-1. Population Status Overlay.

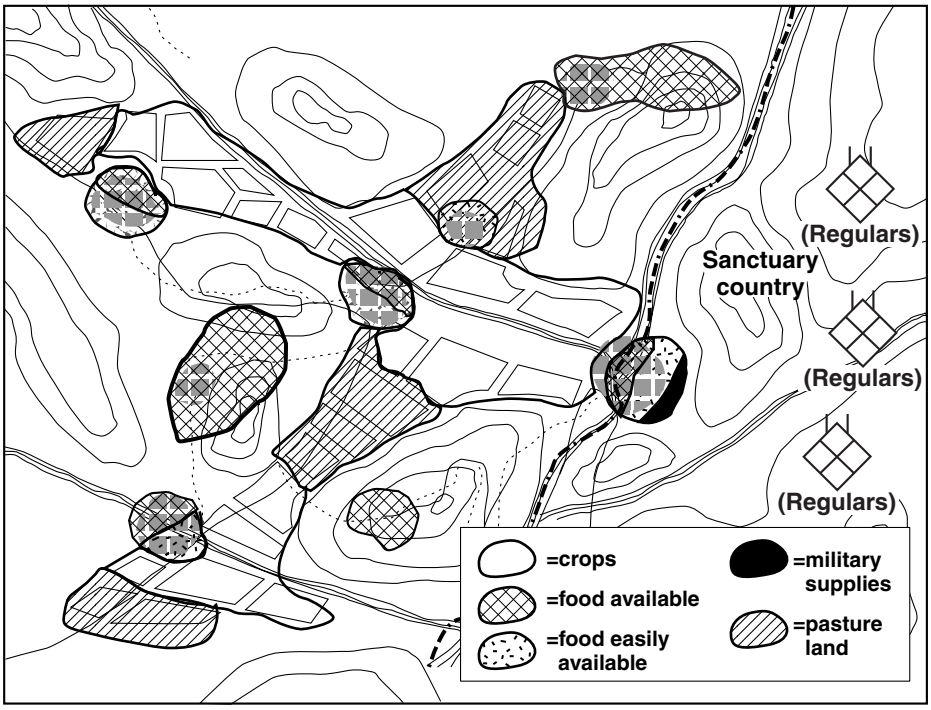


Figure 10-2. Logistics Sustainability Overlay.

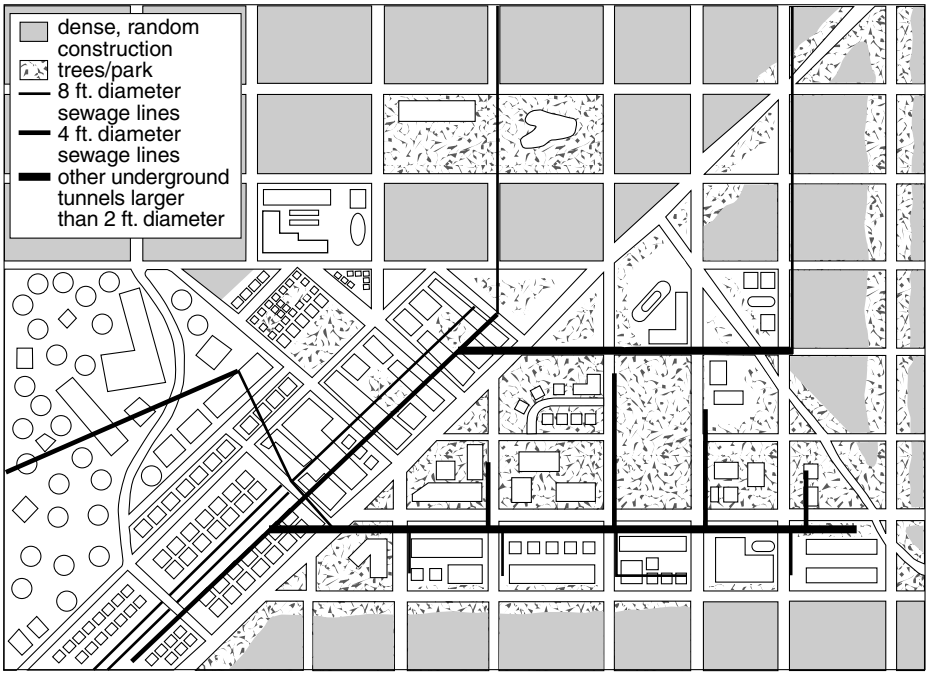


Figure 10-3. Sewers and Subterranean Overlay.

Key Facilities and Target Overlay

Intelligence personnel construct a key facilities and target overlay to depict mission-essential facilities and potential threat targets (e.g., embassies, religious or cultural facilities, military installations, television and radio facilities, government buildings, airports, port facilities, medical facilities, public utilities).

In a noncombatant evacuation operation, the U.S. embassy or the evacuation control center would be considered a mission-essential facility, but it would also be considered a potential target for belligerents.

Coordinates Register and Pattern Analysis Plot Sheet

Because intelligence data bases and doctrinal templates are often limited for many MOOTW situations, intelligence personnel use tools such as the coordinates register and times pattern analysis plot sheets (discussed in chapter 7) to conduct pattern analysis and to rapidly gain an understanding of threat TTP and methodologies.

SECTION IV. JOINT OPERATIONS

Marine Corps forces participate in full partnership with other Services in joint operations, either as a component or as the nucleus of a joint force. A coordinated intelligence effort makes a critical contribution to the success of joint operations. During joint operations, Marine intelligence P&A must be fully integrated with joint intelligence activities to ensure unity of effort, mutual support, and effective employment of limited intelligence resources. Effective intelligence support in joint operations depends on—

- Agreement on policies and procedures.
- Mutual intelligence support.
- Sharing of intelligence capabilities and assets.

- Full interoperability and connectivity among participants.
- Robust liaison.

Responsibilities

The JFC is responsible for intelligence support within the joint command and has responsibility and authority to determine, direct, and coordinate mission-related collection, production, and dissemination activities through centralized or apportioned intelligence requirements management efforts. Component commanders remain responsible for the intelligence function within their commands and employ organic intelligence capabilities to support their assigned missions. The JFC makes national, theater, and joint force intelligence assets available to support the efforts of component commanders. At the same time, component capabilities must be available to assist the joint intelligence effort.

Marine Corps Component Production and Analysis

When assigned as a joint force component, Marine Corps intelligence personnel at each level of command perform the P&A required to support their planning and decisionmaking based on prioritized information requirements; requirements unsatisfied with organic resources are forwarded up the chain of command. Each level of command also disseminates intelligence products to subordinate and adjacent units. Because these higher, adjacent, supporting, and subordinate units may be from a different Service, Marine Corps intelligence sections and units participating in joint operations must—

- Operate according to joint intelligence doctrine, theater TTP, and individual joint force procedures.
- All-source intelligence P&A to satisfy JFC and component IRs.
- Participate in joint intelligence mechanisms for the coordination of IR management (i.e., collection, production, and dissemination requirements).
- Provide P&A support to the joint force headquarters and other component commanders, as required.
- Employ joint or component P&A assets in support of Marine component operations.
- Ensure complete and reliable CIS connectivity within the joint intelligence architecture.
- Exchange liaison elements with the JTF intelligence directorate (J-2), joint intelligence support element (JISE), and/or other joint force component P&A entities as required.

Joint Task Force Headquarters Production and Analysis

A MAGTF may be designated as a JTF with the MAGTF CE forming the nucleus of the JTF headquarters. In this case, the G-2/S-2 must be prepared to function as the JTF J-2 with the MEF CE's intelligence section serving as the base for the establishment of a J-2 section and JISE. The JISE provides intelligence support to the JFC and the entire JTF.

Key Functions

When serving as a JTF J-2, MAGTF intelligence sections must operate according to joint doctrine and theater TTPs. The MAGTF G-2/S-2 must ensure that the P&A portion of the JISE is appropriately augmented or supported by specialists from national agencies, the theater JIC, and other Services possessing the necessary skills to satisfy the force requirements. Key functions performed in the JISE include—

- Centralized collection, production, and dissemination management for joint force and supporting intelligence and reconnaissance assets.

- Development and maintenance of intelligence data bases which support planning, operations, and targeting.
- Production of target studies and materials and intelligence support to force protection.
- Access to supporting national and theater intelligence assets.

Support During Planning

Intelligence product formats, standards, and dissemination means must be defined early to ensure JTF elements can exchange and use intelligence products. When possible, these definitions and standards should be planned for in advance and published in an SOP or TTP that is available to other Service units that may be assigned as part of a Marine-led JTF. The TTP or SOP should be exercised whenever possible to refine procedures and ensure unity of effort.

Support During Execution

The JFC, through the J-2, exercises complete coordination and some specified control over the P&A efforts of the joint force. Often, the J-2 is delegated direct IR validation, prioritization, and tasking authority for intelligence production by the supporting theater JIC. Incumbent with that authority, the J-2 is responsible for managing the force IRs and associated PRs.

SECTION V. COMBINED OPERATIONS

Marine Corps forces may participate in a variety of combined operations, ranging from routine bilateral exercises to coalition warfare in major regional contingencies. Instances of unilateral U.S. military operations are becoming less frequent, particularly in MOOTW. Joint doctrine serves as the doctrinal basis for combined or multinational operations. Each coalition or alliance must develop its own TTP for each operation. The coalition commander determines standardized procedures for coalition forces. NATO STANAGs and quadripartite standing agreements between U.S., British, Canadian, and Australian forces provide standards and guidance for the conduct of military operations by forces in these alliances. See STANAG 2936, *Intelligence Doctrine-AIntP-1(A)*, which governs intelligence operations.

Principles

Successful combined intelligence operations are based on the following principles and considerations.

Adjustment of National Differences Among Nations

Effective combined operations require minimizing the differences in national concepts and TTP for intelligence support. Commanders and their intelligence officers must be prepared to make adjustments to U.S. TTP to facilitate the sharing of intelligence and the integration and interoperability of intelligence and reconnaissance operations.

Unity of Effort Against Common Threat

Intelligence operations must be directed at the common threat. A threat to one alliance member must be considered a threat to all.

Intelligence Determination and Planning

Combined force's IRs and procedures should be identified, planned for, coordinated, and exercised prior to execution of operations.

Special Arrangements

Special arrangements should be considered for developing, communicating, and using intelligence where there are differences in nations' language, culture, doctrine, terminology, organization, as well as intelligence and CIS equipment.

Full Exchange of Intelligence

Each coalition member should share intelligence that supports planning and execution of coalition operations. Intelligence personnel should obtain authorization for foreign disclosure and outline procedures for disclosure and release of intelligence as part of the planning process. During execution, intelligence personnel should monitor the exchange of intelligence and adapt requirements to ensure coalition partners' needs are satisfied.

Complementary Intelligence Operations

Intelligence personnel should integrate and employ each nation's intelligence assets to capitalize on their strengths and offset their weaknesses, providing the coalition with the most effective blend of intelligence and reconnaissance capabilities.

Combined Intelligence Centers

A combined command headquarters should be supported by a combined intelligence center. The center should be manned by personnel from each nation and include appropriate linguist and translator support. This center—

- Develops coalition IRs.
- Validates and establishes priorities.
- Develops integrated intelligence plans.
- Commands and controls intelligence operations.
- Fuses intelligence received from alliance members.
- Disseminates this intelligence to the combined force.

Liaison Exchange

Exchange of intelligence liaison personnel between alliance partners bridges national differences and facilitates the exchange of intelligence and intelligence support.

Foreign Disclosure and Releasability

An important consideration for intelligence P&A in combined operations is the ability to release or disclose intelligence to non-U.S. members of the combined force in a timely manner.

Releasability involves the conveyance of information in documentary form to a foreign national. The document may be a publication, map overlay, imagery, computer disk, or any media that is physically provided to the foreign national.

Disclosure is the conveyance of classified information to a foreign national through either oral or visual means. Disclosure covers classified information that is retained by the United States but is discussed, briefed, or viewed by a foreign national. Often, regardless of whether information and intelligence is released or disclosed, the source(s) of that information and intelligence must not be revealed. Although the members of a coalition are united toward a common goal, it must be assumed that members' intelligence services will attempt to gather information on U.S. capabilities.

Policies and Procedures

The Director of Central Intelligence, DOD, Service, and theater policies and procedures govern foreign disclosure and releasability. The theater CINC is ultimately responsible for establishing policy regarding disclosure and releasability. During crises or contingencies, the CINC may choose to delegate authority to subordinate U.S. joint, combined, or component commanders. When so delegated, each recipient of that authority is responsible for publishing releasability and

disclosure guidance and procedures for their subordinate elements.

During combined operations, MAGTF CEs may be required to act as either a functional or Service component headquarters or as a combined task force headquarters, performing foreign disclosure oversight and guidance. Even when operating as an element of a combined force, every unit and individual Marine must be aware of foreign releasability and disclosure guidance.

Based on the established guidance and procedures, intelligence analysts must pay particular attention to the sources of information and the releasability of the information and intelligence derived from each of those sources. Often one version of an intelligence product must be produced for U.S. forces (and some standing alliance or quadripartite partners), and one version must be releasable to the multinational force.

Security

A balance must be struck between safeguarding classified information and intelligence and ensuring coalition partners are adequately informed and protected. One method for enhancing dissemination while providing necessary security of threat intelligence is to use the tear-line technique in the production process. This process ensures that intelligence and other information below the tear line is releasable to the combined force while simultaneously providing for the protection of U.S. collection intelligence sources and methods. Ultimately, the commander has the final authority to authorize foreign disclosure of information and intelligence directly related to a threat to any coalition partner.

Product Format Considerations

In combined operations, the form in which intelligence is conveyed is critical. Many potential coalition partners lack the technological and functional sophistication to collect, produce, and disseminate intelligence and exercise C2 over intelligence operations. Access to networks using SIPRNET or JWICS is generally not possible due to the inability to restrict the user from accessing unauthorized intelligence and friendly information. Language barriers may affect less sophisticated forms of intelligence dissemination such as text documents or briefings. The ability to exchange and use intelligence may vary from partner to partner.

Solutions for these challenges must be addressed early in planning. Generally, production requirements increase as a result of the need to tailor intelligence for multiple recipients. Increased IRs should be matched with increased analysis, production, and dissemination resources to ensure the timely provision of intelligence throughout the force. Where possible, coalition intelligence personnel should assist in the production of intelligence tailored to support their forces.

Information Sources

The intelligence analyst in a combined operation has the increased burden of assessing the reliability and credibility of non-U.S. information and intelligence sources. While foreign militaries may lack the sophisticated technical means available to the United States, they often enjoy superior capabilities in HUMINT, particularly if they are ethnically or linguistically related to the population of the AO. The analyst may need time to establish the reliability of the source or the accuracy of the information. In addition, the analyst must be aware that foreign forces may withhold, filter, or distort the information provided to the United States to safeguard their intelligence sources and methods. The analyst should apply the techniques and procedures for assessing reliability and accuracy and be conscious of biases that may develop due to preconceived notions regarding the source.

SECTION VI. PRE-CRISIS PHASE

The MAGTF pre-crisis intelligence P&A efforts center on data base management, ongoing production activities, and training.

Data Base Management

The key to effective intelligence and CI P&A is the identification and maintenance of hard copy and electronic intelligence sources and data bases. Intelligence personnel should attempt to develop and maintain relevant data bases during day-to-day operations in garrison. Without the necessary pre-crisis P&A, the ability to provide needed support in a crisis will be diminished. Key sources of intelligence data include the intelligence reference library, statement of intelligence interest, and intelligence data bases.

Intelligence Reference Library

Although intelligence is produced and disseminated increasingly in electronic form, each intelligence section is required to maintain a basic intelligence library in support of command and intelligence functioning. The library should include publications which are tailored to the unit's mission and echelon and are necessary to support day-to-day intelligence planning, operations, and contingency operations. Publications should include maps, charts, imagery, graphics, pertinent finished intelligence, and key supporting documents. Intelligence library publications are categorized as required and nonrequired.

Required Publications

As higher headquarters-directed holdings, these publications represent the minimum required material needed to support intelligence and command functioning. The intelligence officer is responsible for reviewing and validating the command and subordinate command's required holdings to ensure that they meet the minimum intelligence operation support requirements. Requests for additions or deletions of publications will be submitted via the chain of command according to the guidance contained in current directives.

Nonrequired Publications

Intelligence sections maintain nonrequired publications to supplement minimum required holdings, to conduct planning and training, or to use as reference material. The intelligence officer is responsible for ensuring nonrequired publications are available to support intelligence requirements.

National, Service, and unified commands produce intelligence publications that provide intelligence and guidance for intelligence functioning. Procurement procedures are contained in current directives and local SOPs. The manpower or personnel staff officer (G-1/S-1) is responsible for the procurement of doctrinal and tactical publications (e.g., JPs, MCDPs, MCWPs, MCRPs, FMs); however, the intelligence officer is responsible for identifying requirements for these publications.

Statement of Intelligence Interest

The statement of intelligence interest (SII) is the vehicle by which commands register requirements for all-source finished intelligence. Each command must establish an SII with DIA to receive automatic distribution of intelligence publications in support of command requirements. The intelligence officer is responsible for coordinating with the appropriate Dissemination Program Manger (DPM) to ensure the commands's SII is up to date. Statements of intelligence interest are requested through DIA's online Joint Dissemination System (JDS) via INTELINK/INTELINK-S under the Director of Information Systems and Services.

Accounts can be applied for online and are forwarded to the appropriate DPM, which is

Marine Forces, Atlantic, Marine Forces, Pacific, or MCIA, respectively. Once the account is established, it may be modified online. The appropriate MARFOR headquarters or MEF CE intelligence officer determines specific policies governing echelons that may apply for JDS accounts. The Defense Intelligence Production Schedules list DOD planned general intelligence production. Most intelligence producers maintain some type of production forecast on their INTELINK and INTELINK-S web sites.

Intelligence Data Bases

The establishment of intelligence data bases allows the intelligence section to manage and use the large volume of available information and intelligence. Intelligence agencies have established various data bases suited to their needs, resulting in different systems available to support intelligence operations at various levels. The intelligence officer at each command echelon must be aware of relevant intelligence agencies' data bases and plan for their use to support operations. In addition, the intelligence officer should maintain access to appropriate national, theater, and Service data bases.

Data bases are available to Marine Corps commands equipped with the JDISS and the IAS, either as applications or through access to INTELINK and INTELINK-S. As modern information systems technologies mature, the structure and titles of the data bases change frequently. The MCIA 1586-001-96, *MAGTF Contingency Reference Guide*, is a compendium of agencies, products, data bases, and INTELINK sites of potential interest. This publication is available in hard copy, disk, and on-line via both INTELINK and INTELINK-S. In addition, national, theater, and Service producers have created electronic links from their INTELINK web sites to other pertinent sites.

Each intelligence section should create local data bases to support their contingency planning and the development of contingency intelligence support products. Most current intelligence files can be maintained on automated data base systems. Finished intelligence products, imagery, maps, and graphics are available on-line to facilitate data search, access, and retrieval. When assembled, a pre-crisis data base should consist of—

- Current target country intelligence and CI estimates.
- Intelligence reference publications (e.g., intelligence TTP for combatant commands the unit may support, intelligence TTPs or SOPs for other Services with which the unit may operate).
- Standard intelligence data base segments (i.e., modernized integrated data base).
- Mapping, charting, geodetic, and other geospatial holdings.
- Imagery library and related holdings.
- Current intelligence files.
- Open source publications.

Production

Pre-crisis intelligence production includes contingency intelligence production, IPB, exercise intelligence, and other intelligence requirements.

Contingency Intelligence

The main pre-crisis P&A effort of MAGTF and MSC intelligence sections is contingency intelligence production in support of potential missions. The intelligence section must review standing contingency plans and tasking in conjunction with staff operations and plans sections. Intelligence personnel should coordinate with operations and plans personnel to define the mission, scope, and tasks using the following methodology.

Define the Intelligence Requirements

The IRs should be well defined after coordination with commanders and their staffs. Properly focused IRs save time and valuable intelligence assets.

Research Data Bases

Available intelligence data bases should be reviewed before submitting RFIs, ICRs, IPRs, IDRs, or PRs.

Analyze and Synthesize Data

Intelligence personnel must consider data, information, and intelligence from all available sources for analysis and synthesis.

Prepare the Products

Products must be prepared in user-friendly formats and delivered in a timely manner.

Intelligence Preparation of the Battlespace

Pre-crisis IPB is conducted to develop basic and current intelligence needed to support the planning and execution of contingency operations. The extensive and detailed nature of intelligence required to support expeditionary operations demands that a comprehensive research, analytical, and production effort be undertaken far in advance of the initiation of such operations. This demands that commanders and staff principals conduct detailed contingency planning across functional areas and command echelons to identify specific detailed IRs. The pre-crisis period offers the opportunity to carry out a thorough, measured study of potential areas of MAGTF employment. Driving contingency planning efforts, the pre-crisis IPB is the principal contribution of intelligence to combat readiness.

Pre-Crisis Products

The IPB products that can be generated in pre-crisis analysis and production include—

- Battlespace characteristics analysis.
- Terrain and weather analyses and templates.
- Weather effects matrices for various seasons and conditions.
- Threat models.
- Threat capabilities assessments.
- Threat COAs, when possible.

Results

The completed pre-crisis IPB process provides the following products for each potential contingency area:

- Tailored intelligence data base(s).
- Contingency intelligence study.
- Intelligence and counterintelligence estimates.
- Validated intelligence collection, production, and dissemination requirements.
- Integrated intelligence operations plan (collection, production and dissemination).
- Tentative tasks for supporting intelligence and reconnaissance units.

Additional Purposes

In addition to the primary purpose of supporting contingency planning and execution, pre-crisis IPB—

- Develops an intelligence data base for selected areas.
- Educates personnel on potential missions and AOs.
- Identifies intelligence collection, production, and dissemination shortfalls (e.g., IRs, key personnel, and equipment).
- Trains intelligence personnel in the IPB process and the development of intelligence in support of actual contingency missions.

Exercise Intelligence

Exercise intelligence production should follow the same procedures as contingency intelligence production and should result in products that mirror image what will be used in an actual operation. The intelligence section should use real-world data bases, IPB, and scenarios whenever possible to enable realistic training of intelligence personnel and staff and to provide solid area and threat familiarization training for unit Marines and Sailors.

When conducting field training exercises, the intelligence section must provide the same quality of GEOINT, IMINT, SIGINT, CI or HUMINT, and other intelligence support as would be provided in an actual operation. Weather conditions and terrain will factor heavily into the success and safety of an exercise involving the actual maneuver and movement of air, land, and seaborne forces.

Other Intelligence

In garrison, the intelligence section is expected to provide indications and warning information and promote threat awareness. The intelligence section must keep the commander and staff, as well as those of subordinate units, informed on items of interest in the unit's assigned or potential contingency areas. This can be accomplished by providing periodic current intelligence briefings, affording access to intelligence publications, and/or preparing current intelligence read boards for commanders and staff members. With increased access to web technologies, the commander, staff, and subordinate units can review daily pertinent information posted on a web site. The intelligence section should always be prepared to field impromptu requirements as directed by the commander or staff.

Production and Analysis Training

While in garrison, intelligence P&A training is accomplished through individual training, element training, unit training, and MAGTF training.

Individual Training

The intelligence analyst receives an introduction to P&A topics at formal intelligence military occupational specialty training courses. However, to develop P&A proficiency, the intelligence section must have a continuing training program to enhance P&A skills.

Skills Development

The Marine intelligence analyst must train to further develop—

- Comprehensive study and understanding of threat forces' doctrine, operational and functional methodologies, and TTP.
- Familiarity with potential operating areas' cultural, ethnic, sociological, and religious orientations, organization, perspectives, values, and issues.
- IPB skills, which cover analysis of contingency AOs, threat COGs, critical vulnerabilities, tactical practices, capabilities, and COAs.
- Intelligence research methods (e.g., information and intelligence sources, agencies, functions, capabilities, limitations, automated information systems, data base availability and procedures).
- Methods of collecting and reporting information.
- Processing, recording, and filing information methods (e.g., manually and electronically preparing overlays and posting situation maps).

- Integration, analysis, evaluation, interpretation, and information synthesis skills to rapidly produce tailored intelligence products.
- Skills in the use of automated information systems to manage data, analyze information, and produce and disseminate GENSER and SCI intelligence products, using all means of presentation (e.g., briefings, text reports, graphics, overlays).

Exercises

Wargaming and command post exercises (CPXs) are the best vehicles for analytical training and must be done independently of major exercises to enhance analytical skills before they are needed. Normally, the majority of training comes as a result of practical application (i.e., preparation of IPB and other products in response to exercise or contingency requirements). Each product must be evaluated and critiqued with the analyst who developed it to improve their skills. The intelligence officer's wargaming goals should include—

- Providing participants with a thorough area and situation orientation.
- Validating the scope and area coverage of the initial IPB.
- Determining gaps in existing intelligence.
- Identifying areas for additional study.
- Developing new collection, production, and dissemination requirements.
- Developing an initial intelligence concept of operations and supporting contingency collection, production, and dissemination plans.

Element Training

Intelligence sections and elements must have an integrated training program to develop the individual, team, and unit skills and capabilities necessary to execute intelligence and reconnaissance operations during MAGTF operations. Section training should first emphasize building specialized individual production skills. Once individual skills are mastered, cross-training and development of depth should be emphasized. A building block approach is used, starting with small group or team training (e.g., watch section, country team, or production element) and working up to exercises employing the entire G-2/S-2 section and those of subordinate commands.

While a command staff exercise, CPX, or field exercise normally provides the best environment for the conduct of intelligence section training, independent G-2/S-2 section training should be conducted in advance of a major command training event. This allows the section to develop and test SOPs, cross train personnel in a variety of functions, and conduct indepth instruction in intelligence P&A. Each production requirement or exercise is a training opportunity and should have specific training objectives associated with it.

Unit Training

Intelligence units conduct training according to their unit's specific mission and functions. As intelligence specialty units are often employed as small, independent subelements, the majority of their training should be targeted at the team, subteam, or detachment level. Intelligence unit training should also emphasize the planning and execution of operations in response to the supported unit's requirements.

Each unit training evolution is an opportunity to enhance P&A training by requiring the development of objectives for each exercise. In addition, unit training must encompass specific, detailed intelligence objectives for commanders and other staff section personnel. Unit training for P&A should—

- Train intelligence sections in meeting tactical requirements by exercising deliberate and immediate tactical production.
- Exercise the IR management process and intelligence cycle between consumers and producers.
- Test and improve standard product formats and content.

- Critique and provide P&A effort feedback.
- Evaluate the effectiveness of integrating intelligence production operations with those of collection and dissemination.

MAGTF Training

This training combines MAGTF units and trains on a larger scale, which provides intelligence personnel the opportunity to exercise the production management function as well as integrate collections and dissemination with P&A. The MAGTF training provides the opportunity to—

- Test requirement priorities and procedures.
- Test the integrated production between the MEF CE CIC, other intelligence and reconnaissance units, and MSCs.
- Determine if the resulting test products meet the commander and staff's needs.

SECTION VII. WARNING AND DEPLOYMENT PHASE

Warning and deployment sets the intelligence foundation for the entire operation. During this phase, intelligence is expected to produce a high volume of critical planning and decision-making support in a short period of time. This phase is further complicated by the need to prepare P&A elements for deployment within the MAGTF. The IPB and contingency intelligence study prepared in the pre-crisis period and the knowledge and skills gained by intelligence personnel, commanders, and other staff personnel during training exercises is the key to the ability to deliver intelligence support and products early in the warning or deployment phase. Initial P&A efforts, production management, and standardization of products frame the warning and deployment intelligence phase of operations.

Initial Production and Analysis

Determine Initial Requirements

Key to the success in determining initial IRs is a clear understanding of the command's mission, assigned tasks, commander's intent and guidance, and a defined AO. Command and staff element requirements should be integrated so that comprehensive products can be developed to meet as many needs as possible.

The P&A goal should be to produce a product only once to avoid duplicating effort and wasting time and assets. Time is the driving factor in determining the amount of detail that can be put into the P&A effort in the warning and deployment phase.

Assemble and Focus Data Bases

With an understanding of the mission and AO, intelligence personnel can refine data bases and other intelligence holdings. Units should agree on standardization of products and data bases early on in this process. Product and data base standardization should be a minor effort if SOPs or TTPs exist and units have worked and coordinated together previously in IPB contingency intelligence study preparation and training. This effort is more complicated in a joint or combined force.

Develop Initial Estimate and Supporting Studies

Preparing the intelligence estimate is easier if the contingency intelligence study is prepared and IPB is in progress. The initial IPB provides the baseline descriptive intelligence to initiate planning and, when paired with the contingency

intelligence study, supports the preparation of an initial estimate and supporting studies.

Develop Collection, Production, and Dissemination Requirements

Shortfalls identified during preparation of the initial intelligence and CI estimates become the basis for development of new collection, production, and dissemination requirements beyond organic capabilities. New requirements must be turned into collection, production, and dissemination plans, necessitating support requests to component, JTF, and/or theater commands for action. The MAGTF intelligence section is responsible for developing these requirements and for coordinating with the planning section to ensure requirements are focused on operations.

Production Management

Production management validates and prioritizes IPRs among competing requirements to determine which ones have the most impact on the mission's outcome. Production must be managed ruthlessly during this phase to ensure that limited assets are properly focused. The commander must be actively involved in—

- Directing intelligence operation efforts.
- Setting priorities.
- Providing the intelligence officer with guidance on where to focus the effort and what requirements are most important.
- Evaluating the effectiveness of operations.

Continuous interaction with staff planners and subordinate commanders and intelligence officers is required to ensure ongoing production supports the development of friendly COAs. Requirements typically change frequently during this phase as COAs are identified, refined, or rejected. Production management must ensure flexibility and responsiveness. Time is the critical element in production during this phase, because requirements must be met on time, even at the expense of detail.

Standardization of Products

The use of standard products simplifies production and dissemination. To provide a cut-and-paste or fill-in-the-blank capability, products should be standardized and automated. Establishing standard products and a regular update schedule is an effective way of managing production and dissemination during this phase. Product standardization can head off constant requests for updates by organizations, which can drain production and dissemination resources and detract the focus from essential requirements. A system of standard products should be developed during training and carried over with only minor modifications.

SECTION VIII. EXECUTION PHASE

In addition to production management, MAGTF intelligence P&A during the execution phase of operations involves support to current operations, future operations, future plans, and targeting.

Production Management

Production management remains critical during the execution phase, as requirements tend to change rapidly. P&A resources must be focused on the main effort according to the commander's guidance and intent, the PIRs, and the unit's operations and intelligence concepts. The commander must balance the production effort between support to current operations and future operations planning. Usually, the higher the echelon, the greater the focus is on future operations and planning; the lower the echelon the greater the focus is on current operations. Normally, at

higher command echelons, commanders and intelligence personnel must remain responsive to their own and lower echelon commanders' tactical needs. During execution, the time element is even more critical, because execution often depends on timely receipt of intelligence required for decisionmaking.

Support to Current Operations

Support to current operations consists primarily of immediate tactical production that is keyed to the commander's decision points, PIRs, and location of HPTs. Each piece of data, information, or intelligence received undergoes immediate tactical processing and assessment to determine if it is pertinent to the ongoing operation. If deemed pertinent, the information is quickly analyzed, impacts are determined, intelligence estimates are prepared, and results are disseminated. Intelligence personnel must maintain situational awareness and understand the operational situation, current PIRs and IRs, and likely enemy reactions to anticipate and meet the needs for immediate tactical production.

Support to current operations must include P&A in support of deep and rear operations and resist focusing on the close battle. Intelligence support to current operations must be balanced against the need to support future operations and plans. Assets cannot be devoted to current operations at the expense of supporting planning for future operations. In addition to short, tailored, mission-focused products in response to an immediate tactical need, production includes regularly scheduled update briefs and intelligence summaries that help maintain a common picture of the battlespace supporting situation development.

Support to Future Operations

Depending on the timeframe of the operation, scope of the operation, and level of command, support to future operations consists of a mix of immediate and deliberate production. Future operations focus on the deep battle, which is defined either by distance or time. Intelligence products in support of future operations must focus on that same planning window and seek to provide the future operations team with a coherent projection of the battlespace and threat within that window.

The future operations cell focuses on a rolling or near-continuous IPB process by generating new COAs, ICRs, IPRs, IDRs and targeting priorities, DSTs, and synchronization matrixes as the battle or operation unfolds. Intelligence production supporting the future operations cell is focused on products generated during IPB, which have been constantly modified by the results of friendly and threat actions. Daily situation update briefings are necessary to ensure the future operations team remains aware of current actions that may impact future operations.

The primary intelligence P&A contributions are the BDA results and the estimate of the situation focused on the appropriate planning horizon. The BDA provides input into combat assessment, which in turn helps determine the nature of future operations. Derived from the continuous IPB effort, the situation estimate provides the basis for planning.

During future operations planning, IPB and estimates draw on and extend previous work rather than generating new production. The intelligence P&A effort requires continuous interaction with the future operations cell. As decisions are made concerning future operations, integrated collection, production, and dissemination requirements are developed and prioritized, missions are assigned, and mission-specific products are prepared. Management of the time element is critical to ensure that products reach the future operations cell, mission planners, and executers in a timely manner.

Support to Future Plans

The MEF CEs, components, and JTF headquarters often require an additional planning cell focused on the next campaign or major phase change within the CINC's campaign plan. This cell, or operational planning team, in the MEF CE looks into the future and deals more in assumption than fact. Production in support of future planning tends to be deliberate and generalized but still encompasses the basic elements of IPB.

Often, the future plans cell is located out of the immediate operations area and may locate in close proximity to the CINC headquarters to facilitate communication and collaboration. Given the timeframe and location of potential future operations, the supporting theater intelligence center may be more suited to produce required intelligence products, with MAGTF intelligence personnel tailoring these products to support the needs of the future plans cell.

Support to Targeting

Intelligence support to targeting requires a continuous, integrating support effort to current and future operations. This support consists of target development (generated through IPB), immediate tactical production of new intelligence related to particular targets, and BDA of the mission execution results. At higher command echelons, the targeting cycle can span days, while at lower echelons it may span hours or minutes. In MAGTFs with organic fixed-wing aviation, the intelligence support to targeting is driven by the ATO cycle. An important goal is the synchronization of the collection and production phases with the appropriate phases of the PDE&A and ATO cycles to ensure the provision of relevant and timely target intelligence.

APPENDIX A. INTELLIGENCE ESTIMATE FORMAT

An intelligence estimate can be prepared at any level, from the battalion or squadron through the Marine expeditionary force command element and Marine Corps forces headquarters levels. The intelligence estimate should be succinct, yet provide the commander and staff the necessary information for decisionmaking. The scope and detail of an intelligence estimate are governed by the—

- Level of command preparing it.
- Nature of the operation it is intended to support.
- Current availability of intelligence.
- Prior contingency planning.
- Time and resources available.

Whenever possible, the intelligence estimate should clearly present the analysis and conclusions developed during intelligence preparation of the battlespace (IPB). The finished estimate may be in written, graphic, or verbal form, but should always follow the general five-paragraph structure presented in the following pages. Subparagraphs and tabs may be added and omitted based on their relevance to the stated mission. For topics that require a large amount of data, information, and intelligence (i.e., beaches, weapons capabilities, technical characteristics), the salient facts and conclusions should be summarized in the body of the estimate and the detailed data included as a tab.

For a discussion of IPB and the intelligence estimate, see chapter 4. Chapter 5 provides a discussion of the various factors that constitute paragraph 2 of the estimate. Chapter 6 provides a discussion of the factors that constitute paragraph 3.

The sample on page A-2 is the format for an intelligence estimate in support of conventional combat operations. The sample on page A-10 is the format for an intelligence estimate in support of military operations other than war (MOOTW).

SAMPLE FORMAT OF AN INTELLIGENCE ESTIMATE IN SUPPORT OF CONVENTIONAL COMBAT OPERATIONS

(Local variations and modifications may be made as necessary to meet requirements.)

CLASSIFICATION

Copy no.__of__copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date/time of issue
Message reference number

INTELLIGENCE ESTIMATE (NUMBER) (U)

(U) REFERENCES
(a) Maps and charts
(b) Other pertinent intelligence documents and online data bases

Intelligence and Information Cutoff Time Used for this Estimate: (Provide date-time group)

1. (U) Mission. (The command's restated mission as developed during the mission analysis phase of the planning process.)

2. (U) Characteristics of the Area of Operations. (State conditions that exist and indicate the effect of these conditions on enemy capabilities and the assigned mission. Assess the estimated effects of these conditions on both enemy and friendly capabilities and operations.)

a. (U) Military Geography

(1) (U) Topography

(2) (U) Drainage

(3) (U) Vegetation

(4) (U) Surface Materials

(5) (U) Military Aspects of Terrain

(6) (U) Effects of Terrain on Enemy and Friendly Capabilities and Operations

b. (U) Hydrography

(1) (U) Coastline Description

Page number

CLASSIFICATION

CLASSIFICATION

(2) (U) Hydrographic Conditions

(a) (U) Surf

(b) (U) Tides

(c) (U) Currents

(3) (U) Beaches

(4) (U) Effects of Hydrography on Enemy and Friendly Capabilities and Operations

c. (U) Climate and Weather

(1) (U) Type and Characteristics

(2) (U) Temperature

(3) (U) Precipitation

(4) (U) Visibility

(5) (U) Winds

(6) (U) Light Data

(7) (U) Flight Conditions

(8) (U) Effects of Weather on Enemy and Friendly Capabilities and Operations

d. (U) Transportation

(1) (U) Airfields

(2) (U) Helicopter Landing Zones

(3) (U) Port Facilities

(4) (U) Roads

(5) (U) Railroads

(6) (U) Inland Waterways

(7) (U) Effects of Transporation on Enemy and Friendly Capabilities and Operations

CLASSIFICATION

e. (U) Civilian Telecommunications and Media

(1) (U) International

(2) (U) Domestic

(3) (U) Mass Communications. (Types, capabilities, and key facilities.)

(4) (U) Radio

(a) (U) Television

(b) (U) Print Media

(5) (U) Effects of Telecommunications and Media on Enemy and Friendly Capabilities and Operations

f. (U) Economics and Infrastructure

(1) (U) General Economic Activity and Conditions. (Industry, public works and utilities, finance, banking, agriculture, trades and professions, labor force, etc.)

(2) (U) Monetary System

(3) (U) Power and Utilities

(4) (U) Petroleum, Oils, and Lubricants Facilities

(5) (U) Effects of Economics and Infrastructure on Enemy and Friendly Capabilities and Operations

g. (U) Politics

(1) (U) Political System and Climate

(2) (U) Local Political Conditions

(3) (U) Local Political Leaders

(4) (U) Policy and Attitudes Towards the U.S. and the U.S. Military

(5) (U) Effects of Political Situation on Enemy and Friendly Capabilities and Operations

CLASSIFICATION

h. (U) Sociology

(1) (U) Cities and Towns

(2) (U) Population and Distribution of Area and of Key Cities and Towns

(3) (U) Ethnic Composition

(4) (U) Languages

(5) (U) Religions

(6) (U) Customs and Norms

(7) (U) Social Institutions and Attitudes

(8) (U) Effects of Sociological Situation on Enemy and Friendly Capabilities and Operations

i. (U) Health and Medical

(1) (U) Food Supply

(2) (U) Water Supply

(3) (U) Diseases and Other Medical Problems

(4) (U) Plant and Animal Hazards

(5) (U) Sanitation

(6) (U) Medical Facilities

(7) (U) Effects of Health and Medical Situation on Enemy and Friendly Capabilities and Operations

3. (U) Enemy Military Situation

a. (U) Ground Forces

(1) (U) Composition, Organization, and Strengths. (Describe the structure of enemy forces [i.e., order of battle] and describe unusual organizational features, identity, etc. State the number and size of enemy units in and others available for use in the area of operations. Provide estimated combat effectiveness of enemy forces.)

CLASSIFICATION

(2) (U) Disposition, Locations, Movements, and Activities. (Describe the geographic location and latest known activities of enemy forces, including command and control facilities; fire support elements; and other key combat support forces.)

(a) (U) Committed Forces. (For ground forces, include units currently in contact or with which contact is imminent within the unit's area of operations, regardless of the specific friendly course of action. For amphibious or forcible entry operations, committed forces would be those that could immediately engage friendly units at their point of insertion. All fire support assets within range are normally considered committed, regardless of subordination. Conventional military forces are referred to by numbers of unit types [e.g., armor, infantry] two echelons below the friendly unit. Guerrilla or insurgent forces are expressed in terms of total numbers of personnel and fire support weapons.)

(b) (U) Reinforcements. (Describe the enemy's reinforcement capabilities in terms of possible forces and weapons that can react in time to affect the accomplishment of the mission. Factors to be considered include time available to react, terrain, weather, road and rail nets, transportation, replacements, and possible aid from sympathetic or participating neighbors.)

(3) (U) Weapons and Equipment. (Describe the operational capabilities and technical characteristics of major items of equipment in the enemy's inventory.)

(4) (U) Command and Control

(a) (U) Organization

(b) (U) Key Command and Control Nodes

(c) (U) Communications and Information Systems

(5) (U) Logistics. (Describe levels of supply, resupply ability, and capacity of beaches, ports, roads, railways, airfields, and other facilities to support supply and resupply. Consider transportation, hospitalization and evacuation, military construction, labor resources, and maintenance of combat equipment, etc.)

(6) (U) Training, Tactics, Operating Patterns

(7) (U) Capabilities and Effectiveness

Page number

CLASSIFICATION

CLASSIFICATION

b. (U) Naval Forces

(1) (U) Composition, Organization, and Strengths

(2) (U) Disposition, Locations, Movements, and Activities

(3) (U) Weapons and Equipment

(4) (U) Command and Control

(a) (U) Organization

(b) (U) Key Command and Control Nodes

(c) (U) Communications and Information Systems

(5) (U) Logistics

(6) (U) Training; Operational and Tactical Doctrine and Tactics, Techniques, and Procedures; Methods of Operations; and Operating Patterns

(7) (U) Capabilities and Effectiveness

c. (U) Air Forces

(1) (U) Composition, Organization, and Strengths

(2) (U) Disposition, Locations, Movements and Activities

(3) (U) Weapons and Equipment

(4) (U) Command and Control

(a) (U) Organization

(b) (U) Key Command and Control Nodes

(c) (U) Communications and Information Systems

(5) (U) Logistics

(6) (U) Training; Operational and Tactical Doctrine and Tactics, Techniques, and Procedures; Methods of Operations; and Operating Patterns

(7) (U) Capabilities and Effectiveness

CLASSIFICATION

d. (U) Air Defense Forces

(1) (U) Composition, Organization, and Strengths

(2) (U) Disposition, Locations, Movements, and Activities

(3) (U) Weapons and Equipment

(4) (U) Command and Control

(a) (U) Organization

(b) (U) Key Command and Control Nodes

(c) (U) Communications and Information Systems

(5) (U) Logistics

(6) (U) Training; Operational and Tactical Doctrine and Tactics, Techniques, and Procedures; Methods of Operations; and Operating Patterns

(7) (U) Capabilities and Effectiveness

e. (U) Paramilitary and Security Forces

(1) (U) Composition, Organization, and Strengths

(2) (U) Disposition, Locations, Movements, and Activities

(3) (U) Weapons and Equipment

(4) (U) Command and Control

(a) (U) Organization

(b) (U) Key Command and Control Nodes

(c) (U) Communications and Information Systems

(5) (U) Logistics

(6) (U) Training; Operational and Tactical Doctrine and Tactics, Techniques, and Procedures; Methods of Operations and Operating Patterns

(7) (U) Capabilities and Effectiveness

f. (U) Command and Control Warfare Capability

Page number

CLASSIFICATION

CLASSIFICATION

(1) (U) Intelligence, Counterintelligence, and Reconnaissance Capabilities

(2) (U) Electronic Warfare Capabilities

(3) (U) Psychological Warfare Capabilities

(4) (U) Deception Capabilities

(5) (U) Operational Security Capabilities

g. (U) Nuclear, Biological and Chemical Capabilities

h. (U) Night Combat Capabilities

i. (U) Unconventional Warfare Capabilities (e.g., guerrilla, subversion, sabotage, terrorism)

4. (U) Capabilities and Analysis. (List separately each enemy capability that can affect the accomplishment of the assigned mission. Each enemy capability should contain information on what the enemy can do, where they can do it, when they can start it and get it done, and what strength they can devote to the task. Analyze each capability in light of the assigned mission, considering applicable factors from paragraphs 2 and 3, and attempt to determine and give reasons for the estimated probability of adoption by the enemy. Examine the enemy's capabilities by discussing the factors that favor or militate against its adoption by the enemy. The analysis of each capability should also include a discussion of enemy strengths and vulnerabilities associated with that capability. Also, the analysis should include a discussion of any indications that point to possible adoption of the capability. Finally, state the estimated effect the enemy's adoption of each capability will have on the accomplishment of the friendly mission. The term "capabilities" includes not only the general courses of action open to the enemy (e.g., attack, defend, withdraw), but also the particular courses of action possible under each general course of action. These courses of action should correspond exactly to enemy course of action models developed during step 4 of IPB.)

CLASSIFICATION

5. (U) Conclusions and Vulnerabilities. (State conclusions resulting from discussion in paragraph 4 to include: enemy centers of gravity, critical and other vulnerabilities and estimated exploitability of these by friendly forces, enemy courses of action beginning with the most probable and continuing down the list in the estimated order of probability, and the estimated effects adoption of each capability would have on the friendly mission.)

/s/ _____
_____

TABS: (omit or add other tabs as required)
A - Tactical Study of Terrain
B - Beach Studies
C - Climatology Study
D - Airfield Studies
E - Helicopter Landing Zone and Drop Zone Studies
F - Port Studies
G - Lines of Communications Study
H - Order of Battle Study

SAMPLE FORMAT OF AN INTELLIGENCE ESTIMATE IN SUPPORT OF MILITARY OPERATIONS OTHER THAN WAR

CLASSIFICATION

Copy no.__of__copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date/time of issue
Message reference number

INTELLIGENCE ESTIMATE (NUMBER) (U)

(U) REFERENCES
(a) Maps and charts
(b) Other pertinent intelligence documents and online data bases

Intelligence and Information Cutoff Time Used for this Estimate: (Provide date-time group)

1. (U) Mission. (The command's restated mission as developed during the mission analysis phase of the planning process.)

2. (U) Characteristics of the Area of Operations. (Discuss characteristics of the host nation [HN], the area, and their probable effects upon the threat, the mission force, and the host government.)

a. (U) Geography

(1) (U) Strategic Location

(a) (U) Neighboring Countries and Boundaries

(b) (U) Natural Defenses, Including Frontiers

(c) (U) Points of Entry and Strategic Routes

(2) (U) Size and Dimensions

(3) (U) Relief

(4) (U) Beach Data

(5) (U) Hydrography

(a) (U) Coastal

Page number

CLASSIFICATION

CLASSIFICATION

(b) (U) Lakes

(c) (U) Rivers

(6) (U) Land Use

(7) (U) Geological Basics

(8) (U) Vegetation

(9) (U) Water Sources

(10) (U) Natural Foods

(11) (U) Population Centers

(12) (U) Wildlife

b. (U) Climate and Weather

(1) (U) Type and Characteristics

(2) (U) Temperature

(3) (U) Precipitation

(4) (U) Visibility

(5) (U) Winds

(6) (U) Light Data

(7) (U) Flight Conditions

(8) (U) Seasonal Effects of Weather on Terrain and Visibility

c. (U) Demographics

(1) (U) History

(2) (U) Ethnic Composition

(3) (U) Languages

(4) (U) Social System

(5) (U) Education

CLASSIFICATION

(6) (U) Living Conditions

(7) (U) Cultural Customs

(8) (U) Religions

(9) (U) Taboos

(10) (U) Grievances

(11) (U) Psychology. (Behavior patterns and motivating factors.)

d. (U) Transportation

(1) (U) Airfields

(2) (U) Helicopter Landing Zones

(3) (U) Port Facilities

(4) (U) Roads

(5) (U) Railroads

(6) (U) Inland Waterways

e. (U) Civilian Telecommunications and Media

(1) (U) International

(2) (U) Domestic

(3) (U) Mass Communications Types, Capabilities, and Key Facilities

(a) (U) Radio

(b) (U) Television

(c) (U) Print Media

f. (U) Politics. (Address existing situation, effects on threat, HN, and military force.)

(1) (U) National Government

(a) (U) Structure

CLASSIFICATION

(b) (U) Regional and/or International Role

(c) (U) Degree of Popular Support

(2) (U) Political Parties. (Both sanctioned and unsanctioned.)

(3) (U) Foreign Dependence or Alliances

(4) (U) Controls and Restrictions

(5) (U) Legal System. (Civil and religious.)

(6) (U) Grievances

g. (U) Economics. (Address existing situation, effects on threat, HN, and mission force.)

(1) (U) Current Value of Currency and Wage Scales

(2) (U) Financial Structure to Include National and International

(3) (U) Foreign Dependence

(a) (U) Assistance Programs

(b) (U) Foreign-Owned Businesses and Enterprises in Country

(c) (U) Trade Agreements

(4) (U) Agriculture and Domestic Food Supply

(5) (U) Natural Resources and Degree of Self-Sufficiency

(6) (U) Industry

(a) (U) Types

(b) (U) Production Levels

(c) (U) Consumer Demands

(d) (U) Unions

(7) (U) Black Market and Illicit Trades. (Drugs, weapons, etc.)

(8) (U) Technology

(a) (U) Capabilities

CLASSIFICATION

(b) (U) Expertise

h. (U) Health and Medical

(1) (U) Food Supply

(2) (U) Water Supply

(3) (U) Diseases and Other Medical Problems

(4) (U) Plant and Animal Hazards

(5) (U) Sanitation

(6) (U) Medical Facilities

3. (U) Threats. (For each category of threat, except medical/environmental and natural disasters, discuss organization and leadership, to include composition; strength and dispositions; recent and present significant activities, strengths and weaknesses; and relationships with other threat categories.)

a. (U) Conventional

b. (U) Insurgent

c. (U) Clans, Tribes, or Factions

d. (U) Terrorist

e. (U) Drug Producers or Traffickers

f. (U) Criminal Organizations

g. (U) Third-Party Nation and External

h. (U) Civil Unrest

i. (U) Medical and Environmental

j. (U) Natural Disasters

4. (U) Capabilities and Analysis. (List current threat capabilities and discuss in regard to probability of adoption.)

a. (U) Enumeration. (Includes what, where, when, and how, for each category of threat.)

CLASSIFICATION

(1) (U) Basic Capabilities

(a) (U) Conventional

(b) (U) Insurgent

(c) (U) Clans, Tribes, or Factions

(d) (U) Terrorist

(e) (U) Drug Producers or Traffickers

(f) (U) Criminal Organizations

(g) (U) Third-Party Nation and External

(h) (U) Civil Unrest

(i) (U) Medical and Environmental

(j) (U) Natural Disasters

(2) (U) Supporting Capabilities. (Includes intelligence, security, recruitment, organization, training, finance, and logistics.)

(a) (U) Conventional

(b) (U) Insurgent

(c) (U) Clans, Tribes, or Factions

(d) (U) Terrorist

(e) (U) Drug Producers or Traffickers

(f) (U) Criminal Organizations

(g) (U) Third-Party Nation and External

(h) (U) Civil Unrest

(i) (U) Medical and Environmental

(j) (U) Natural Disasters

b. (U) Analysis and Discussion. (Includes evidence supporting or rejecting the adoption of each capability.)

CLASSIFICATION

5. (U) HN Security

a. (U) Situation. (For each subparagraph, describe organization and leadership; strength and disposition; recent and present significant activities; and strengths and weaknesses.)

(1) (U) Public Order or Internal Security Forces

(2) (U) Armed Forces

(3) (U) External Support Forces and Dependency. (Regional peacekeeping, foreign forces, mercenaries, etc.)

b. (U) Capabilities. (What, where, when, how for basic capabilities and supporting capabilities.)

(1) (U) Public Order or Internal Security Forces

(2) (U) Armed Forces

(3) (U) External Support Forces and Dependency

c. (U) Analysis and Discussion

6. (U) Friendly and Neutral Third-Party

a. (U) Situation. (For each subparagraph, as defined in paragraph 5.a.)

(1) (U) Embassies and Consulates

(2) (U) Military

(3) (U) Business Interests

(4) (U) Nongovernmental Organizations (NGO) and/or Private Voluntary Organizations (PVO)

b. (U) Capabilities. (As defined in paragraph 5.b.)

(1) (U) Embassies and Consulates

(2) (U) Military

(3) (U) Business Interests

CLASSIFICATION

(4) (U) NGO/PVO

c. (U) Analysis and Discussion

7. (U) Conclusions and Vulnerabilities

a. (U) Effects of the Operational Environment. (State total effect of the area of operations upon courses of action.)

b. (U) Probable Threat Courses of Action. (Listed in order of relative probability of adoption.)

c. (U) Threat Vulnerabilities. (List exploitable threat vulnerabilities.)

/s/_____

_____

TABS: (as necessary)

APPENDIX B. WEATHER CRITICAL VALUES

Establishing weather critical values is essential to weather effects analysis on threat and friendly operations. Critical values provide the parameters for assessing the exact impact of particular weather conditions. Critical values can be established for personnel, specific types of equipment, and types of military operations and tailored to the echelon of command, the composition of the force, and the likely operations the force will be expected to conduct. For example, a MEF may be concerned with general categories such as amphibious operations, fixed-wing aviation operations, and visual reconnaissance operations. A battalion may be concerned with foot mobility, line-of-sight restrictions, and effects on indirect fire support, while an unmanned aerial vehicle unit might be more concerned with visibility, cloud cover, precipitation, and temperatures aloft. Each level of command should focus on the unit mission-essential functions and specific equipment categories.

For each category or function, only weather elements that may have an impact are listed. For example, troops operating in a desert environment (depending on the desert and time of year) are generally not affected by snowfall. Similarly, windchill is not a critical factor when assessing fixed-wing aviation operations, but windchill may affect ground crews.

For each weather element selected, critical values are established that define impact levels. In table B-1, the levels of impact are defined as favorable, marginal, and unfavorable or as unrestricted, restricted, and severely restricted. An effective technique is to assign each level a color-code, such as green, yellow, or red, that can be transferred easily to a graphic weather effects matrix.

The companion weather effects matrix lists the same functions. If a weather element falls within the unfavorable or severely restricted range, the weather effects matrix is color-coded red for that function during the period of time the unfavorable element is forecast to occur. Weather elements that result in a marginal or unfavorable assessment are noted on the weather effects matrix (see chapter 6, figure 6-3).

The MEF command element intelligence section personnel, assisted by the G-2 section's staff weather officer, the intelligence support coordinator, and intelligence battalion personnel, usually compile the weather critical values chart. The commander, operations staff, and friendly force's functional elements define selected functions, weather elements, and critical values. Within a MAGTF, for example, the air officer and aviation combat element should establish weather elements that may impact aviation operations and platforms and define the values that constitute impact levels. Within an infantry battalion, the artillery liaison officer is the best source for effects on supporting fires and artillery delivered munitions.

Regardless of who compiles the list, the commander defines weather intelligence elements that are critical to decisionmaking. The identified weather elements and their established critical values are tracked closely and serve as the basis for weather effects graphics and updates. Like other intelligence requirements, the weather elements and their critical values must be reevaluated as the mission or season changes.

Unit intelligence section personnel develop mission, type unit, and equipment-focused critical values lists during peacetime operations, to include those equipment types and units which will normally be attached or in direct support during operations. Upon receipt of an alert or execute order, these critical values lists can then be refined and tailored to the forces, mission,

and environment assigned. See MCWP 3-35.7, *MAGTF Meteorological and Oceanographic Support,* and FM 34-81-1, *Battlefield Weather Effects*, for additional doctrine and tactics, techniques, and procedures guidance.

Weather critical values are established for threat as well as friendly forces. Due to differences in weapons and personnel characteristics, the same weather may have differing effects on the threat. For example, threat tanks without thermal sights will be severely restricted during periods of reduced visibility, while friendly tanks may be only marginally affected. Comparing the varying effects of weather on friendly and threat forces helps to identify advantages and vulnerabilities that may be exploited by either side.

Table B-1. Weather Critical Values Chart.

Function	Weather Element	Favorable (Unrestricted)	Marginal (Restricted)	Unfavorable (Severely Restricted)
Maneuver: Mobility (track vehicles, day)	visibility rainfall snow depth	> 1.5 km < 0.1 in/hr < 12 in	0.8 to 1.5 km > 0.5 in/hr > 12 to 20 in	< 0.8 km > 0.5 in/hr > 20 in
Maneuver: Mobility (track vehicles, night)	visibility rainfall snow depth	> 0.2 km < 0.1 in/hr < 12 in	0.1 to 0.2 km 0.1 to 0.5 in/hr 12 to 20 in	<0.1 km > 0.5 in/hr > 20 in
Maneuver: Mobility (dismounted infantry)	visibility rainfall snow depth temperature windchill	> 0.3 km < 0.1 in/hr < 3 in < 89.6 °F/32 °C > 32 °F/0 °C	0.1 to 0.3 km 0.1 to 0.5 in/hr 3 to 6 in > 89.6 °F/32 °C 32° F/0 °C to -22° F/-30° C	< 0.1 km > 0.5 in/hr > 6 in ---------- < -22 °F/-30 °C
Fire Support (155mm)	visibility ceiling surface wind snow depth	> 5.0 km > 800 ft < 35 knots < 4.0 in	1.5 to 5.0 km 500 to 800 ft 35 to 50 knots 4.0 to 6.0 in	< 1.5 km < 500 ft > 50 knots > 6 in
Fire Support (close air support)	visibility ceiling	> 8.0 km > 3000 ft	5.0 to 8.0 km 500 to 3000 ft	< 5.0 km < 500 ft
Aviation (rotary wing)	visibility ceiling surface wind precipitation	> 1.5 km > 500 ft < 20 knots none	0.4 to 1.5 km 300 to 500 ft 20 to 30 knots light	< 0.4 km < 300 ft > 30 knots freezing rain or hail
Aviation (air defense)	visibility ceiling rainfall	> 5.0 km > 5000 ft < 0.5 in/hr	3.0 to 5.0 km 3000 to 5000 ft 0.5 to 1.0 in/hr	< 3.0 km < 3000 ft > 1.0 in/hr

°C=degree Celsius °F=degree Fahrenheit ft=feet in/hr=inches per hour km=kilometer

APPENDIX C. TACTICAL INDICATORS

Indicators are any positive or negative evidence of threat activity or any characteristic of the operations area that points toward threat capabilities, vulnerabilities, or intentions. Each indicator is integrated with other factors, indicators, information, and intelligence before patterns are detected and threat intentions are established. Intelligence analysts develop indicators to—

- Assist in discerning answers to a commander's priority intelligence requirements and intelligence requirements.
- Correlate particular events or activities with probable threat courses of action.
- Determine what events or activities must occur for a threat to follow a particular course of action (COA).

As named areas of interest and the event template are developed during intelligence preparation of the battlespace (IPB), analysts develop corresponding indicators which, when detected, will assist in rapidly identifying the particular COA the threat may adopt. While some indicators may apply to most or all of the possible threat courses of action, other indicators may be unique to a particular COA. Well-developed indicator lists also aid in detecting threat deception operations. By comparing indicators, intelligence, and operations reporting, the analyst arrives at an accurate picture of the battlespace and intelligence estimates.

Indicators may be present for more than one COA in the same threat force. For example, a threat division forced to withdraw (and providing indicators accordingly) may employ a subordinate unit (brigade, regiment, or battalion) in a delaying action to cover the withdrawal. Units in contact with the delaying force may characterize the indicators as delaying in nature, but the threat force overall is withdrawing. Indicators from all sources must be analyzed to assess the threat's true intentions.

The tables on the following pages provide some intelligence indicators commonly associated with operations. These lists are intended to provide a basis from which intelligence personnel can develop indicators specific to the threat and environment they are faced with. No one indicator can stand alone; indicators must be examined within the context of the doctrine, tactics, and structure of the specific threat force.

OFFENSIVE INDICATORS

Activity	Explanation
Massing of maneuver elements, armor, artillery, and logistical support.	May strengthen the main effort by weakening areas of secondary importance.
Deployment of combat elements on a relatively narrow frontage (not forced by terrain).	May provide maximum combat power at the point of attack by reducing frontages.
Massing of indirect fire support assets.	May indicate initiation of a main attack.
Extensive artillery preparation of up to 50 minutes in duration or longer.	Indicates preparation preceding an attack.
Dispersal of tanks and self-propelled or towed artillery to forward units.	Can indicate formation of combined arms assault formations with tanks accompanying the leading maneuver elements and artillery following in bounds.
Surface-to-surface missile units located forward.	Provides depth to threat offensive operations; places friendly support and rear areas in range. May also indicate, when employed alone, harassing or special weapons delivery.
Antiaircraft artillery and mobile surface-to-air missiles located well forward with maneuver elements.	Provides increased protection to massed forces prior to attack; extends air defense umbrella forward as units advance.
Demonstrations and feints.	May precede an attack; may deceive actual point of attack.
Establishment and strengthening of counter-reconnaissance screen.	Covers assembly and preparation of forces for attack.
Concentration of mass toward one or both flanks within the forward area.	May indicate intent for single or double envelopment, particularly if massing units are armor-heavy.
Increased patrolling (ground reconnaissance).	May indicate efforts to gather detailed information regarding friendly dispositions prior to attack.
Command posts located well forward; mobile command posts identified.	Enhances command and control during offensive operations.
Movement of noncombatants out of the combat zone.	Removes noncombatants, which hinder rapid forward movement of follow-on forces.
Extensive conduct of drills and rehearsals in rear areas.	Often indicates major attacks, particularly against fortified positions or strongly defended natural or man-made barriers, which require rehearsal of specialized tactics and skills.
Increased activity in supply, maintenance, and motor transport areas.	May indicate movement of additional forces to the front to sustain major attack.
Increased aerial reconnaissance (including unmanned aerial vehicles).	Refines threat's intelligence picture prior to operations.
Establishment of forward arming and refueling points, auxiliary airfields, or activation of inactive airfields.	Increases sortie rate and turnaround time by forward basing aircraft and aviation sustainment.
Clearing lanes through own obstacles.	Facilitates forward movement and grouping of assault units, particularly at night, usually immediately precedes an attack.
Reconnaissance, marking, and destruction of opponent's obstacles.	Facilitates movement of assault echelons through opposing obstacles.
Gap-crossing equipment (e.g., swimming vehicles, bridging, ferries, boats) located in forward areas (provided there is a water or large gap obstacle).	Maintains tempo of the assault echelons when faced with significant gap obstacles, normally concentrated with main effort.
Staging of airborne, air assault, or special forces with modes of transportation/insertion.	Such elements are used to provide depth to the assault and target friendly centers of gravity.
Increased signals traffic or radio silence.	May indicate intent to conduct offensive operations. (Increased traffic may be an attempt to deceive. Radio silence denies information derived from opponent's signals intelligence.
Signals intelligence and electronic warfare assets located forward.	Provides enhanced electronic attack and electronic warfare support for assault forces.

DEFENSIVE INDICATORS

Activity	Explanation
Preparation of battalion and company defensive areas consisting of company and platoon strong points.	Indicates intent for holding terrain with defense in depth, normally supported by armored counterattack forces.
Extensive preparation of field fortifications, obstacles, and minefields.	Indicates strong positional defense.
Attachment of additional antitank assets to frontline defensive positions.	Indicates intent to contest friendly armor in forward positions, and attempts to attrite and channel friendly armor into engagement areas for armor counterattack forces.
Formation of antitank strong points in depth along avenues of approach.	May allow penetration of friendly armor into rear engagement areas.
Preparation of alternate artillery positions.	Increases survivability of artillery in the defense.
Concentration of armor units in rear area assembly areas.	Indicates holding armor units in reserve for possible counterattack or counteroffensive.
Presence of concentrated antitank reserves.	Provides quick reaction capability against armor penetrations.
Displacement of logistics and medical units towards the rear.	Facilitates maneuver defense and counterattack.
Prestocking of ammunition, supplies, and engineer or pioneer equipment in forward positions.	Reduces the burden on logistics during the battle, reduces vulnerability of interdiction of supplies, and ensures strong points can survive for reasonable periods if bypassed or cut off.
Increased depth from the forward line of troops of artillery and surface-to-surface missile units.	Allows continued employment of artillery during maneuver defense without significant rearward displacement.
Increased use of land line communications.	Implies intent to remain in position because landlines are less vulnerable to electronic warfare.
Presence of dummy positions, command posts, and weapons.	Complicates friendly targeting and analysis of actual threat locations and strengths.
Air defense more concentrated in rear areas.	Indicates location of numerous high-value targets (e.g., armor, logistics, artillery, command posts) that dictates strong air defenses in rear areas.

DELAYING INDICATORS

Activity	Explanation
Withdrawal from defensive position(s) before becoming heavily engaged.	Indicates units' delaying actions to avoid decisive engagements.
Numerous local counterattacks with limited objectives; counterattacks broken off before position is restored.	Assists in disengaging units in contact, rather than restoring positions.
Units leapfrogging to new defensive positions.	Indicates units engaging then conducting local withdrawals to new positions while another force takes up the engagement
Maximum firepower located forward; firing initiated at long ranges.	Intends to inflict casualties, slow advance, and provide sufficient combat power to avoid decisive engagement.
Extremely large unit frontages as compared to normal defense.	Indicates delaying actions to economize force, allowing larger formations to withdraw.
Chemical or biological agent weapons in forward areas.	Causes significant delays to the advancing force when employed as barriers or in minefields.
Identification of dummy positions and minefields.	Causes delays by forcing the advancing force to determine whether minefields are active or inert.

WITHDRAWAL INDICATORS

Indications of threat intent to withdraw are often the same as those for delaying actions, with the addition of the following indicators.

Activity	Explanation
Systematic destruction of bridges, communications facilities, and other assets.	Denies the advancing force the use of infrastructure and installations in withdrawal areas.
Establishment of a covering force or rear guard.	Covers the withdrawal of the main body; usually consists of a sub-element of the main force; and usually engages only the rear guard element.
Increased rearward movement noted at night, particularly during inclement weather.	Attempts to withdraw units under the concealment of darkness and weather.
Minimal presence of logistic and medical units. Destruction of dumps and depots.	Indicates withdrawal of nonessential logistic and medical elements and the inability to move depots and dumps.
Establishing and marking withdrawal routes and traffic control points.	Facilitates the rapid movement of forces rearward.
Preparation of new defensive positions beyond supporting range of present positions.	Indicates attempt to establish new positions along suitable terrain prior to the arrival of deliberately withdrawn forces.
Increased engineer activity and stockpiling of explosives in the threat rear area near bridges, tunnels, built-up areas, etc.	Facilitates maintenance of lines of communications for own forces; indicates demolition of infrastructure in front of opposing force.
Rearward movement of long-range artillery.	Positions long-range artillery before withdrawal takes place.
Activation of command posts well removed (beyond doctrinal norms) from the present battle area.	Creates command and control nodes in the new position or assembly area to command and control arriving forces.

MILITARY OPERATIONS OTHER THAN WAR INDICATORS

Given the wide range of military operations other than war (MOOTW), the possible indicators of various activities can be enormous. However, most MOOTW evolutions still involve the requirement to identify risks to friendly forces. By their nature, MOOTW are generally concerned with indigenous populations, regardless of the nature of the mission. The following indicators focus on those indicators associated with possible threats emerging from indigenous populations. These lists provide the analyst with a point of departure for developing case specific indicators.

THREAT POPULATION INDICATORS

General Activities
Identification of agitators, insurgents, militias or criminal organizations, their supporters, and sympathizers who suddenly appear in, or move out of, an area.
New faces in a rural community.
Unusual gatherings among the population.
Disruption of normal social patterns.
Mass urban rural migration or vice versa.
Massing of combatants of competing power groups.
Increase in the size of embassy or consulate staffs from a country or countries which support indigenous disaffected groups, particularly those hostile to the United States and/or the current intervention.
Increase in neighboring countries of staff and activities at embassies or consulates of countries associated with supporting indigenous disaffected groups.
Increased travel by suspected subversives or leaders of competing power bases to countries hostile to the United States or opposed to the current intervention.
Influx of opposition resident and expatriate leaders into the operations area.
Reports of opposition or disaffected indigenous population receiving military training in foreign countries.
Increase of visitors (e.g., tourists, technicians, businessmen and businesswomen, religious leaders, officials) from groups or countries hostile to the United States or opposed to the current intervention.
Close connections between diplomatic personnel of hostile countries and local opposition groups.
Communications between opposition groups and external supporters.
Increase of disaffected youth gatherings.
Establishment of organizations of unexplained origin and with unclear or nebulous aims.
Establishment of a new organization to replace an existing organizational structure with identical aims.
Appearance of many new members in existing organizations such as labor unions.
Infiltration of student organizations by known agitators.
Appearance of new organizations stressing grievances or interests of repressed or minority groups.
Reports of large donations to new or revamped organizations.
Reports of payment to locals for engaging in subversive of hostile activities.
Reports of the formation of opposition paramilitary or militia organizations.
Reports of lists of targets for planned opposition attacks.
Appearance of “professional” agitators in gatherings or demonstrations that result in violence.
Evidence of paid and armed demonstrators’ participation in riots.
Significant increase in thefts, armed robberies, and violent crime in rural areas; increase in bank robberies in urban areas.

Opposition-Directed Activities
Refusal of population to pay or unusual difficulty to collect rent, taxes, or loan payments.
Trends of demonstrated hostility toward government forces and/or mission force.
Unexplained population disappearance from or avoidance of certain areas.
Unexplained disappearance or dislocation of young people.
Reported incidents of attempted recruitment to join new movements or underground organizations.
Criminals and disaffected youth who appear to be acting with and for the opposition.
Reports of extortion and other coercion by opposition elements to obtain financial support from the population.
Use of fear tactics to coerce, control, or influence the local population.
Reports of host nation government and/or mission force facilities and personnel surveillance.
Activities Directed Against the Government/Mission Force
Failure of police and informer nets to report accurate information, which may indicate sources are actively supporting opposition elements or are intimidated.
Decreasing success of government law enforcement or military infiltration of opposition or disaffected organizations.
Assassination or disappearance of government sources.
Reports of attempts to bribe or blackmail government officials, law enforcement employees, or mission personnel.
Reports of attempts to obtain classified information from government officials, government offices, or mission personnel.
Classified information leaked to the media.
Sudden affluence of certain government and law enforcement personnel.
Recurring failure of government or mission force raids on suspected opposition organizations or illegal activities apparently due to forewarning.
Increased hostile or illegal activity against the government, its law enforcement and military organizations, foreigners, minority groups, and/or competing political, ethnic, linguistic, or religious groups.
Demonstrations against government forces, minority groups, or foreigners designed to instigate violent confrontations with government or mission forces.
Increased antigovernment or mission force rhetoric in local media.
Occurrence of strikes in critical areas intended to cast doubt on the government's ability to maintain order and provide for the people.
Unexplained loss, destruction, or forgery of government identification cards and passports.
Recurring unexplained disruption of public utilities.
Reports of terrorist acts or extortion attempts against local government leaders, businessmen, and/or businesswomen.
Murder or kidnapping of government, military, and law enforcement officials or mission force personnel.
Closing of schools.

PROPAGANDA INDICATORS

General Propaganda Activities
Dissident propaganda from unidentified sources.
Increase in the number of entertainers with a political message.
Increase of political themes in religious services.
Increase in appeals directed at intensifying general ethnic or religious unrest in countries where ethnic or religious competition exists.
Increase of agitation on issues for which there is no identified movement or organization.
Renewed activity by dissident or opposition organizations thought to be defunct or dormant.
Circulation of petitions advocating opposition or dissident demands.
Appearance of opposition slogans and pronouncements by word-of-mouth, graffiti, posters, leaflets, etc.
Propaganda linking local ethnic groups with those in neighboring countries or regions.
Clandestine radio broadcasts intended to appeal to those with special grievances or to underprivileged ethnic groups.
Use of bullhorns, truck-mounted loudspeakers, and other public address equipment in “spontaneous” demonstrations.
Presence of nonmedia photographers among demonstrators.
Rallies to honor “martyred” opposition personnel. Mass demonstrations honoring local dissident heroes or dates significant to the opposition.
Nationwide strikes called to demonstrate the strength of the opposition movement(s).
Propaganda Activities Directed Against the Established Government
Attempts to discredit or ridicule national or public officials.
Attempts to discredit the judicial and law enforcement system.
Characterization of government leaders as puppets and tools of foreign intervention forces.
Agitation against government projects and plans.
Radio propaganda from foreign countries that is aimed at the target country’s population and accuses the target country’s government of failure to meet the people’s needs.
Propaganda Activities Directed Against the Mission Force and Host Nation Military and Law Enforcement
Spreading accusations that the host nation military and police are corrupt and out of touch with the people.
Spreading accusations that mission force personnel will introduce customs or attitudes that are in opposition to local cultural or religious beliefs.
Character assassinations of mission, military, and law enforcement officials.
Demands to remove strong anti-opposition or anticrime military and law enforcement leaders from office.
Calls for the population to cease cooperating with the mission force and/or host nation military and law enforcement.
Deliberate incidents to provoke mission, military, or police reprisals during demonstrations or strikes.
Widespread hostile media coverage of even minor criminal violations or incidents involving mission force personnel.
Accusations of brutality or ineffectiveness or claims that mission or government forces initiated violence following confrontations.
Publication of photographs portraying repressive and violent acts by mission force or government forces.
Refusal of businessmen, businesswomen, and/or shop owners to conduct business with mission force personnel.

Propaganda Activities Directed Against the Education System
Appearance of questionable doctrine and teachings in the educational system.
Creation of ethnic, tribal, religious, or other interest group schools outside the government educational system, which propagate opposition themes and teachings.
Charges that the educational system is only training youth to do the government's bidding.
Student unrest manifested by new organizations, proclamations, demonstrations, and strikes against authority.

COMMODITIES INDICATORS

Food-Related Activities
Diversion of crops or meat from markets.
Unexplained shortages of food supplies when there are no reports of natural causes.
Increased reports of foodstuffs pilfering.
Sudden increase in food prices, possibly indicating an opposition-levied tax.
Unwillingness of farmers to transport food to population centers, indicating a fear of traveling highways.
Spot shortages of foodstuffs in regions or neighborhoods associated with a minority group or weaker competing interest group, while food supplies are generally plentiful in other areas. Conversely, sudden local shortages of foodstuffs in rural areas may indicate the existence of an armed opposition group operating in that region.
Sudden increase of meat in markets, possibly indicating slaughtered livestock because of a lack of fodder to sustain them.
Appearance of emergency relief supplies for sale in black markets, possibly indicating diversion from starving population.
Appearance of relief supplies for sale in normal markets in a country or region recently suffering from large-scale hunger, which may indicate the severity of the food crisis is diminishing.
Arms and Ammunition-Related Activities
Increased loss or theft of weapons from military and police forces.
Discovery of arms, ammunition, and explosives being clandestinely manufactured, transported, or cached.
Attacks on patrols resulting in the loss of weapons and ammunition.
Increased purchase of surplus military goods.
Sudden increase in prices for arms and ammunition on the open market.
Reports of large arms shipments destined for neighboring countries, but not intended for that government.
Reports of known arms traffickers establishing contacts with opposition elements.
Increase in armed robberies.
Reports of thefts or sudden shortages of chemicals, which could be used in the clandestine manufacture of explosives.
Reports of large open-market purchases of explosives-related chemicals without an identifiable industrial user.
Appearance of manufactured or smuggled arms from noncontiguous foreign countries.
Clothing-Related Activities
Unusual, systematic purchase or theft of clothing materials, which could be used for the manufacture of uniforms or footwear.
Unusual scarcity of clothing or material used in the manufacture of clothing or footwear.
Distribution of clothing to underprivileged or minority classes by organizations of recent or suspect origin.
Discovery of caches of uniforms and footwear or the materials which could be used to manufacture uniforms and footwear.
Increase of males in the streets wearing military style clothing or distinctive markings.

Medicine-Related Activities
Large-scale purchasing or theft of drugs and medicines or the herbs used to manufacture local remedies.
Scarcity of drugs and medical supplies on the open or black markets.
Diversion of medical aid donations.
Discovery of caches of medical supplies.
Communications-Related Activities
Increase in the purchase and use of radios.
Discovery of caches of communications equipment.
Unusual increase in amateur radio or cellular telephone communications traffic.

ENVIRONMENT-RELATED INDICATORS

Rural Activities
Evidence of increased foot traffic in the area.
Increased travel within and into remote or isolated areas.
Unexplained trails and cold campsites.
Establishment of new, unexplained agricultural areas, or recently cleared fields.
Unusual smoke, possibly indicating the presence of a campsite or a form of communication.
Concentration of dead foliage in an area, possibly indicating use of camouflage.
Presence of foot traps, spikes, boobytraps, or improvised mines along routes and trails.
Urban Activities
Apartments, houses, or buildings being rented, but not lived in as homes.
Slogans written on walls, bridges, and streets.
Defacement of government and mission force information signs.
Sabotage of electrical power network; pollution of urban area's water supply.
Terrorist acts against physical targets such as bridges, dams, airfields, or buildings.
Change of residence of suspected agitators or opposition leaders.
Discovery of message dead-drops.
Increased smuggling of currency, gold, gems, narcotics, medical supplies, and arms into urban centers.
Appearance of abnormal amounts of counterfeit currency.
Increase in bank robberies.
Work stoppages or slowdowns in essential industries.
Marked decline in product quality in essential industries.
Marked increase in equipment failures in essential industries.
Unexplained explosions in essential utilities and industries.
Establishment of roadblocks or barricades around neighborhoods associated with opposition elements.
Attempts to disrupt public transport through sabotage.
Malicious damage to industrial products or factory machinery.

APPENDIX D. BATTLE DAMAGE ASSESSMENT REPORT FORMAT

The periodic summary battle damage assessment (BDA) report on page D-2 is an example format that may be used by MEF major subordinate command intelligence personnel to provide consolidated Phase I BDA, physical damage assessment, to the intelligence battalion's production and analysis cell. The report is a compilation of BDA reporting from subordinate elements as well as BDA obtained at the MSC level during the designated time period. The theater intelligence tactics, techniques, and procedures or the joint task force commander establishes BDA reporting formats for the joint task force, theater, and national level.

Normally, the aviation combat element is responsible for providing BDA on any air tasking order-related missions, while the ground combat element focuses on their subordinate elements' engagement results, to include observed close air support effects.

The target intelligence and BDA team, production and analysis company, intelligence battalion, is responsible for—

- Consolidating, deconflicting, and refining BDA reports.
- Introducing additional information and intelligence obtained from other sources.
- Preparing the Phase I BDA, physical damage assessment, for the MEF commander.
- Preparing Phase II BDA, functional damage assessment, based on the consolidated reporting from subordinate, higher, and adjacent commands.
- Adjusting the MEF order of battle data bases to reflect combat losses.
- Developing the combat strength assessment for each unit.

BATTLE DAMAGE ASSESSMENT REPORT FORMAT EXAMPLE

SUBJECT: 6 HR BDA REPORT (SUBMIT TO INTELLIGENCE BATTALION'S TARGET INTELLIGENCE/ BDA TEAM, P&A CELL, AT SPECIFIED TIMES.)

REPORTING UNIT:

REPORTING PERIOD: (FROM/TO)

ENEMY UNIT OR FACILITY #1: (DOWN TO BDE NAME FOR MANEUVER, BN FOR FIRE SUPPORT, OR AS DIRECTED IN UNIT SOP OR OPORD. REPEAT THIS SECTION FOR EACH UNIT OR FACILITY.)

UIC OR BE#: DHGKNXXXXX

DAMAGED/DESTROYED:

	LOC	TYPE	#DEST	#DMGD/EXTENT
1. ARMOR:				
2. FIRE SUPPORT:				
3. TRUCKS:				
4. AIR DEFENSE:				
5. C2 SYSTEMS:				
6. MOB/CNTRMOB: (ENGINEERS ASSETS, BRIDGES, LINES OF COMMUNICATIONS, MINES, ETC.)				

7. CSS:

	LOC	WIA	KIA
8. PERSONNEL:			

REMARKS:

IF UNIT NAME IS UNKNOWN, INCLUDE TIME OF REPORT (TOR), UNDER HEADING "ENEMY UNIT: UNKNOWN". DO NOT SUMMARIZE; LIST EACH REPORT. FOR EXAMPLE:

ENEMY UNIT: UNKNOWN

UIC: UNKNOWN

DAMAGED/DESTROYED: LIST ALL UNKNOWN UNIT BDA REPORTS BY TIME

	TOR*	LOC	TYPE	#DEST	#DMGD/EXTENT
1. ARMOR:					
2. FIRE SUPPORT:					
3. TRUCKS:					
4. AIR DEFENSE:					
5. C2 SYSTEMS:					
6. MOB/CNTRMOB: (ENGINEERS ASSETS, BRIDGES, LINES OF COMMUNICATIONS, MINES, ETC.)					

7. CSS:

	TOR*	LOC	WIA	KIA	EPW
8. PERSONNEL:					

REMARKS: *TOR: TIME OF REPORT. (NOTE: REMARKS ARE A MEANS OF REPORTING INFORMATION THAT DOES NOT FIT INTO THE TABLES DESCRIBED ABOVE. SPELL IT OUT IN A REMARKS SECTION, FOR EACH UNIT IF NECESSARY OR IF YOUR ASSESSMENT GOES BEYOND NUMBER COUNTS.)

APPENDIX E. MAGTF INTELLIGENCE PRODUCTION PLAN FORMAT

Tab B (Intelligence Production Plan) to Appendix 16 (Intelligence Operations Plan) to Annex B (Intelligence) should explain how intelligence production elements under the command or supporting the MAGTF would be used to support this plan. Additionally, it provides basic guidance and direction to subordinate commanders and intelligence officers for the conduct of MAGTF intelligence production operations and the support of intelligence elements and personnel identified to fulfill the intelligence requirements (IRs) in support of this plan.

CLASSIFICATION

Copy no. __ of __ copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date/time group
Message reference number

TAB B TO APPENDIX 16 (INTELLIGENCE OPERATIONS PLAN) TO ANNEX B (INTELLIGENCE) TO OPERATION ORDER (Number) (Operation CODEWORD) (U)
INTELLIGENCE PRODUCTION PLAN (U)

(U) REFERENCES**:** (The annex B originator must ensure that all receiving units and executing units have cited references.)
(a) Unit standing operating procedures (SOP) for intelligence, counterintelligence, reconnaissance, and others as appropriate.
(b) Joint task force, naval task force, other components, theater and national intelligence plans, orders and tactics, techniques, and procedures; and multinational agreements pertinent to intelligence operations.
(c) Documents, products, and online intelligence data bases that provide intelligence required for planning.
(d) Appropriate Marine Corps, naval, joint, and other doctrine publications.
(e) Others as appropriate.

(U) Time Zone: Zulu

1. (U) Situation**.** (May refer to Appendix 11 [Intelligence Estimate] as appropriate.)

   a. (U) Definition of the Area of Operations and Area of Interest. (Describe the limits of the area of operations [AO] and area of interest [AOI]. Summarize pertinent

CLASSIFICATION

weather, terrain, and other area characteristics and conditions that may influence MAGTF production operations.)

b. (U) Enemy. (Refer to annex B and current intelligence estimates for threat capabilities, limitations, vulnerabilities, and order of battle pertinent to intelligence production operations.)

c. (U) Assigned MAGTF Organic and Supporting Production Assets. (Identify organic and supporting forces available to perform intelligence production and related functions.)

d. (U) Facts and Assumptions. (State facts and assumptions derived during the mission analysis step of the Marine Corps Planning Process.)

e. (U) MAGTF Intelligence Production Considerations. (List key production and intelligence or other considerations, which impact this operation plan [OPLAN] or contingency plan [CONPLAN].)

(1) (U) Current Priority Intelligence Requirements (PIRs), Unit Concept of Operations, Unit Main Effort's PIRs, and Other Commander's Guidance

(2) (U) Availability of Intelligence

(3) (U) Intelligence Production Support to and from Joint Task Force (JTF) and Other Component Headquarters

(4) (U) Subordinate Units' Production Capabilities and Needs. (Include necessary establishment and manning of forward production elements.)

2. (U) Mission. (State concisely the MAGTF intelligence production mission as it relates to the command's planned operation.)

3. (U) Execution

a. (U) Concept of Operations. (Reference the unit's intelligence SOP and the basic Appendix 16 to Annex B. Restate as appropriate the commander's intent and pertinent aspects of the unit's overall concept of operations as they relate to production operations. Outline the purpose and concept of MAGTF production operations and specified priorities. Summarize the means and agencies to be employed in planning and directing, collection, processing and exploiting, analyzing and producing, disseminating, and using intelligence during execution of the operation order [OPORD]. Address the integration of JTF, other components, theater, national, and allied forces' production operations.)

CLASSIFICATION

b. (U) Tasks for Production and Related Units and Organizations, Subordinate Units, and Task Force Commanders or Officers in Charge (OICs)

(1) (U) Orders to Subordinate, Attached, and Supporting Units. (Use separate numbered subparagraphs to list detailed instructions for each unit conducting production operations, including the originating headquarters, subordinate commands, and separate intelligence support units with critical support to production roles. Some or all of the below units and sections may be addressed here; specific major subordinate commands [MSCs] and other intelligence producers will be tasked according to the unit SOP and mission, enemy, terrain and weather, troops and support available, and time available [METT-T].)

(a) (U) Major Subordinate Commanders

(b) (U) Commanding Officer, Intelligence Battalion

1 (U) OIC, Support Cell

2 (U) OIC, Production and Analysis (P&A) Cell

a (U) Analysis Teams

b (U) Order of Battle Teams

c (U) Target Analysis and Battle Damage Assessment Teams

d (U) Intelligence Preparation of the Battlespace Teams

e (U) Platoon Commander, Imagery Intelligence Platoon

f (U) Platoon Commander, Topographic Platoon

g (U) Staff Noncommissioned OICs, Direct Support Teams

h (U) Weather Analysis Element (if assigned)

3 (U) OIC, Surveillance and Reconnaissance Cell

4 (U) Commanding Officer, Counterintelligence (CI)/Human Intelligence (HUMINT) Company

(c) (U) Commanding Officer, Radio Battalion

(d) (U) Commanding Officer, Force Reconnaissance Company

(e) (U) Commanding Officer, Marine Unmanned Aerial Vehicle Squadron (VMU)

CLASSIFICATION

(f) (U) Commanding Officer, Marine Tactical Electronic Warfare Squadron (VMAQ)

(g) (U) Commander, Marine Corps Imagery Support Unit (if tasked to provide support to the MAGTF)

(h) (U) Others (as appropriate)

(2) (U) Requests to Higher, Adjacent, and Cooperating Units. Provide separate numbered subparagraphs pertaining to each unit not organic, attached, or supporting from which production support is requested, including other components, JTF headquarters, allied or coalition forces, as well as theater and national operational and intelligence elements.

c. (U) Coordinating Instructions. (Reference Appendix 16, and command and other pertinent forces and organizations intelligence SOPs. Detail here or in supporting enclosures, key changes to SOPs. Include or emphasize additional topics [e.g., requesting production support; intelligence production requirement [IPR] numbering and other management issues; direct liaison among subordinate commanders and production elements' leaders, staff officers, and pertinent external organizations and agencies; routine and time-sensitive reporting procedures and formats; releasability to non-U.S. military organizations; security guidance].)

4. (U) Administration and Logistics

a. (U) Logistics. Reference Annex D (Logistics). (Identify production-unique logistic requirements and concerns [e.g., unique combat service support requirements, procedures, and other guidance to support MAGTF production units and operations; or procedures for specialized technical logistic support necessary from external organizations].)

b. (U) Personnel. (Identify unique production personnel requirements and concerns [e.g., critical personnel shortages, global sourcing requirements, security clearance issues, contractor support].)

5. (U) Command and Control

a. (U) Command Relationships. Reference Annex J (Command Relationships). (Provide necessary instructions regarding MAGTF command relationships that will influence production operations.)

CLASSIFICATION

b. (U) Information Management. Reference Annex U (Information Management), Annex C (Operations), Appendix 16, and Tab C (Intelligence Dissemination Plan) to Appendix 16. (Provide any instructions necessary regarding information management [e.g., time-sensitive and routine reporting criteria, intelligence data base administration and authorities, periodic production status reporting from production elements, reports formats and changes] that will influence MAGTF production operations.

c. (U) Communications and Information Systems. Reference Appendix 16 and Annex K (Communications and Information Systems). (Provide any instructions necessary regarding communications and information systems [CIS] that will influence MAGTF production operations and its effective integration with MAGTF collection and dissemination operations.

d. (U) Intelligence Command and Control Nodes and Facilities. Reference the unit's intelligence SOP and Appendix 16. Provide necessary guidance and instructions regarding the establishment, relationships, and operations of MAGTF intelligence production nodes and facilities (e.g., P&A cell, the radio battalion operations control and analysis center, CI/HUMINT company command post).

ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

ENCLOSURES:

1–Intelligence Production Matrix
2–Periodic Intelligence Production Status Report Instructions and Format

OFFICIAL:

//s//
NAME
Rank and Service
Title

INTELLIGENCE PRODUCTION MATRIX
INSTRUCTIONS AND FORMAT

The intelligence production matrix is a tool used by MAGTF intelligence officers, the intelligence support coordinator (ISC), and production leaders to effectively plan, direct, and manage intelligence production operations. Making the matrix accessible to subordinate units' intelligence officers and intelligence producers will improve overall collaborative intelligence planning and execution.

The sample below is one format for the intelligence production matrix. The unit specifies the particular format for a given operation. The complexity of the operation and other METT-T factors will determine which format is used.

PIR, IR, or IPR Number	Date Requested	Production Requirement	Event/ Operation/ Exercise	Requesting Unit/POC	Tasked Unit(s)	Tasked Unit(s) POC	Due Date or DTG	First Review Date or DTG	First Review Remarks	Second Review Date or DTG	Second Review Remarks

Third Review Date or DTG	Third Review Remarks	Status	Feedback	Estimated Man-Hours	Actual Man-Hours*	Estimated Cost*	Actual Cost*	Quality and Distribution	Distribution Follow-ups & New IRs/ IPRs	Additional Remarks
*Garrison use only										

PERIODIC INTELLIGENCE PRODUCTION STATUS REPORT INSTRUCTIONS AND FORMAT

The periodic intelligence production status report is used by designated MAGTF units with all-source or other significant intelligence production capabilities to keep commanders, intelligence officers and sections, and other staff elements apprised of the status of current and future intelligence production operations. For the effective management of unit production activities, intelligence officers or their production leaders may require that this report be used by designated production elements under their staff cognizance to report their production status.

The example report on page E-8 is only one format (refer to the unit's SOP for specific format and direction). Normally, variations of the SOP format will be established for text, voice, and record message traffic purposes. Changes for a particular operation will be clearly identified in Annex B.

The unit SOP or Annex B also establishes the timeframe covered by each report and identifies routine and nonroutine recipients. The report may be disseminated by various methods. Interim reports, when required, generally will be disseminated via either briefings or via the tactical data network (TDN). Principal dissemination methods for the production status report include—

- Intelligence section's homepage on the MAGTF SECRET-TDN (S-TDN), with necessary sensitive compartmented information (SCI) production status posted on the SCI-TDN intelligence section homepage.
- Stand-alone record message.
- Production data bases accessible via the S-TDN or SCI-TDN (or SECRET Internet Protocol Router Network [SIPRNET] and Joint Worldwide Intelligence Communications System [JWICS] for external commands).
- Separate paragraph within the daily intelligence summary.

CLASSIFICATION

Copy no. ___ of ___ copies
OFFICIAL DESIGNATION OF COMMAND
PLACE OF ISSUE
Date/time group
Message reference number

ENCLOSURE 2 TO TAB B TO APPENDIX 16 TO ANNEX B TO OPERATION ORDER (NUMBER) (OPERATION CODEWORD) (U)
PERIODIC INTELLIGENCE PRODUCTION STATUS REPORT INSTRUCTIONS AND FORMAT (U)

Subj: MEF PERIODIC INTELLIGENCE PRODUCTION STATUS REPORT FOR THE PERIOD 180001Z–182359Z NOV 99

1. (U) Production Operations Status. (Provide essential details to ensure supported commanders, intelligence officers, and other planners are apprised of the current status of key intelligence production operations. At a minimum, PIRs and IPR priorities should be included.)

a. (U) PIR/IR MEF 01-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
MEF 01-99	intelligence estimate	III MEF CG and staff; copies to MSCs	031457Z NOV 99	2100001Z NOV 99

(1) (U) Task Production Element(s). P&A cell and assistance from radio battalion operations control and analysis center, CI/HUMINT company and Marine Corps Imagery Support Unit (MCISU) as directed by ISC.

(2) (U) Remarks. Production in support of contingency planning. Final product is the initial Appendix 11 (Intelligence Estimate) with supporting CI estimate. Product is 95 percent complete.

Page number

CLASSIFICATION

CLASSIFICATION

b. (U) PIR/IR MEF 002-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
MEF 002-99; Division 002-99, MAW 003-99, and FSSG 002-99 relate	OPLAN Support	III MEF G-2/3/5; copies to MSCs	031645Z NOV 99	230700Z NOV 99

(1) (U) Task Production Element(s). MEF lead P&A cell developing, in coordination with JFT joint intelligence support element (JISE) and the joint force land component commander intelligence section.

(2) (U) Remarks. Production in support of contingency planning. (Provide template locations and dispositions of estimated enemy command and control [C2] headquarters, maneuver, and logistic elements down to the brigade and regiment level, and fires elements down to battalion level, in support of the five locations specified to support MEF course of action development.) Product is currently in work. Current intelligence is available on the MEF G-2 SCI-TDN homepage. Spreadsheet will be forwarded to staff sections and MSCs upon completion.

c. (U) MEF 003-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
MEF 003-99	expeditionary support product (phase 1)	Originator, III MEF G-2/3/4/5/6; copies to Division, FSSG, MAW	062207Z NOV 99	240700Z NOV 99

(1) (U) Task Production Element(s). P&A cell; imagery intelligence platoon (IIP), topographic platoon, and MCISU assist as directed.

(2) (U) Remarks. Expeditionary support product in support of phase 1 scheme of maneuver and course of action analysis. Product is 75 percent complete. Completed helicopter landing zone study, which is posted on MEF G-2 S-TDN homepage. Targets within G-2 designated priority areas are 95 percent scanned.

CLASSIFICATION

d. (U) PIR/IR Division 005-00

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
Division 005-99	map update and reproduction	Division; copy to FSSG	080423Z NOV 99	Initial 10, 140100Z NOV 99; remainder, 270001Z NOV 99

(1) (U) Task Production Element(s). Topographic platoon lead; IIP assist as required.

(2) (U) Remarks. Production in support of division planning and C2. Integrating current geographic intelligence (GEOINT) products with current external imagery in order to update 1993 edition maps. Initial distribution requirement made; remainder 85 percent complete. Anticipate full IR satisfaction by 230001Z NOV 99.

e. (U) PIR/IR MAW 003-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
MAW 003-99	CIB graphics	1st MAW G-2; Division, MEF G-5 and FFC	101457Z NOV 99	011000Z DEC 99

(1) (U) Task Production Element(s). IIP assisted by P&A cell, red team, and force fires cell (FFC) future operations personnel as required.

(2) (U) Remarks. Production to support MAW target development and planning. Produce kill boxes using controlled image base (CIB) imagery. Product will be a 5-meter CIB overview of indicated areas, including a graphic reference grid with kill boxes annotated. Product is 80 percent completed.

f. (U) PIR/IR Division 007-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
Division 007-99; FSSG 004-99	LOC study	Division G-2; III MEF G2, FSSG	120937Z NOV 99	140200Z DEC 99

CLASSIFICATION

(1) (U) Task Production Element. Topographic platoon assisted by IIP and P&A cell.

(2) (U) Remarks. Production in support of wargaming and planning. Produce a detailed lines of communications (LOC) intelligence study. Product must maintain a classification level of unclassified. The bridge portion of this product can only be completed 45 percent due to lack of data sets and imagery.

g. (U) PIR/IR MEF 010-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
MEF 010-99; Division 009-99	target area/objective studies	MEF G-3 and FFC; Division and MAW	072103Z DEC 99	100400Z DEC 99

(1) (U) Task Production Element(s). P&A cell; IIP and topographic platoon support as required.

(2) (U) Remarks. Production of imagery products and supporting all-source intelligence reports for six specified areas within the division's area of operations. Production is completed; final dissemination ongoing and will be completed by 191000Z Nov 99. Follow-up conference call between MEF G-3/G-2 (P&A cell lead), division G-3/G-2 and MAW G-3/G-2 to verify fully satisfied IR and new IRs scheduled for 191600Z Nov 99.

h. (U) PIR/IR FSSG 016-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
FSSG 016-99	elevation/slope tint	FSSG; Division	130303Z NOV 99	050600Z DEC 99

(1) (U) Task Production Element. Topographic platoon.

CLASSIFICATION

(2) (U) Remarks. Production in support of FSSG site locations assessments and rear area security planning. Produce elevation and slope tint at 1:50,000 scale for defined areas. Slope tint will be provided in place of comprehensive cross-country movement study for two areas because there is no terrain data; possible new information from yesterday's JTF imagery collection missions. Product is 80 percent complete.

i. (U) PIR/IR MEF 012-99

PIR/IR #	Intelligence Product	Requester; Other Recipients	Date Received	Latest Time Information of Value
MEF 012-99	enemy C2 and CIS template	MEF G-5/G-3; MAW and Division	071457Z DEC 99	140100Z DEC 99

(1) (U) Task Production Element(s). Radio battalion operations control and analysis center; P&A cell, MAW G-2, and VMAQ tactical electronic reconnaissance processing and evaluation system assist as required.

(2) (U) Remarks. Production in support of MEF C2 warfare and targeting planning. Provide template locations and dispositions of estimated enemy C2 headquarters, maneuver, and logistic elements down to the brigade and regiment level, and fires elements down to battalion level, with estimated key CIS emitters in support of the five locations specified to support MEF COA development and wargaming. IR modified 071800Z DEC 99 to incorporate specified enemy radars and other noncommunications emitters to support MAW suppression of enemy air defenses planning. Product is 75 percent complete. Final product dissemination will be restricted to U.S. and designated multinational intelligence and operations elements.

2. (U) Production Problems. (Identify and describe significant production problems [e.g., anticipated delays meeting the latest times information of value for validated PIRs and higher priority IRs; CIS difficulties; releasability issues].)

CLASSIFICATION

3. (U) Production Detachments. (In initial report, identify intelligence detachments in support of MAGTF subordinate units that have a production capability. In subsequent reports, identify detachment name and annotate "NO CHANGE," if applicable, and new detachments deployed since the last status report. Other supporting information will be according to unit SOP and may include: period of support; detachment's intelligence support purpose; personnel and military occupational specialty information; anticipated near-term detachments support.)

Who	Dates/Period	Supported Unit	Purpose
Intelligence Battalion 1-99 (P&A cell)	01 Nov 00–(to be determined)	JTF J-2/ JISE	one 0202, two 0231s, and one 0241 for liaison and targeting support
Intelligence Battalion 2-99 (P&A Company, Direct Support Team #1)	10 Nov 99–(to be determined)	Division G-2	MEF main effort support
Intelligence Battalion 3-99 (P&A Company, Direct Support Team #2)	15 Nov 00–(to be determined)	FSSG G-2	rear area security support
Intelligence Battalion 4-99 (HUMINT Support Team #1)	19 Nov 99–(to be determined)	Division G-2	CI force protection support
Intelligence Battalion 5-99 (HUMINT Support Team #2)	22 Nov 99–(to be determined)	FSSG G-2	CI force protection support
Intelligence Battalion 6-99 (HUMINT Support Team #3)	22 Nov 99–(to be determined)	MAW G-2	CI force protection support
Intelligence Battalion 7-99 (Topographic Platoon, Geographic Intelligence Support Team #1)	19 Nov 99–(to be determined)	Division G-2	GEOINT support
Intelligence Battalion 8-99 (Topographic Platoon, Geographic Intelligence Support Team #2)	1 Dec 99–(to be determined)	FSSG G-2	GEOINT support
Radio Company Command Element (Signals Support Unit lead echelon element)	1 Dec 99–(to be determined)	Division G-2	Signals Intelligence support
Intelligence Battalion 9-99 (Topographic Platoon, Geographic Intelligence Support Team #3)	5 Dec 99–(to be determined)	MAW G-2	GEOINT support

CLASSIFICATION

4. (U) Miscellaneous. (Detail other information pertinent to ongoing collaborative intelligence production planning, direction, and operations. This may include items such as anticipated CIS problems, intelligence data base changes, nonscheduled cells or other intelligence briefings, critical intelligence collection and production issues, key external intelligence production items, security, and dissemination issues.)

ACKNOWLEDGE RECEIPT

Name
Rank and Service
Title

OFFICIAL:
//s//
NAME
Rank and Service
Title

APPENDIX F. INTELLIGENCE SUMMARY FORMAT

The intelligence summary (INTSUM) provides a synopsis of the reporting unit's intelligence situation covering a specified period of time. It is used to report threat activities, changes to threat capabilities, and results of further collections, analysis, and production to higher, adjacent, and subordinate forces. The INTSUM updates the current intelligence estimate and provides a continual intelligence assessment of threat actions and estimated capabilities and courses of action.

The theater intelligence directorate (J-2) provides guidance on INTSUM reporting periods and submission deadlines. Theater tactics, techniques, and procedures (TTP) and the specific operations plan or operation order (OPORD) designate INTSUM reporting requirements for subordinate joint task forces (JTFs) or Service and functional components. Based on those requirements, MAGTF intelligence officers (G-2/S-2) establish INTSUM reporting requirements for their major subordinate commands (MSCs) or elements; at the MEF CE level, the intelligence support coordinator establishes reporting requirements.

Established deadlines allow the intelligence battalion's production and analysis cell sufficient time to incorporate subordinate INTSUMs into intelligence products. The MAGTF MSCs and elements' G-2/S-2s determine INTSUM requirements for their headquarters and subordinate elements. The MEF TTP and standing operating procedures (SOP), which reflect anticipated theaters of operations TTP, should establish standard INTSUM reporting requirements.

Although any unit can produce INTSUMs, normally they are generated by major subordinate or higher level commands. An abbreviated INTSUM format focused on significant threat actions and anticipated future actions may be more appropriate for lower tactical echelons.

Higher command levels, particularly JTFs and unified commands, usually publish a daily intelligence summary (DISUM) every 24 hours. While INTSUMs generally provide a fine-grained tactical perspective, the DISUM encompasses more aspects of a threat country's elements of national power and focuses on operational-level intelligence analysis and estimates. Generally, MAGTF command elements tasked as JTF headquarters are required to submit DISUMs to the combatant command's commander in chief. The combatant command's TTP provides for the DISUM format, which may vary from theater to theater.

Generally based on the intelligence estimate format, the INTSUM should be tailored and focused on the mission, type of unit, and information and intelligence needs of the commander. Formats for INTSUMs can be in written or graphic and text formats.

WRITTEN INTELLIGENCE SUMMARY FORMAT

The sample below provides a written INTSUM format that may be posted on a website. This format is representative of an INTSUM format used at the MAGTF or MSC level for conventional military operations. Generally, this format is modified to meet the unique needs of military operations other than war (MOOTW).

Note: Paragraphs not applicable to the reporting unit are annotated "NA" or the paragraph may be skipped (paragraph numbering should remain the same). If no significant information or intelligence is available for a particular paragraph, the notation "NSTR" (nothing significant to report) may be used. The annotation "( )" reflects classification of that information line.

CLASSIFICATION/RELEASABILTY
INTSUM #: (Sequentially numbered such, as "DD-001-97")
DTG: DDHHMM (time zone) (month) YY
INFO cutoff DTG
PERIOD: DDHHMM TO DDHHMM (month) YY

I. (U) Highlights:

A. (U) Ground: Highlights of the current ground situation, usually divided by area or sector.

B. (U) Air: Highlights of the current air situation.

II. (U) Summary of Enemy Situation: (Each category should use the commander's related priority intelligence requirements [PIRs] as the basis for the analysis and assessment. For MOOTW operations, separate paragraphs for each category of threat or significant power group may be created to supplement or replace the below categories.)

A. (U) Ground: Detailed analysis of the battlefield by area or sector with comments on projected activity in the next 12 hours.

B. (U) Air: Detailed analysis of the air and air defense situation with comments on projected activity in the next 12 hours.

C. (U) Naval: Detailed analysis of the naval situation with comments on projected activity in the next 12 hours.

D. (U) Surface-to-Surface Missile and Weapons of Mass Destruction: Detailed analysis of the surface-to-surface missile and weapons of mass destruction situation with comments on projected activity in the next 12 hours.

E. (U) Special Operations Forces: Detailed analysis of the special operations forces, force protection, and rear area security situation with comments on projected activity in the next 12 hours.

F. (U) Other: May be used for detailed analysis of paramilitary, insurgent, terrorist, or other significant threat categories not discussed elsewhere.

III. (U) MEF or MSC Assessment:

A. (U) Most Likely Course of Action:

B. (U) Most Dangerous Course of Action:

C. (U) Others: (as necessary)

IV. (U) Enemy Movement During the Reporting Period: Major enemy units (to include at least two levels below that of the reporting command) and universal transverse mercator [UTM] coordinates of the new position.

V. (U) PIRs: The commander's PIRs and current satisfaction level (i.e., partially satisfied, satisfied, not satisfied) assessment for each requirement.

VI. (U) Intelligence Plans, Missions, and Systems Status: Key intelligence collection, production, and dissemination plan updates; information on planned intelligence and reconnaissance missions; and intelligence systems status (generally only those systems that are less than fully operational). (The unit SOP or annex B to the OPORD prescribes the period covered by this paragraph.)

GRAPHIC INTELLIGENCE SUMMARY INSTRUCTIONS

In an effort to enhance the understanding of the INTSUM and to save dissemination time, the INTSUM is graphically portrayed as a single or set of map overlays. Intelligence summaries can be posted in graphic and text formats on web-based automated information systems, which provides MAGTF intelligence users with access to the web site the option of pulling intelligence and products.

There are limitations to electronically generated graphic INTSUMs. Graphics can require large bandwidth and processing power to be pulled over a web-based system, with possible degradation of the overall MAGTF tactical data network. Lower-level tactical units and allied nation forces may not possess the means to access and use the information, which generally requires graphic and text INTSUMs to be disseminated using other electronic transmission methods and hard copy delivery.

Graphic INTSUMs must convey essential intelligence and other information in a clear, concise, and easy to understand visual format. Because of the volume of detail to be presented, most graphic INTSUMs, particularly at higher commands, have evolved into digital slide shows. The unit SOP or Annex B to the OPORD establishes graphic INTSUM formats, which are tailored to the level of command, type of operation, and the commander's intelligence requirements. Generally graphic INTSUMs contain the same elements. The following are examples of common graphic INTSUM elements:

- Weather Graphics—Composite graphics, based on satellite imaging, showing area weather fronts, cloud coverage, high and low pressure areas, etc. May include forecast graphics for specified future periods.
- 5-Day Forecast—Similar to television weather forecasts, showing forecast weather conditions (e.g., cloudy, partly cloudy, rainy), high and low temperatures, winds, normal temperatures based on climatology, and any other elements that may be of interest to the commander; should also include light data for the same period.
- Weather Impacts Graphics—Normally presented in green, yellow, and red colored chart format; should include those forces, types of operations, or critical items of equipment that are essential to friendly and enemy unit mission performance.
- PIRs—Current and new PIRs, and may include a satisfaction level (i.e., not answered, partially answered, answered) assessment for each requirement.
- Activities and Assessments—Consists of a graphical situation map denoting locations of threat forces of interest and, if possible, graphically indicating status or combat effectiveness using color coding or other symbology. Depending on the level of command and information needs, separate graphics for categories of threat forces (i.e., ground, air, air defense) may be created to increase clarity. Each graphic should—
  - Note significant threat activity over the reporting period with text comment boxes tied to locations or an event numbering system with marginal text comments.
  - Provide an assessment based on the commander's PIRs.
  - Use supporting graphics to examine items in detail, such as aircraft sortie analysis or the location and status of a particular category of force or equipment (e.g., heavy equipment transporter systems, specialized units).

- Collection, Production, and Dissemination Plans and Status of Planned Missions and Tasks—Graphically presents locations of organic collection assets (e.g., reconnaissance teams, radio battalion assets, unmanned aerial vehicle tracks, sensor strings) and/or provides a time line showing daily projected availability windows and mission tracks (as applicable) of nonorganic supporting assets (e.g., Airborne Warning and Control System, RC-135, U2); also identifies changes to previous production and dissemination plans and any new plans.
- Outlook or Assessment—Provides an overall assessment of estimated threat courses of action (at a minimum, the threat's most likely and most dangerous courses of action). The assessment may be broken into estimate time periods, such as 24-48 hours, 48-96 hours, or whatever periods of time are applicable to the commands requirements to plan future actions. Courses of action should be graphically portrayed. In prehostilities or MOOTW, these graphics may be used to address anticipated political or societal actions or events that may impact the force.

APPENDIX G. INTELLIGENCE REPORT FORMAT

An intelligence report (INTREP) is a standardized report that is used to disseminate important intelligence without regard to a specific schedule. The first intelligence element acquiring the information prepares and disseminates the INTREP as rapidly as possible to units requiring the information. Generally, each report will concern only a single item.

An INTREP is generally required whenever an event occurs that is likely to result in a change in the friendly plan or when a change to the current or future analytical assessment is made. The intelligence element generally initiates an INTREP when facts influencing threat capabilities have been observed or when a change in threat capabilities has taken place. The commander's priority intelligence requirements serve as the basis for determining what information warrants an INTREP.

Whenever possible, the INTREP should include the originator's significant intelligence assessment as well as a source reliability and accuracy evaluation. The format below is a sample INTREP that would be posted on a web site or forwarded via SECRET internet protocol router network (SIPRNET) or MAGTF tactical data network (TDN) electronic mail.

CLASSIFICATION/RELEASABILITY

INTREP#: DD-001-97 (Sequentially numbered by originating unit)

DTG: DDHHMM(Time Zone) (Month) YY

I. ( ) Significant Event(s): Summarize the significant event(s) or developments that initiated the INTREP. Answer either the 5Ws (i.e., who, what, where, when, and why) or the SALUTE (i.e., size, activity, location, unit, time, equipment) formats.

II. ( ) Assessment: Describe the effect of the current activity on threat capabilities or courses of action.

III.( ) Evaluation of Source: State the original information source and evaluate the accuracy and reliability of that source.

Note: ( ) Reflects classification of that information line.

APPENDIX H. INTELLIGENCE INFORMATION BRIEF

The intent of the intelligence information brief is to enhance situational awareness and impart understanding. Intelligence information briefings may be as simple as a quick verbal update to a commander in front of a situation map or as complex as a Marine expeditionary force or joint task force level daily update to the commanding general and staff. At lower tactical levels, briefings are generally less formal and often short-notice. Higher commands generally employ regularly scheduled daily update briefings, which include intelligence. Regardless of the degree of formality or the level of command, a standard briefing format or outline can help intelligence personnel to rapidly and effectively organize for the brief.

To develop and deliver an effective intelligence information brief, intelligence personnel should—

- Know the audience. Is the audience the commander, the staff, or subordinate commanders? Who is the focus of the brief? What is audience's level of knowledge concerning the subject? Does the commander have any briefing preferences?
- Know the purpose and intent of the briefing. Is the brief a critical events update, or is it intended to describe in detail the threat and area of operations prior to crisis action planning?
- Concentrate on essential information and intelligence; prepare to provide details or expand intelligence should questions arise.
- Use clear, concise, readable graphics; ensure graphics can be seen from the rear of the room.
- Know the information; anticipate questions on unfamiliar subjects and arrange to have a subject matter expert present or take questions for follow-up research; never make up an answer.
- Distinguish between known facts and gaps or estimates.

The most common type of intelligence information briefing is the boardwalk. The boardwalk is an informal, on-demand brief conducted using the combat operations center map boards or screen displays from automated systems. Generally, the brief only presents significant changes to threat capabilities or courses of action. This brief also provides the commander an opportunity to ask direct questions.

At higher command echelons, the most common type of intelligence information brief is the commander's morning or evening update brief. Usually more formal and detailed, these briefs are scheduled for set times either once or twice per day. The planning, decision execution, and assessment cycle or unit standing operating procedure determines the schedule. In addition to briefing the current situation and significant events, this brief may address the commander's priority intelligence requirements (PIRs); collection, production, dissemination plans and status; weather; and estimates of future threat actions. Often briefings are presented using graphics software.

By focusing on intelligence and events that correspond to the commander's PIRs, the briefer can quickly organize information and intelligence as well as ensure that the commander is given the most essential information in the shortest amount of time. The brief is also used to present significant occurrences affecting current or future plans.

The following are examples of update briefing elements:

- Weather Forecast.
- Weather Effects Assessment.
- PIRs and Intelligence Requirements (IRs).
- Situation (e.g., ground, air, air defense) Keyed to PIRs.

- Collection, Production, and Dissemination Plan Status.
- Intelligence Estimate (at a minimum, the most likely and most dangerous enemy courses of action).

These elements closely follow the elements of the web-based intelligence summary (INTSUM) graphic. See appendix F. Because the INTSUM and the update provide the same intelligence and other information, using the same format and graphics can save time and resources. To save more time, elements that have not changed since the last briefing can be briefed as "no change." However, the weather forecast, PIRs, plans status, and intelligence estimate should always be briefed.

APPENDIX I. PRODUCTION REQUIREMENT AND REQUEST FOR INTELLIGENCE FORMAT

An intelligence production requirement (IPR), production requirement (PR), or request for intelligence (RFI) begins as an intelligence requirement (IR) levied on a unit's intelligence section. If the unit cannot satisfy the requirement with the available resources, the requirement must be forwarded up the chain of command for satisfaction. The requirement then becomes either an intelligence collection requirement (ICR), an RFI, or an IPR. Single or multiple requests for information may be combined into one PR.

A requirement must contain the following four basic elements:

- Who—Organization and specific office or individual that submitted the original requirement.
- What—Statement describing the intelligence required.
- When—Latest time information of value.
- How—Requested product format (e.g., hard copy, soft copy, verbal report), quantities, all receiving units.

Most theater tactics, techniques, and procedures (TTP) combine the three forms of requirements into one basic PR or RFI format. The joint task force headquarters intelligence directorate or combatant command joint intelligence center receiving the requirement determines whether collection or product development is necessary.

Defense Intelligence Agency also has an established basic PR or RFI format. This format is used in the Community On-Line Intelligence System for End Users and Managers (COLISEUM), which has become the standard medium for requirements submission throughout the Department of Defense intelligence production community. The following COLISEUM format is from Defense Intelligence Management Document (DIMD) 0000-151C-95, *Department of Defense Intelligence Production Program (DODIPP): Production Procedures.* Although theater TTP formats generally follow the same elements, they are modified according to the specific theater needs. Marine air-ground task forces and Marine Corps forces headquarters must follow the procedures established in their theater of operation.

Item 1. PR Number—A 12-space number with 10 alphanumeric characters and 2 separation dashes (e.g., C610-94-0001). The unit intelligence section requesting the information or production enters this number, which is unique to the unit. The first four characters are the customer's statement of intelligence interest (SII) account number or in a crisis, the customer's unit identification code (UIC). The second two numbers are the fiscal year. The last four numbers are the customer's sequence number for PRs or RFIs submitted in the fiscal year.

Item 2. Subject—A short descriptive, unclassified (if possible) title. Clarity is more important than keeping the subject unclassified.

Item 3. Customer's Organization—This line should include the end user's name, organization, mailing address, electronic-mail address (clearly identify Joint Worldwide Intelligence Communications Systems [JWICS] or Secret internet protocol router network [SIPRNET]), naval message address, and if possible, the customer's commercial and DSN phone numbers.

Item 4. Date of Request—Entered by the supporting intelligence office in YYMMDD format.

Item 5. Date Product Required—The latest date the product or information will be of value to the customer. Also referred to as latest time information of value (LTIOV).

Item 6. Form and Frequency of Response—This item is key to getting the desired response to the requirement. Sub items should be narrative with an emphasis on clarity:

- **Media—**Identify the preferred product form and second and third alternatives. Examples are message, floppy disk, CD-ROM, on-line data base, data base printout, bound hard copy report, study, or handbook. In addition to the media requested, the production element often disseminates intelligence and pertinent information in other media to increase access to a wider number of potential users.
- **Frequency**—Specify request for scheduled, non-crisis-related production as one-time, as required, or recurring. Crisis or immediate production requests are normally handled as one-time requests unless otherwise specified.
- **Revision or New Product**—Specify the existing product requiring update as completely as possible, or specify as a new PR.
- **Classification and Releasability**—Provide the desired classification and the highest classification that can be used by the customer. If the product needs to be releasable to foreign forces, specify which forces, if known, and justify the release.

Item 7. Statement of Requirement—The first paragraph should provide a summary of the requirement in 50 words or less. If the requirement supports an operation plan or contingency plan, the first sentence should identify which plan. Subsequent paragraphs should provide greater detail, specific intelligence and information elements, and a justification. The justification should specify what intelligence and other information sources have been consulted and why they were not sufficient to answer the requirement. If the requirement addresses separate questions, or multiple countries or topics, they must be prioritized. If all requests carry the same priority, list them by time urgency.

Item 8. Comments—Additional comments as necessary.

Item 9. Security Classification—The highest classification of the question and information contained in the requirement. The lower the classification, the easier it will be to process and use; however, clarity should not be sacrificed for lower classification. Codeword or special access program requirements will be submitted through appropriate channels and may require additional time to transmit and process.

APPENDIX J. GLOSSARY

SECTION I. ACRONYMS AND ABBREVIATIONS

AA . . . . . avenue of approach
ACE . . . . . aviation combat element
AC/S . . . . . assistant chief of staff
ADA . . . . . air defense artillery
AFP . . . . . all-source fusion platoon
AI . . . . . air interdiction
AIntP . . . . . allied intelligence publication
AO . . . . . area of operations
AOA . . . . . amphibious objective area
AOI . . . . . area of interest
ATARS . . . . . advanced tactical airborne reconnaissance system
ATF . . . . . amphibious task force
ATO . . . . . air tasking order
AWACS . . . . . Airborne Warning and Control System

BDA . . . . . battle damage assessment
BDE . . . . . brigade
BE . . . . . basic encyclopedia
BP . . . . . battle position

C2 . . . . . command and control
C2W . . . . . command and control warfare
CA . . . . . combat assessment
CAS . . . . . close air support
CATF . . . . . commander, amphibious task force
CATK . . . . . counterattack
CCIR . . . . . commander's critical information requirements
CD-ROM . . . . compact disc read only memory
CE . . . . . command element
CG . . . . . commanding general
CHATS . . . . . CI/HUMINT automated tool set
CI . . . . . counterintelligence
CIA . . . . . Central Intelligence Agency
CIB . . . . . controlled image base
CIC . . . . . combat intelligence center
CINC . . . . . commander in chief
CIS . . . . . communications and information systems
CNTRMOB . . . . . countermobility
COA . . . . . course of action
COC . . . . . combat operations center
COG . . . . . center of gravity
COLISEUM . . . . . Community On-Line Intelligence System for End Users and Managers
CONPLAN . . . . . contingency plan
COO . . . . . combined obstacle overlay
CP . . . . . command post
CPX . . . . . command post exercise
CSS . . . . . combat service support

D3A . . . . . decide, detect, deliver, assess
DDHHMM . . . . . day, hour, minute
DEST . . . . . destination
DIA . . . . . Defense Intelligence Agency
DIMD . . . . . defense intelligence management document
DISUM . . . . . daily intelligence summary
DMGD . . . . . damaged
DMS . . . . . Defense Message System
DOD . . . . . Department of Defense
DODIPP . . . . . Department of Defense Intelligence Production Program
DON . . . . . Department of the Navy
DP . . . . . decision point
DPM . . . . . Dissemination Program Manager
DSN . . . . . Defense Switched Network
DST . . . . . decision support template
DTG . . . . . date-time group
DZ . . . . . drop zone

EA . . . . . electronic attack
e.g. . . . . for example
EPW . . . . . enemy prisoner of war

FARP . . . . . forward arming and refueling point
FDA . . . . . functional damage assessment
FFC . . . . . force fires cell
FFIR . . . . . friendly force information requirements
FLIR . . . . . forward-looking infrared
FM . . . . . field manual (Army)
FMFRP . . . . . Fleet Marine Force reference publication
FSSG . . . . . force service support group

G-1 . . . . . manpower or personnel staff officer/organization

G-2 . . . . . intelligence staff officer/organization
G-3 . . . . . operations staff officer/organization
G-4 . . . . . logistics staff officer/organization
G-5 . . . . . plans officer/organization
GCE . . . . . ground combat element
GENSER. . . . . general service
GEOINT . . . . . geographic intelligence

HF . . . . . high frequency
HLZ. . . . . helicopter landing zone
HN. . . . . host nation
HPT. . . . . .high-payoff target
HPTL . . . . . .high-payoff target list
HQ. . . . . .headquarters
HUMINT . . . . . .human intelligence
HVT . . . . . high-value target

i.e. . . . . that is
I&W . . . . . .indications and warning
IAS . . . . . .intelligence analysis system
ICR . . . . . intelligence collection requirement
IDR . . . . intelligence dissemination requirement
IIP . . . . . imagery intelligence platoon
IMINT. . . . . .imagery intelligence
IMO. . . . . .imagery and mapping officer
intel bn . . . . . intelligence battalion
INTELINK . . . . . intelligence link
INTELINK-S . . . . . intelligence link-SECRET
INTREP . . . . . intelligence report
INTSUM. . . . . .intelligence summary
IOC . . . . . intelligence operations center
IPB . . . . . .intelligence preparation of the battlespace
IPR . . . . . intelligence production requirement
IR . . . . . .intelligence requirement
ISC . . . . . intelligence support coordinator
ISM . . . . . .intelligence synchronization matrix
ISS. . . . . .intelligence synchronization sheet

J-2 . . . . . .intelligence directorate
JAC . . . . . joint analysis center
JCS . . . . . .Joint Chiefs of Staff
JDISS . . . . . Joint Deployable Intelligence Support System
JDS . . . . . .Joint Dissemination System
JFC . . . . . .joint force commander
JFIC. . . . . .Joint Forces Intelligence Command
JIC . . . . . joint intelligence center
JISE. . . . . joint intelligence support element
JOG-A. . . . . joint operations graphic-air

JP. . . . . .joint publication
JSIPS. . . . . .Joint Services Imagery Processing System
JSTARS . . . . . joint surveillance, target attack radar system
JTF . . . . . joint task force
JWICS. . . . . .Joint Worldwide Intelligence Communications System

KIA . . . . . killed in action
km . . . . . kilometer
KOCOA . . . .key terrain, observation and fields of fire, cover and concealment, obstacles, and avenues of approach, and mobility corridors

LCAC . . . . . .landing craft air cushion
LOA . . . . . limit of advance
LOC . . . . . line of communications
LOS. . . . . line of sight
LTIOV . . . . . .latest time information of value
LZ . . . . . .landing zone

MAGTF . . . . . Marine air-ground task force
MARFOR . . . . . .Marine Corps forces
MAW . . . . . .Marine aircraft wing
MCDP . . . . . Marine Corps doctrinal publication
MCIA . . . . . Marine Corps Intelligence Activity
MCISU . . . Marine Corps Imagery Support Unit
MCOO . . . modified combined obstacle overlay
MCRP . . . . .Marine Corps reference publication
MCWP . . . . . Marine Corps warfighting publication
MEA . . . . . mission effectiveness assessment
MEF . . . . . Marine expeditionary force
METT-T . . . . . .mission, enemy, terrain and weather, troops and support available-time available
MEU(SOC) . . . . . Marine expeditionary unit (special operations capable)
MIDB . . . . . .modernized integrated database
mm . . . . . millimeters
MOB . . . . . mobility
MOOTW. . . . military operations other than war
MOS . . . . . military occupational specialty
MSC . . . . . major subordinate command
MSE . . . . . .major subordinate element
MTI. . . . . moving target indicator
MTW. . . . . major theater war

NA. . . . . .not applicable

NAI . . . . . named area of interest
NAIC. . . . . National Air Intelligence Center
NATO . . . . .North Atlantic Treaty Organization
NBC . . . . . .nuclear, biological, and chemical
NEF. . . . . .naval expeditionary force
NEO . . . . . noncombatant evacuation operation
NGIC. . . . .National Ground Intelligence Center
NGO . . . . . .nongovernmental organization
NIMA . . . . . .National Imagery and Mapping Agency
NIPRNET . . . . . nonsecure internet protocol router network
NIS . . . . . .national input segment
NIST . . . . . .national intelligence support team
NMIC . . National Maritime Intelligence Center
NOE . . . . . .nap of the earth
NSA . . . . . National Security Agency
NSTR . . . . . .nothing significant to report
NVG . . . . . .night vision goggles

obj . . . . . .objective
OCAC . . . . . operations control and analysis center
OIC . . . . . .officer in charge
OMFTS . . . operational maneuver from the sea
OOB . . . . . .order of battle
OPCON . . . . . .operational control
OPLAN. . . . . .operation plan
OPORD. . . . . .operation order

P&A . . . . . production and analysis
PDA . . . . . physical damage assessment
PDE&A. . . . . planning, decision, execution, and assessment
PIR . . . . . priority intelligence requirement
POC. . . . . point of contact
POL. . . . . .petroleum, oils, and lubricants
PR . . . . . production requirement
PVO . . . . . .private voluntary organization

RAG . . . . . regimental artillery group
RC. . . . . reconnaissance capable
recon . . . . . .reconnaissance
rep . . . . . .representative
RFI . . . . . .request for intelligence
RR. . . . . .reattack recommendation
RRS. . . . . remote receive station

S-1. . . . . .manpower or personnel staff officer/organization
S-2. . . . . intelligence staff officer/organization
S-3. . . . . operations staff officer/organization
SALUTE. . . . . .size, activity, location, unit, time, equipment
SAM . . . . . surface-to-air missile
SARC . . . . surveillance and reconnaissance cell
SATCOM . . . . . satellite communications
SCI . . . . . sensitive compartmented information
SCR. . . . . single channel radio
SIDS . . . . . secondary imagery dissemination system
SIGINT . . . . . .signals intelligence
SII . . . . . .statement of intelligence interest
SIPRNET . . . . . .SECRET Internet Protocol Router Network
SOA . . . . . sustained operations ashore
SOP. . . . . .standing operating procedure
SPMAGTF . . . . . special-purpose Marine air-ground task force
SPP . . . . . shared production program
STANAG . . . . . standardization agreement (NATO)

TAA . . . . . .tactical assembly area
TAI . . . . . targeted area of interest
TCAC . . . .technical control and analysis center
TDN . . . . . tactical data network
T/E . . . . . table of equipment
TEG. . . . . tactical exploitation group
TERPES . . . . tactical electronic reconnaissance processing and evaluation system
T/O . . . . . table of organization
topo . . . . . topographic
TOR . . . . . time of report
TPC. . . . . topographic production capability
TPL . . . . . time phase lines
TRSS. . . . . .tactical remote sensor system
TSA. . . . . target system assessment
TTP . . . . . tactics, techniques, and procedures

UAV . . . . . .unmanned aerial vehicle
UIC . . . . . unit identification code
U.S. . . . . United States
UTM . . . . . .universal transverse mercator

VHF . . . . . very high frequency
VMAQ . . . . . .Marine tactical electronic warfare squadron
VMU. . . . . .Marine unmanned aerial vehicle squadron
VO. . . . . validation office

WIA . . . . . wounded in action
YYMMDD . . . . . .year, month, day

SECTION II. DEFINITIONS

***a priori*—**Probabilities, in the absence of other information; presupposed by experience.

all-source intelligence—Intelligence products and/or organizations and activities that incorporate all sources of information, including, most frequently, human resources intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence, and open source data, in the production of finished intelligence. (JP 1-02)

amphibious force—An amphibious task force and a landing force together with other forces that are trained, organized, and equipped for amphibious operations. (Proposed by JP 3-02 for inclusion in JP 1-02)

amphibious objective area—A geographical area, delineated in the initiating directive, for purposes of command and control within which is located the objective(s) to be secured by the amphibious task force. This area must be of sufficient size to ensure accomplishment of the amphibious task force's mission and must provide sufficient area for conducting necessary sea, air, and land operations. Also called AOA. (JP 1-02)

amphibious task force—A Navy task organization formed to conduct amphibious operations. The amphibious task force, together with the landing force and other forces, constitutes the amphibious force. Also called ATF. (Proposed by JP 3-02 for inclusion in JP 1-02)

analysis—In intelligence usage, a step in the processing phase of the intelligence cycle in which information is subjected to review in order to identify significant facts for subsequent interpretation. See also intelligence cycle. (JP 1-02) The sifting and sorting of evaluated information to isolate significant elements with respect to the mission and operations of the command. (MCWP 2-1)

area of interest—That area of concern to the commander, including the area of influence, areas adjacent thereto, and extending into enemy territory to the objectives of current or planned operations. This area also includes areas occupied by enemy forces who could jeopardize the accomplishment of the mission. Also called AOI. (JP 1-02)

area of operations—An operational area defined by the joint force commander for land and naval forces. Areas of operation do not typically encompass the entire operational area of the joint force commander, but should be large enough for component commanders to accomplish their missions and protect their forces. Also called AO. (JP 1-02)

aviation combat element—The core element of a Marine air-ground task force that is task-organized to conduct aviation operations. The aviation combat element provides all or a portion of the six functions of Marine aviation necessary to accomplish the Marine air-ground task force's mission. These functions are anti-air warfare, offensive air support, assault support, electronic warfare, air reconnaissance, and control of aircraft and missiles. The aviation combat element is usually composed of an aviation unit headquarters and various other aviation units or their detachments. It can vary in size from a small aviation detachment of specifically required aircraft to one or more Marine aircraft wings. The aviation combat element may contain other Service or foreign military forces assigned or attached to the Marine air-ground task force. The aviation combat element itself is not a formal command. Also called ACE. (Approved for inclusion in next version of MCRP 5-12C)

basic intelligence—Fundamental intelligence concerning the general situation, resources, capabilities, and vulnerabilities of foreign countries or areas which may be used as reference material in the planning of operations at any level and in evaluating subsequent information relating to the same subject. (JP 1-02)

battle damage assessment—1. The timely and accurate estimate of damage resulting from the application of military force, either lethal or non-lethal, against a predetermined objective. Battle damage assessment can be applied to the employment of all types of weapon systems (air, ground, naval, and special forces weapon systems) throughout the range of military operations. Battle damage assessment is primarily an intelligence responsibility with required inputs and coordination from the operators. Battle damage assessment is composed of physical damage assessment, functional damage assessment, and target system assessment. Also called BDA. (JP 1-02) **2**. In Marine Corps usage, the timely and accurate estimate of the damage resulting from the application of military force. BDA estimates physical damage to a particular target, functional damage to that target, and the capability of the entire target system to continue its operations. (MCWP 5-12C)

battlespace—All aspects of air, surface, subsurface, land, space, and electromagnetic spectrum which encompass the area of influence and area of interest. (MCRP 5-12C)

battlespace dominance—The degree of control over the dimensions of the battlespace which enhances friendly freedom of action and denies enemy freedom of action. It permits force sustainment and application of power projection to accomplish the full range of potential operational and tactical missions. It includes all actions conducted against enemy capabilities to influence future operations. (MCRP 5-12C)

branch(es)—A contingency plan or course of action (an option built into the basic plan or course of action) for changing the mission, disposition, orientation, or direction of movement of the force to aid success of the operation based on anticipated events, opportunities, or disruptions caused by enemy actions. See also sequel(s). (MCRP 5-12C)

centers of gravity—1. Those characteristics, capabilities, or localities from which a military force derives its freedom of action, physical strength, or will to fight. Also called COG. (JP 1-02) **2**. A key source of strength without which an enemy cannot function. (MCDP 1-2)

centralized control—In military operations, a mode of battlespace management in which one echelon of command exercises total authority and direction of all aspects of one or more warfighting functions. It is a method of control where detailed orders are issued and total unity of action is the overriding consideration. (MCRP 5-12C)

collate—1. The grouping together of related items to provide a record of events and facilitate further processing. **2**. To compare critically two or more items or documents concerning the same general subject; normally accomplished in the processing phase in the intelligence cycle. (JP 1-02)

collection—Acquisition of information and the provision of this information to processing and/or production elements. (JP 1-02) In Marine Corps usage, the gathering of intelligence data and information to satisfy the identified requirements. (MCWP 5-12C)

collection agency—Any individual, organization, or unit that has access to sources of information and the capability of collecting information from them. (JP 1-02)

collection asset—A collection system, platform, or capability that is supporting, assigned, or attached to a particular commander. (JP 1-02)

collection management—The process of converting intelligence requirements into collection requirements, establishing priorities, tasking or coordinating with appropriate collection sources or agencies, monitoring results, and retasking, as required. (JP 1-02)

collection manager—An individual with responsibility for the timely and efficient tasking of organic collection resources and the development of requirements for theater and national assets that could satisfy specific information needs in support of the mission. (JP 1-02)

collection plan—A plan for collecting information from all available sources to meet intelligence requirements and for transforming those requirements into orders and requests to appropriate agencies. (JP 1-02)

combat assessment—The determination of the overall effectiveness of tactical force employment during military operations. Combat assessment is composed of three major components, (a) battle damage assessment (BDA), (b) munitions effects assessment, and (c) future course-of-action (COA) or reattack recommendation. Also called CA. (Proposed by JP 3-60 for inclusion in JP 1-02.)

combat data—Data derived from reporting by operational units. (MCWP 5-12C)

combatant command—A unified or specified command with a broad continuing mission under a single commander established and so designated by the President, through the Secretary of Defense and with the advice and assistance of the Chairman of the Joint Chiefs of Staff. Combatant commands typically have geographic or functional responsibilities. (JP 1-02)

combined operation—An operation conducted by forces of two or more allied nations acting together for the accomplishment of a single mission. (JP 1-02)

command and control—The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. Also called C2. (JP 1-02) Also in Marine Corps usage, the means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken. (MCRP 5-12C)

command and control warfare—The integrated use of operations security, military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Also called C2W. (Excerpt from JP 1-02)

command element—The core **element** of a Marine air-ground task force that is the headquarters. The command element is composed of the commander, general or executive and special staff sections, headquarters section, and requisite communications support, intelligence and reconnaissance forces, necessary to accomplish the MAGTF's mission. The command element provides command and control, intelligence, and other support essential for effective planning and execution of operations by the other elements of the Marine air-ground task force. The command element varies in size and composition and may contain other Service or foreign military forces assigned or attached to the MAGTF. Also called CE. (Approved for inclusion in next version of MCRP 5-12C)

commander's critical information requirements—Information regarding the enemy and friendly activities and the environment identi-

fied by the commander as critical to maintaining situational awareness, planning future activities, and facilitating timely decisionmaking. Also called CCIR. NOTE: CCIRs are normally divided into three primary subcategories: priority intelligence requirements; friendly force information requirements; and essential elements of friendly information. (MCRP 5-12C)

commander's intent—A commander's clear, concise articulation of the purpose(s) behind one or more tasks assigned to a subordinate. It is one of two parts of every mission statement which guides the exercise of initiative in the absence of instructions. (MCRP 5-12C)

commander's planning guidance—Directions and/or instructions which focus the staff's course of action development during the planning process. (MCRP 5-12C)

communications intelligence—Technical and intel-ligence information derived from foreign communications by other than the intended recipients. (JP 1-02)

communications security—The protection resulting from all measures designed to deny unauthorized persons information of value which might be derived from the possession and study of telecommunications, or to mislead unauthorized persons in their interpretation of the results of such possession and study. (Excerpt from JP 1-02)

coordination—The action necessary to ensure adequately integrated relationships between separate organizations located in the same area. Coordination may include such matters as fire support, emergency defense measures, area intelligence, and other situations in which coordination is considered necessary. (MCRP 5-12C)

counterintelligence—1. Information gathered and activities conducted to protect against espionage, other intelligence activities, sabotage, or assassinations conducted by or on behalf of foreign governments or elements thereof, foreign organizations, or foreign persons, or international terrorist activities. (JP 1-02) **2.** Within the Marine Corps, counterintelligence constitutes active and passive measures intended to deny a threat force valuable information about the friendly situation, to detect and neutralize hostile intelligence collection, and to deceive the enemy as to friendly capabilities and intentions. Also called CI. (MCRP 5-12C)

crisis action planning—The time-sensitive planning for the deployment, employment, and sustainment of assigned and allocated forces and resources that occurs in response to a situation that may result in actual military operations. Crisis action planners base their plan on the circumstances that exist at the time planning occurs. (JP 1-02)

critical information—Specific facts about friendly intentions, capabilities, and activities vitally needed by adversaries for them to plan and act effectively so as to guarantee failure or unacceptable consequences for friendly mission accomplishment. (JP 1-02)

critical intelligence—Intelligence which is crucial and requires the immediate attention of the commander. It is required to enable the commander to make decisions that will provide a timely and appropriate response to actions by the potential/actual enemy. It includes but is not limited to the following: **a**. strong indications of the imminent outbreak of hostilities of any type (warning of attack); **b**. aggression of any nature against a friendly country; **c**. indications or use of nuclear-biological-chemical weapons (targets); **d**. significant events within potential enemy countries that may lead to modification of nuclear strike plans. (JP 1-02)

critical node—An element, position, or communica-tions entity whose disruption or destruction immediately degrades the ability of

a force to command, control, or effectively conduct combat operations. (JP 1-02)

critical vulnerability—An aspect of a center of gravity that if exploited will do the most significant damage to an adversary's ability to resist. A vulnerability cannot be critical unless it undermines a key strength. (MCRP 5-12C)

daily intelligence summary—A report prepared in message form at the joint force headquarters that provides higher, lateral, and subordinate headquarters with a summary of all significant intelligence produced during the previous 24-hour period. The "as of" time for information, content, and submission time for the report will be as specified by the joint force commander. Also called DISUM. (JP 1-02)

data—Representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Any representations such as characters or analog quantities to which meaning is or might be assigned. (JP 1-02)

data base—Information that is normally structured and indexed for user access and review. Data bases may exist in the form of physical files (folders, documents, etc.) or formatted automated data processing system data files. (JP 1-02)

database replication—Process by which like databases reflect commonality in information and timeliness of that information. (MCRP 5-12C)

debriefing—Interviewing of an individual who has completed an intelligence or reconnaissance assignment or who has knowledge, whether through observation, participation, or otherwise, of operational or intelligence significance. (MCRP 5-12C)

decentralized control—In military operations, a mode of battlespace management in which a command echelon may delegate some or all authority and direction for warfighting functions to subordinates. It requires careful and clear articulation of mission, intent, and main effort to unify efforts of subordinate leaders. (MCRP 5-12C)

deception operation—A military operation conducted to mislead the enemy. A unit conducting a deception operation may or may not make contact with the enemy. Deception operations include demonstrations, diversions, displays, feints, ruses, actions, events, means, and objectives. (MCRP 5-12C)

decision point—An event, area, or point in the battlespace where and when the friendly commander will make a critical decision. Also called DP. (MCRP 5-12C)

deliberate planning—A planning process for the deployment and employment of apportioned forces and resources that occurs in response to a hypothetical situation. Deliberate planners rely heavily on assumptions regarding the circumstances that will exist when the plan is executed. (JP 1-02)

deliberate targeting—The methodical identification, compilation, and analysis of potential fixed or semifixed targets followed by the decision of which potential targets will be attacked, when, and/or by what weapon and ordnance. It is practiced primarily during the planning phase of an operation, when planning for an attack, or when the tempo of combat is slow. (MCRP 5-12C)

descriptive intelligence—Class of intelligence which describes existing and previously existing conditions with the intent to promote situational awareness. Descriptive intelligence has two components: *basic intelligence*, which is general background knowledge about established and relatively constant conditions; and *current intelligence*, which is concerned with describing the existing situation. (MCRP 5-12C)

detachment—1. A part of a unit separated from its main organization for duty elsewhere. **2.** A temporary military or naval unit formed from other units or parts of units. (JP 1-02)

direction finding—A procedure for obtaining bearings of radio frequency emitters by using a highly directional antenna and a display unit on an intercept receiver or ancillary equipment. (JP 1-02)

direct support—A mission requiring a force to support another specific force and authorizing it to answer directly the supported force's request for assistance. (JP 1-02)

dissemination—Conveyance of intelligence to users in a suitable form. (JP 1-02)

dissemination management—Involves establishing dissemination priorities, selection of dissemination means, and monitoring the flow of intelligence throughout the command. The objective of dissemination management is to deliver the required intelligence to the appropriate user in proper form at the right time while ensuring that individual consumers and the dissemination system are not overloaded attempting to move unneeded or irrelevant information. Dissemination management also provides for use of security controls which do not impede the timely delivery or subsequent use of intelligence while protecting intelligence sources and methods. (MCRP 5-12C)

effective damage—That damage necessary to render a target element inoperative, unserviceable, nonproductive, or uninhabitable. (JP 1-02)

effectiveness—The measurement of the results of military action against a target by lethal or nonlethal means. (Proposed by JP 3-60 for inclusion in JP 1-02.)

effects—The result of military action against a target by lethal or nonlethal means. (Proposed by JP 3-60 for inclusion in JP 1-02.)

effects assessment—A determination of the overall effectiveness of force or weapon system employment during military operations and recommends future courses of action. Effects assessment is conducted at the strategic, operational, and tactical levels-of war or MOOTW. Effects assessment is the assessment of all execution effects, and includes steps commonly associated with combat assessment. (Proposed by JP 3-60 for inclusion in JP 1-02.)

electromagnetic spectrum—The range of frequencies of electromagnetic radiation from zero to infinity. It is divided into 26 alphabetically designated bands. (JP 1-02)

electronic attack—That division of electronic warfare involving the use of electromagnetic, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. (JP 1-02)

electronic intelligence—Technical and geolocation intelligence derived from foreign noncommunications electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (JP 1-02)

electronic protection—That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment or electronic warfare that degrade, neutralize, or destroy friendly combat capability. (JP 1-02)

electronic reconnaissance—The detection, identification, evaluation, and location of foreign electromagnetic radiations emanating from other than nuclear detonations or radioactive sources. (JP 1-02)

electronic warfare—Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. The three

major subdivisions within electronic warfare are electronic attack, electronic protection, and electronic warfare support. Also called EW. (Excerpt from JP 1-02)

electronic warfare support—That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and tactical actions such as threat avoidance, targeting, and homing. Electronic warfare support data can be used to produce signals intelligence (SIGINT), communications intelligence (COMINT), and electronic intelligence (ELINT). (JP 1-02)

essential elements of friendly information—**1.** Key questions likely to be asked by adversary officials and intelligence systems about specific friendly intentions, capabilities, and activities so they can obtain answers critical to their operational effectiveness. Also called EEFI. (JP 1-02) **2.** Specific facts about friendly intentions, capabilities, and activities needed by adversaries to plan and execute effective operations against our forces. (MCRP 5-12C)

estimative intelligence—Class of intelligence which attempts to anticipate future possibilities and probabilities based on an analysis of descriptive intelligence in the context of planned friendly and assessed enemy operations. See also **descriptive intelligence**. (MCRP 5-12C)

evaluation—In intelligence usage, appraisal of an item of information in terms of credibility, reliability, pertinence, and accuracy. Appraisal is accomplished at several stages within the intelligence cycle with progressively different contexts. Initial evaluations, made by case officers and report officers, are focused upon the reliability of the source and the accuracy of the information as judged by data available at or close to their operational levels. Later evaluations by intelligence analysts, are primarily concerned with verifying accuracy of information and may, in effect, convert information into intelligence. Appraisal or evaluation of items of information or intelligence is indicated by a standard letter-number system. The evaluation of the reliability of sources is designated by a letter from A through F, and the accuracy of the information is designated by numeral 1 through 6. These are two entirely independent appraisals, and these separate appraisals are indicated in accordance with the system indicated below. Thus, information adjudged to be "probably true" received from a "usually reliable source" is designated "B-2" or "B2," while information of which the "truth cannot be judged" received from a "usually reliable source" is designated "B-6" or "B6."

Reliability of Source

A - Completely reliable
B - Usually reliable
C - Fairly reliable
D - Not usually reliable
E - Unreliable
F - Reliability cannot be judged

Accuracy of Information

1 - Confirmed by other sources
2 - Probably true
3 - Possibly true
4 - Doubtful
5 - Improbable
6 - Truth cannot be judged (JP 1-02)

fires—The effects of lethal or nonlethal weapons. (JP 1-02)

force protection—Security program designed to protect Service members, civilian employees, family members, facilities, and equipment, in all locations and situations, accomplished through planned and integrated application of combatting terrorism, physical security, operations

security, personal protective services, and supported by intelligence, counterintelligence, and other security programs. (JP 1-02)

force reconnaissance company—A unit whose mission is to conduct preassault and deep postassault reconnaissance operations in support of a landing force and its subordinate elements. (MCRP 5-12C)

friendly force information requirements—Information the commander needs about friendly forces in order to develop plans and make effective decisions. Depending upon the circumstances, information on unit location, composition, readiness, personnel status, and logistics status could become a friendly force information requirement. Also called FFIR. (MCRP 5-12C)

functional damage assessment—The estimate of the effect of military force to degrade/destroy the functional or operational capability of the target to perform its intended mission and on the level of success in achieving operational objectives established against the target. This assessment is based upon all-source information, and includes an estimation of the time required for recuperation or replacement of the target function. (Upon approval of JP 3-60, this term and its definition will be included in JP 1-02.)

fusion—In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of activity. (JP 1-02)

fusion center—In intelligence usage, a physical location to accomplish fusion. It normally has sufficient intelligence automated data processing capability to assist in the process. (JP 1-02)

future operations section—1. In MAGTF operations, a section normally under the staff cognizance of the G-3 which focuses on planning/producing new fragmentary orders or the next change of major subordinate command mission; this section forms and leads the integrated planning effort with a planning horizon of 72-120 hours out. It develops branch plans and sequels. **2.** In Marine aviation, that portion of the tactical air command center and aviation combat element commander's battlestaff responsible for the detailed planning and coordination of all future air operations conducted by the aviation combat element in support of the Marine air-ground task force. The future operations section plans for and publishes the next air tasking order(s) (normally a 48/72-hour period). (MCRP 5-12C)

general military intelligence—Intelligence concerning the (1) military capabilities of foreign countries or organizations or (2) topics affecting potential US or allied military operations, relating to the following subjects: armed forces capabilities, including order of battle, organization, training, tactics, doctrine, strategy, and other factors bearing on military strength and effectiveness; area and terrain intelligence, including urban areas, coasts and landing beaches, and meteorological, oceanographic, and geological intelligence; transportation in all modes; military materiel production and support industries,; military and civilian C4 systems; military economics, including foreign military assistance; insurgency and terrorism; military-political-sociological intelligence; location, identification, and description of military-related installations; government control; escape and evasion; and threats and forecasts. (Excludes scientific and technical intelligence.) (JP 1-02)

general support—That support which is given to the supported force as a whole and not to any particular subdivision thereof. (JP 1-02)

geographic coordinates—The quantities of latitude and longitude which define the position of a point on the surface of the earth with respect to the reference spheroid. (JP 1-02)

geographic intelligence—The process of collecting, organizing, analyzing, synthesizing, disseminating and utilizing geospatial information and services (GI&S) with regards to the military aspects of the terrain. Also called GEOINT. GEOINT is the integration and analysis of all-source geospatial information in support of specific Marine Corps operations. The analysis is focused on a specific mission and includes intensification of information detail and resolution to meet tactical requirements. GEOINT analysis is focused on the intelligence preparation of the battlespace (IPB) process and addresses key terrain, observation & fields of fire, cover & concealment, obstacles, avenues of approach & mobility corridors. This analysis is commonly referred to as KOCOA for easy reference.

geospatial information and services—The concept for collection, information extraction, storage, dissemination, and exploitation of geodetic, geomagnetic, imagery (both commercial and national source), gravimetric, aeronautical, topographic, hydrographic, littoral, cultural, and toponymic data accurately referenced to a precise location on the earth's surface. These data are used for military planning, training, and operations including navigation, mission planning, mission rehearsal, modeling, simulation and precise targeting. Geospatial information provides the basic framework for battlespace visualization. It is information produced by multiple sources to common interoperable data standards. It may be presented in the form of printed maps, charts, and publications; in digital simulation and modeling data bases; in photographic form; or in the form of digitized maps and charts or attributed centerline data. Geospatial services include tools that enable users to access and manipulate data, and also includes instruction, training, laboratory support, and guidance for the use of geospatial data. (JP 1-02)

global sourcing—A process of force provision or augmentation whereby resources may be drawn from any location/command worldwide. (MCRP 5-12C)

ground combat element—The core element of a Marine air-ground task force that is task-organized to conduct ground operations. It is usually constructed around an infantry organization but can vary in size from a small ground unit of any type, to one or more Marine divisions that can be independently maneuvered under the direction of the MAGTF commander. It includes appropriate ground combat and combat support forces and may contain other Service or foreign military forces assigned or attached to the Marine air-ground task force. The ground combat element itself is not a formal command. Also called GCE. (Approved for inclusion in next version of MCRP 5-12C)

helicopter landing zone—A specified ground area for landing assault helicopters to embark or disembark troops and/or cargo. A landing zone may contain one or more landing sites. Also called HLZ. (JP 1-02)

high-payoff target—A target whose loss to the enemy will significantly contribute to the success of the friendly course of action. High-payoff targets are those high-value targets, identified through wargaming, which must be acquired and successfully attacked for the success of the friendly commander's mission. Also called HPT. (JP 1-02)

high-value target—A target the enemy commander requires for the successful completion of the mission. The loss of high-value targets would be expected to seriously degrade important enemy functions throughout the friendly commander's area of interest. Also called HVT. (JP 1-02)

human intelligence—1. A category of intelligence derived from information collected and provided by human sources. (JP 1-02) **2.** In Marine Corps usage, human intelligence operations cover a wide range of activities encompassing reconnaissance patrols, aircrew debriefs,

debriefing of refugees, interrogations of prisoners of war, and the conduct of counterintelligence force protection source operations. Also called HUMINT. (JP 1-02)

humanitarian assistance—Programs conducted to relieve or reduce the results of natural or manmade disasters or other endemic conditions such as human pain, disease, hunger, or privation that might present a serious threat to life or that can result in great damage to or loss of property. Humanitarian assistance provided by US forces is limited in scope and duration. The assistance provided is designed to supplement or complement the efforts of the host nation civil authorities or agencies that may have the primary responsibility for providing humanitarian assistance. (JP 1-02)

hydrography—The science which deals with the measurements and description of the physical features of the oceans, seas, lakes, rivers, and their adjoining coastal areas, with particular reference to their use for navigational purposes. (JP 1-02)

imagery exploitation—The cycle of processing and printing imagery to the positive or negative state, assembly into imagery packs, identification, interpretation, mensuration, information extraction, the preparation of reports, and the dissemination of information. (JP 1-02)

imagery intelligence—Intelligence derived from the exploitation of collection by visual photography, infrared sensors, lasers, electro-optics, and radar sensors such as synthetic aperture radar wherein images of objects are reproduced optically or electronically on film, electronic display devices, or other media. Also called IMINT. (JP 1-02)

imagery interpretation—The process of location, recognition, identification, and description of objects, activities, and terrain represented on imagery. (JP 1-02)

immediate targets—Targets upon which are detected too late to be included in the normal targeting process, therefore, effects have not been scheduled. Immediate targets have three subcategories: unplanned, unanticipated, and time-sensitive. (Upon approval of JP 3-60, this term and its definition will be included in JP 1-02.)

indications and warning—Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to US citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorists' attacks; and other similar events. Also called I&W. (JP 1-02)

indirect effects—Result created through an inter-mediate effect or mechanism to produce the final outcome, which may be physical or psychological in nature. Indirect effects tend to be delayed, and may be difficult to recognize. (Proposed by JP 3-60 for inclusion in JP 1-02.)

information—1. Facts, data, or instructions in any medium or form. **2.** The meaning that a human assigns to data by means of the known conventions used in their representation. (JP 1-02)

information exchange requirement—The requirement for information to be passed between and among forces, organizations, or administrative structures concerning ongoing activities. Information exchange requirements identify who exchanges what information with whom, as well as why the information is necessary and how that information will be used. The quality (i.e., frequency, timeliness, security) and quantity (i.e., volume, speed, and type of information such as data, voice, and video) are attributes of the information exchange included

in the information exchange requirement. (MCRP 5-12C)

information report—Report used to forward raw information collected to fulfill intelligence requirements. (JP 1-02)

information requirements—Those items of information regarding the enemy and his environment which need to be collected and processed in order to meet the intelligence requirements of a commander. (JP 1-02)

integration—A stage in the intelligence cycle in which a pattern is formed through the selection and combination of evaluated information. (JP 1-02)

intelligence—1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. **2.** Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding. (JP 1-02) Also in Marine Corps usage, intelligence is knowledge about the enemy or the surrounding environment needed to support decision-making. This knowledge is the result of the collection, processing, exploitation, evaluation, integration, analysis, and interpretation of available information about the battlespace and threat. (MCRP 5-12C)

intelligence annex—A supporting document of an operation plan or order that provides detailed information on the enemy situation, assignment of intelligence tasks, and intelligence administrative procedures. (JP 1-02)

intelligence cycle—The steps by which information is converted into intelligence and made available to users. (Excerpt from JP 1-02)

intelligence data—Data derived from assets primarily dedicated to intelligence collection such as imagery systems, electronic intercept equipment, human intelligence sources, etc. (MCRP 5-12C)

intelligence discipline—A well-defined area of intelligence collection, processing, exploitation, and reporting using a specific category of technical or human resources. There are five major disciplines: human intelligence, imagery intelligence, measurement and signature intelligence, signals intelligence (communications intelligence, electronic intelligence, and foreign instrumentation signals intelligence), and open-source intelligence. (JP 1-02)

intelligence estimate—The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to the enemy or potential enemy and the order of probability of their adoption. (JP 1-02)

intelligence journal—A chronological log of intelligence activities covering a stated period, usually 24 hours. It is an index of reports and messages that have been received and transmitted, and of important events that have occurred**,** and actions taken. The journal is a permanent and official record. (JP 1-02)

intelligence operations—The variety of intelligence tasks that are carried out by various intelligence organizations and activities. (Excerpt from JP 1-02)

intelligence preparation of the battlespace—1. An analytical methodology employed to reduce uncertainties concerning the enemy, environment, and terrain for all types of operations. Intelligence preparation of the battlespace builds an extensive data base for each potential area in which a unit may be required to operate. The data base is then analyzed in detail to determine the impact of the enemy, environment, and terrain on operations and presents it in graphic form. Intelligence preparation of the battlespace is a continuing process. Also called IPB. (JP 1-02) **2.** In Marine Corps usage, the systematic,

continuous process of analyzing the threat and environment in a specific geographic area. (MCRP 5-12C)

intelligence report—A specific report of information, usually on a single item, made at any level of command in tactical operations and disseminated as rapidly as possible in keeping with the timeliness of the information. Also called INTREP. (JP 1-02)

intelligence requirement—**1**. Any subject, general or specific, upon which there is a need for the collection of information, or the production of intelligence. (JP 1-02) **2**. In Marine Corps usage, questions about the enemy and the environment, the answers to which a commander requires to make sound decisions. Also called IR. (MCRP 5-12C)

intuitive decisionmaking—The act of reaching a conclusion which emphasizes pattern recognition based on knowledge, judgment, experience, education, intelligence, boldness, perception, and character. This approach focuses on assessment of the situation vice comparison of multiple options. (MCRP 5-12C)

joint deployable intelligence support system—A transportable workstation and communications suite that electronically extends a joint intelligence center to a joint task force or other tactical user. Also called JDISS. (JP 1-02)

joint force—A general term applied to a force composed of significant elements, assigned or attached, of two or more Military Departments, operating under a single joint force commander. (JP 1-02)

joint intelligence center—The intelligence center of the joint force headquarters. The joint intelligence center is responsible for providing and producing the intelligence required to support the joint force commander and staff, components, task forces and elements, and the national intelligence community. Also called JIC. (JP 1-02)

joint intelligence support element—A subordinate joint force forms a joint intelligence support element as the focus for intelligence support for joint operations, providing the joint force commander, joint staff, and components with the complete air, space, ground, and maritime adversary situation. Also called JISE. (JP 1-02)

joint operations—A general term to describe military actions conducted by joint forces, or by Service forces in relationships (e.g., support, coordinating authority), which, of themselves, do not create joint forces. (JP 1- 02)

joint targeting coordination board—A group formed by the joint force commander to accomplish broad targeting oversight functions that may include but are not limited to coordinating targeting information, providing targeting guidance and priorities, and preparing and/or refining joint target lists. The board is normally comprised of representatives from the joint force staff, all components, and if required, component subordinate units. (JP 1-02)

joint task force—A joint force that is constituted and so designated by the Secretary of Defense, a combatant commander, a subunified commander, or an existing joint task force commander. Also called JTF. (JP 1-02)

Joint Worldwide Intelligence Communications System—The sensitive compartmented information portion of the Defense Information System Network. It incorporates advanced networking technologies that permit point-to-point or multipoint information exchange involving voice, text, graphics, data, and video teleconferencing. Also called JWICS. (JP 1-02)

large-scale map—A map having a scale of 1:75,000 or larger. (JP 1-02)

line of communications—A route, either land, water, and/or air, which connects an operating military force with a base of operations and along which supplies and military forces move. (JP 1-02)

list of targets—A tabulation of confirmed or suspect targets maintained by any echelon for informational and fire support planning purposes. (JP 1-02)

main effort—The designated subordinate unit whose mission at a given point in time is most critical to overall mission success. It is usually weighted with the preponderance of combat power and is directed against a center of gravity through a critical vulnerability. (MCRP 5-12C)

maneuver warfare—A warfighting philosophy that seeks to shatter the enemy's cohesion through a variety of rapid, focused, and unexpected actions which create a turbulent and rapidly deteriorating situation with which the enemy cannot cope. (MCRP 5-12C)

mapping, charting, and geodesy—Maps, charts, and other data used for military planning, operations, and training. These products and data support air, land, and sea navigation; weapon system guidance; target positioning; and other military activities. These data are presented in the forms of topographic, planimetric, imaged, or thematic maps and graphics; nautical and aeronautical charts and publications; and, in digital and textual formats, gazetteers, which contain geophysical and geodetic data and coordinate lists. (JP 1-02)

Marine air-ground task force—The Marine Corps principal organization for all missions across the range of military operations, composed of forces task-organized under a single commander capable of responding rapidly to a contingency anywhere in the world. The types of forces in the MAGTF are functionally grouped into four core elements: a command element, an aviation combat element, a ground combat element, and a combat service support element. The four core elements are categories of forces, not formal commands. The basic structure of the Marine air-ground task force never varies, though the number, size, and type of Marine Corps units comprising each of its four elements will always be mission dependent. The flexibility of the organizational structure allows for one or more subordinate MAGTFs, other Service and/or foreign military forces, to be assigned or attached. Also called MAGTF. (Approved for inclusion in next version of MCRP 5-12C)

Marine Corps Planning Process—A six-step methodology which helps organize the thought processes of the commander and staff throughout the planning and execution of military operations. It focuses on the threat and is based on the Marine Corps philosophy of maneuver warfare. It capitalizes on the principle of unity of command and supports the establishment and maintenance of tempo. The six steps consist of mission analysis, course of action development, course of action analysis, comparison/decision, orders development, and transition. Also called MCPP. NOTE: Tenets of the MCPP include top down planning, single battle concept, and integrated planning. (MCRP 5-12C)

Marine expeditionary force—The largest Marine air-ground task force and the Marine Corps principal warfighting organization, particularly for larger crises or contingencies. It is task-organized around a permanent command element and normally contains one or more Marine divisions, Marine aircraft wings, and Marine force service support groups. The Marine expeditionary force is capable of missions across the range of military operations, including amphibious assault and sustained operations ashore in any environment. It can operate from a sea base, a land base, or both. It may also contain other Service or foreign military forces assigned or attached to the MAGTF. Also called MEF. (Approved for inclusion in next version of MCRP 5-12C)

Marine expeditionary unit—A Marine air-ground task force that is constructed around an infantry battalion reinforced, a helicopter squadron reinforced, and a task-organized combat service support element. It normally fulfills Marine Corps forward sea-based deployment requirements. The Marine expeditionary unit provides an immediate reaction capability for crisis response and is capable of limited combat operations. It may contain other Service or foreign military forces assigned or attached. Also called MEU. (Approved for inclusion in next version of MCRP 5-12C)

Marine expeditionary unit (special operations capable)—The Marine Corps standard, forward-deployed, sea-based expeditionary organization. The MEU(SOC) is a MEU, augmented with selected personnel and equipment, that is trained and equipped with an enhanced capability to conduct amphibious operations and a variety of specialized missions, of limited scope and duration. These capabilities include specialized demolition, clandestine reconnaissance and surveillance, raids, in-extremis hostage recovery, and enabling operations for follow-on forces. The Marine expeditionary unit (special operations capable) is not a special operations force but, when directed by the National Command Authorities, the combatant commander in chief, and/or other operational commander, may conduct limited special operations in extremis, when other forces are inappropriate or unavailable. It may also contain other Service or foreign military forces assigned or attached to the Marine air-ground task force. Also called MEU (SOC). (Approved for inclusion in next version of MCRP 5-12C)

measurement and signature intelligence—Scientific and technical intelligence obtained by quantitative and qualitative analysis of data (metric, angle, spatial, wavelength, time dependence, modulation, plasma, and hydromagnetic) derived from specific technical sensors for the purpose of identifying any distinctive features associated with the target. The detected feature may be either reflected or emitted. (JP 1-02)

medium-scale map—A map having a scale larger than 1:600,000 and smaller than 1:75,000. (JP 1-02)

meteorological data—Meteorological facts pertaining to the atmosphere, such as wind, temperature, air density, and other phenomena which affect military operations. (JP 1-02)

military operations other than war—Operations that encompass the use of military capabilities across the range of military operations short of war. These military actions can be applied to complement any combination of the other instruments of national power and occur before, during, and after war. Also called MOOTW. (JP 1-02)

modified combined obstacle overlay—A product used to depict the battlespace's effects on military operations. It is normally based on a product depicting all obstacles to mobility, modified to also depict the following, which are not prescriptive nor inclusive: cross-country mobility classifications (such as RESTRICTED); objectives; avenues of approach and mobility corridors; likely locations of countermobility obstacle systems; likely engagement areas; and key terrain. Also called MCOO. (MCRP 5-12C)

multinational operations—A collective term to describe military actions conducted by forces of two or more nations, typically organized within the structure of a coalition or alliance. (JP 1-02)

multi-spectral imagery—The image of an object obtained simultaneously in a number of discrete spectral bands. (JP 1-02)

munitions effects assessment. Conducted concurrently and interactively with battle damage assessment, the assessment of the military force applied in terms of the weapon system and munitions effectiveness to determine and

recommend any required changes to the methodology, tactics, weapon system, munitions, fusing and/or weapon delivery parameters to increase force effectiveness. Munitions effects assessment is primarily the responsibility of operations with required inputs and coordination from the intelligence community. Also called MEA. (Proposed by JP 3-60 for inclusion in JP 1-02.)

named area of interest—A point or area along a particular avenue of approach through which enemy activity is expected to occur. Activity or lack of activity within a named area of interest will help to confirm or deny a particular enemy course of action. Also called NAI. (MCRP 5-12C)

national intelligence support team—A nationally sourced team composed of intelligence and communications experts from either Defense Intelligence Agency, Central Intelligence Agency, National Security Agency, or any combination of these agencies. Also called NIST. (JP 1-02)

near real time—Pertaining to the timeliness of data or information which has been delayed by the time required for electronic communication and automatic data processing. This implies that there are no significant delays. (JP 1-02)

noncombatant evacuation operations—Operations directed by the Department of State, the Department of Defense, or other appropriate authority whereby noncombatants are evacuated from foreign countries when their lives are endangered by war, civil unrest, or natural disaster to safe havens or to the United States. Also called NEO. (JP 1-02)

no-strike target list—A list designated by a commander containing targets not to be destroyed. Destruction of targets on the list would interfere with or unduly hamper projected friendly military operations, or friendly relations with indigenous personnel or governments. (JP 1-02)

open-source intelligence—Information of potential intelligence value that is available to the general public. (JP 1-02)

operational architecture—A description (often graphical) of the operational elements, assigned tasks, and information flows required to support the warfighter. It defines the type of information, the frequency of exchange, and what tasks are supported by these information exchanges. (MCRP 5-12C)

operational control—Transferable command authority that may be exercised by commanders at any echelon at or below the level of combatant command. Operational control is inherent in combatant command (command authority). Operational control may be delegated and is the authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives, and giving authoritative direction necessary to accomplish the mission. Operational control includes authoritative direction over all aspects of military operations and joint training necessary to accomplish missions assigned to the command. Operational control should be exercised through the commanders of subordinate organizations. Normally this authority is exercised through subordinate joint force commanders and service and/or functional component commanders. Operational control normally provides full authority to organize commands and forces and to employ those forces as the commander in operational control considers necessary to accomplish assigned missions. Operational control does not, in and of itself, include authoritative direction for logistics or matters of administration, discipline, internal organization, or unit training. Also called OPCON. (JP 1-02)

operations control and analysis center—Main node for the command and control of radio battalion signals intelligence operations and the overall coordination of MAGTF signals intelli-

gence operations. Processes, analyzes, produces, and disseminates signals intelligence-derived information and directs the ground-based electronic warfare activities of the radio battalion. Also called OCAC. (MCRP 5-12C)

operational level of war—The level of war at which campaigns and major operations are planned, conducted, and sustained to accomplish strategic objectives within theaters or areas of operations. Activities at this level link tactics and strategy by establishing operational objectives needed to accomplish the strategic objectives, sequencing events to achieve the operational objectives, initiating actions, and applying resources to bring about and sustain these events. These activities imply a broader dimension of time or space than do tactics; they ensure the logistic and administrative support of tactical forces, and provide the means by which tactical successes are exploited to achieve strategic objectives. (JP 1-02)

order of battle—The identification, strength, command structure, and disposition of the personnel, units, and equipment of any military force. Also called OOB. (JP 1-02)

paramilitary forces—Forces or groups which are distinct from the regular armed forces of any country, but resembling them in organization, equipment, training, or mission. (JP 1-02)

physical damage assessment—The estimate of the quantitative extent of physical damage (through munitions blast, fragmentation, and/or fire damage effects) to a target resulting from the application of military force. This assessment is based upon observed or interpreted damage. (Proposed by JP 3-60 for inclusion in JP 1-02.)

planned targets—Targets that are known to exist in an operational area and which effects are scheduled in advance or are on-call. Examples range from targets on joint target lists (JTLs) in applicable campaign plans, to targets detected in sufficient time to list in the air tasking order (ATO), mission-type orders, or fire support plans. Planned targets have two subcategories: *scheduled* or *on call.* (Proposed by JP 3-60 for inclusion in JP 1-02.)

priority intelligence requirements—1. Those intelligence requirements for which a commander has an anticipated and stated priority in his task of planning and decisionmaking. Also called PIR. (JP 1-02) **2.** In Marine Corps usage, an intelligence requirement associated with a decision that will critically affect the overall success of the command's mission. (MCRP 5-12C)

production—The conversion of information into intelligence through the integration, analysis, evaluation, and interpretation of all-source data and the preparation of intelligence products in support of known or anticipated user requirements. Production is a process of synthesis—the most important action in developing usable intelligence for the commander. (MCWP 2-1)

production management—Encompasses determining the scope, content, and format of each intelligence product, developing a plan and schedule for the development of each product, assigning priorities among the various production requirements, allocating processing, exploitation, and production resources, and integrating production efforts with intelligence collection and dissemination. (MCRP 5-12C)

reach back—The ability to exploit resources, capabilities, expertise, etc., not physically located in the theater or a joint operations area, when established. (MCRP 5-12C)

reactive target—The method used for targeting targets of opportunity. It is used when time and situation do not allow for targeting; i.e., during deliberate targeting, during an attack, when defending against an attack, or upon discovery of the location of a target such as a

radio jammer, tank, or antiaircraft weapon. (MCRP 5-12C)

reattack recommendation—An assessment, derived from the results of battle damage assessment and munitions effects assessment, providing the commander systematic advice on reattack of targets and further target selection to achieve objectives. The reattack recommendation considers objective achievement, target, and aimpoint selection, attack timing, tactics, weapon system and munitions selection. The reattack recommendation is a combined operations and intelligence function. (Proposed by JP 3-60 for inclusion in JP 1-02.)

request for information—Any specific time-sensitive ad hoc requirement for intelligence information or products to support an ongoing crisis or operation not necessarily related to standing requirements or scheduled intelligence production. A request for information can be initiated to respond to operational requirements and will be validated in accordance with the theater command's procedures. (JP 1-02)

scheduled targets—Planned targets that are known to exist in an operational area and are located in sufficient time for deliberate planning to meet specific campaign objectives. (Proposed by JP 3-60 for inclusion in JP 1-02.)

scientific and technical intelligence—The product resulting from the collection, evaluation, analysis, and interpretation of foreign scientific and technical information which covers: **a**. foreign developments in basic and applied research and in applied engineering techniques; and **b**. scientific and technical characteristics, capabilities, and limitations of all foreign military systems, weapons, weapon systems, and materiel, the research and development related thereto, and the production methods employed for their manufacture. (JP 1-02)

SECRET internet protocol router network—Worldwide SECRET level packet switch network that uses high-speed internet protocol routers and high-capacity Defense Information Systems Network circuitry. Also called SIPRNET. (JP 1-02)

sensitive compartmented information—All information and materials bearing special community controls indicating restricted handling within present and future community intelligence collection programs and their end products for which community systems of compartmentation have been or will be formally established. Also called SCI. (JP 1-02)

sensitive compartmented information facility—An accredited area, room, group of rooms, or installation where sensitive compartmented information may be stored, used, discussed, and/or electronically processed. SCIF procedural and physical measures prevent the free access of persons unless they have been formally indoctrinated for the particular SCI authorized for use or storage within the SCIF. (JP 1-02)

sensor data—Data derived from sensors whose primary mission is surveillance or target acquisition, such as air surveillance radars, counterbattery radars, and remote ground sensors. (MCRP 5-12C)

sequel(s)—Major operations that follow the current major operations. Plans for these are based on the possible outcomes (success, stalemate, or defeat) associated with the current operation. (MCRP 5-12C)

signals intelligence—1. A category of intelligence comprising either individually or in combination all communications intelligence, electronics intelligence, and foreign instrumentation signals intelligence, however transmitted. **2.** Intelligence derived from communications, electronics, and foreign instrumentation signals. Also called SIGINT. (JP 1-02)

situational awareness—Knowledge and understanding of the current situation which promotes timely, relevant, and accurate assessment of

friendly, enemy, and other operations within the battlespace in order to facilitate decisionmaking. An informational perspective and skill that foster an ability to determine quickly the context and relevance of events that are unfolding. (MCRP 5-12C)

special purpose Marine air-ground task force—A Marine air-ground task force organized, trained and equipped with narrowly focused capabilities. It is designed to accomplish a specific mission, often of limited scope and duration. It may be any size, but normally it is a relatively small force--the size of a Marine expeditionary unit or smaller. It may contain other Service or foreign military forces assigned or attached to the Marine air-ground task force. Also called SPMAGTF. (Approved for inclusion in next version of MCRP 5-12C)

staff cognizance—The broad responsibility and authority over designated staff functions assigned to a general or executive staff officer (or their subordinate staff officers) in their area of primary interest. These responsibilities and authorities can range from coordination within the staff to the assignment or delegation to the staff officer by the commander to exercise authority for a specified warfighting function or sub-function. Staff cognizance includes the responsibility for effective use of available resources and may include the authority for planning the employment of, organizing, assigning tasks, coordinating, and controlling forces for the accomplishment of assigned missions. Marine Corps orders and doctrine provide the notional staff cognizance for general or executive staff officers, which may be modified by the commander to meet requirements. (Draft MCWP 6-2)

surveillance and reconnaissance cell—Primary element responsible for the supervision of MAGTF intelligence collection operations. Directs, coordinates, and monitors intelligence collection operations conducted by organic, attached, and direct support collection assets. Also called SARC. (Change approved for inclusion in next version of MCRP 5-12C)

sustained operations ashore—The employment of Marine Corps forces on land for an extended duration. It can occur with or without sustainment from the sea. Also called SOA. (MCRP 5-12C)

synthesis—In intelligence usage, the examining and combining of processed information with other information and intelligence for final interpretation. (JP 1-02) Note: The piecing of information into a coherent, meaningful picture of the battlespace based on the ongoing or previous analysis of information and events taking place in the area of operations.

tactical intelligence—Intelligence that is required for planning and conducting tactical operations. (JP 1-02) In Marine Corps usage, tactical intelligence is concerned primarily with the location, capabilities, and possible intentions of enemy units on the battlefield and with the tactical aspects of terrain and weather within the battlespace. (MCRP 5-12C)

tactical effect—Result of action(s) at the individual unit, mission, or engagement level. Can be either direct or indirect, and typically acts in concert with other tactical effects to produce results at higher levels of war. (Proposed by JP 3-60 for inclusion in JP 1-02.)

target—A geographical area, complex, or installation planned for capture or destruction by military forces. (JP 1-02)

target analysis—An examination of potential targets to determine military importance, priority of attack, and weapons required to obtain a desired level of damage or casualties. (JP 1-02)

targeted area of interest—The geographical area or point along a mobility corridor where successful interdiction will cause the enemy to either abandon a particular course of action or

require him/her to use specialized engineer support to continue, where the enemy can be acquired and engaged by friendly forces. Not all targeted areas of interest will form part of the friendly course of action; only targeted areas of interest associated with high-payoff targets are of interest to the staff. These are identified during staff planning and war-gaming. Target areas of interest differ from engagement areas in degree. Engagement areas plan for the use of all available weapons. Targeted areas of interest might be engaged by a single weapon. Also called TAI. (MCRP 5-12C)

target complex—A geographically integrated series of target concentrations. (JP 1-02)

target component—A major element of a target complex or target. It is any machinery, structure, personnel, or other productive asset that contributes to the operation or output of the target complex or target. (JP 1-02)

target concentration—A grouping of geographically proximate targets. (JP 1-02)

target critical damage point—The part of a target component that is most vital. Also called critical node. (JP 1-02)

target dossier—A file of assembled target intelligence about a specific geographic area. (JP 1-02)

target folder—A folder containing target intelligence and related materials prepared for planning and executing action against a specific target. (JP 1-02)

targeting—The process to detect, select, and prioritize targets, match the appropriate action, and assess the resulting effects based on the commander's objective, guidance, and intent. (Proposed by JP 3-60 for inclusion in JP 1-02.)

target intelligence—Intelligence which portrays and locates the components of a target or target complex and indicates its vulnerability and relative importance. (JP 1-02)

target materials—Graphic, textual, tabular, digital, video, or other presentations of target intelligence, primarily designed to support operations against designated targets by one or more weapon(s) systems. Target materials are suitable for training, planning, executing, and evaluating military operations. (JP 1-02)

target of opportunity—A target visible to a surface or air sensor or observer, which is within range of available weapons and against which fire has not been scheduled or requested. (JP 1-02)

target priority—A grouping of targets with the indicated sequence of attack. (JP 1-02)

target signature—The characteristic pattern of a target displayed by detection and identification equipment. (JP 1-02)

target stress point—The weakest point (most vulnerable to damage) on the critical damage point. Also called vulnerable node. (JP 1-02)

target system—1. All the targets situated in a particular geographic area and functionally related. (DOD) **2.** A group of targets which are so related that their destruction will produce some particular effect desired by the attacker. (JP 1-02)

target system assessment—The broad assessment of the overall impact and effectiveness of the full spectrum of military force applied against the operation of an enemy target system or total combat effectiveness (including significant subdivisions of the system) relative to the operational objectives established. (Proposed by JP 3-60 for inclusion in JP 1-02.)

target system component—A set of targets belonging to one or more groups of industries and basic utilities required to produce compo-

nent parts of an end product such as periscopes, or one type of a series of interrelated commodities, such as aviation gasoline. (JP 1-02)

technical control—The performance of specialized or professional service, or the exercise of professional guidance or direction through the establishment of policies and procedures. (Proposed USMC definition per MCWP 6-2 and the next revision of MCRP 5-12C.)

tempo—The relative speed and rhythm of military operations over time. (MCRP 5-12C)

terrain analysis—The collection, analysis, evaluation, and interpretation of geographic information on the natural and manmade features of the terrain, combined with other relevant factors, to predict the effect of the terrain on military operations. (JP 1-02)

terrain study—An analysis and interpretation of natural and manmade features of an area, their effects on military operations, and the effect of weather and climate on these features. (JP 1-02)

time-sensitive targets—Those targets requiring immediate response because they pose (or will soon pose) a clear and present danger to friendly forces or are highly lucrative, fleeting targets of opportunity. (JP 1-02)

validation—A process normally associated with the collection of intelligence that provides official status to an identified requirement and confirms that the requirement is appropriate for a given collector and has not been previously satisfied. (JP 1-02)

vulnerability—1. The susceptibility of a nation or military force to any action by any means through which its war potential or combat effectiveness may be reduced or its will to fight diminished. **2.** The characteristics of a system which cause it to suffer a definite degradation (incapability to perform the designated mission) as a result of having been subjected to a certain level of effects in an unnatural (manmade) hostile environment. **3.** In information operations, a weakness in information system security design, procedures, implementation, or internal controls that could be exploited to gain unauthorized access to information or an information system. (JP 1-02)

warfighting functions—The six mutually supporting military activities integrated in the conduct of all military operations are:

1. **command and control**—The means by which a commander recognizes what needs to be done and sees to it that appropriate actions are taken.
2. **maneuver**—The movement of forces for the purpose of gaining an advantage over the enemy.
3. **fires**—Those means used to delay, disrupt, degrade, or destroy enemy capabilities, forces, or facilities as well as affect the enemy's will to fight.
4. **intelligence**—Knowledge about the enemy or the surrounding environment needed to support decision-making.
5. **logistics**—All activities required to move and sustain military forces.
6. **force protection**—Actions or efforts used to safeguard own centers of gravity while protecting, concealing, reducing, or eliminating friendly critical vulnerabilities. (MCRP 5-12C)

weaponeering—The process of determining the quantity of a specific type of lethal or nonlethal weapons required to achieve a specific level of damage to a given target, considering target vulnerability, weapon effect, munitions delivery accuracy, damage criteria, probability of kill, and weapon reliability. (JP 1-02)

APPENDIX K. REFERENCES

North Atlantic Treaty Organization Standardization Agreements (STANAGs)

2022	Intelligence Reports
2077	Orders of Battle
2936	Intelligence Doctrine-AIntP-1(A)

Defense Intelligence Management Documents (DIMDs)

0000-151-94	Department of Defense Intelligence Production Program (DODIPP)
0000-151C-95	Department of Defense Intelligence Production Program (DODIPP): Production Procedures

Defense Intelligence Report

DI-2820-2-99	Battle Damage Assessment (BDA) Reference Handbook (final draft)

Joint Publications (JPs)

1-02	Department of Defense Dictionary of Military and Associated Terms
2-0	Doctrine for Intelligence Support to Joint Operations
2-01	Joint Intelligence Support to Military Operations
2-01.3	Joint Tactics, Techniques, and Procedures for Joint Intelligence Preparation of the Battlespace
2-02	National Intelligence Support to Joint Operations
2-03	Joint Tactics, Techniques, and Procedures for Geospatial Information and Services Support to Joint Operations
3-02	Joint Doctrine for Amphibious Operations
3-02.1	Joint Doctrine for Landing Force Operations
3-07	Joint Doctrine for Military Operations Other Than War
3-09	Doctrine for Joint Fire Support
3-13	Joint Doctrine for Information Operations
3-13.1	Joint Doctrine for Command and Control Warfare
3-50.3	Joint Doctrine for Evasion and Recovery
3-55	Doctrine for Reconnaissance, Surveillance, and Target Acquisition Support for Joint Operations
3-60	Doctrine for Joint Targeting (Draft)
5-00.2	Joint Task Force (JTF) Planning Guidance and Procedures

Marine Corps Intelligence Activity Publications

1586-001-96	MAGTF Contingency Reference Guide
1586-005-99	Urban Generic Information Requirements Handbook

Marine Corps Doctrinal Publications (MCDPs)

1	Warfighting
1-2	Campaigning
2	Intelligence
3	Expeditionary Operations
5	Planning
6	Command and Control

Marine Corps Warfighting Publications (MCWPs)

0-1.1	Componency
2-1	Intelligence Operations
2-12.1	Geographic Intelligence
2-14	Counterintelligence
2-15.2	Signals Intelligence
3-2	Aviation Operations
3-16	Fire Support Coordination in the Ground Combat Element
3-35.3	Military Operations on Urbanized Terrain (MOUT)
3-35.7	MAGTF Meteorological and Oceanographic Support
4-1	Logistics Operations
5-1	Marine Corps Planning Process
6-22	Communications and Information Systems

Marine Corps Reference Publications (MCRPs)

5-12C	Marine Corps Supplement to the Department of Defense Dictionary of Military and Associated Terms
5-12D	Organization of Marine Corps Forces

Fleet Marine Force Manual (FMFM)

6	Ground Combat Operations (under revision as MCWP 3-1)

Army Field Manuals (FMs)

34-8-2	Intelligence Officer's Handbook
34-81	Weather Support for Army Tactical Operations
34-81-1	Battlefield Weather Effects
34-130/FMFRP 3-23.2	Intelligence Preparation of the Battlefield (under revision as MCRP 2-12A)
101-5-1/MCRP 5-2A	Operational Terms and Graphics

To Our Readers

Changes: Readers of this publication are encouraged to submit suggestions and changes to Doctrine Control Branch via e-mail: doctrine@usmc.mil.

Suggestions and changes must include the following information:

- Location of change
  - Publication number and title
  - Current page number
  - Paragraph number (if applicable)
  - Line number
  - Figure or table number (if applicable)
- Nature of change
  - Addition/deletion of text
  - Proposed new text

Additional copies: If this publication is not an electronic only distribution, a printed copy may be obtained from Marine Corps Logistics Base, Albany, GA 31704-5001, by following the instructions in MCBul 5600, *Marine Corps Doctrinal Publications Status.* An electronic copy may be obtained from the United States Marine Corps Doctrine web page:

https://homeport.usmc.mil/sites/mcdoctrine/SitePages/Home.aspx

This Page Is Intentionally Left Blank

REF ID:A58489

~~RESTRICTED~~

DEPARTMENT OF THE ARMY TECHNICAL MANUAL TM 32-250

DEPARTMENT OF THE AIR FORCE MANUAL AFM 100-80

FUNDAMENTALS OF TRAFFIC ANALYSIS (RADIO-TELEGRAPH)

RESTRICTED. DISSEMINATION OF RESTRICTED MATTER.—No person is entitled solely by virtue of his grade or position to knowledge or possession of classified matter. Such matter is entrusted only to those individuals whose official duties require such knowledge or possession. (See also AR 380–5.)

DEPARTMENTS OF THE ARMY AND THE AIR FORCE
OCTOBER 1948

~~RESTRICTED~~

Declassified and approved for release by NSA on 12-24-2013 pursuant to E.O. 13526

REF ID:A58489

WARNING

Authority for release of this document to a foreign government must be secured from the Assistant Chief of Staff, G–2.

When this document is released to a foreign government, it is released subject to the following conditions: This information is furnished with the understanding that it will not be released to another nation without specific approval of the United States of America, Department of the Army; that it will not be used for other than military purposes; that individual or corporation rights originating in the information whether patented or not will be respected; and that the information will be afforded substantially the same degree of security as afforded by the United States of America, Department of the Army.

REF ID:A58489

TM 32–250—AFM 100–80

FUNDAMENTALS OF TRAFFIC ANALYSIS (RADIO-TELEGRAPH)

RESTRICTED. ***DISSEMINATION OF RESTRICTED MATTER.***—**No person is entitled solely by virtue of his grade or position to knowledge or possession of classified matter. Such matter is entrusted only to those individuals whose official duties require such knowledge or possession. (See also AR 380–5.)**

United States Government Printing Office
Washington; 1948

REF ID:A58489

DEPARTMENTS OF THE ARMY AND THE AIR FORCE
Washington 25, D C, 1 October 1948

TM 32-250—AFM 100-80, Fundamentals of Traffic Analysis (Radio Telegraph) is published for the information and guidance of all concerned

[AG 300.7 (9 Jun 48)]

BY ORDER OF THE SECRETARIES OF THE ARMY AND THE AIR FORCE

OFFICIAL
EDWARD F WITSELL
Major General
The Adjutant General

OMAR N BRADLEY
Chief of Staff, United States Army

OFFICIAL
L L JUDGE
Colonel, USAF
Air Adjutant General

HOYT S VANDENBERG
Chief of Staff, United States Air Force

DISTRIBUTION

Army

GSUSA (1), Arm & Sv Bd (2), AFF (15), OS Maj Comd (5), Base Comd (2), MDW (16), A (ZI) (30), (Overseas) (15), CHQ (5), D (3), USMA (20), Sch (10) except Ground Gen and 11 (25), ROTC (1), T/O & E 32-952 (20), 32-1027 (20)

Air Force

USAF (10), USAF Maj Comds (5), USAF Sub Comds (3), Div (Air) (2)

For explanation of distribution formula, see TM 38-405

REF ID:A58489

CONTENTS

		Paragraphs	Page
CHAPTER 1.	**INTRODUCTION.**		
Section I	General	1–5	1
II	General Approach	6–7	4
CHAPTER 2.	**RADIO OPERATIONS.**		
Section I	Introduction	8–9	6
II	Operating Data	10–15	7
III	Elements of Radio Procedure	16–20	28
IV	The Message Externals	21–29	34
V	Textual Features	30–36	40
VI	Collateral Material	37–40	42
CHAPTER 3.	**RECONSTRUCTION OF THE RADIO NETWORK.**		
Section I	Introduction	41–43	45
II	Analysis of Radio Operations	44–52	45
III	Net Reconstruction	53–59	73
IV	Methodology of Analysis	60–62	86
CHAPTER 4.	**APPLICATIONS OF TRAFFIC ANALYSIS.**		
Section I	Intercept Operations	63–69	90
II	Applications to Cryptanalysis	70–74	94
III	Applications to Intelligence	75–79	98
APPENDIX.	**REFERENCES**		102

REF ID:A58489

CHAPTER 1

INTRODUCTION

Section I. GENERAL

1. Purpose

The purpose of this manual is to present a standard approach to traffic analysis problems of the military type in order to furnish signal intelligence personnel with a knowledge of traffic analysis techniques, capabilities, and applications. It is to be recognized that no text on analytic techniques can be definitive because techniques are subject to continual improvement and change in order to meet changing problems. This text is intended merely as a guide. Specific application is dependent on the ability and ingenuity of the analyst.

2. Scope

This manual is concerned only with traffic analysis of military radio communications, but the techniques covered will also be found of value in the analysis of other kinds of communication networks. Discussion of other means of communication, such as wire or cable, has not been included; in the reconstruction of the radio communication system it should be remembered that often these other means will account for missing portions of the system. Further, the scope is limited to the study of Morse transmissions. Non-Morse transmissions, such as radio-teletype and radio-telephone, are not discussed. The differences, however, are largely technical and procedural and involve the material transmitted only to a limited extent. It is thought, therefore, that this text will serve as a basis for all traffic analysis and that, with some minor modification, the methodology described will be found applicable to all types of transmission.

REF ID:A58489

3. References

A general knowledge of radio theory, Morse code, and radio procedure is assumed. For reference purposes the field and technical manuals listed in the appendix will be found useful.

4. Definition of Traffic Analysis

Traffic analysis is that branch of signal intelligence analysis which deals with the study of the external characteristics of signal communications and related materials for the purpose of obtaining information concerning the organization and operation of a communication system. This information is used (1) as a guide to efficient intercept operation, (2) as an aid to cryptanalysis, and (3) as a basis for drawing deductions and inferences of value as intelligence even in the absence of specific knowledge of the contents of the message.

5. Objectives

To achieve planned and coordinated action, it is necessary for the components of a military force to communicate with each other from the highest headquarters through all intermediary channels to the individual man in the field or the airplane in the air. Much of this communication, for reason of speed and efficiency, is conducted by radio, and radio is vulnerable to intercept. Therefore, disguises are devised to conceal both the traffic passed and the structure of the communication network. Traffic is disguised through the employment of codes and ciphers, and it is the task of cryptanalysis to solve these codes and ciphers. The communications net work is disguised through the use of a number of techniques which relate, for example, to the use of call signs and frequencies, the method of routing messages, and the use of secret procedure signs. These techniques, the means for attacking them, and the resulting reconstruction of the network are the study of traffic analysis. The responsibility of the traffic analyst, however, does not stop with the reconstruction of the communication network. It is also part of his mission to discover practical applications for his knowledge in the associated fields of intercept, cryptanalysis, intelligence, and security. The objectives of traffic analysis, then, fall into two main groups:

a. The acquisition of a detailed knowledge and a complete understanding of a communications network. This involves the reconstruction of the nets, the determination of the features of their operation, the solution of call sign and routing systems, analysis of the components of the message externals, the interpretation of radio procedure, and the use of the various cryptographic systems passed; in

REF ID:A58489

other words, everything about communications except the actual cryptanalysis of the text.

b. The application of this knowledge to—

(1) *Intercept operations.* Traffic analysis contributes to three aspects of the intercept problem. First, by providing the intercept station with certain necessary information, such as call sign and frequency lists, target locations, schedules, etc., it assists the station in the accomplishment of its mission and encourages the best possible results. Second, in coordination with cryptanalytic and intelligence interests, it determines the priorities governing the interception of individual circuits. Third, through a study of intercept, it checks the performance of the station in relation to its mission.

(2) *Cryptanalysis.* Aid to cryptanalysis is furnished in a great variety of ways, largely dependent on the cryptanalytic and traffic analytic peculiarities of the communications under study. *In most instances, traffic analysis and cryptanalysis become so interrelated that it is impossible to determine where one begins and the other leaves off, and it is necessary to set an arbitrary dividing line.* In general, however, assistance takes the following forms: the solution of the routing systems, where disguised, and the placing of the routings in the clear on traffic; the study of the uses of the various cryptographic systems; the reading of chatter for items of cryptanalytic interest; the discovery of crib, or stereotype, texts from message externals; the location of isolog messages; and the application of other traffic analysis data, such as message serial numbers, which may be of value in specific cryptanalytic problems.

(3) *Intelligence.* Military communications, including both the organization of the nets and the traffic passed, reflect the disposition of troops and the intentions for movements and operations. A careful analysis, therefore, of net structure, traffic contacts and patterns, traffic volumes, and similar signals features, assists in the building of the final intelligence picture. The exact techniques to be used are, again, dependent on the individual problem and involve the recruitment, training, organization, and order of battle of the military forces under study as well as characteristics of communications.

(4) *Security.* Because the traffic analyst becomes skilled in probing the weaknesses of communication systems, he is in an ideal position to assist in maintaining high standards of security within our own communication networks. This function of traffic analysis is mentioned merely in passing. It will not be discussed further in this text.

REF ID:A58489

Section II. GENERAL APPROACH

6. The Raw Material

The traffic analyst begins his study of a communications network with three types of raw (basic) data:

a. INTERCEPT DATA. This is the information supplied by the intercept operator. It consists of the frequencies to which he is listening, the times during which he hears signals, and occasional comments such as notes on the quality of the signal or the characteristics of the radio operator.

b. THE TRANSMISSION. The transmission is the sum total of everything sent by the radio operators. It includes the initial call-up, the exchange of call signs, the traffic, servicing, miscellaneous chatter, and signing off. Traffic may be divided into two parts: the message externals (preamble and postamble) and the text. The externals generally contain radio station and message center numbers of a variety of types, routing instructions, addresses, precedence indicators, and file times, all of value in traffic analysis. The text usually exhibits a number of cryptographic features in the clear which are likewise of use.

c. COLLATERAL INFORMATION. Besides the above material, there is a large amount of data which is available or which can be made available for traffic analysis purposes. Some of these are directly related to intercept, such as goniometric bearings. Other items are message decodes, captured documents, and intelligence reports.

7. The Analytic Approach

a. Traffic analysis is partly analytic, partly synthetic. Analysis is performed on each feature of the communications network and then, through exploiting the relationships between these features or within them, traffic analysis synthesizes them into a unified whole. In other words, the types of raw data noted in paragraph 6 are first analyzed until everything possible is known about each item independently, after which, though often seemingly unrelated, they can be pieced together to produce a complete picture of the radio nets. This means that the analyst must pay particular attention to detail and must carry much of this detail in his mind so that he can readily perceive the relationships between discrete items and integrate them to form the whole.

b. The actual approach to a traffic analysis problem is broadly determined by the stage of development of the problem. These stages of development are threefold, but it should be understood that what is represented are not clear-cut divisions in operation, but rather, gradual shiftings of emphasis as the problem matures.

REF ID:A58489

(1) *Initial attack.* (*a*) In the initial period, little is known about the problem and it may first be necessary to identify the radio nets and traffic involved so that they can be distinguished from all other types. When this has been accomplished, the characteristics are furnished to the intercept station which embarks on a large-scale search mission, scanning the entire range of frequencies for transmissions of the desired nature. During this time, it is the task of the traffic analyst to give direction to this mission and to evolve from it a definite assignment. It should be noted here that the search mission, in reduced scale, should always continue until the problem has ceased to exist, in order to cover new net developments.

(*b*) As soon as material begins to accumulate, an elementary study may be conducted on the elements of the transmission, particularly the message externals. The functions of the various preamble components should be observed, the method of routing noted, and in general, the significance of each component determined.

(2) *Development.* During the second period, emphasis is placed on the study of the communications system with a view to learning all its details of organization, operation, and procedure. There are usually two phases to this: the research phase, which involves thorough analysis of every item, such as call signs, procedure signs, message numbers, routing codes, and cryptographic features; and the actual net reconstruction, consisting of the building of the entire radio net complete with call signs, frequencies, schedules, and station locations.

(3) *Application.* When this knowledge has been gained, and even while it is being gained, it can be put to use in the three related fields of control, cryptanalysis, and intelligence. From the very first moment that traffic analysis is performed, it begins contributing to these phases of communications intelligence, but it is not until a substantial amount of information has been gathered that these applications receive full emphasis. The final goal of traffic analysis operations is the reconstruction of the complete radio network against its cryptographic and order of battle background, and the production on a day-to-day basis of items of cryptanalytic application and intelligence importance.

REF ID:A58489

CHAPTER 2

RADIO OPERATIONS

Section I. INTRODUCTION

8. Radio Operations

a. The operation of a radio network requires a set of fixed rules and regulations which define the manner and form of communications. These rules are in part subject to the laws of nature, in part to the necessities of communication itself, and in part to the whim and ingenuity of the personnel formulating them. The first two factors impose some degree of uniformity on radio networks, no matter what the type or nationality. This makes it possible to set down the basic features of communications, e.g., call signs, frequencies, message numbers, and routing instructions. However, the third factor acts to vary those features by determining the way that they are used. This chapter outlines what these basic features are and some of the ways in which they may be manipulated. It is, of course, not possible to include all the types which may be encountered, but it is hoped that what is given will serve to indicate the general patterns the traffic analyst is likely to meet in studying radio operations and will serve to set up general lines of traffic analysis thinking.

9. Phases of Radio Operations

Radio operations for purposes of study may be divided into four main phases:

a. Operating Data. The first considerations in the creation of a communication net relate to the structure or form of the net, the use of frequencies and call signs, and the system of schedules. These are the basic operating data of the net and involve its mechanical functioning. In the case of some nets, the military for instance, attempts are made to conceal these data; in other cases, such as commercial, they can be determined with little effort.

b. The Radio Transmission. Once the operating data have been determined, the next step is to devise the form and language of radio transmission. There must be regulations governing the Morse code to be used (largely dependent on the alphabet concerned), the pro-

REF ID:A58489

cedure signals which make for brevity and speed and which may be encoded for reasons of security, the order of elements in the transmission, the plain-language chatter of the radio operators, and the plain-language and simple cipher messages usually considered part of the traffic analysis task.

c. THE MESSAGE EXTERNALS. The message externals are actually a part of the radio transmission and belong under *b* above, but because of their importance a separate section (sec. IV, this ch.) is devoted to them. They include the preamble and postamble and generally contain serial numbers of various types, group check, file date and time, precedence indicators, and routing instructions.

d. TEXTUAL FEATURES. Some of the cryptographic aspects of the text are in the clear to make possible proper handling of the traffic by message center personnel and to permit decrypting. These features in the clear are often of great assistance to the traffic analyst. They may merely involve whether the text is in letters or numbers, or the length of the code groups, or they may be somewhat more complex as discriminants, indicators, or pad numbers.

Section II. OPERATING DATA

10. General

The operating data enable the network to function. They consist of the frequencies, call signs, and schedules used in communication. Traffic analysis is interested not only in the operating data as used by the network, but also in the general system on which the allocation of operating data to specific nets and radio stations is based. This section is devoted to a discussion of radio nets and of the ways in which the operating data are used and assigned.

11. Definitions

a. A radio network is composed of radio stations organized for the purpose of intercommunication. This organization is not haphazard but follows very definite and detailed patterns. These patterns are based on the order of battle since the lines of communication themselves must coincide with the echelon of command and the military requirements. Before it is possible to enter into a discussion of these patterns, however, it is necessary to define some of the terminology to be used.

(1) *Link:* Any system of telecommunication between two points.

(2) *Group:* One or more links whose stations work together as a communication entity under a common operating control.

REF ID:A58489

(3) *Net:* One group or a number of groups assembled on the basis of common operating characteristics, presumably under the administrative direction of an immediate common superior headquarters.

(4) *Network:* The radio system of a service of a nationality, as United States Army network, United States Naval network, United States Air Force network.

b. These definitions may appear somewhat obscure to the student for the moment, but it should be kept in mind that they are formulated from a traffic analysis point of view, that is, from the outside looking in. These terms must be so categorized in order to be of value analytically and, therefore, they represent the situation as it appears rather than as it actually is. Figure 1 will help to clarify these terms, and it is suggested that the student study the diagram from time to time as its understanding is essential to the proper approach to net reconstruction.

c. Figure 1 illustrates the general organization of the military network, proceeding from Department of the Army Headquarters through theater, army group, army, corps, and division. The equivalent Department of the Air Force organizations are shown in figure 2. (The following pertains equally to the Department of the Air Force.) Each line or connection represents a radio link within the terms of the definition in *a*(1) above—any telecommunication system between two points. It is to be emphasized that only *two* stations are involved in a link, never any more. Thus, the line from Department of the Army HQ to Theater "A" is a link; the line from Department of the Army HQ to Theater "B" is another; the line from 2d Corps to 1st Division is one; as is the connection from 1st Division to 2d Division. The links which form the triangle, 2d Corps, 1st Division, 2d Division, constitute a group; those forming the triangle, 2d Corps, 3d Division, 4th Division, constitute another. These links are placed in groups because they work together as a communication entity under a common operating control (the group control being at the highest headquarters of the group, here the 2d corps), yet do not, in themselves, comprise the complete net. The net is made up of the two groups together and is, in this instance, the 2d Corps net with the 2d Corps headquarters as net control. It should be observed that very often the link and the group may be the same thing, or the link, group, and net may be the same. Each definition of the larger unit enfolds the lesser. For example, the line from Department of the Army HQ to Theater "A" may be termed a link, for it is composed of only two stations, or a group because its stations work as a communication entity under the control of the Department of the Army station; the three links, or groups, however, running out from Department of the Army HQ form the Department of the Army net.

REF ID:A58489

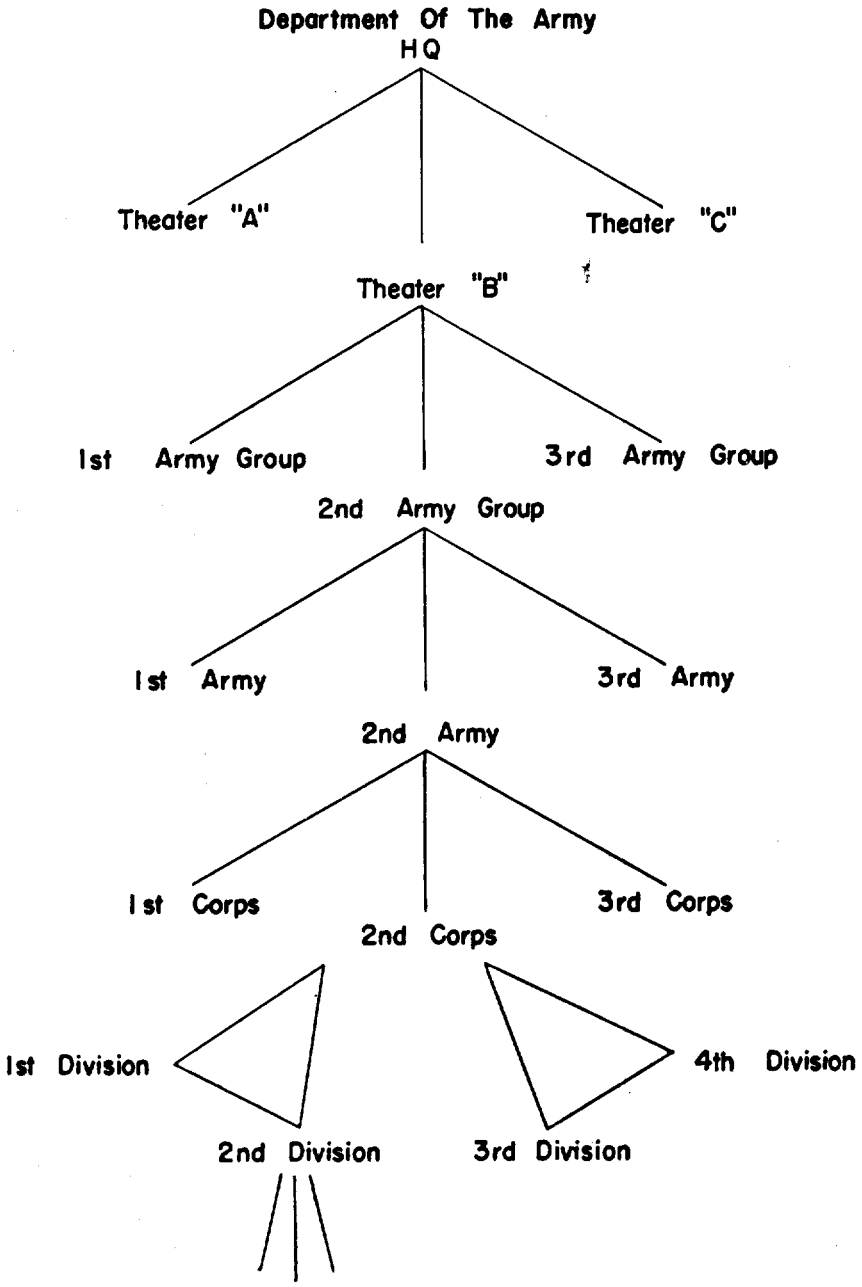


Figure 1. General organization of military network—United States Army.

REF ID:A58489

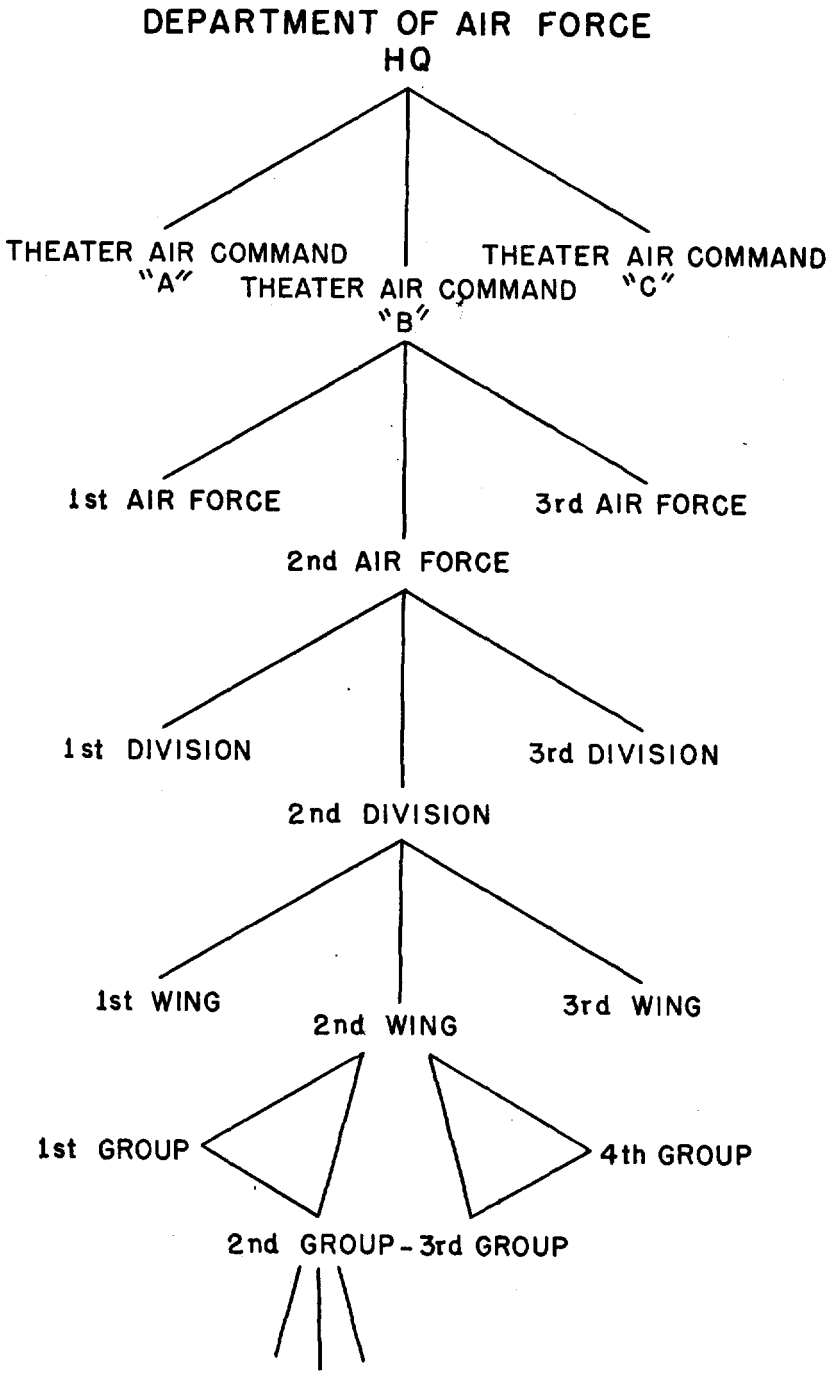


Figure 2. General organization of military network—United States Air Force.

REF ID:A58489

d. It will be recalled that, in discussing these definitions in *b* above, it was stated that they were formulated from an analytic point of view. This is particularly true of the definition of the net. In the reconstruction of the radio network, one of the first problems is the organizing of a number of radio links into groups and nets. In the case of the group, this is fairly simple to accomplish for the group is a communication entity, that is, all of its stations either work each other or have contact with a central operating control. The net, on the other hand, often does not exhibit such cohesive characteristics. A number of groups, apparently unrelated, may eventually fall into a single net when the order of battle is finally derived. There are two touchstones for the association of groups into nets:

(1) *Common operating characteristics.* Since the links and groups of the net all have a common superior headquarters, it may be assumed that certain rules of procedure and operation will be promulgated by this superior and that, therefore, all links and groups of the net will exhibit these in common.

(2) *Administrative direction of an immediate superior headquarters.* When the order of battle is known, it is often possible to associate groups and links through the knowledge that they are controlled by the same unit.

e. The net, the group, and the link, then, are merely units of organization in the radio network, just as armies are broken down into corps, divisions, regiments, companies, and platoons. Likewise, air forces are broken down into divisions, wings, groups, squadrons, and flights. And these nets, groups, and links may be characterized by the unit served and the function performed. For instance, figure 1 represents command channels so that there is a Department of the Army command net, a Theater "B" command net, a 2d Army Group command net, and so on. Radio, however, serves many other military functions than that of command. Military nets, for example, may be organized to contain an antiaircraft artillery group, an artillery air-ground group, an artillery observation group, a reconnaissance group, an air warning group, and others beside the command group.

12. Examples of Radio Nets

Figures 3 through 9 illustrate some of the type nets which may be encountered. These types will vary in individual instances; they serve, however, to indicate some of the possibilities.

REF ID:A58489

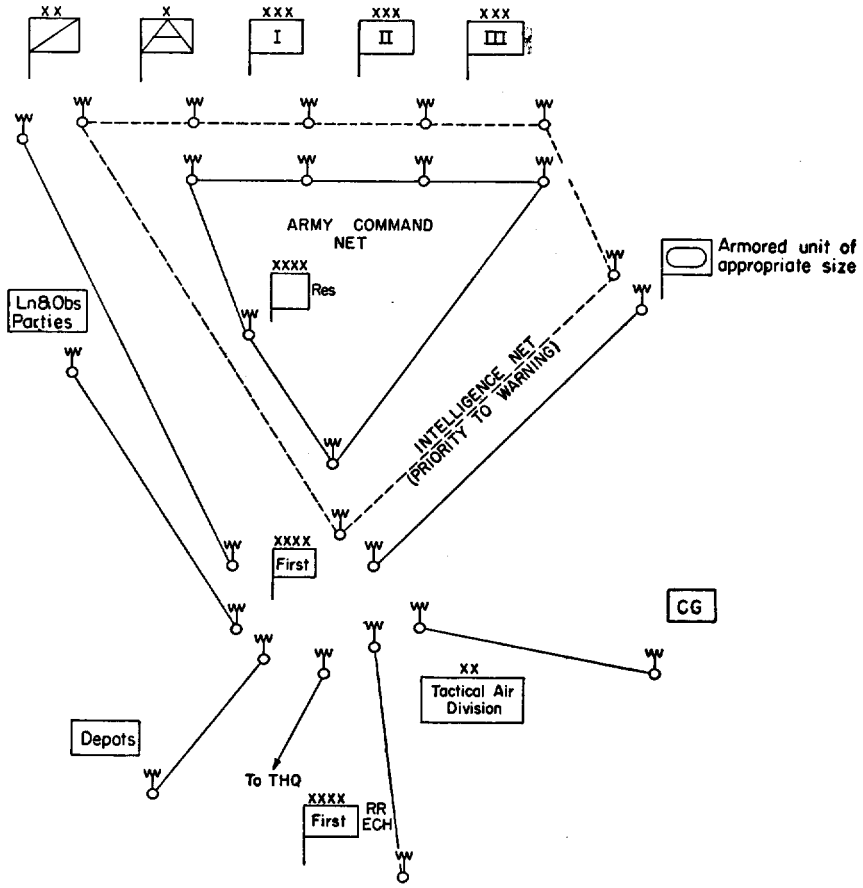


Figure 3. Type radio nets, Army.

REF ID:A58489

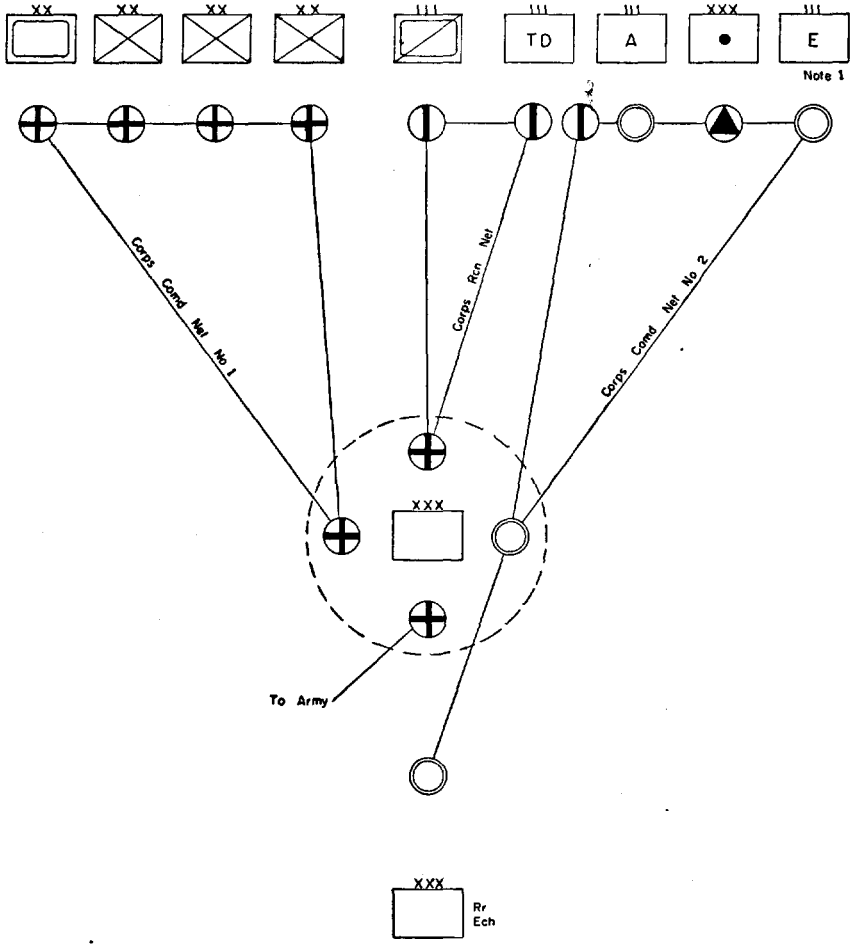


Figure 4. Type radio nets, corps.

REF ID: A684682

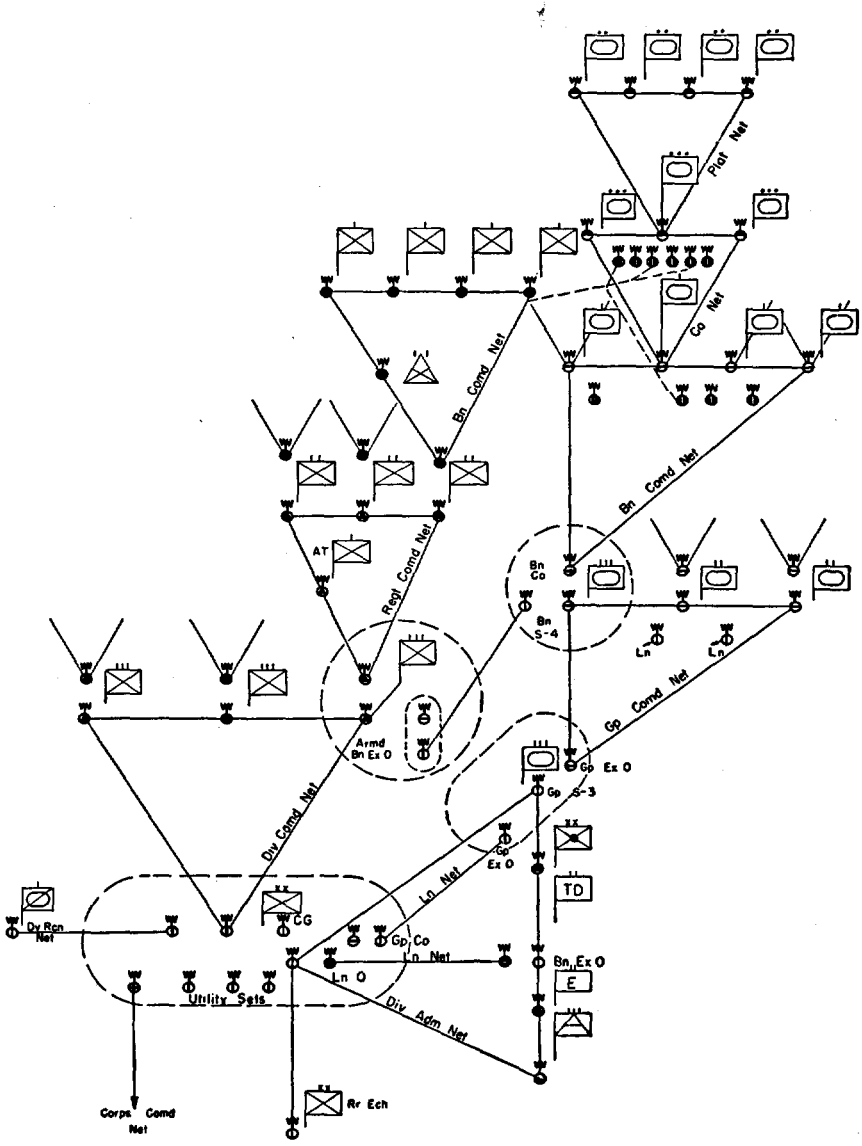


Figure 5. Type radio nets, infantry division, with attached units.

REF ID: A684682

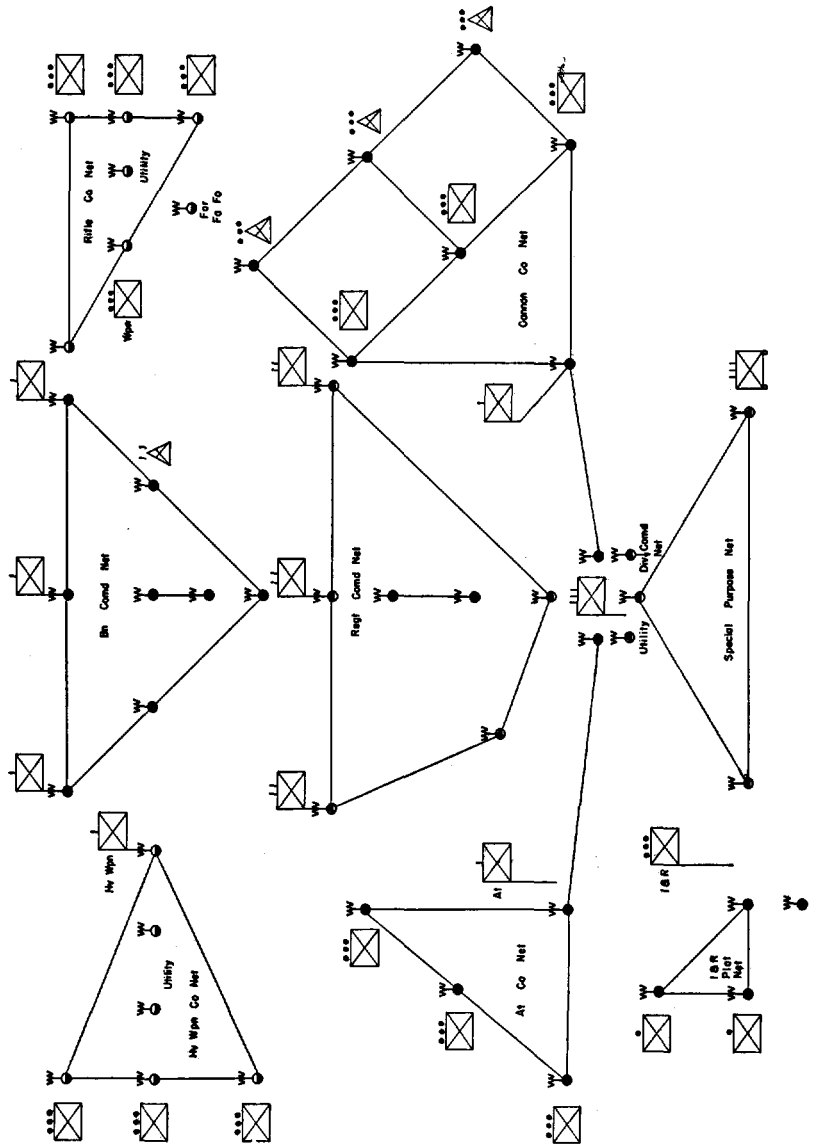


Figure 6. Various radio nets in an infantry regiment.

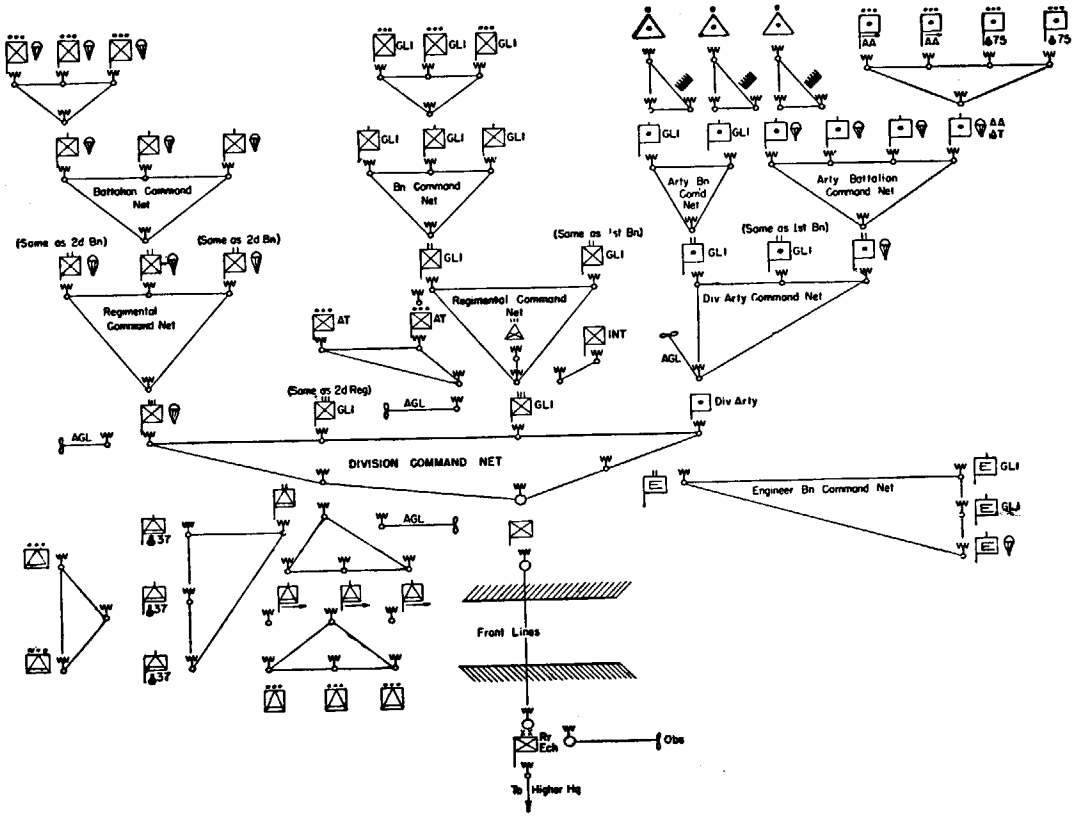


Figure 7. Type radio nets, airborne division.

REF ID:A584489

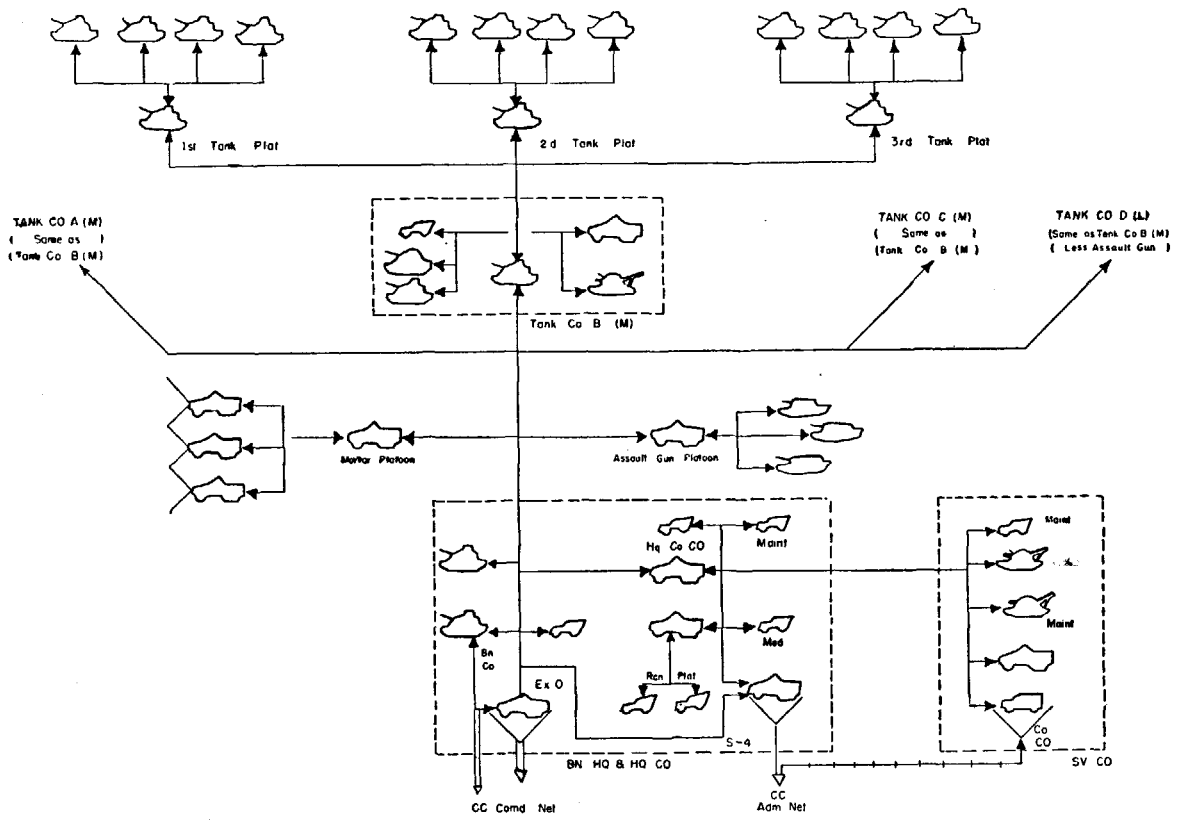


Figure 8. Type radio nets, tank battalion.

REF ID:A58489

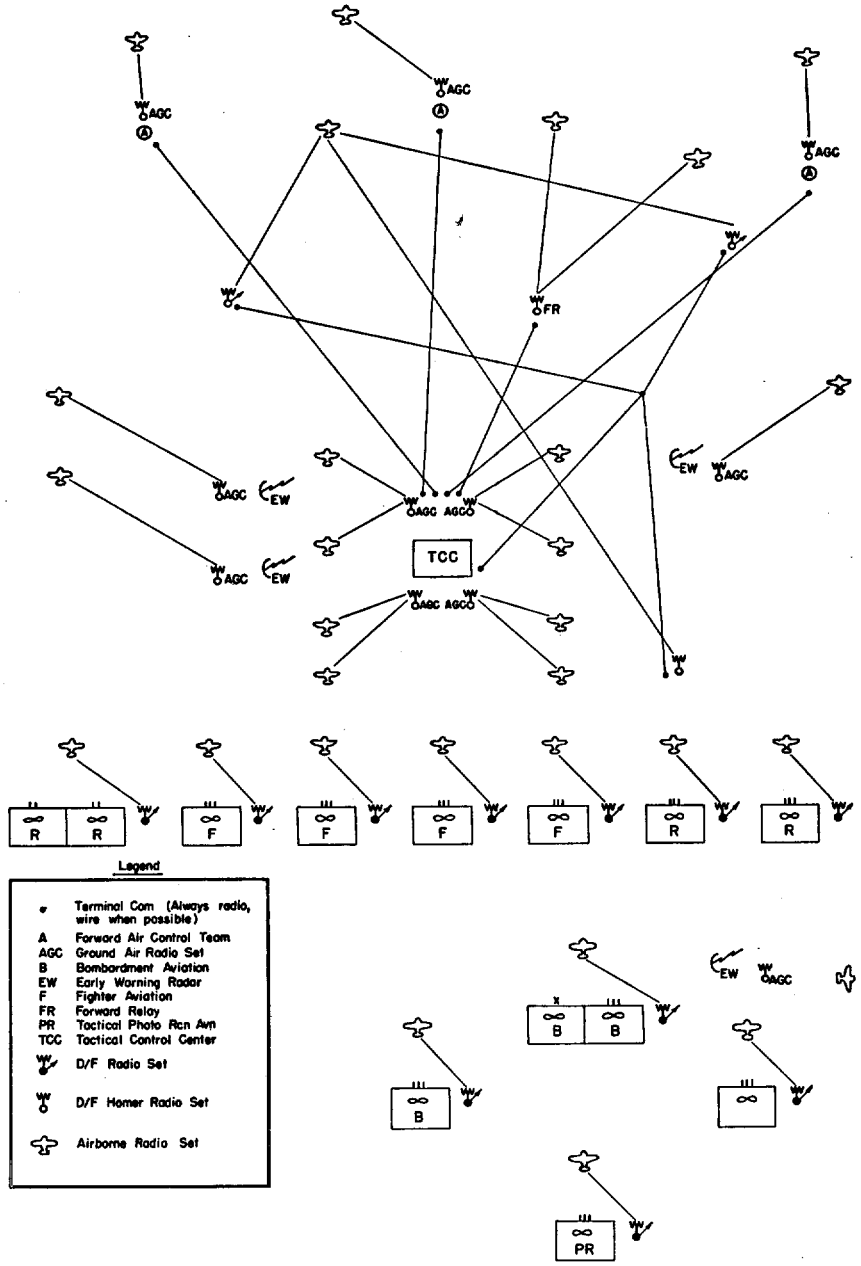


Figure 9. Tactical Air Force control channels.

REF ID:A58489

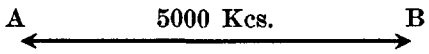
13. Frequencies

a. GENERAL. The analysis of the use of frequencies on a network may be divided into two parts:

(1) *Systems of use.* The system of use is concerned with the manner in which frequencies are employed on the net, i.e., whether the entire net uses one frequency, whether each station sends on an individual frequency, etc.

(2) *Systems of allocation.* The system of allocation is the method used to assign specific frequencies for communications so that different stations will not interfere with each other. It also involves the rotation of frequencies for security purposes.

b. SYSTEMS OF USE. (1) *Simplex:* Two stations intercommunicating on the same frequency.



(*a*) A sends to B on 5,000 Kcs.

(*b*) B sends to A on 5,000 Kcs.

(2) *Complex sending* (fig. 10): Two or more stations on different sending frequencies. A different frequency is assigned to each radio transmitter in the net, and each transmitter uses its assigned frequency to contact the other stations.

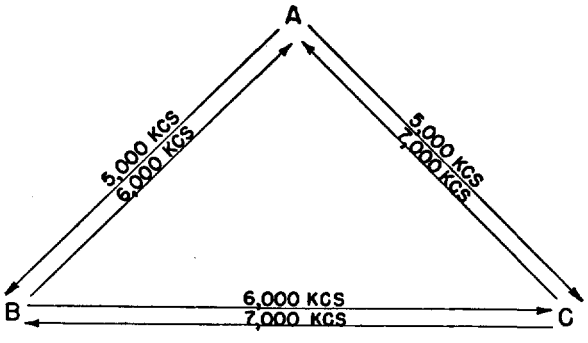


Figure 10.

(*a*) A sends to B and C on 5,000 Kcs.

(*b*) B sends to A and C on 6,000 Kcs.

(*c*) C sends to A and B on 7,000 Kcs.

(3) *Complex receiving* (fig. 11): Two or more stations on different receiving frequencies. A frequency is assigned to each station for receiving transmissions. All stations in the net when sending to a particular station will use the frequency assigned to the receiving station.

REF ID:A58489

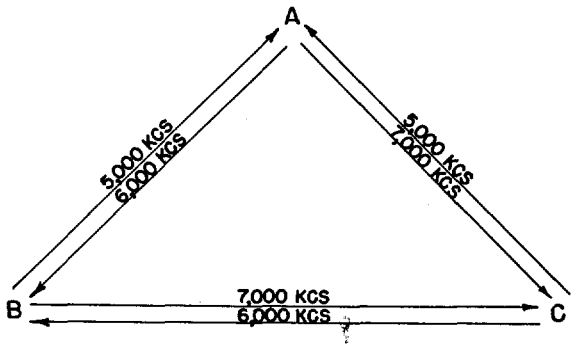


Figure 11.

(*a*) B and C send to A on 5,000 Kcs.

(*b*) A and C send to B on 6,000 Kcs.

(*c*) A and B send to C on 7,000 Kcs.

(4) *Star* (fig. 12): A number of stations on the same frequency with no normal lateral working. This is an extension of the simplex system, as the latter involves only two stations on the same frequency. In the star form, if one outstation wishes to contact another, it must obtain permission from control.

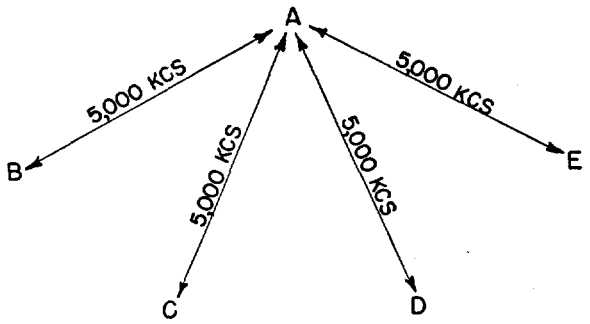


Figure 12.

(*a*) A sends to B, C, D, and E on 5,000 Kcs.

(*b*) B, C, D, and E send to A on 5,000 Kcs. B, C, D, and E may not intercommunicate without express authorization from A. Normally, messages between outstations will be relayed through A (control).

(5) *Star with lateral* (fig. 13): Number of stations on the same frequency with some lateral working. In many of the star nets, lateral working will be a regular procedure between some, but not all, of the outstations.

REF ID:A58489

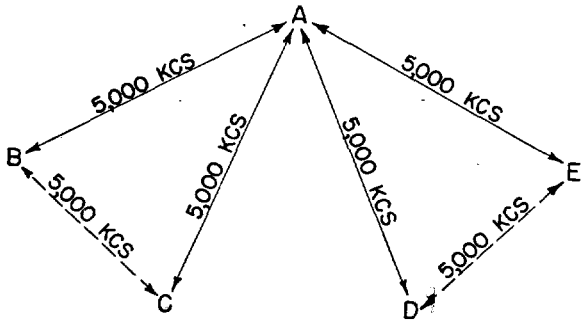


Figure 13.

(*a*) A sends to B, C, D, and E on 5,000 Kcs.
(*b*) B, C, D, and E send to A on 5,000 Kcs.
(*c*) B sends to C on 5,000 Kcs. and C to B on 5,000 Kcs.
(*d*) D sends to E on 5,000 Kcs. and E to D on 5,000 Kcs.

(6) *Free star* (fig. 14): Number of stations on the same frequency with free operation. One frequency is assigned to the entire net and any station in the net may contact any other on the assigned frequency.

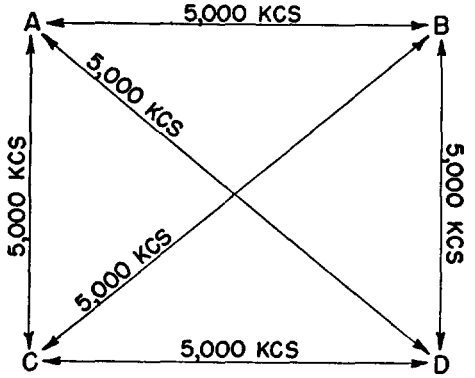


Figure 14.

(*a*) A sends to B, C, and D on 5,000 Kcs.
(*b*) B sends to A, C, and D on 5,000 Kcs.
(*c*) C sends to A, B, and D on 5,000 Kcs.
(*d*) D sends to A, B, and C on 5,000 Kcs.

(7) *Complex star* (fig. 15): Number of stations with control on one frequency, outstations on others. This is similar to the star in its form, but it uses several frequencies instead of only one. Often, a number of the outstations will operate on one frequency, others on another.

REF ID:A58489

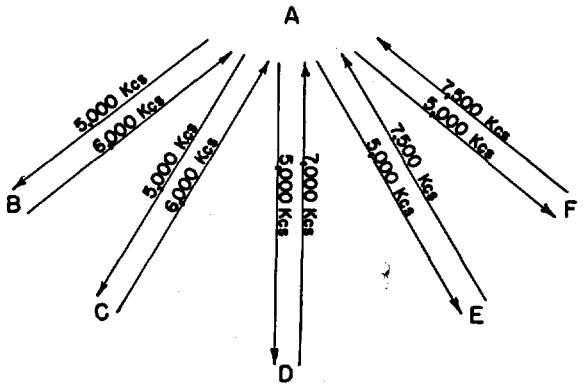


Figure 15.

(*a*) A sends to B, C, D, E, and F on 5,000 Kcs.
(*b*) B and C send to A on 6,000 Kcs.
(*c*) D sends to A on 7,000 Kcs.
(*d*) E and F send to A on 7,500 Kcs.

(8) *Broadcast* (fig. 16): A frequency is assigned to the broadcasting station. Usually no frequency is assigned to the outstations for reply.

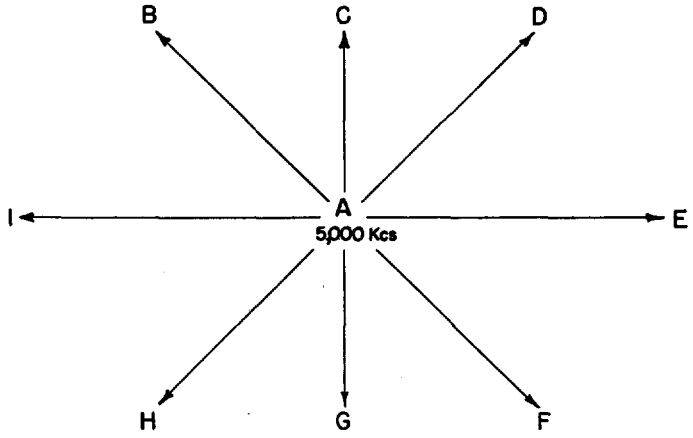


Figure 16.

(*a*) A sends to all stations simultaneously on 5,000 Kcs.

(*b*) Because a broadcast must be heard at so many scattered places, care must be taken in the selection of a frequency in order to choose one that will be heard by all stations. Sometimes, where this has not proved possible, double-keying is resorted to, i.e., the broadcasting station sends on two or more different frequencies at the

REF ID:A58489

same time. Outstations may receipt for traffic on regularly assigned frequencies in the net. In many such nets, however, no receipt is given.

c. SYSTEMS OF ALLOCATION. (1) *General.* Several factors enter into the selection of specific frequencies for use. These involve two basic considerations: readability (the ability of the receiving station to hear) and security. A number of miscellaneous factors, such as the type of power supply available, the nature of the transmitting and receiving equipment, and military and operational requirements, also affect the choice.

(2) *Readability.* The readability of a frequency is dependent on certain factors of wave propagation. These factors involve consideration of the distances between stations, ionospheric conditions, including night and day effects which usually make it necessary to allocate several frequencies to each radio station or net for night and day use, seasonal changes, and the type of terrain, e.g., water, high mountains, and jungle. Furthermore, the possibility of interference between transmitters on approximately the same frequency in the same area must be borne in mind and care taken to avoid such conflict. In any allotment of frequencies, therefore, central control must be established and an over-all plan of allocation devised.

(3) *Security.* One of the methods of attaining security against communications analysis is to hinder the act of intercept. This may be accomplished by changing frequency so that the intercept operator will be forced to "search" the entire frequency range for the desired transmissions. A second effect achieved by these changes is to increase the difficulty of identifying stations or units with frequencies. Maximum effectiveness is obtained by changing call signs along with the frequency. Plans for changes of frequency may operate in a patterned or random fashion, but in any event, such plans must take into consideration the factors noted under (2) above; thus these plans are usually rather detailed and complex.

(4) *Range of frequencies.* Frequencies may range from very low to ultra-high. The latter are not usable for long distance operation and find their chief applications in low echelon, air-ground, and plane to plane communication. Many of the applications of ultra-high frequency transmissions are still in the experimental stage. Low frequencies, such as 300 or 400 kilocycles, may be used for close field contact or air-ground and plane to plane nets. However, the major portion of military transmissions presently falls between 1,500 and 20,000 kcs. In passing, mention should also be made of the use of frequency modulation. FM has found its main application in tank, air, and small combat units where distances are not great and a minimum of noise level is desired for reception.

(5) *Secret frequencies.* As a countermeasure to possible jamming

RET ID: A584489

operations, some nets are provided with secret reserve frequencies These frequencies are not employed except in the case of jamming of the usual frequencies and circumstances demand that communication be kept open The secret frequency, of course, only remains secret for as long as it takes intercept to scan the bands and pick it up, but this interval may be sufficient to complete the transmission

(6) *Example of allocation of frequencies* The following chart illustrates a system which might be used for the allocation and rotation of frequencies

	Jan	*Feb*	*Mar*	*Apr*	*May*	*Jun*	*Jul*	*Aug*		*Dec*
A	1955	2035	2150	1910						
	2035	2150	1910	2305						
	2150	1910	2305	2070						
B	1910	2305	2070	2190						
	2305	2070	2190	2210						
	2070	2190	2210	1940						
C	2190	2210	1940	2350						
	2210	1940	2350	1925						
	1940	2350	1925	2240						
D	2350	1925	2240	1955						
	1925	2240	1955	2035						
	2240	1955	2035							

The months are listed across the top of the chart The squares are divided into three portions representing ten day periods within each month, 1–10, 11–20, 21–31 Each station of the net is assigned a letter and finds its frequency for each period in the square opposite the letter The frequencies which have been selected on the basis of their operational characteristics can be inscribed in the squares at random, in this instance, they are moved up one each month For example, on 1–10 January, A uses 1955 kilocycles, B, 1910 kilocycles, C, 2190 kilocycles On 11–20 January, A uses 2035 kilocycles, B, 2305 kilocycles, C, 2210 kilocycles

14. Call Signs

a General Call signs are actually names for the correspondents in a radio net They are usually composed of letters, numbers, or combinations of both and serve as a convenient means of identification The analysis of call signs falls into the same categories as does the study of frequencies systems of use, and systems of allocation

b Systems of Use (1) *Single station call* One call only is nor-

REF ID:A58489

mally used by the calling station This call may be either the sending station's or the receiving station's call

1 (ABC) _____ 2 (DEF)

Call up	1 to 2	DEF DEF DEF
	2 to 1	DEF DEF DEF
	or	
	1 to 2	DEF DEF DEF
	2 to 1	ABC ABC ABC

Note in this last instance that only one call was used by the calling station This makes the procedure single call even though the reply used a second call

(2) *Double-station call* Both the sending station s and the receiving station's calls are normally used by the calling station

1 (ABC) _____ 2 (DEF)

Call-up	1 to 2	DEF DEF DEF de ABC ABC ABC
	2 to 1	ABC ABC ABC de DEF DEF DEF

(3) *Link call* (fig 17) A common call sign is used for intercommunications between two stations Unlike the previous two types, here the call sign does not belong to an individual station but to a link

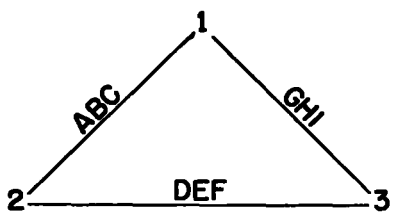


Figure 17

Call up	1 to 2	ABC ABC ABC
	2 to 1	ABC ABC ABC
	1 to 3	GHI GHI GHI
	3 to 1	GHI GHI GHI

(4) *Collective call* In addition to one of the above assignments, a collective call may also be allocated This call is used to alert all stations in the net preparatory to the transmission of broadcast traffic There are also some nets which are maintained only for broadcast purposes and this type of call is usually assigned to such groups The use of "CQ" may be classified under this heading

(5) *Split call working* Usually a single call is assigned to a transmitter or receiver position or to a link However, the use of separate calls for each frequency, one for day, one for night, is also valid This variation may be applied to any of the systems enumer-

REF ID: A684682

ated above and is known as split call working. It has the advantage of dissociating the night and day frequencies, but requires the use of twice as many calls.

(6) *Secondary calls.* In some systems of communication a secondary call is employed in conjunction with link call procedure. These secondary calls are of the station call type and serve as a more definite identification of each station than is supplied by the link call.

(7) *Authenticators.* In order to prevent outside stations from entering a net and confusing its operations, authenticators are sometimes used. They generally consist of a word or a combination of letters and/or digits to which there is a secret, prearranged reply.

c. SYSTEMS OF ALLOCATION. (1) *Composition.* Call signs may be composed of any combination of letters and/or numbers. Usually they are kept as brief as possible and the general range is from 2 to 5 characters. Calls may be composed at random or in some methodical fashion, such as the use of sliding alphabets. An example is included in *d* (2) below.

(2) *Methods of assignment.* Since calls are used as identifying marks, it is necessary to assign them so that two stations operating in proximity or in the same net do not have the same call. Otherwise, confusion would result on call-ups and the passage of traffic hindered. This necessitates some form of over-all control of call sign allocation. This control may be of a very tight nature in which every call is allotted from headquarters down to the smallest unit, or it may be rather loose with considerable discretion left to major subordinate groups whose commands are sufficiently separated geographically to prevent the possibility of confusion. A second consideration in the assignment of calls involves the problem of security since calls are identifications and thereby, if unchanged, furnish continuities for intercept and analysis. Most systems, therefore, cover not only the allotment of calls, but also provisions for change or rotation. These changes may be made daily, weekly, monthly, or at any other interval thought desirable. Calls which change frequently are called "changing calls", those which remain constant for some length of time, are called "fixed".

d. In general, call-sign systems may be divided into two basic groups:

(1) *Book systems.* These systems are founded on a call-sign book from which all calls are taken. These books will usually contain thousands of call signs and some method is provided for the allocation of calls from the book to individual radio stations. The recovery of these books often requires traffic intercept for a period of a year or more.

(2) *Cipher systems.* Call signs may be generated by the use of simple cipher devices such as sliding alphabets and square tables.

REF ID:A58489

The number of call signs available through such systems is usually limited and the method of assigning the call signs to individual radio stations is often bound up with the method for generating the calls. Figure 18 illustrates the use of a cipher system for the allocation and rotation of calls.

1	B	M	A	K	D
2	R	W	C	T	I
3	Z	G	N	O	U
4	H	L	S	X	E
5	V	J	P	F	Y

Figure 18.

The square is filled in random fashion. Station 1 begins with the letter "B" and takes off its calls in diagonal fashion, moving over one diagonal each day. At the end of each line, it drops down one line. Station 2 begins with "R", 3 with "Z", etc. Every 25 days, the calls repeat.

	Station No. ( )				
Date	1	2	3	4	5
1	BWN	RGS	ZLP	HJA	VMC
2	MCO	WNX	GSF	LPK	JAT
3	ATU	COE	NXY	SFD	PKI
4	KIZ	TUH	OEV	XYB	FDR
5	DRG	IZL	UHJ	EVM	YBW
6	RGS	ZLP	HJA	VMC	BWN
7	WNX	GSF	LPK	JAT	MCO
to					
25					

15. Times of Communication

a. GENERAL. An integral part of the operating data of the net is the setting of the times for communication. There are two main systems for accomplishing this: Unrestricted signaling and restricted signaling.

b. UNRESTRICTED SIGNALING. Under the system of unrestricted signaling, the stations of a net are free to contact each other at any time they choose. This method may be implemented either by the stations setting the time for the next schedule at the close of the

REF ID:A58489

previous one or by "alert" operating. In alert operating, which finds its greatest use in tactical and warning nets, all stations are always tuned to receive on certain assigned frequencies.

c. RESTRICTED SIGNALING. Restricted signaling limits the time at which contacts may be made between two radio stations. It is divided into two types: period signaling and priority signaling.

(1) *Period signaling.* The times of communication are assigned by definite schedule and contacts are made only at those specific times.

(2) *Priority signaling.* Priority signaling sets down a definite order in which the stations of a net will send traffic. It differs from unrestricted signaling in that one station may not call another at any time; and from period signaling in that no particular time is set aside for one station to call another. An example of priority signaling is shown in figure 19.

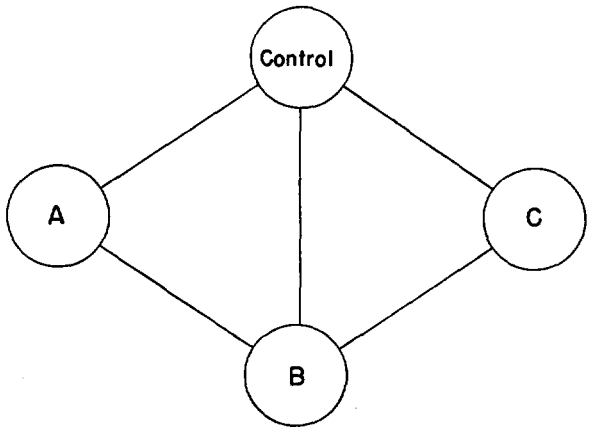


Figure 19.

In this net, "control" is permitted to send first, then stations A, B, and C in order. Schedules may be set up for the hours at which "control" comes on the air.

Section III. ELEMENTS OF RADIO PROCEDURE

16. Morse Code

Morse code is a system of dots and dashes used to transmit letters and numbers by electrical means. In the case of the English alphabet the Morse code is standardized by international convention, is used the world over, and is known as International Morse. In the instance of some nations whose alphabets differ from the English, however, special combinations of dots and dashes have been devised. For

REF ID:A58489

example, in German Morse, the German letters which correspond to the English follow the International, but the umlauted letters and "ch", for which there are no equivalents, are designated by new combinations:

A .—.—
O ———.
U ..——
CH ————

Morse code may be transmitted automatically or manually. In lower-echelon communications, the latter is usually employed, in the higher echelons sending is often automatic. Automatic transmission permits of speeds as high as 400 or 500 words per minute, though generally it averages somewhere between 75 and 200. Manual sending of coded traffic rarely rises above 35 words per minute. Atmospheric conditions, operator abilities, equipment, and similar items are, of course, limiting factors.

17. Procedure Signals

a. In order to facilitate conversation between radio operators, certain signals and signs have been composed. The most common sets of such signals used internationally, are made up of three-letter combinations beginning with "Q" or "Z", and are called "Q Signals" and "Z Signals". The use of these signals saves considerable time and simplifies transmission. Examples are—

QSV Send V's.
QRN I am troubled by atmospherics.
QSA? What is my signal strength?
QSA 4 Your signal strength is 4.

b. Beside these signals, there are a number of standard signs called prosigns which are likewise considered part of international procedure. Some of these are—

AA all after
R received
K go ahead

c. Another type of standard signal is the International Service Code. These signals are made up of five letters in pronounceable form:

UPBAG—for your information

d. Since much information may be derived from a study of chatter, military nets often make up sets of secret procedure signals and, in some cases, may encipher these signals on a periodic basis. For instance, the standard Q signal list may be used, but the last two letters of the signal enciphered by means of a daily changing alphabet.

899152 O - 50 - 5

REF ID:A58489

18. Elements of the Transmission

a. GENERAL. Just as a definite procedure is followed in making a telephone call, so in the normal radio transmission there is also a more or less fixed procedure which covers the basic elements involved. These elements are—

(1) *The call-up.* This embodies the rules of procedure by which one station makes contact with another and prepares for the transmissions of traffic.

(2) *The order of traffic.* After contact has been established, it is necessary to determine which station is to send traffic first.

(3) *Transmission of traffic.* The traffic is transmitted according to a prescribed form.

(4) *Receipting for traffic.* The receiving station acknowledges receipt of the message.

(5) *Corrections and services.* Messages are frequently garbled because of reception difficulties or operators' errors. Thus methods are provided for the efficient and speedy correction of these garbles.

(6) *Signing off.* At the conclusion of the schedule, the two stations follow certain procedures in signing off.

b. If allowance is made for differences in language and procedure signs and signals, it will be found that the above elements are generally standard for most communication systems. The detail, however, may vary somewhat between countries and also within the military of any one country. For instance, different units may observe different rules relative to the transmission of the call or the method of servicing. This often stems from individual requirements arising from strategic or tactical situations, e.g., an air unit as against an infantry unit. Furthermore, the echelon will also alter procedures. The lower echelons will usually abbreviate their procedures as much as possible because of the necessities of time and because they do not require all the data and detail that higher echelons do. Similarly, transmissions on low-echelon nets are liable to be confusing since a number of stations are often on the air at the same time and on approximately the same frequency.

c. THE CALL-UP. The calling station usually comes on the air with a series of V's sent for tuning purposes and the appropriate calls. The calls are generally sent three times, though this number may vary. The called station replies with a series of V's and calls. If the contact between the two stations is quickly made, readability reports are exchanged. Should these reports be unsatisfactory, transmitters and receivers will be adjusted, frequencies changed, etc., until signals are readable. If contact cannot be made, the calling station may hold its traffic for a later schedule, relay it through a third station, or send it blind. In sending blind, messages are generally

REF ID:A58489

transmitted twice and at a slow speed in the hope that the called station can hear although it cannot be heard.

d. THE ORDER OF TRAFFIC. Once contact has been successfully established, it becomes necessary to determine who will send traffic first. Various methods are employed. It may be ordered, for example, that the station of higher echelon send first, or that the calling station have this privilege, or that the highest priority traffic be cleared before all else regardless of which station is involved. One-for-one procedure may be used; i.e., the calling station is permitted one message, then the called station sends one, thus alternating back and forth until one of the stations has cleared all its traffic. Duplex working may be employed when the stations have the available operators and equipment and there is a large amount of traffic to be passed by both. Four operators are required in this type of working. For example, in figure 20, Operator No. 1 at station A sends

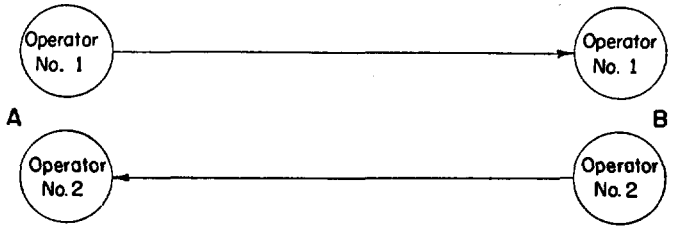


Figure 20

to Operator No. 1 at station B, at the same time that Operator No. 2 at B is sending to No. 2 at A. The chief difficulty with this sort of sending arises when No. 1 at B requires a service on a message from A. Since No. 1 at B is then using the frequency channel of the station, No. 2 at B must stop his transmission.

e. THE TRANSMISSION OF TRAFFIC. Traffic is usually preceded by a commence signal indicating that a message is about to be sent. The traffic itself is composed of the message externals and the text. The message externals contain such items as message numbers, file date and time, group count, addresses, routing instructions, precedences, and similar data. These externals may either precede or follow the text (preamble and postamble) or may be split between the two locations. Most commonly, however, these data appear in the preamble position. The text may be transmitted in code groups of letters, numbers, or both, or in plain text. In the case of coded traffic there are often signals indicating the end of a line and page of text as a check for the receiving operator. Signals usually appear preceding and following the text, the former separating the preamble from the text, the latter indicating the end of the message.

f. RECEIPTING FOR TRAFFIC. After the transmission of a message,

REF ID:A58489

the sending operator waits for a receipt from the receiving operator. This is generally rendered as simply "R". There are also procedures for provisional receipts and other special forms. In some cases, time of receipt may be given following the receipt sign.

g. Corrections and Services. A variety of methods are employed for the servicing of traffic depending on the nature and magnitude of the difficulty. A missed digit, for instance, may be serviced immediately; on the other hand, if a group were omitted this would not be known until the conclusion of the message and might be serviced at that time or might be held until all traffic has been sent. This latter procedure is fairly common, since it is convenient to transmit all traffic without interruption and then to take care of all necessary servicing. Some methods of servicing follow:

(1) *Break-in procedure.* When reception between two stations is good, "break-in" procedure may be used for quick servicing. It is useful only for minor corrections such as garbles caused by a moment of static, is very fast, and calls for alert operating.

A. 6403 3661 9626 - - -
B. 2 — B sends "2" as it is the last number he received correctly.
A. 26 8139 5560 — A picks it up from 2.
or:
A. 6403 3661 9826 - - -
B. (Merely depresses his key)
A. 9826 8139 5560 — A re-sends the last group and continues.

(2) *Correction of error (U. S. Army procedure).*

A. QXTU SRV EEEEEEEE SRWP TSTL — Actually eight or more dots indicating that "V" is in error.

(3) *Repetitions (U. S. Army procedure):*

A. IMI 3–6 to 8 K — Repeat groups 3 and 6 to 8 of last message.
B. 3–LAJY–6 to 8–MUCU KAWC GUXO K

(4) *Verifications and corrections (U. S. Army procedure).*

A. J 271545 Z 3–6 to 8 K — Verify and repeat groups 3 and 6 to 8 of message filed at 271545 Z.
B. C 271545 Z 3–LAJY–6 to 8–MUCU KAWC GUXO K

(5) *RQ's and BQ's.* Services which are more complex than the types noted above are usually sent as short messages. A request for

REF ID:A58489

service in international procedure is preceded by the sign "RQ", the reply by "BQ". Services which relate to cryptographic features, however, are generally sent as regular encrypted messages.

h. SIGNING OFF. When there is no further traffic to be transmitted, or at the end of the schedule time, the two stations will sign off. Usually, each station sends the "I have no more traffic" signal and then the "sign-off" signal. In many nets, the time of the next schedule is included just prior to the sign-off. These times may be enciphered for security purposes. Stations in lower-echelon nets will often sign off in order. An example from U. S. Army procedure follows:

A.	2SN	V	6F2	QNW	K	"2SN" is net call. QNW is the "close down" signal.
B.	6F2	V	G94	R	AR	
C.	6F2	V	KFR	R	AR	

19. Chatter

Radio operators, particularly the lesser-trained and on the lower echelons, exhibit a disposition to chatter amongst themselves. This chatter is the source of much information of value. It does not fall into the categories discussed above as it may relate to anything from discussions of personal problems to mentions of units or cryptographic features. This sort of talk is forbidden since it represents not only idling but a serious breach of security. Nevertheless, depending on the degree of discipline, it will occur in some volume in almost every radio net.

20. Plain-language and Low-grade Cipher Messages

Very often the error is made of transmitting, in plain language or low-grade cipher, messages which are apparently of no analysis value, yet when properly used prove of enormous assistance in the traffic analysis processes. Such messages may involve personal items or routine affairs which serve to reveal such important data as personalities, units, and locations. This type of traffic is particularly prevalent in the lower units where speed may be of the essence and where it is cumbersome to use complex cryptographic devices. Radio station personnel also indulge in this practice for exchange of technical data. They often find it necessary to ask, or reply to, questions of a semi-secret nature relative to their own operations. For this purpose, they may not use a standard system which would involve the delay of the code room and message center, but instead devise their own relatively simple ciphers.

REF ID:A58489

Section IV. THE MESSAGE EXTERNALS

21. Usual Components

a. In order to insure the proper handling of messages in both the message center and the radio station, some information must be sent in the clear or in simple code relative to message routing and accounting. This information is usually embodied in the preamble or postamble although, in some instances, it may be buried in the text. It may include any or all of the following items:

(1) Serial numbers, such as radio station numbers, message center numbers, etc.

(2) Group count.

(3) File date and time.

(4) Routing systems which serve to indicate message centers or units of origin, destination, and sometimes relay points of traffic. Distinction is also often made as to action and informational destinations. Routings may be in plain language, code, and/or cipher.

(5) Addresses and signatures, either in clear or cryptographed.

(6) Priorities, indicating the transmission and delivery precedence of traffic.

(7) Special instructions, as "time of receipt requested," "personal," "service," "repeated message," "relay message."

b. As a general rule, high-echelon traffic will contain most of these items, low-echelon traffic will cut them to a minimum. Their uses, positions, and surrounding procedure vary considerably according to communication system.

22. Serial Numbers

a. Serial numbers appearing on traffic may be enciphered or unenciphered and may represent any of the various stages through which the message passes before it is actually transmitted. The serial number acts as a reference to the message, and generally there are as many numbers in the externals as are necessary for convenient reference. The points at which such numbers may be attached to the message are—

(1) *The writer.* The writer of the message may have a personal series of numbers allotted for his use. Usually, however, numbers of this type, if present, will be included in the text.

(2) *Message center.* The message center of the unit in which the message originates generally assigns it a number. A number of this nature, if used, will usually remain constant through various relays of the traffic as it is the basic reference.

(3) *Signal center.* At large locations, several unit message centers often forward their traffic to a central signal center. The signal

REF ID:A58489

center also gives a number to the message. This number may appear in place of the message center number, along with it (though this is rare), or it may not be included at all. It is often difficult, where only one number is transmitted, to determine whether it is a message center or a signal center number.

(4) *Code room.* The code room, whether located in the message or signal center, may add a number to the traffic. Again this number may replace, or be used along with, the other types.

(5) *Radio station in-desk.* Each radio station maintains some form of in-desk for the handling of incoming messages and their routing to the proper radio positions for transmission. Here, too, a number may be put on the message. There may be several such desks for the forwarding of different types of traffic and this may result in several different series of numbers. In relayed traffic, these numbers (as well as the type included in (6), (7), and (8), below) may accumulate on the message, or a new one may be substituted for the old on each retransmission so that only the latest number appears.

(6) *Transmitter.* A number is often put directly on traffic by the radio operator as his reference. This number may be assigned in different ways. One method is to allot a series of numbers to a transmitter position and regardless of the receiving station this series is continued.

(7) *Link.* A second method is the employment of a link number, i.e., separate series are allocated for each station worked.

(8) *Operator.* A third system is the allocation of a personal series of numbers to each operator. A diagram of the above possibilities is given in figure 21.

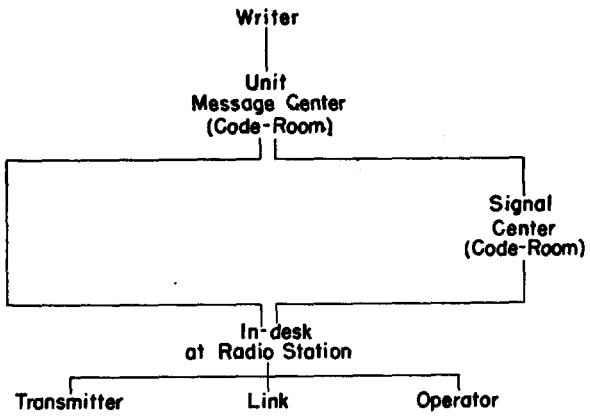


Figure 21

b. As a general rule, not more than two numbers will appear in the message externals, one representing some stage of the message or signal center phase, the other the radio station phase. In the lower

REF ID:A684682

echelons often only one number is used since the whole operation is usually so small that these fine distinctions lose much of their significance.

c. Series of numbers are allotted in some organized fashion, though this fashion may differ from net to net and from unit to unit. The series may be allocated in block form, e.g., 1 to 100 or 501 to 1000, etc. The blocks may be used until completed and then started over again; or the series may begin over on a periodic, such as a daily, basis, but if the prescribed limit is reached within the period, it is likewise recommenced. The series, on the other hand, may be open-end and repeat only at the close of a fixed period as a week, a month, or a year. In some types of series, the date or similar feature may be incorporated in the number.

d. These numbers may be enciphered in order to conceal the volume of traffic passed. It is not likely that this would be done with any of the radio station numbers because of the complexity of the operation, but it may be done at message center or signal center level. In this procedure, the plain text numbers run in serial order and messages are filed in the sending center by it. Another center referring to a specific message would do so by the enciphered number, the sending unit would then decipher same and locate the traffic. Thus, it is not necessary for the receiving center to know the system of encipherment and this permits considerable latitude in the employment of enciphering methods between the various centers.

23. Group Count

The group count may cover only the text of the message or it may include both externals and text. In some types of preamble separate counts are given for each. The group count may represent either the number of cryptographic groups, number of plain language words, or the number of individual letters and/or digits according to the method used.

24. Date Time Group

The date time group appears in the message externals and is expressed in six digits followed by a time zone suffix. It is intended to indicate the time the message was authorized for transmission, but may be used to indicate the time the message was filed at the message center, signal center, or at the radio station for transmission. Time is expressed in terms of the 24-hour clock and may be based on Greenwich Mean Time or on some local time zone. Whatever the base, it is generally kept standard for the entire net, if not for the entire communication system, regardless of the geographical area covered.

RECD 10 : AD684682

25. Routing Systems

a. GENERAL. Some method is required on radio traffic to indicate points of origin and destination and, in many cases, relay points. These methods must be relatively simple as they are designed chiefly as an aid to radio station personnel in the routing of messages. In this respect, it is necessary to understand the distinction between the routing designations and the addresses when both appear. The routing designations usually refer to message or signal centers, the addresses to specific units or persons. (There is nothing to bar the use of routing designations for specific persons but this is not generally the case.) It may be compared with the address on a letter, the routing designation representing the city of address, the address representing the company or person. On high-echelon traffic this difference is generally made, but in low-echelon traffic the routing designation often suffices for both purposes since message centers are small and traffic is almost always intended for the commanding officer. Thus, addresses as such do not usually appear on messages at this level. This distinction similarly holds true for routing designations used to indicate origin and signature.

b. The discussion of routing systems has been divided into two portions, the first dealing with the composition of routing systems, the second with their use.

(1) *Composition of routing systems.* Routing systems may be divided into three main types, plain text, call sign, and code. Plain text is seldom used on military nets because of its insecurity. Thus, generally, either the call signs of the stations are used for routing or a separate code is set up for this purpose. A routing code usually consists of two parts: code and syllabary. The code is composed of short number and/or letter combinations which may represent a location, message center, or unit. The syllabary provides code equivalents for the spelling out of place names or units not provided for in the regular code. These codes are usually rather simple, often being one-part in nature so as to be convenient for application. In some cases they are not used for security reasons, but rather for brevity. Generally, however, they serve both purposes and an encipherment of the code may be a feature of a few of these systems.

(2) *Use of routing systems.* Methods of using routing designations and the placement of these designations on traffic vary to a considerable extent. It may be set forth as a cardinal principle, however, that in most systems routing designations are used only when absolutely necessary. This increases their security and also makes it more difficult for the traffic analyst to determine the origin and destination of a message. On traffic which is point-to-point in nature, therefore, there are usually no routings at all. For example, in figure 22, A has a message for B. This message will be transmitted over

REQ: DD: AD684639

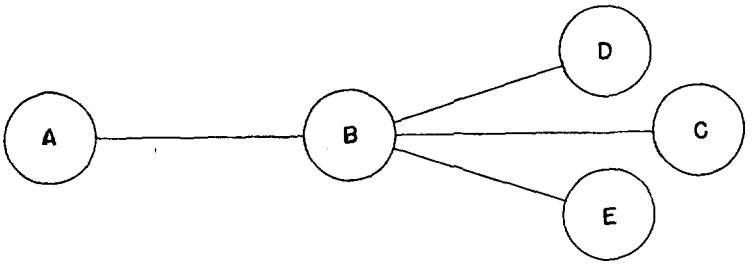


Figure 22

the A-B link and since it has originated with A and is destined for B, routing designations are not required. On the other hand, if A has a message for C, this is generally indicated in the externals so that B knows that it is to be forwarded. (It should be remembered that it is always possible to bury routing instructions in the text, but this is, as a rule, not done since it would necessitate the decoding of the message at each stage of the transmission.) This may be handled in two ways. The message may carry the routing "A to C," or it may only carry "to C" with the originator omitted. When the message is relayed from B to C, it may state "A to C," "from A," or have no routing at all. In some systems the relay point is noted, as "A to C through B."

c. Messages to several addressees can be indicated in several ways. For instance, in figure 22, A may originate a message for B, C, D, and E. All of these destinations could be incorporated in one preamble, "A to B, C, D, and E," or a separate preamble could be added at the end of the message for each location. Thus, the preamble preceding the message may carry no routing since it is being forwarded direct from A to B, but each of the preambles following the text would note "A to C," "A to D," "A to E." When this message reached B, B would transmit a copy with the proper preamble to each of the stations indicated. In this manner each copy would be numbered separately; in the single preamble method, only one message number would appear for all the recipients. It is further to be observed that if various specific addresses at one location, or routing designation, were involved, it would be possible to handle it in either of these ways or to indicate the addresses internally.

d. Distinction also may be made externally as to information and action destinations by the use of appropriate procedure. For example, in U. S. Army procedure, "W" is used to separate action from information addresses, e.g., "ABC W XQR" where ABC is the action addressee, XQR the information.

REF ID:A58489

26. Addresses and Signatures

Addresses and signatures may or may not appear externally on messages. Very often it is standard procedure to conceal them as part of the text. When they do appear externally, however, they are usually encoded and/or enciphered by means of complex cryptographic systems since they contain the specific names of units and persons and thereby are of high intelligence value. The address, unless it is in simple cipher or plain text, is usually considered a cryptanalytic, rather than a traffic analytic problem. Nevertheless, there are some features of the address and signature, such as length and manner of encipherment, which are of interest and use to traffic analysis.

27. Precedence Indicators

a. In order to insure the most expeditious handling of important traffic in both message center and radio station, some means of designating such traffic through the use of precedence indicators is usually devised. The precedences may be in the form of plain text, abbreviations of plain-text words, or number or letter code groups. Furthermore, in some military systems, these code groups may be enciphered.

b. The number of precedences used varies considerably from one nation to another and may range through several classifications of high priority to routine and deferred. There is, very often, no precedence designated "routine" and messages in this category, which are generally the most numerous, carry no marking at all.

28. Special Items

There are a great number of special items which are often included in the message externals. Some of the more common follow.

a. Part Messages. Long messages are usually broken up into several parts for ease of handling or for reasons of cryptographic security. Indications of this may be transmitted in the preamble.

b. Message Type. Indicators may be included to designate the type of message, for example, service, air warning, personal, weather, practice, repeated message, etc.

c. Miscellaneous Items. Procedures may also be provided for the transmission of miscellaneous items such as, "Time of receipt requested," "Each group sent twice," "Message sent blind," "Text in five (5) digit groups," "Relay message."

29. Message Examples

The elements discussed in the preceding paragraphs appear in message preambles and postambles in fixed positions according to the

REF ID: A5384682

procedure prescribed. These procedures differ from country to country and also often from one branch of service to another and from one echelon to another. Examples taken from U. S. Army procedures follow:

a. AB9 V PT3 291155Z GR12
BT Text
BT 291155Z K
AB9—Receiving call and destination.
PT3—Transmitting call and origin.
291155Z—File date and time, repeated as postamble.
GR12—Group count.
BT—Break before and after text.
K—"Go ahead" sign sent after message.

b. 3XF B79 V FR8–O–P B79–T–RST–A–FR8
152312Z 3XF RST B79 GR 19
BT TEXT.
BT 152312Z K
3XF B79—Multiple call-up; receiving calls.
FR8—Transmitting call.
O–P—Operational priority. (Precedence designation.)
B79–T–RST—B79 to transmit message to RST.
A–RF8—Denotes origin.
152312Z—File date and time.
3XF RST B79—Action destinations.
GR 19—Group count.

c. A45 BR6 B STX P–A45 BR6–T–N–A45
A–79K 011046Z A45–W–F2P SLW BR6
GR 28
BT TEXT.
BT 011046Z K
A45 BR6—Multiple call-up; receiving calls.
STX—Transmitting call.
P–A45—Message is priority to A45 only; to others routine.
BR6–T–N–A45—BR6 is to relay to all destinations except A45.
A–79K—Originator of message.
011046Z—File date and time.
A45—Action destination.
W–F2P SLW BR6—Denotes information destinations.
GR 28—Group count.

Section V. TEXTUAL FEATURES

30. General

While textual features and cryptographic systems are chiefly the field of the cryptanalyst, the traffic analyst should also understand

REF ID:A58489

certain aspects, both for the purpose of assisting in his study of communication nets and in the accomplishment of his responsibility to the cryptanalyst. These aspects relate to the distribution, use, and identification of systems, and to the use of indicators.

31. Distribution of Systems

Many cryptographic systems are limited in distribution; this limitation constitutes a cryptonet. For example, a system may be distributed only to the corps headquarters of a theater. These corps then are a cryptonet. Or it may be given only to units along a line of communications. There may be several reasons for the delineation of these nets but the chief ones are security, the nature of the system involved, and the physical problems of distribution. Forward units, for instance, are generally furnished different systems than the rear echelons because first, they are more liable to capture; second, they cannot handle the more complex methods of encipherment; and third, their traffic does not require the same degree of security. Within the higher echelons, divisions are made to prevent the overuse of any one system and thus deny depth. Such divisions also arise from the major break-down in command which allows some latitude in the composition of codes and ciphers to individual services or units. Furthermore, special systems may be prepared for use in particular operations where a high degree of security is desired. The important point, however, for the traffic analyst is to think of cryptonets not in terms of locations, but in terms of order of battle units, and to recognize the exact relationship existing between a system and a unit or group of units. It should also be observed that the existence of cryptonets necessitates the re-encrypting of traffic which passes from one net to another.

32. Use of Systems

Many times cryptonets will exhibit another distinguishing feature. This feature concerns the use of the system. For example, a system may be used only for confidential material, or only for secret material; or it may carry only information about supply, or shipping, or personnel, or operations. Again, this distinction is of high traffic analysis value and provides, as well, assistance to the cryptanalyst.

33. Identification of Systems

Some external feature usually appears in the text of a message to designate the system used. Where only one system of a given external appearance (as 4-letter, 5-digit) is used between two correspondents, this is not necessary, but in most instances, this designation is required and it can be accomplished in two main ways. The first is

REF ID:A5384682

the use of the form of the message itself. For example, the last group of the message may contain a repeat of the group count or the indicators may be peculiar in their formation, or they may be placed in a unique position. Any distinction of this sort will serve. The second method is the addition of a discriminant to the message, generally as a part of the text, most often as the first group. This discriminant is usually composed in a distinctive manner, as five like letters, repeated digraphs, ascending or descending numbers. It may be enciphered. Where a discriminant is lacking, it is often the task of the traffic analyst to determine means of identifying systems and to isolate homogeneous traffic.

34. Use of Indicators

The difference between the discriminant and the indicator should be understood. The discriminant identifies the general system used, while the indicator provides the specific key for decipherment. These indicators are often in the clear and, if they display any peculiarities of use, they become a valuable traffic analysis weapon. The pages of a one-time pad, for example, may be applied in order and the page indicators will thus reflect the number of messages enciphered. The pad numbers themselves will also be of value since each pad will be limited as to its users.

35. Practice Traffic

When new nets are being established, or operators are being trained, practice traffic is often devised for exercise purposes. Sometimes special nets are set up to this end, and they carry nothing but practice material. On the other hand, certain schedules may be set aside on regular links.

36. Control Traffic

In order to mislead enemy traffic analysts, control traffic may be used. Such operations may range from the formation of dummy nets to the passing of dummy traffic over the usual links. Control traffic can be employed merely to hide an operation through maintaining a volume level on all nets, or it can be used deliberately to deceive by creating high volumes at points of slight military activity.

Section VI. COLLATERAL MATERIAL

37. General

Aside from the usual intercept material discussed in the preceding sections, there are many other sources of raw data which are of value to traffic analysis. They may be divided into two groups, the first

REF ID:A58489

directly related to intercept, the second more or less miscellaneous in nature. The first group includes direction finding. The second is concerned with the study of nets other than military, the use of decode material, intelligence reports, prisoner-of-war reports, and captured documents. With reference to this second group, it should be observed that traffic analysis, in both its analytic and applied phases, often involves the fusing of information and material of all types and from all sources toward the production of a complete communication picture. In this respect, traffic analysis touches to some degree upon almost every phase of intelligence, and to a great degree upon every phase of signal intelligence.

38. Direction Finding

a. Direction finding (D/F) is a method of locating radio stations through use of specially constructed receiving antennae. These antennae register the direction along which a radio signal is travelling as it passes on a great-circle path through the D/F location. When the direction of a radio signal is determined at more than one D/F site, the location of the transmitter may be plotted by noting the point at which the bearing lines intersect (fig. 23). A location determined in this manner is called a "fix."

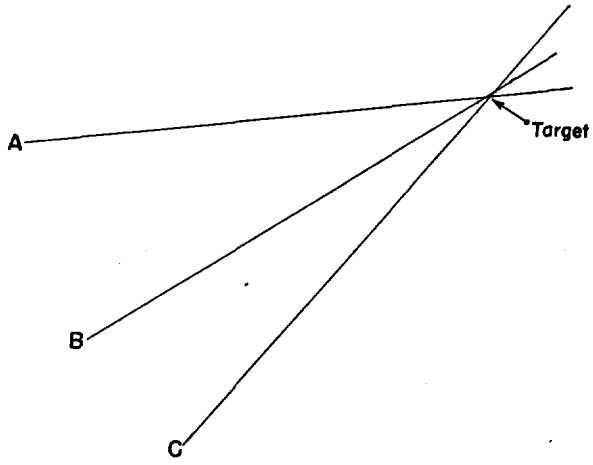


Figure 23

b. Usually, bearings will not yield a perfect fix, but will, depending on a number of factors, give a more or less restricted area. These factors include (1) the distance from the D/F station to the target, (2) the number of D/F stations involved in locating a target and the number of bearings taken, (3) the amount of the signal's deflection as encountered (for example, when the radio wave passes over mountains or shore lines), and (4) the quality of the D/F equipment.

RECD: 10 Jun 1946

Despite these and other limitations, D/F bearings seldom are misleading because the D/F operator is able to recognize whether or not a bearing is reliable and furnishes an evaluation of each bearing as it is forwarded to the plotting unit. The plotting unit also is in a position to make an accurate judgment on the reliability of a fix. An adequate arrangement for accurate direction finding requires a number of D/F stations (at least 3) located along a rather broad base (relative to the distance from the target) and so connected that they can all listen to the same signal and take their bearings simultaneously. It should be noted that D/F is particularly useful in low-echelon traffic analysis, but that over distances running into the thousands of miles it loses much of its effectiveness.

39. Information Derived from Cryptanalytic Results

Cryptanalytic solutions of traffic furnish, very often, the relationship between nets and order of battle. Since this is one of the ultimate goals of traffic analysis, detailed study of all solved messages, against the background of the nets, is a necessity. Study of solved messages should also be carried on for the purpose of relating internal information to external characteristics. This has an application to cryptanalysis for the identification of crib messages and to intelligence for the determination of the significance of traffic contacts and patterns. Message plain texts also yield a certain amount of signal information, as station locations and data concerning calls, frequencies, and schedules.

40. Intelligence Reports

Intelligence reports may vary from predigested order of battle lists to raw materials, such as captured documents or prisoner of war reports. Order of battle is the basis for the entire radio network and for the traffic passed over it. As such, an understanding of the order of battle is the necessary foundation for traffic analysis and its cryptanalytic and intelligence applications. The relationship is a circular one—intelligence added to traffic analysis yields additional intelligence. Aside from the broad phase of relating nets and battle order, this integration has specific applications in the analysis of traffic contacts and patterns and in the study of the uses of cryptographic systems and the transmission of routine messages.

REF ID:A58489

CHAPTER 3

RECONSTRUCTION OF THE RADIO NETWORK

Section I. INTRODUCTION

41. General

This chapter is concerned with the first objective of the traffic analyst, that of the reconstruction of the radio network. There are two phases to this objective, analysis of radio operations and net reconstruction.

42. Analysis of Radio Operations

This phase involves the identification and study of the elements discussed in the preceding chapter. It includes the identification of all components of the transmission, the analysis of their use, and the determination of their operating data.

43. Net Reconstruction

The nets are reconstructed coincidently with the study of radio operations. Each task helps the other; the distinction made here is only for academic purposes. In actual practice, attack must be carried out on all elements simultaneously, so far as possible, because analysis depends on the perception of relationships. Net reconstruction is concerned with the grouping of stations into nets, the determination of the links operating between those stations, and the identification of the stations with geographic locations, culminating in the production of the net diagram. The pertinent features of radio operations, such as calls, frequencies, and serial number blocks, may then be added to this diagram to complete the "pure" traffic analysis picture. The superimposition of the cryptonets and order of battle on the diagram is discussed in later chapters.

Section II. ANALYSIS OF RADIO OPERATIONS

44. Frequency Analysis

The main objectives of frequency study are (1) the determination of the system of use and (2) the solution of the system of allocation,

899152 O - 50 - 7

REF ID: A684682

including the method of original assignment, the pattern of rotation, and the reconstruction of the basic charts involved.

a. ANALYSIS OF THE SYSTEM OF USE. (1) The chief problem in the study of the system of use is the determination of accurate basic data. Once these data have been properly recorded the conclusion will usually be apparent. The basic data consist of who sends to whom and on what frequencies. To simplify study, a rough circuit diagram may be prepared. Two examples of these data and the conclusion to be drawn are given below.

(*a*) In the following example the net is a free star (fig. 24):

A to B on 5,000 KCS.
A to C on 5,000 KCS.
B to A on 5,000 KCS.
B to C on 5,000 KCS.
C to A on 5,000 KCS.
C to B on 5,000 KCS.

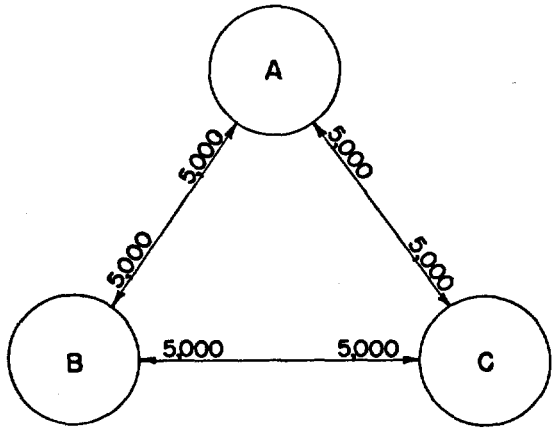


Figure 24. The net is a free star.

(*b*) In the following example the net uses the complex-sending system (fig. 25):

A to B on 5,000 KCS and 10,500 KCS.
A to C on 5,000 KCS and 10,500 KCS.
B to A on 4,000 KCS and 7,500 KCS.
B to C on 4,000 KCS and 7,500 KCS.
C to A on 3,000 KCS and 6,000 KCS.
C to B on 3,000 KCS and 6,000 KCS.

REF ID:A58489

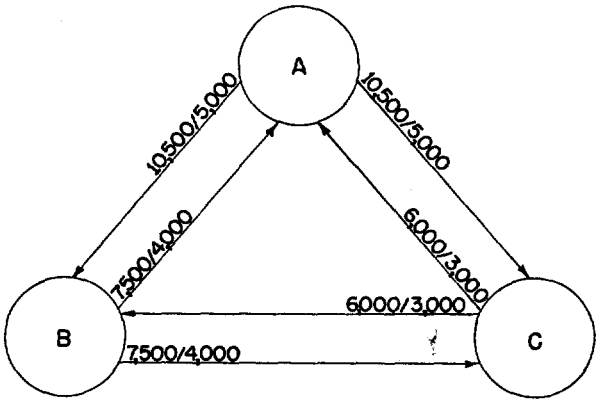


Figure 25. The net uses the complex-sending system.

(2) Arriving at accurate data, however, is often a fairly difficult task. It requires a detailed study of chatter for at least a week's period and usually somewhat longer, depending on the completeness of coverage during the period and the complications involved in the use of the frequencies. It is well to mention that, for the analysis of many features of radio operations, it is often desirable to have complete cover on a net for a limited period, such as a day, than to have spotty cover over a longer time. Generally, however, cover will be incomplete, that being one of the reasons why careful study of chatter is necessary before a decision is reached. A second difficulty arises where the enemy stations drift from the assigned channel. For example, a station allocated 4,650 kcs may vary all the way from 4,600 to 4,700 kcs. In the case of simplex and star working, much of this variation is intentional so that the one station can reply a little off the correspondent's frequency. A third problem is created by the assignment, as sometimes happens, of four or five or more wave lengths to a station. These wave lengths are not restricted to fixed times of day, but the station is at liberty to use whichever one can best be heard. It should be pointed out that there will often be exceptional uses of frequencies which cause the net to vary from its basic form of working. These exceptional uses should be carefully studied and explained, but they should not be considered as changing the net type.

(3) To illustrate some of these problems, assume that a cursory examination of a week's transmissions reveals the following:

A to B on 5,000 KCS, 11,600 KCS.
B to A on 5,000 KCS, 7,000 KCS, 11,590 KCS.
A to C on 5,000 KCS, 5,500 KCS, 11,625 KCS.
C to A on 5,010 KCS, 5,025 KCS, 6,995 KCS.

REF ID: A584682

B to C not heard.
C to B not heard.

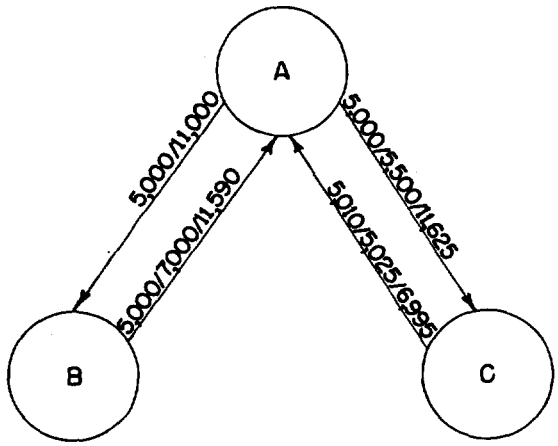


Figure 26.

The net, at first glance, appears to be a star (fig. 26) though there are several discrepancies to be explained. It may be assumed that C's 5,010 and 5,025 kcs are drifts of the base frequency 5,000 kcs, that A's 11,600 and 11,625 and B's 11,590 should all be 11,600 and that B's 7,000 and C's 6,995 are both 7,000. However, A uses 5,500 kcs to C, but neither B nor C have been heard on this frequency. This runs counter to the principle of the star. A check is made of the appearance of 5,500 kcs and it is found to have been used twice during the period under study, both times under the same circumstances. A came up on 5,000 kcs, C reported interference on this frequency, and A switched to 5,500 kcs. It is likely, then, that 5,500 kcs is an extra wave length assigned to the net for emergency purposes and that, in time, the other stations will also make use of it. In this instance the net is not working star since 5,500 kcs at A is corresponding with 5,010 kcs at C, but it is known that A did try to make contact under the established procedure first, so that this becomes the exceptional case and does not contradict the theory as to the star form. The 7,000 kcs at B and C also create a problem since A has never used this frequency. Again reference is made to the chatter logs where it is discovered that this frequency is used during the evening hours and has been heard once from B, twice from C. However, on all three occasions the A end of the circuit was not heard at all. It is possible that A was up on this approximate wave length but, because of some propagation or reception peculiarity, the intercept station was unable to hear it, or that the intercept station, for one reason or another, may only have been

REF ID:A58489

able to cover one end. Whatever the reason, imperfect coverage is apparent and, until A has been monitored on this schedule, nothing can be determined which would affect the star hypothesis. The net picture, as mentioned above, indicates that the star is controlled rather than free since B and C have not been observed in contact. Study of chatter, however, casts some doubt. At one point, A has asked B for a special schedule at 1500. B replies he cannot make it then since he has a schedule at that hour with C. On another occasion, A sends two messages to C for relay to B, A stating he has not been able to contact B. This chatter suggests that B and C work each other and that the net is a free, rather than a controlled, star. The evidence is slim since the schedules mentioned in the chat may only have been emergency ones, but it is sufficient to justify reserving decision and waiting for further developments.

b. Solution of the System of Allocation. Solution of systems of allocation requires at least several months of observation and, if some complex method of rotation is involved, may run into much longer periods. The problem is twofold: (1) the method of basic allocation and (2) the method of rotation, if present.

(1) It should be stated at the outset that usually a method of basic allocation will not be used except as it is tied into a system of rotation. Where frequencies are fixed, they have generally been assigned because they can be heard between two points and because there is no interference from other frequencies. This is particularly true on high-eschelon nets. It is always worthwhile, however, to check the frequencies of the various nets of a radio network for characteristics, if only to be sure. Some pattern may appear, for example, air-ground nets, wherever located, may be restricted to a definite set of frequencies, or divisional nets may be limited to a certain band. Anything in the way of a pattern, naturally, is possible. A tabulation of frequencies against net and the seeking of relationships in frequencies between related nets should serve to reveal most such patterns. Related nets may be so determined on the basis of function, such as air, shipping, line of communications, divisional artillery, by echelon, or by command.

(2) Whether a frequency system is fixed or changing, and if changing what the period of change is, can be discovered merely by observation. If a changing system is used, the first step in analysis is to determine some method of maintaining continuity so that if station A transmits on 4,300 kcs one day and 3,750 kcs the next day, there is some way of knowing that 4,300 and 3,750 are both the same station. Continuities may be established in two main ways:

(*a*) *Characteristics of radio operations.* Almost any item of radio operations may serve the purpose:

RECD 10 : AD684682

1.

Calls. If frequencies change and calls do not, identification is a relatively simple matter.

2.

Schedules. Taken in conjunction with other data, schedules may provide a clue to continuities. They are likely to be characteristic for the stations of a net, but care must be exercised in the use of this technique and supporting evidence should always be present. Also of value is any mention of future schedules at the time of the sign off, for example, "QRX 0100" (next schedule at 0100). It is then possible to relate stations heard at 0100 on the following day back to the stations involved in the chatter.

3.

Serial numbers. If serial numbers do not begin over at the time of each frequency change, they may be utilized. In the case of message center serials, care must be exercised to avoid the use of relayed traffic. For example, in figure 27, A, on the 15th, may

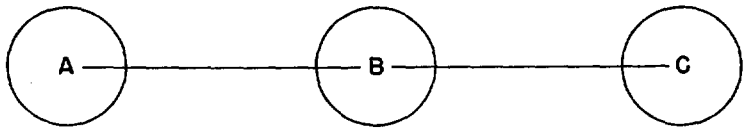


Figure 27.

send a series of messages over the A–B circuit with the message center serial range 1544–1573. On the 16th, the entire net changes frequency, and several messages are intercepted with the routing instructions A to C and the serials 1578–1581. It cannot be assumed that the new frequency heard on this transmission is at A since the traffic might have been passing on the B–C link. If some of the traffic, however, was routed A to B or else carried no routing indicating a local message, then the continuity might tentatively be established. Of far greater value in this respect are the radio station members, and, except in the case of the in-desk number where it is possible for several different circuits to be transmitting the same series, these ranges are reliable. Where serial ranges are fairly distinctive they may also be used in reverse. For example, station A may receive traffic in only a certain message center serial range from a correspondent. This may be caused by the fundamental assignment of the range to a definite service, for example, supply. Station A is at a quartermaster depot; consequently all the traffic to A from the correspondent will be in the one series.

REF ID:A58489

4.

Routings. Routing codes can also be of value when used by nets. It may be assumed that, as a general rule, a radio station will originate and receive more of its own traffic than it will handle on relay for other stations. For example, station A is at Gettysburg. If A changed frequency daily, it could probably still be spotted because of the large amount of Gettysburg correspondence transmitted and taken.

5.

Routines. Because of the requirements of military operations, it is necessary for units to make routine periodic reports. Very often these reports can be identified because of the stereotyped nature of the message externals. For example, a situation report, or a strength report, may be sent from station A to B, C, and D each day at approximately 2000. It would be a relatively easy matter to watch for this report to pass and to identify it purely by these external characteristics. Such routines furnish a trade-mark for the originating station and can be discovered and utilized without any knowledge of the text.

6.

Cryptographic systems. Cryptographic systems which are unique to certain correspondents can likewise be used as identifications. This also holds for some of the cryptographic features such as pad numbers of one-time pad systems. The 10th Division, for example, which sends through station A, is enciphering its traffic in pad number 1234. Usually, only one originator is permitted to encipher messages in a given pad because of its one-time nature. There may be one or several holders who can receive. Thus, until completely used, the pad will identify the originating station and, in some cases, also the recipient. Caution must again be exercised, however, with regard to relay messages and to the possi-

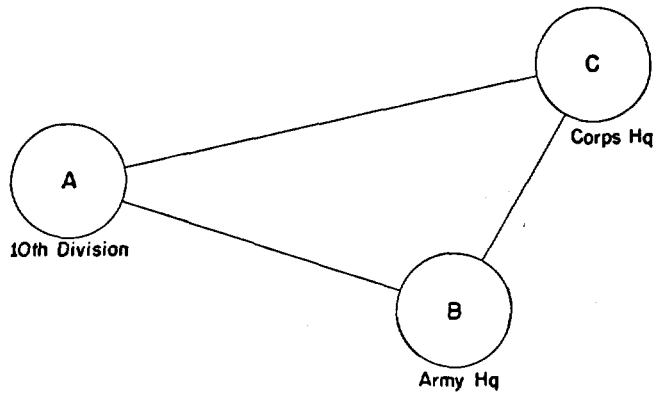


Figure 28.

REF ID:A5384682

bility of this traffic being transmitted over a different circuit of station A. If, for instance, the pad is used between the division and headquarters for some special purpose it could pass by several different paths (fig. 28). According to which route is available or readable, 10th Division's traffic may go directly to Corps or be relayed through Army.

7.

Services. Messages transmitted on one day may be serviced at some later date. If the date span bridges the frequency change, it may be possible to determine continuity.

8.

Chatter. Items of chatter often serve continuity purposes. Names of radio operators, for instance, may be observed in chatter, and, on recurring after a change, act as an identification.

9.

Procedural peculiarities. Some stations and operators develop unique habitual procedures which mark them. A station might, for example, regularly misspell a place name, or transpose the digits of a routing code number because of an error in the chart; an operator might send his call signs four times instead of the three used by others on the net, or send a separator between the hours and minutes of the file time though no one else does. Such peculiarities, which often arise from personal quirks, are usually rather difficult to discover because they involve painstaking attention to detail, but they are well worth the trouble. It is one of the phases to which the intercept operator, through his knowledge of the usual, can make an important contribution.

(*b*) *Use of direction finding.* This identification technique, described in paragraph 38, is a valuable means of providing continuities where efforts to use procedural characteristics have proved inconclusive. It is to be pointed out that, in general, procedural characteristics furnish a faster, less expensive, and more accurate method if they can be so utilized.

(3) Some of the techniques outlined above can stand by themselves, but it will always be found wise to apply several of them in combination so that one checks the other and reinforcing evidence is supplied. For example, the message center serials may indicate a continuity, and a routine message or the use of a restricted cryptographic system serves to confirm it. Incidentally, these methods of determining continuities are applicable to any sort of frequency change, whether periodic or irregular, and will also serve to tie together night and day frequencies and variant frequencies of the same station.

(4) When continuities have been established, the next task is the

REF ID:A58489

listing of the frequencies against the date breaks and the search for patterns of change or rotation. Once the general system has been solved, it will usually not be too difficult to keep abreast of changes. No attempt will be made in this manual to describe actual methods of solution further than to say that the problem, at this point, becomes one of cryptanalytic attack.

45. Call-sign Analysis

The main objectives of call-sign analysis correspond with those of frequency analysis, that is, (1) the determination of the system of use, and (2) the solution of the system of allocation.

a. Analysis of the System of Use. This analysis is conducted through a study of call signs as they are reported in the chatter. The period of call-up furnishes the most fruitful material, but all allusions to calls must be noted. A listing of the call-ups will generally provide sufficient information to identify the system.

(1) *Net using double-station call procedure* (fig. 29):

A calls B	DEF de ABC
B replies	ABC de DEF
A calls C	GHI de ABC
C replies	ABC de GHI
B calls C	GHI de DEF
C replies	DEF de GHI
B calls A	ABC de DEF
A replies	DEF de ABC
C calls A	ABC de GHI
A replies	GHI de ABC
C calls B	DEF de GHI
B replies	GHI de DEF

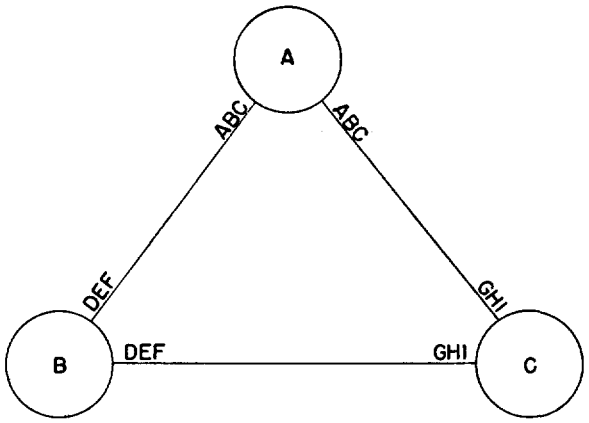


Figure 29.

REF ID:A58489

(2) *Net using link call system* (fig 30)

A calls B	ABC
B replies	ABC
A calls C	DEF
C replies	DEF
B calls C	GHI
C replies	GHI
B calls A	ABC
A replies	ABC
C calls A	DEF
A replies	DEF
C calls B	GHI
B replies	GHI

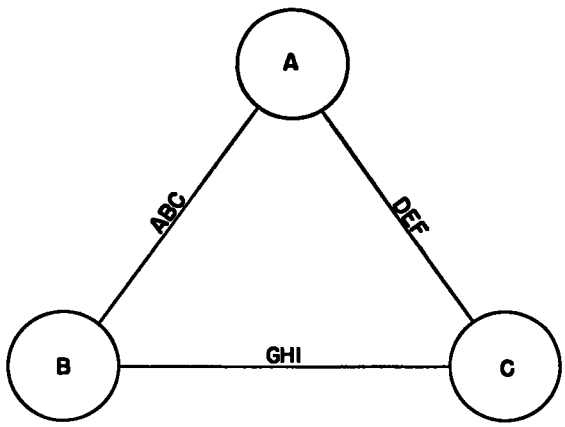


Figure 30

(3) *Net using single station call* (fig 31)

A calls B	DEF
B replies	DEF
A calls C	GHI
C replies	GHI
B calls C	GHI
C replies	GHI
B calls A	ABC
A replies	ABC
C calls A	ABC
A replies	ABC
C calls B	DEF
B replies	DEF

REF ID:A58489

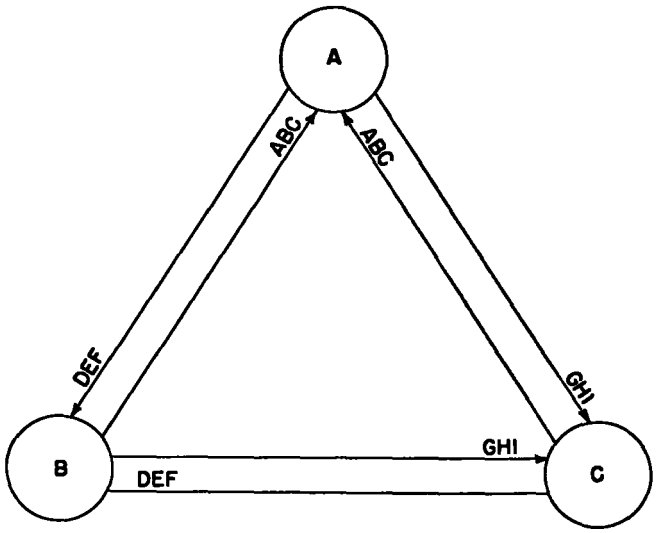


Figure 21

b Solution of the System of Allocation Like the study of frequency systems, the analysis of call sign systems may require anywhere from several months to several years Again like the frequency systems, the problem is twofold (1) the method of basic allocation and (2) the method of rotation, if present

(1) Calls must first be classified as to composition, for example, 3 digit, digit-letter-digit, etc, then these break-downs checked for pattern The allocation of calls may or may not be centralized. In the former instance, there will generally not be more than two or three systems to be solved, e g, Army and Air Force In the latter, however, depending upon the amount of decentralization, there may be a great many small systems Thus, in the initial analysis, calls should be listed by net, and the composition of the calls on each individual net observed If, for example, of all the nets under study, only two nets use 4 letter calls, it may be assumed, for the moment, that these nets employ a common call allocation After nets have been grouped by composition of calls, a search is made on each net for pattern For instance, the calls on three of the nets may carry "T" as a middle letter, indicating a possible grouping for study If a number of other nets also display similar characteristics, one using "R", another "V", etc, it is likely that all of the calls on these nets originate in the same general system The following lists of calls by net will serve to illustrate the general procedure

REF ID: A684682

Net I	*Net II*	*Net III*	*Net IV*
ABD	CDF	V7K	BCE
EFH	GHJ	V8J	KLN
FGI	LMO	X3M	OPR
JKM	MNP	Y4T	
		Y6S	

Net V	*Net VI*	*Net VII*	*NET VIII*
BAO	IJL	DEA	FQR
HIU	NOQ	HOA	JLT
KOE	PQS	JIE	SRM
MEA	STV		VTR
PAE			XOM
			XOA

(*a*) In the first quick grouping, the following division could be made:

Nets I, II, IV, V, VI, VII, VIII—3-letter.
Net III—letter-digit-letter.

(*b*) The first group then splits into three:
Nets V, VII—consonant-vowel-vowel.
Nets I, II, IV, VI—1st and 2d letters are in alphabetic order, 3d letter skips one from 2d.
Net VIII—apparently random.

(*c*) Thus, there are at least four systems of call distribution involved. On the other hand, studies of the calls on a number of nets may reveal no pattern at all. This is usually indicative of a large, general system in which control is highly centralized and the randomization carefully planned.

(2) Other features may also be employed to assist in the establishment of homogeneous call-sign systems for relationships between any of the elements of different nets that indicate possible relationships in other elements. For example, there may be some question as to whether or not the calls appearing on two separate nets can be grouped together. A cryptographic system, found nowhere else, is discovered on circuits of both nets. This suggests that there is some connection between the two nets and increases the possibility of a common call system. Procedural peculiarities of any type may likewise be used to associate nets. Order of battle, if known, furnishes another valuable method. All the nets of a given Army, for instance, will probably use the same call allocation. It may be that, in a highly centralized organization, a dichotomy can be established simply between Army and Air Force.

(3) Once the various systems have been segregated, it becomes possible to attack each separately. If a pattern exists within the call itself (as in Nets I, II, IV, and VI in (1) above), all possible

REF ID:A58489

calls can be listed and this used as a basis for the reconstruction of the allocation chart. If no pattern can be found, however, (as in Net VIII), it becomes infinitely more difficult to reconstruct these charts, and if the system is a large one it may be necessary to collect data over a period of years before a solution can be effected.

(4) Often these allocation charts serve as a base for the change or rotation of calls or for the choice of alternate calls at the same station. In analysis of the system of rotation, the first step is to determine the periodicity, which can usually be done simply by observation, and the second to establish continuities so that the calls related to each station or link and the order of their use are known. The techniques outlined in paragraph 44*b* (2) for the determination of continuities when frequencies change also apply to call signs with one exception (par. 44*b* (2) (*a*)*1*) and need not be further discussed here. In this one exception the reverse is true—if calls change and frequencies remain constant, the frequencies furnish the continuities to the calls. When continuities have been established, the calls may be listed in order for each station, and through the application of cryptanalytic techniques, the system attacked.

(5) In the practical aspects of call-sign system solution, it will be found that garbled and missed calls account for much of the difficulty in the initial stages of attack. Where there is a pattern to the call composition, garbles can be resolved with relative simplicity. In random composition, however, the problem is more complex and care must be taken to eliminate all spurious calls before beginning analysis. Garbles occur with some frequency in calls partly because the enemy makes an attempt to restrict their use, and partly because his operators become so familiar with them that they tend to send them in a quick, sloppy manner. In general, a call should be intercepted several times, preferably at different schedules, before it is accepted as genuine. Garbles can often be corrected by reference to the actual Morse equivalents. For example, if the call "AHV" has been established and the call "ASV" appears once on the same net, the Morse will indicate the possibility of error:

AHV .— ....—
ASV .— ... ...—

the difference being only a dot. Other link characteristics such as frequency, serial numbers, etc., will assist in confirming or disproving the identity of the two calls.

(6) Missed calls also present a problem to the analyst. They arise from imperfect coverage, and there is no remedy except to give more complete coverage and schedule information to the monitoring stations. Since calls are often sent only at the start of each schedule, this time is most important.

REF ID:A584489

(7) The following example, based on the call composition used in Nets I, II, IV, and VI in (1) above, will illustrate the general approach (since these calls have a definite pattern, all possible calls can be listed):

ABD
BCE
CDF
DEG
EFH
FGI
GHJ
HIK
IJL
JKM
KLN
LMO
MNP
NOQ
OPR
PQS
QRT
RSU
STV
TUW
UVX
VWY
WXZ
XYA
YZB
ZAC

(*a*) It is noted that calls change daily on the four nets involved; after the completion of one week, a tabulation by net and station can be made. (Garbled calls have been corrected.)

	1	2	3	4	5	6	7
Net I							
Station A	ABD	PQS	TUW	KLN	BCE	RSU	....
Station B	....	WXZ	BCE	EFH	HIK	....	UVX
Station C	MNP	JKM	MNP	WXZ	NOQ	XYA	CDF
Net II							
Station A	CDF	....	IJL	YZB	....	ABD	JKM
Station B	UVX	LMO	VWY	STV	JKM	GHJ	....
Station C	IJL	STV	OPR	ABD	DEG	MNP	WXZ

REF ID:A58489

Net IV

Station A	TUW	RSU	....	RSU	UVX	FGI	IJL
Station B	....	EFH	....	FGI	IJL	LMO	....
Station C	NOQ	KLN	....	XYA	OPR	YZB	VWY
Station D	HIK	XYA	....	LMO	CDF	STV	DEG

Net VI

Station A	....	ABD	DEG	MNP	PQS	BCE	....
Station B	VWY	....	PQS	TUW	....	HIK	....
Station C	DEG	YZB	JKM	GHJ	EFH	TUW	....

(*b*) Observation of the calls indicates that they are being rotated in a simple manner, and a check against the list of all possible calls shows that the difference of six between calls on the same net is fairly common. For example, on the 1st, MNP is 12 calls away from ABD; IJL is 6 away from CDF; NOQ is 6 away from HIK. It is also noted that the calls QRT and ZAC do not appear, probably to prevent confusion with Q and Z signals. This leaves 24 possible calls, and the periodicity of 6 suggests that the basic table is arranged as follows:

ABD	GHJ	MNP	TUW
BCE	HIK	NOQ	UVX
CDF	IJL	OPR	VWY
DEG	JKM	PQS	WXZ
EFH	KLN	RSU	XYA
FGI	LMO	STV	YZB

and that the calls are taken off across the chart and allotted to Net I, Net IV, Net II, and Net VI in that order. Within each net the calls are assigned to individual stations in what appears to be a random order.

46. Schedule Analysis

Schedule analysis is designed to discover what system is in use, whether the signalling is restricted or unrestricted and, if the former, what the time of each schedule is.

a. Analysis of the System. Analysis involves a tabulation of times of communication together with a study of chatter. Time is correlated with circuit and, if a definite pattern shows up several weeks running, it may be assumed that period signalling is in use. In the preparation of the data, record should be made of such chatter items as, "I have a schedule at 2200 with XYZ." Such information helps to fill in the gaps in cover. Also note must be taken of the very brief schedules where the stations have no traffic and merely call up, say, "I have no traffic," and sign off; or where a station is running over his schedule time and calls his regular correspondent

REF ID: A684682

to say, "I am busy," and then goes back to the first correspondent. If no pattern appears, however, it is then likely that either unrestricted signalling or priority signalling is in use. This can be determined by a check of the tabulation, since in priority signalling the control station will usually come up at regular schedule times. Chatter will also prove characteristic for this type of operating since the order of transmitting is fixed and usually only one message is sent at a time by each station. The type of unrestricted signaling can likewise be identified from chatter. Where arbitrary schedules are used, the stations will arrange for the next schedule at the time of sign-off. Incidentally, in period signaling, the stations also sometimes mention the time of their next schedule so care should be exercised not to confuse the two. The regular pattern of times over a long period will usually distinguish period signaling. In alert operating, no arrangements are made, all stations standing by for transmissions at any time.

b. Determination of Schedules. The tabulations made for the above purpose will also serve to determine the times of regular schedules. Each circuit may be plotted on cross-section paper with hours down the side and days across the top. This will give a month's picture at a glance (fig. 32). The letters in each square indicate

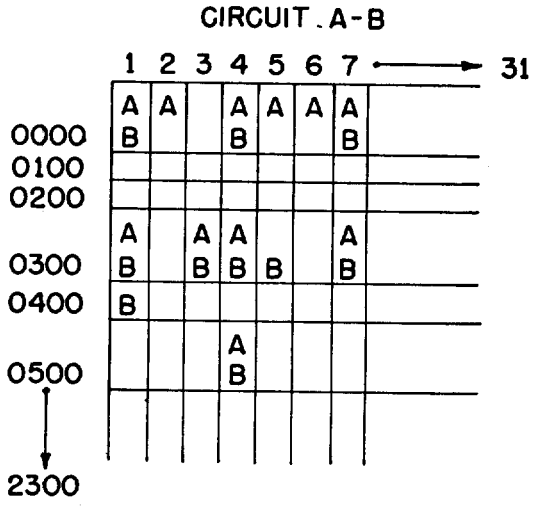


Figure 32.

the end of the circuit that was heard. On the 2d at 0000, for instance, only A was intercepted. Other items may be added to this tabulation if desired. These might include number of messages passed, indication as to which of the alternate frequencies was being used, and special notes from chatter relating to schedules. Two irregulari-

REF ID:A586489

ties will be noted in the pattern in figure 32. On the 1st at 0400 B ran over the regular 0300 schedule. Reference to chatter discloses that B asked A for additional time. On the 4th at 0500, A-B worked a special schedule. A check of chatter on other A circuits shows that A arranged for this schedule through a third station, which could contact both A and B, for the purpose of passing urgent traffic.

47. Procedure Analysis

Analysis of procedure is undertaken (1) to discover characteristics which will assist in identifications and continuities, and (2) to solve any encipherments employed.

a. Study of Characteristics. The normal characteristics of the procedure under study should first be established. This includes the call-up, exchange of readability, order of traffic, message externals, servicing methods, and sign off. In many communication systems, several normal procedures may be apparent, each representing a major division of nets. When this task has been completed, variations from the normal as applied to individual nets, groups, links, and stations must be identified. These variations may be of any sort. For example, one net may use break-in procedure for servicing, or may place the priority of the message in a different preamble position, or may tune up with a letter other than "V"; or a station may regularly place an NR before the link serial number while others do not, or fail to use an RQ before its request for services. These variations arise in several ways. They may be due to an oversight on the part of personnel, such as failing to change to a new method of procedure because of habit or because the station was not included in the distribution of the new instructions. Such situations will usually be corrected in time, or, if distribution is impossible, continue to serve as an important identifying feature. Or they may arise from the latitude permitted nets or stations in compiling their own rules. The only approach to this analysis is through the detailed study of chatter and the recording of the normal and the unusual.

b. Solution of Enciphered Procedures. The solution of enciphered procedures depends on the ability to determine the meaning of procedure signs and signals in context and, where a periodic change is involved, the equating of the same procedure in terms of different encipherments. For example, in the opening minutes of a schedule, procedures such as "Send V's," "How is my readability," "I cannot hear you," "Readability is poor," "Adjust your transmitter," etc., will be common. By study of the context over a period of time, it should be possible to identify the appropriate meaning.

RECD 100 : 2684682

48. Serial Number Analysis

The analysis of serial numbers is directed toward the determination of the type of number, the manner of assignment, the solution of any encipherments, and the identification of the series with units.

a. ANALYSIS OF TYPE. The type of the serial number, that is, indesk, message center, signal center, etc., is determined through a correlation of the numbers with other signal features. The numbers should be tabulated for a period of a week or more as necessary against call signs, file times, intercept times, cryptographic systems, routings, and similar items. The following discussion is not intended to be complete since there are so many possibilities involved in these manifold relationships, but it is hoped to give some general indications on how to think about them.

(1) Serials which run in order by cryptographic systems may be a code room number, a message center number, or a signal center number. It will rarely be a radio station number. The caution to be observed is that the cryptographic system may not be the basic factor and the serial the result, but rather the system, like the serial, may be the effect of something more basic. For example, a series is found which agrees with the cryptographic system and every message in that system is always in that series. It is noted, however, that the system is the only one held by the unit involved. Thus, both the system and the series are representative of the unit, and the number only accidentally follows the system.

(2) Serials which correlate with routings are also usually in the message/signal center phase. Sometimes several series which do not match with other features are observed originating at the same routing. These are often the expressions of several units operating through a single signal center. Such numbers may be put on at the unit message center or they may be added at the signal center, the latter maintaining several series, one for each of the units involved.

(3) Serials which run in order by file time may represent either the message/signal center or radio station stage. Usually, file times are put on at the radio station, but, since the traffic comes to the station direct from the message or signal center, its order is seldom disturbed, so that it could be numbered in one place and time-stamped in another and still demonstrate a relationship. In the case of radio station numbers, it will usually be found that several call signs, used at the same station, will run in a common series.

(4) Transmitter numbers will, as a rule, correlate with the sending call signs and the intercept time. Link serials will be evidenced by the further distinction of a separate series for each station called. Operator numbers are indicated by several series originating at one call, regardless of reply, unless the station works to only one correspondent.

REF ID:A58489

(5) It is just as important in the study of serials to have negative evidence as positive, so note should also be taken of what does not fit the series. If several routings fall in the same series, for instance, the number was not assigned at the message center if that is what the routing represents. Such a series is more likely to relate to the radio station which handles traffic for several different routings.

(6) Many times series will appear which bear a relationship to several items. It is then necessary to determine what is the basic consideration. For example, a tabulation of serial numbers reveals:

Serial	*Crypt. System*	*Routing*		*Call sign*		*File date and time*	*Intercept date and time*
		From	*To*	*From*	*To*		
326	A	A	B	PQR	XYZ	08 1040	08 1215
327	A	A	B	PQR	XYZ	.....	08 1217
328	B	A	C	PQR	XYZ	08 1040	08 1220
335	A	A	B	....	....	09 1230	09 1530
339	C	A	C	PQR	XYZ	09 1210	09 1532
340	A	A	B	PQR	XYZ	09 1235	09 1535
343	B	A	C	PQR	....	09 1300	09 1538
344	C	A	C	PQR	XYZ	09 1300	09 1600
345	C	A	C	PQR	XYZ	09 1250	09 1615
346	A	A	D	PQR	XYZ	09 1310	09 1619
362	C	A	C	PQR	XYZ	11 1240	11 1525
367	C	A	C	PQR	....	11 1500	11 1801
368	C	A	C	PQR	XYZ	.....	11 1820
429	B	A	C	PQR	XYZ	08 1100	08 1223
437	B	A	C	PQR	XYZ	09 1315	09 1623

Except for the last two numbers which are garbled, the serials correlate with origin, calls from and to, and intercept time. File time is slightly off in several places. Since intercept time fits so well, it may be assumed that this is a radio station number. Reference is now made to the circuit diagram and it is noted that PQR is on the edge of the net and that it is connected to it by the single circuit to XYZ. Thus the routing "A" is probably the only message center routing through PQR and, therefore, the relation between "A" and the serials is forced and not the true one. If it were the true one, it is likely that the intercept times would be somewhat out of order because of the routine of processing traffic and the passing of priority messages. But since there is only one link out of the station, the type of radio station number used cannot be defined. It may be an in-desk, a transmitter, or a link number. If the picture is expanded, however, to include an additional link with numbers, it will appear as follows:

REF ID: A584682

Serial	Crypt. System	Routing From	Routing To	Call sign From	Call sign To	File date and time	Intercept date and time
372	B	A	C	PQR	STN	08 0900	08 1025
733	A	A	B	PQR	STN	08 0910	08 1030
734	A	A	B	PQR	STN	08 0910	08 1033
759	B	A	C	PQR	STN	11 1535	11 1911
765	C	A	C	PQR	STN	11 1820	11 1914

The serial is a link number since the numbers run in a separate series for the PQR–STN channel.

Serial	Crypt. System	Routing From	Routing To	Call sign From	Call sign To	File date and time	Intercept date and time
603	B	A	C	PQR	MNO	171441	172010
604	A	A	C	PQR	MNO	171411	172013
605	B	A	C	PQR	MNO	171411	172016
606	B	A	C	PQR	MNO	171415	172021
610	B	B	D	GHI	STN	171430	171810
612	C	B	D	GHI	STN	171430	171812
612	C	B	D	CHI	STN	171430	171812
613	A	B	C	PQR	MNO	171440	172005
634	A	A	C	PQR	MNO	181120	181523
636	A	A	E	GHI	STN	181135	181803
639	A	A	D	GHI	STN	181150	181809
640	B	A	C	PQR	MNO	181155	181520
641	A	A	C	PQR	MNO	181155	181535

Note the correlation with file date and time and the interlocking of the call signs. This is an instance where file date and time are entered at the radio station.

(7) The following tabulation is that of a signal center number:

Serial	Crypt. System	Routing From	Routing To	Call sign From	Call sign To	File date and time	Intercept date and time
020	A	A	C	GHI	PQR	230910	231233
023	A	A	C	GHI	PQR	230910	231230
024	A	A	C	GHI	PQR	230925	231225
026	B	B	D	JKL	STN	230910	231413
029	C	B	D	JKL	STN	230915	231416
153	A	A	C	GHI	PQR	241120	241236
155	A	A	E	MNO	XYZ	241125	241228
156	D	A	E	MNO	XYZ	241130	241231
164	A	A	E	MNO	XYZ	241130	241238
166	B	B	D	JKL	STN	241145	241411
167	B	B	D	JKL	STN	241130	241402
170	C	B	D	JKL	STN	241145	241409
171	C	B	D	JKL	STN	241150	241421
172	D	A	C	GHI	PQR	241145	241250

REF ID:A58489

Both A and B route through the signal center where a common series is applied to the traffic of both. The possibility of this being an in-desk number is largely ruled out by the failure to correlate with file time.

b. Analysis of Assignment. Study of the manner of assignment of serial numbers is concerned with three phases: (1) composition of the numbers, (2) range of the series, and (3) over-all pattern of assignment.

(1) *Composition.* The numbers may consistently be two-digit, or three, or four, etc. They may incorporate such features as the date. Composition, if sufficiently distinctive, often furnishes a means of quick recognition.

(2) *Range.* The range of the series may be readily determined, or it may take several years. It can be established by observation of the reversion to the lowest number of the range, which will fix its limits in terms of either time or numbers, or both.

(3) *Over-all assignment.* Serial ranges of the same type of number should be checked for pattern of assignment against each other. In the case of message center numbers, for example, it may be found that each division of an army has been given separate blocks, 1–100, 101–200, 201–300, 301–400, etc. Similar patterns may appear with regard to signal center or radio station numbers. These patterns can be analyzed through a comparison of ranges representing groups which bear an order of battle or a net relationship to each other.

c. Solution of Encipherments. The solution of enciphered serial numbers is a matter of cryptanalytic approach. The initial break, however, can often be made by gathering a group of messages on which it is thought that the serials run in order. If, for instance, an in-desk number is involved, messages arranged by file time should assist in attacking the system. It also may be helpful to select the first message of the day, if possible, and use it as No. 1. It will serve as a base even though that may not be its actual number. If the numbers are thought to repeat daily a selection of this message each day may yield different encipherments of the same number. As a rule, these systems should not prove too difficult to solve unless the method is one of complete randomization.

d. Identification of Series. Once the type of series is known, the next step is to determine the actual unit behind each series. In the case of a message center number, for example, what message center is it? Or if there are three series of in-desk numbers out of the same station, what do each of these series represent? These identifications are established by "pure" traffic analysis plus the use of collateral material on the basis of the axiom that things equal to the same thing are equal to each other. For instance, a range of in-desk numbers appears only with codes A and B. Codes A and B are known to be

REF ID: A5384682

transportation systems. Therefore, the serial range represents the transportation unit at the signal center. Care must always be taken, in chaining data of this sort, that the basic assumptions are valid (in this case, that A and B are transportation codes) and that the things compared demonstrate an exact relationship (if A and B were also used on another range of numbers out of the same station, then it is unlikely that the first range represents transportation, but rather that it represents some other type of unit or else a specific transportation unit, these possibly being two at the station). Decode and order of battle material are invaluable in the study of these series. If some of the traffic related to a series can be read, solid evidence for conclusions is provided and often a definite unit can be identified. Order of battle will do much the same. For example, where only one air unit is carried at a given location and a series, tied to the air cryptographic systems, is observed out of that location, it may be assumed that the series represents the air unit.

49. Analysis of Priorities

The analysis of priorities is directed toward determining their order and the solution of any encipherments. The order is determined by comparing file times with intercept times. In general, the shorter the average time lapse, the higher the priority. However, time lapses should be compared within stations not between them since the size of the station and the volume of traffic handled will cause individual differences. Relayed traffic, of course, should not be included in the comparisons. The cryptanalysis of encipherments is naturally dependent on the system used, but it is of assistance to group messages according to expected priority, thus providing isologs.

50. Analysis of Routing Systems

The main objectives of routing system analysis are to discover the manner of use and to solve the routing codes.

a. Analysis of Use. When routings appear on traffic, it is first necessary to determine what they represent in terms of origin and destination. This is done by observation. If necessary a tabulation can be made against call signs which will readily reveal which routing is the originator and which the addressee. The difference where present between information and action addressees may be a little more difficult, but checks, for example against priorities, should assist. Further observation will indicate the manner of handling local and relay traffic and the nature of the routings in these instances. Any peculiar use of routings, as in the readdressing of traffic, can also be determined. Following these routings against the net diagram is often helpful.

REF ID: A584682

b. Solution of Routing Codes. The initial step in the solution of routing codes is to check the code groups for characteristics in composition and range. Once these patterns, if present, have been recovered, the next step is the specific identification of code and syllabary groups. Identifications are chiefly based on cribs from known systems to unknown, on net diagrams, on breaches of security, on decode and order of battle material, and on a number of variations of these. As identifications are produced, it may be possible to ascertain the structure of the code and syllabary, such as alphabetical, geographic, order of battle, etc., and this, in turn, assists in future recoveries. In order to suggest methods of attacking this problem, some of the possibilities are discussed below:

(1) *Tying the code group to a known radio station.* Where the station locations are known, several methods present themselves according to the use of the routing codes. The predominant originator out of a station may ordinarily be assumed to be located there. This also applies to the predominant destination, unless destinations are dropped on local traffic. But, because the identification is made with a location, this identification is a true one only if the routing numbers represent locations. If they represent units, then it is necessary to seek further, and the recovery of the location can only be considered tentative in lieu of something more exact. Along with the use of this technique, the lapse between file and intercept times should be averaged for each originator. Messages originating locally will show a shorter time lapse than those previously relayed. If destinations are habitually dropped on the last, or local, leg of a relay, they may be related to the receiving station. For instance, a message from A to C carries the routing "123–567" on the A–B link (fig. 33), but when B relays to C, it only carries "123", thus matching 567 with C.

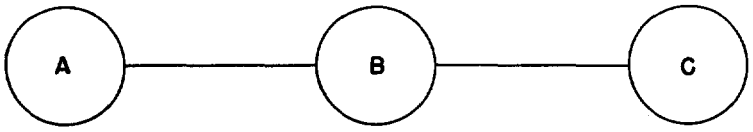


Figure 33.

When the same message is sent to several locations, the local copies may not carry routings while the relayed ones do, making possible the identification of the origin with the sending station. For example, in figure 34, A sends the same message to C and D. The message to C on the A–B channel is marked "123–567", that to D has no routings, thus identifying 123 with A.

(2) *Cribs.* The availability of cribs is chiefly based on the existence of several different routing systems. This may involve checking into networks other than military, such as Naval or domestic, for

REF ID: A684682

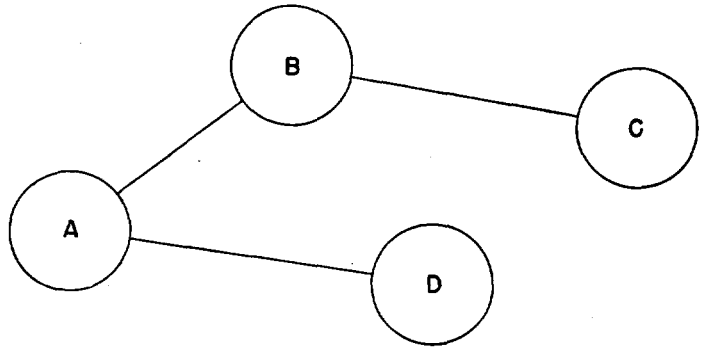


Figure 34.

such data. No possibility should be overlooked. Some of the crib techniques follow.

(*a*) *Relay crib.* If it is necessary for a message to pass over different nets with different routing systems, origins, and destinations can be correlated, and if one system is known, the other can be identified. For example, the message on Net I carries "123–567", on Net II "ABC–JKL", then 123 equals ABC and 567, JKL. One caution here relates to the destination. If this is a book message going to several addressees, there may be a direct correspondence between the originators, but not the destinations, since 567 may be one receiver and JKL another. Sometimes, this can be verified by checking the address and serial numbers.

(*b*) *Book message crib.* Where the same message goes to a number of destinations over different nets employing different routing codes, it is possible to crib originators. This often happens with large centers who work in several nets and may use several routing codes. It also occurs where traffic is relayed out of the net. Naturally, this would also yield a relay crib, but if the first transmission has been missed, the later relay can be used as a book message crib.

(*c*) *Serial number crib.* Serial numbers may be used to crib originators if the serial is a message or signal center number. For example, if a tabulation of serials reveals the following:

Serial	*Routing*	*File date and time*
53	123	092005
54	123	092005
55	123	092005
58	ABC	092005
59	123	092005
60	123	092015
65	ABC	092020
67	ABC	092020

then 123 may be cribbed with ABC.

REF ID:A684682

(*d*) *Error crib.* Where several routing systems are available to a station which works in a number of nets, it may occasionally happen that the wrong system is used. Such errors will generally be corrected yielding a crib between the two codes.

(*e*) *Address and signature cribs.* A unit or person addressed at one routing group in a known system will yield a crib against the same unit addressed at an unknown group. For instance, the 37th Division may be addressed at ABC, known to be Mannheim, on one message, and to 123 on another on the same day; 123 may then be identified with Mannheim. The possibility of unit movement, however, must be considered, and also that of detachments being addressed. The new recovery should be checked against the pattern, if present, of the routing system. In address systems where solution is only partial, but unenciphered code is available, the same address code groups may be used to crib the routing groups. Address code groups, for example, 1234, 5678, may appear with destination group ABC and also with 135. It is not necessary to know the value of 1234 5678 to crib ABC with 135. These same techniques are applicable to signatures and points of origin.

(3) *Operator chatter.* Operator chatter may give away the identity of a code group through the mention of a place name or a unit.

(4) *Address information.* Where addresses are separate from routing codes, use may be made of the address when readable. A unit, whose location is known from other order of battle sources, may be addressed at an unknown routing group thus identifying this group. Consideration must be given in such an instance to the possibility of the unit having moved. If there is some pattern to the composition of the code, the new value should be checked for fit. The recency of the date of the unit's identification and the trustworthiness of the source should also be noted.

(5) *Solved message information.* Solved messages may contain outright assignments of routing code values; more usual, however, is the traffic which permits correlation of internal originators, addressees, or subject matter with externals. All solved messages should be read for clues to routing code identities.

(6) *Miscellaneous sources.* These involve prisoner-of-war reports, captured documents, and similar materials.

(7) *Syllabary solution.* The syllabary to the routing code may be solved by using any of the above methods, but also available is the use of word patterns. If, for example, the routings consist of place names, a list may be constructed of all likely places which will show patterns of repeated or doubled letters, digraphs, etc., within each location, and this may be applied against similar patterns in the encipherments.

REF ID: A5384682

(8) *System change.* If the routing system changes, the continuity techniques discussed in paragraph 44 *b* (2) may be applied. For example, the continuation of a series of serial numbers may serve to identify a new routing designation with an old. Also of value are the contact patterns or associations in which a routing designation may be involved. If, for instance, routing number 123 sends traffic daily to three particular locations, and after the change of system, ABC is discovered following the same pattern, then 123 and ABC may be equated.

c. The above listing of methods of identification is only partial and specific application is dependent on the nature of the communication system under study and on the structure of the routing codes. Identifications, as made, should be evaluated and some sort of validity indicator attached to them as a guide to the reliability of the value. These validities are the result of personal judgment and the peculiarities of evidence and no rules can be laid down for their use on a general basis though in any specific problem definite standards can be set up. Where identifications are based on a crib, however, it should be remembered that the validity of the cribbed value can be no higher than that of the base value.

51. Analysis of Textual Features

The analysis of cryptographic features is concerned with the recognition, use, and distribution of systems, the use of indicators, and the identification of practice and dummy traffic.

a. Recognition. The recognition of cryptographic systems is the first step in their analysis either for traffic analysis or cryptanalytic purposes. Where a discriminant in the clear is present, this becomes a simple matter; encipherment somewhat complicates the problem. But, if there is no discriminant, it is necessary to make use of other features. In the attack, traffic should be sorted down by net and then studied for individual peculiarities. For instance, the following differences may appear as to the type of text:

Net	Type of text	No. of messages
I	4-letter	65
	4-digit	40
	3-digit	29
II	4-letter	48
	5-digit	73
	4-digit	51

Since the net usually represents an order of battle entity it also often represents a crypto-entity. Therefore, all 4-letter traffic passing on Net I (barring the discovery of any further distinction) may be assumed to belong and may be considered for the moment a hemo-

REF ID:A58489

geneous system in itself. Further study is then necessary on the relationships of the two possible systems. Some elemental difference as to form may be apparent which will distinguish them as separate systems, such as the presence of a digit indicator in one. On the other hand, no distinction may be noted and it will be up to the cryptanalyst to determine if the same or different systems are involved. Routings should also be checked in this respect, a relationship between routings (as to echelon, for example) evidencing the likelihood of the same system though passed on different nets. Other factors, beside type of text, are of course also valuable. These include priorities, characteristic serial number ranges, or features of the text such as the nature of the indicators.

c. Analysis of Use. Tabulations of the nets and routings of traffic will often indicate the use of a system. A system, for example, passing only over a water transport net may be identified tentatively as a water transport system, or one used only between intelligence units may be considered a special intelligence system. Caution should always be exercised in making such assumptions because of the ever present possibility that the transmitting of certain traffic over specific nets may result from communications necessity. Peculiarities as to priorities, serial number ranges, and miscellaneous preamble classifications may also assist.

d. Analysis of Distribution. Directly related to the study of use is the analysis of distribution which can be accomplished on the basis of the same tabulation. For instance, a given system may be identified as Air Force and, furthermore, it may be discovered that its distribution is limited to a certain type of Air unit. The tabulation may be as follows:

Net	*Routings*	*Volumes*	*Other characteristics*
I	A–B	354	All traffic uses 5-digit message center numbers.
	A–D	251	
	B–A	240	
	B–D	223	
	C–A	112	
II	A–E	232	5-digit message center numbers.
	A–F	227	
	E–F	116	
	F–E	34	
III	A–G	249	5-digit message center numbers.
	B–G	245	
	G–C	121	
	G–H	112	
	H–G	78	

REF ID: A5384682

Nets I, II, and III are known to be high-echelon Air Force administrative nets. The system under study appears only on these nets and a further check reveals that it composes the bulk of the traffic passed, indicating that it is probably the high-echelon administrative Air system. The 5-digit message center numbers are of interest because numbers of this size appear only on traffic of Air division or higher. Furthermore, most of the routings involved are known to be locations of Air divisions and higher headquarters. Thus, the limits of the distribution of the system are established and now the reasoning may be reversed: any routing appearing with this system may be assumed to be an Air division or above. One-time pads lend themselves to this type of analysis because of their highly restricted distribution. Tabulation of the pad numbers against other features will generally define the users, and since these pads are usually used in only one direction, fix the originator and the one or more recipients.

e. Analysis of Indicators. Where indicators appear in the clear they may be of traffic analysis value. Observation will reveal any peculiarities of the indicators and, if present, they can be correlated with other features.

f. Analysis of Practice Traffic. Practice traffic can often be identified through a study of the text. Messages may be made up at random which generally leads to a patterning and repetition of combinations of letters or digits. Also since there is usually no desire to disguise practice traffic, it may carry a designation in the heading. On the other hand, skillfully designed practice traffic, particularly if an effort is made to conceal it, may be undetectable except for security breaches in operator chatter.

g. Analysis of Control Traffic. Control traffic, if properly handled, may prove very difficult to identify. The usual means of analysis, such as operator chatter, distinctive serial number ranges, etc., are always open. For example, very fast receipting for traffic and few services may indicate that the operators know that the traffic is dummy and are not particularly concerned about it. On the other hand, in an efficient control operation, the operators will not know that they are dealing with dummy traffic and hence will furnish no clues. Another method open to the analyst, however, is the study of traffic volumes and proportions. A level traffic volume on a number of circuits may indicate an attempt to conceal the natural peaks and troughs of a military operation. Moreover, high volumes in areas which other intelligence sources reveal as inactive should be viewed with suspicion. Abnormal rises of certain types of priorities of traffic should be carefully checked for evidences of spuriousness. Control operations carefully planned will take into account the

REF ID:A584489

proper proportions between the various types, but, because of their complexity, breaches of security will often occur.

52. Miscellaneous Items

Every communication system has its own peculiarities in its procedure and traffic. No rules can be given for their analysis except to observe the manner of use and to seek out the relationships between them and other features. It is hoped that the foregoing discussion of certain specific components will not only serve to set the pattern for research on these miscellaneous items, but, more than that, will encourage the traffic analyst to use his ingenuity in the development of new techniques.

Section III. NET RECONSTRUCTION

53. Introduction

The reconstruction of the radio net proceeds simultaneously with the analysis of radio operations. (Furthermore, it is a continuing task since net formations and operating data are seldom static factors.) As noted before, it involves the grouping of stations into nets, the building of the net structure, and the identification of the stations with geographic locations and military units. The resulting net diagram may be drawn in either a schematic or geographic design, according to purpose, and signal features added. This involves, in effect, the reproduction of the radio communications section of the enemy "Signal Operation Instructions" (SOI). These instructions are the orders issued setting up the required signal nets for each military operation and include the assignment of frequencies, call signs, schedules, and miscellaneous data. For a more complete description of the "Signal Operation Instructions," and for United States Army examples of same, see chapter 4, FM 24–16.

54. Grouping of Stations

a. The initial step in analysis is to list all stations and their correspondents. This will yield a rudimentary grouping. For example, the study of a day's chatter reveals—

ABC works DEF
ABC works GHI
ABC works JKL
DEF works MNO
DEF works PQR
MNO works PQR
XYZ works STU
XYZ works ?

REF ID: A384682

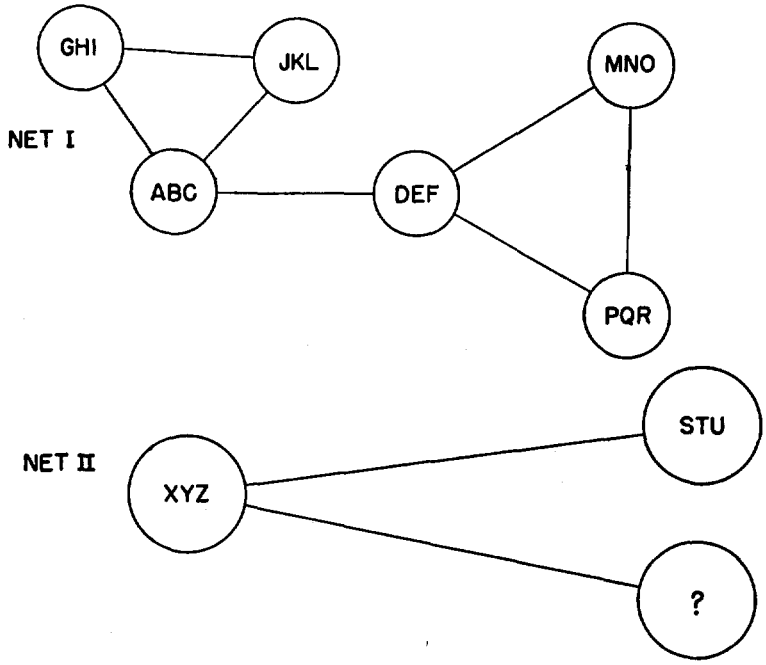


Figure 35.

Thus there are, for the moment, two separate groupings of stations with Net I apparently divided into two groups (fig. 35). It should be remembered that one day's intercept will rarely result in anything as complete as this, and that where daily changing calls are employed, the continuity techniques covered in paragraph 44 must be used. Missed calls present a similar problem. The next task is to study the characteristics of these stations as far as radio operation and procedure is concerned in order to refine the above groupings. It may be found, for example, on the one hand, that the ABC group and Net II exhibit such like characteristics that they appear to belong to the same net and that the connecting link between them has not yet been monitored; and, on the other hand, that the DEF group displays such different characteristics that it must be considered separate and that the DEF call must serve two groups (DEF–MNO–PQR and DEF–ABC).

b. The characteristics to be compared relate to all the features of radio operations:

(1) *Frequencies:*
(*a*) System of use.
(*b*) System of allocation.
(2) *Call signs:*
(*a*) System of use.
(*b*) System of allocation.

REF ID: A584682

(3) *Schedules:*
(4) *Procedure:*
(*a*) Call up.
(*b*) Order of traffic.

(c) Message externals (form and composition of preamble and postamble).

(*d*) Receipting.
(*e*) Corrections and services.
(*f*) Signing off.
(5) *Cryptographic systems.*

c. These items may be used as a check list. Stations, or circuits, do not have to agree in every particular to be grouped, but they should on the major features and, often, on the more characteristic of the minor. What constitutes this latter depends on the net itself. If, for example, strict instructions are issued by the net relative to the order of the preamble components, any deviation, however slight, may be taken as evidence of a separate net. On the other hand, if instructions are rather lax, deviations may not hold any significance. The traffic analyst seldom knows about the nature of the orders on operating procedure, but he can, through careful observance of the net, gain a general impression of how closely it is controlled and how well it is disciplined.

d. The following example illustrates the use of these techniques:

ABC works DEF
ABC works GHI
ABC works ?
XYZ works MNO
XYZ works PQR
STU works ?
? works ?

(1) *The diagrams* (see fig. 36).

(2) *The characteristics:*

(*a*) *Frequencies:*

Net I: Complex-sending Frequency Fixed.
Net II: Star Frequency Fixed.
Net III: Complex-sending Frequency Fixed.
Net IV: Complex-sending Frequency Fixed.

(*b*) *Call signs:*

Net I: Double-station Calls Monthly Changing.
Net II: Double-station Calls Monthly Changing.
Net III: Double-station Calls Daily Changing.
Net IV: Double-station Calls Monthly Changing.

REF ID:A584482

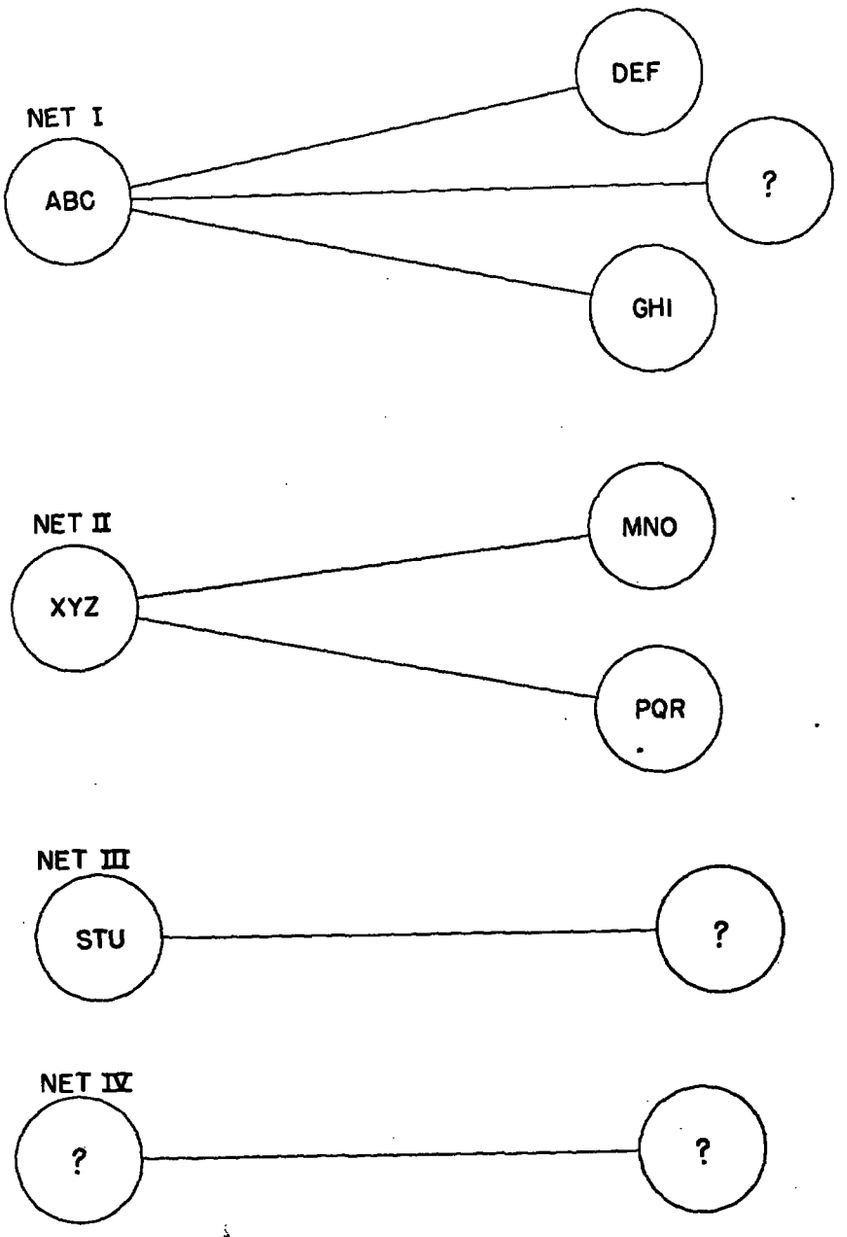


Figure 36.

REF ID:A58489

(*c*) *Schedules:*

Net I: Period.
Net II: Period.
Net III: Unrestricted.
Net IV: Period.

(*d*) *Procedure:*

All Nets: Q signals; International.

1. Call up:

All Nets: Usual.

2. Order of traffic:

All Nets: Precedence traffic first.

3. Message externals:

Net I:
Preamble: Circuit No.; Precedence; Message Center No.; Group Count; File Date and Time; Routings.

Net II:
Preamble: Circuit No.; Message Center No.; Group Count; File Date and Time; Routings.

Net III:
Preamble: In-desk No.; Precedence; Message Center No.; Group Count; File Date and Time; Routings.

Net IV:
Preamble: Circuit No.; Precedence; Message Center No.; Group Count; File Date and Time; Routings.

Separators: Same for all nets.

4. Receipting:

All Nets: Usual.

5. Corrections and services:

All Nets: Usual.

6. Signing off:

Net I: Usual.
Net II: Usual.
Net III: Makes next schedule.
Net IV: Usual.

(*e*) *Cryptographic systems:*

Net I: A, B, C, D.
Net II: A, E, F.
Net III: A, G, H, I, J.
Net IV: A, B, D.

e. It will be observed from the above that Nets I and IV have similar characteristics, and that II and III differ in certain important respects. Net II uses a net frequency. This alone would be insuffi-

REQ# 109:AS84819

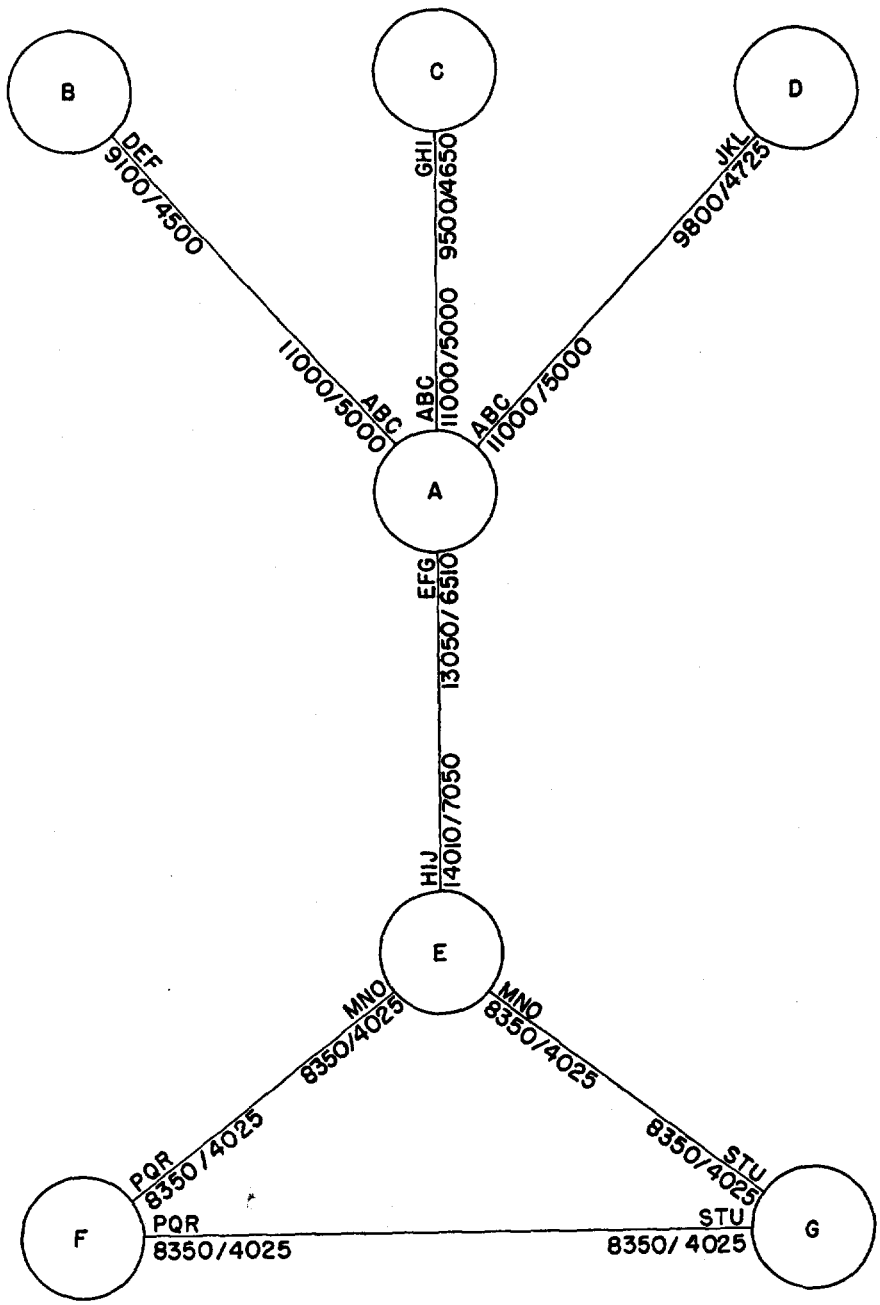


Figure 87.

REF ID: A58489

cient grounds for isolating it, but the position of the precedence in the preamble, and the use of different cryptographic systems furnishes enough additional evidence. Net III employs daily changing calls, usually adequate premise for setting a net apart. In this instance, added weight is given by the use of unrestricted signaling, the in-desk number, and the distinctive cryptographic systems.

55. Building the Net Structure

a. An elementary amount of net building is accomplished in the process of grouping the stations into nets. A number of additional techniques are now brought into play to complete the task. The crux of the problem involves the identification of different frequencies and calls with a station, in other words, that call ABC is at the same station as DEF, or that 11,000 kcs is at the same station as 9,050 kcs. When this has been done, the links and groups will fall into place and the net reconstruction be completed. It is difficult to set down definite methods to be pursued because much depends on the individual characteristics of the network. The following paragraphs discuss some of the principles involved and are suggestive of the general approach. Examples used are based on the diagram in figure 37.

b. Frequencies, Calls, Schedules. As a general rule, like calls or like frequencies may be assumed to be at the same station. Thus, in figure 37, the call ABC on frequencies 11000/5000 kcs was always considered the same regardless of station called. But caution should be exercised in arriving at this decision because it is always possible that no relationship may exist. A check of schedules is helpful. If ABC is heard working two different stations at the same time, it is likely that the two ABC's are separate stations. Other checks are traffic routings, cryptographic systems, etc.

c. Interlocking Serials. Where a radio station in-desk number is used, the serials out of different calls can be interlocked. When the serial is a message or signal center number, the interlocking technique may also be used, but account must be taken of the relay possibility. For instance, in figure 38 A and C are under analysis in an attempt to tie them together. Message center numbers on traffic out of ABC run:

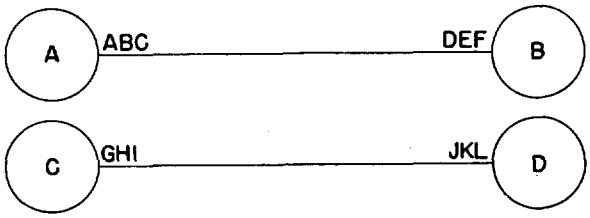


Figure 38.

RHQR 109:AD684682

1578	1607
1579	1608
1585	1609
1586	1610
1587	1629
1588	1630
1589	1631
1603	1641
1605	1642
1606	1643

Message center numbers on traffic out of GHI run:

1581
1582
1583
1584

But, if the latter traffic shows evidence of being relayed and, if there are no other grounds for identification, a conclusion cannot be reached. On the other hand, if it is found that nonrelay traffic on this net carries no routings, but that relay traffic does, and that all the messages listed above under both ABC and GHI have no routings, it may be assumed that ABC and GHI are co-located. Other types of serials, such as link numbers, generally cannot be used for this purpose.

d. Traffic Routings. On the theory that the predominant originator out of a call or frequency and the predominant destination into a call or frequency represent the location of the call or frequency, a tabulation of traffic routings may be used for net-building. For example, tabulations of routings relative to ABC and GHI reveal:

Call	*Routing*	*Volume*
Out of ABC	1234	75
	2345	43
	3456	10
	4567	3
Into ABC	1234	58
	2345	12
	4567	1
Out of GHI	1234	158
	2345	79
Into GHI	1234	101
	2345	39

The similarities in routings suggest their co-location though further proof is necessary for positive identification.

(1) Also useful is the system of omitting routings on local traffic. Calls of the same station will demonstrate similar relay routing lists

REF ID:A584482

with the station's own routing rather low in the tabulation. Book messages can be used as explained in paragraph 50*b* (2) (*b*).

(2) A somewhat different use of routings is in the inferring of links which have not been heard. For example, the routing 1234–6789 is noted on a message from A to B. 1234 has been located at C, but no link from C to A has been observed. Nevertheless, there must be some connection either through another station or directly. It is difficult to determine which is the case; a check of file time against intercept time will sometimes serve to indicate whether, considering the precedence of the message and the usual time lapses on the net, how many prior relays are likely. A tentative diagram could be drawn as shown in figure 39.

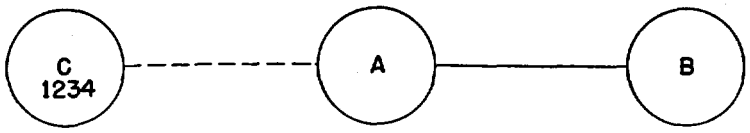


Figure 39.

e. Cryptographic Systems. On locally originated traffic, distinctive cryptographic systems, such as one-time pads, may be used to tie calls or frequencies together. As in the application of all message center features to radio stations, care must be taken to avoid relayed traffic.

f. Chatter. Items of chatter furnish important clues to net-building. In many instances, outright statements are made which relate one link to another. For example, ABC tells DEF, "At 1100 I have schedule with GHI." At 1100, JKL is heard calling GHI, indicating the identity of JKL and ABC. Mention of operators names or other local personalities also assist by the appearance of the same personality on different links.

g. Relayed Traffic. The study of relayed traffic presents one of the most important techniques in net-building. As messages pass from station to station, the net automatically reconstructs itself since it is only necessary to trace the messages' path to determine the structure. The chief caution to be observed is the possibility of having missed a relay, but this can generally be checked by differencing the intercept times. For example, a message is transmitted from ABC to DEF and an hour later from GHI to JKL. The diagram in figure 40 may then be drawn.

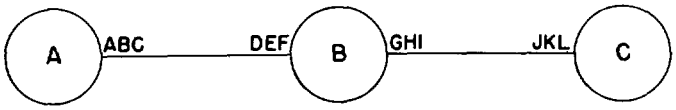


Figure 40.

REF ID:A684682

The possibility of the picture being as shown in figure 41, however,

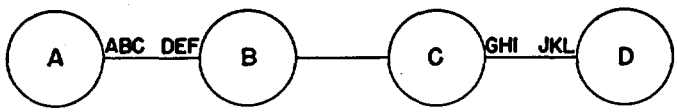


Figure 41.

does exist, but the short time lapse of one hour makes it unlikely that the extra relay took place. Of course, what constitutes a short time lapse is dependent on the habitual lapses and on the precedence of the messages under study.

h. COLLATERAL INFORMATION. Direction-finding is an important technique and, when the radio system is highly secure, may furnish the chief method of net building. Decode material, captured documents, prisoner-of-war reports, when available, should also be used to the fullest extent.

56. Location of Stations

The geographic location of stations is the third step to be performed in the reconstruction of the radio system.

a. IDENTIFICATION WITH A KNOWN ELEMENT. Identification with a known element is one of the chief means of locating the station. For instance, the tying-in of a station to an identified routing number will place the station. Similarly, calls, frequencies, serial ranges, and cryptographic systems which have been matched to locations may serve this purpose. The techniques involved can be derived from those discussed in this section and in section II. A validity should be attached to each station identification dependent on the weight of the identifying evidence.

b. CHATTER. Chatter often furnishes identifications through operator carelessness. Clues to locations, such as mentions of weather, local conditions, and similar items, should be carefully appraised.

c. DIRECTION-FINDING. Direction-finding is here listed separately because of its importance in the locating of stations. Often it is the only means available. This is particularly true in low-echelon nets where movement is liable to be frequent and where message externals are held to a minimum. It may sometimes be necessary to utilize a knowledge of order of battle, geography, and military strategy in connection with direction-finding. Bearings will usually give a general area, larger or smaller according to the distance from the target and the accuracy of the bearings, but seldom will pin-point a location. However, inference as to the most likely location within narrow limits is permissible provided it is backed with sound reasoning.

d. COLLATERAL MATERIAL. Order of battle information, decode

REF ID:A58489

material, captured documents, and similar items are often of great value in placing stations. For example, a division headquarters, whose radio station has been identified, moves to a new location. This new location is revealed by other sources. It may then be assumed that the headquarters radio station is also at this point.

57. Unit Identifications

a. The last step in the reconstruction of the radio system is the imposition of the order of battle. The order of battle underlies the entire net organization and each radio station must be identified with the units which it serves. In the high echelons, the nets are usually composed of large fixed installations which serve a number of units in the vicinity. Generally, however, there will be one major unit which the station represents. In the lower echelons, on the other hand, there will be a close correlation between unit and station. This is partially the result of the customary policy of manning large installations with an independent signal organization, while in the lower echelons the signal sections operate as an integral part of the unit.

b. The techniques of matching units with stations are only outlined below since it is felt that the preceding discussion sets the pattern of reasoning.

(1) *Identification with a known element.* This involves such items as call sign or frequency patterns which may be distinctive for certain commands or echelons, serial number ranges, routing systems, cryptographic systems, and procedural characteristics.

(2) *Chatter.*

(3) *Order of battle.* Beside the usual method of identifying a unit with a location and a location with a station, it is sometimes possible to force identification. For example, the order of battle information given in figure 42 is known, and a net is reconstructed as illustrated in figure 43.

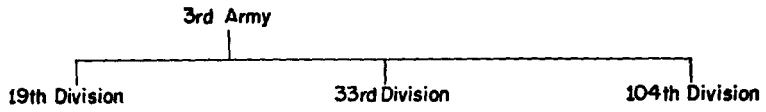


Figure 42.

It becomes apparent that station D is probably the 104th Division. In many cases, the echelon of command can be determined from the structure of the network and this may later lead to the identification with specific units. For example, the network shown in figure 44 is built.

REF ID: A384682

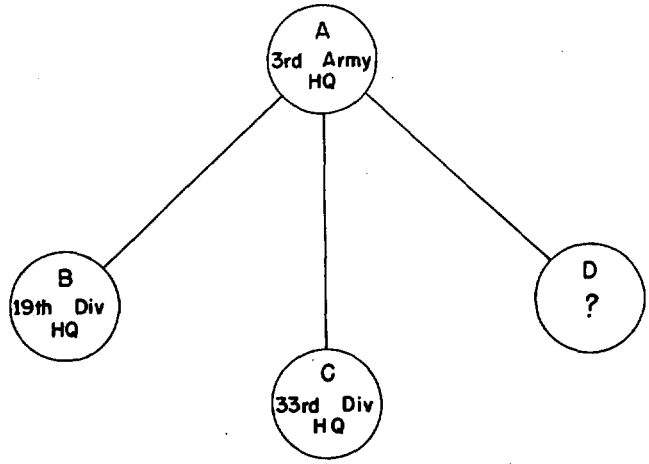


Figure 43.

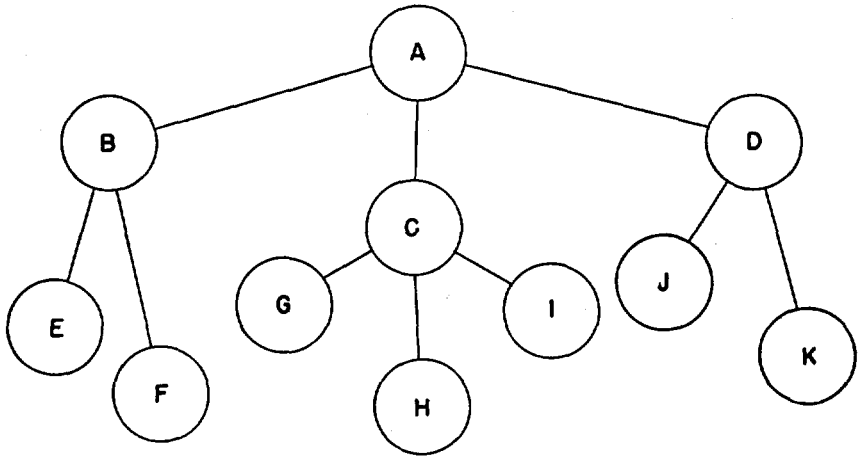


Figure 44.

It will be observed that A is probably the top headquarters, that B, C, and D are lower equivalent units, and that their out-stations are still further down the line. If anything is known of the order of battle in this area, it may be possible to match it with the net diagram.

(4) *Collateral material.*

58. Dummy Nets

Dummy nets and stations may be set up for the same purpose as that served by control traffic. Often when a headquarters is moved, a radio station is left operating at the former location to conceal the redeployment. Similarly, when it is desired to misdirect the

REF ID:A58489

enemy's attention, entire spurious nets may be employed to create the appearance of activity in an inactive area. The detection of such nets and stations may be difficult to accomplish and is largely dependent on the ability to uncover breaches of security resulting from careless chatter or ineptitude.

59. The Integrated Diagram

The immediate objective of the reconstruction of the nets is the production of the integrated network diagram which will serve as a

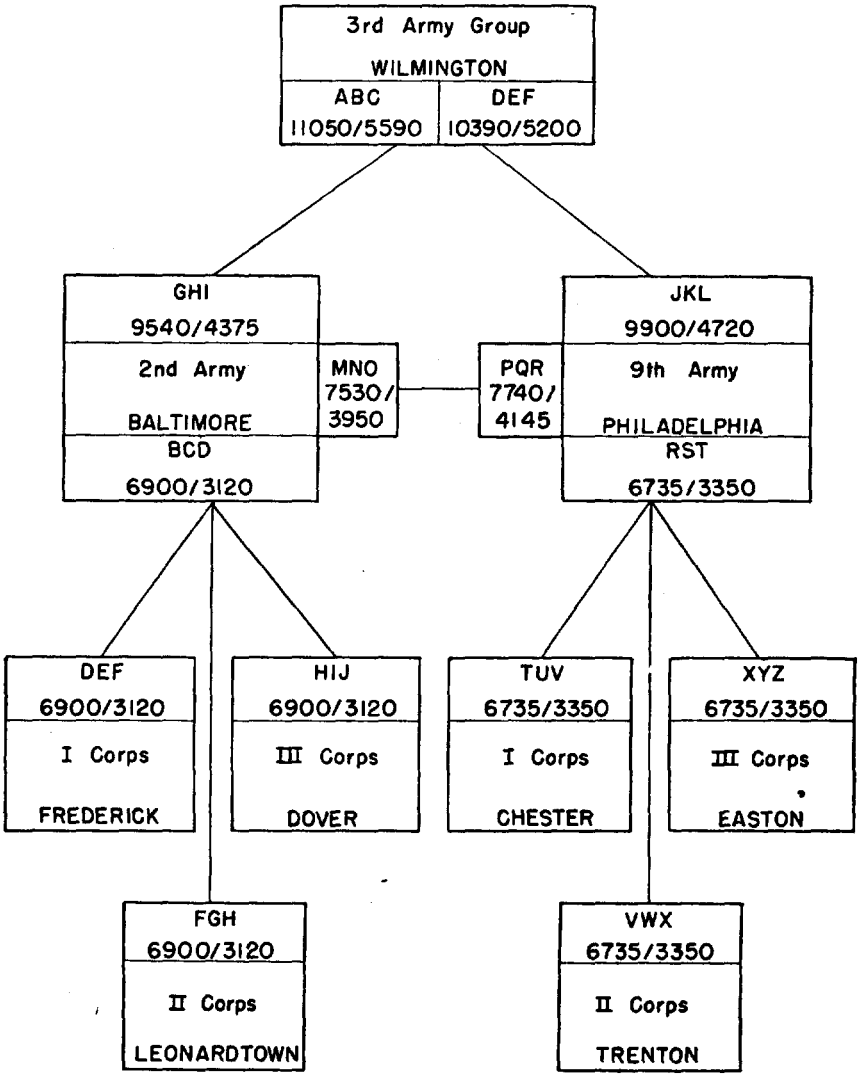


Figure 45.

REF ID: A5384682

backdrop for future study of the nets and for the production of intelligence and cryptanalytic aids. Because of the limitations of space and the complexities of some of the data, however, it is often not possible to include all the information necessary to a complete network picture in diagrammatic form. Therefore, certain basic diagrams may be produced either in schematic or geographic arrangement, and the omitted data supplied in accompanying charts. An example of such a basic diagram is given in figure 45. It will be noted that it contains order of battle units, locations, frequencies, and call signs, and is drawn schematically. Other data, which could be appended in chart form, might include range of serial numbers at each location or on each link, cryptographic systems used, and routings which appear or are identified with units or locations.

Section IV. METHODOLOGY OF ANALYSIS

60. Introduction

The preceding sections of this chapter dealt with the techniques of traffic analysis in regard to the study of radio operations and the reconstruction of the nets. In order to perform this analysis and achieve these ends, the proper machinery for processing raw material must be employed. This section is concerned with this machinery, and includes the processing of the chatter logs and the maintenance of appropriate files. The methods and forms outlined are only suggestive of the possibilities and changes should be made as necessary to meet individual situations.

61. Intercept Operator's Log

a. The raw material of traffic analysis is the chatter log. This is a complete record of the transmission as it is copied by the intercept operator and includes both traffic and chatter. An example of a portion of such a log follows (procedure is Q signals and international):

ABC	(2765 kcs) VVVVVVVVVV	
	DEF DEF DEF de ABC ABC ABC VVV QSV K	2133Z
DEF	(3152 kcs) VVVVVVVVVV	
	VVVVVVVVVVV ABC ABC ABC de DEF DEF	
	DEF VVVVV K	2135Z
ABC	V's QSA ? QSA ? K	2138Z
DEF	QSA4 QSA4 QSA? K	2139Z
ABC	QSA4 QTC 2 OP	
	QTC2 OP K	2140Z
DEF	QRV QRV K	2141Z

REF ID:A58489

ABC	QTC QTC	
	NR695 OP GR14 121541 BT	
	1904 2391 6025 8034 1709	
	6123 8051 6843 2967 1035	
	4114 EEEEEEEEE 4104 5281 7399	2144Z
DEF	3? 3?	
ABC	7399 1211 BT QSL? QSL? K	2145Z
DEF	R	2145Z
ABC	AS5 AS5 K	2146Z
DEF	OK OK OK	
	SAW TOM IN TOWN LAST NITE	2148Z
ABC	WHERE WAS HE GNG?	2149Z
DEF	31 Div They lost 2 ops in raid	2151Z
ABC	TOO BD AS AS	2151Z
ABC	QTC QTC QRV? K	2155Z
DEF	QRV QRV QRV K	2156Z

b. The important items of this chatter log must be extracted and recorded. The usual method to accomplish this is the use of the intercept operator's log on which is entered the significant features of the transmission as they occur. A sample log based on the above chatter is shown in figure 46.

c. The log is the basic analysis recording. Once it has been completed it should not be necessary, except in rare instances, to go back to the chatter logs. Consequently, considerable care should go into its preparation. It should contain all the data required for analysis and for the compilation of files.

62. Files

The contents of files are largely determined by the particular problem. It will generally be found advantageous, however, to maintain files based on the following:

a. Frequency. A master-frequency file containing a record of all frequencies, the time and date when first heard, associated frequencies, location, calls if reasonably fixed, net, etc.

b. Call Signs. A master call-sign file containing a record of all calls, date when first heard, associated calls, location, frequencies, net, etc. The information on the card here or in the frequency file may be kept to a minimum if one is adequately cross-indexed to the other.

c. Serial Numbers. Where practicable, files should be maintained on the various serial number ranges together with related features.

d. Routing System. A file of routing code groups with proofs of identifications.

e. Cryptographic Systems. A file of all cryptographic systems, how they can be identified, by whom used, for what purpose, and net.

REF ID: A584682

Date_____

GMT	Freq.	C/S	No.	Serial	Origin	Dest.	Remarks
2133	3152	ABC					V's DEF de ABC
2135	2765	DEF					V's ABC de DEF
2138		ABC					QSA?
2139		DEF					QSA4
2140		ABC					QSA4
2144		ABC	695				OP GR14 121541 1904 . . . . 7399 1211
2148		DEF					SAW TOM IN TOWN LAST NITE
2149		ABC					WHERE WAS HE GNG?
2151		DEF					31 DIV. THEY LOST 2 OPs IN RAID

Figure 46. Sample intercept operator's log.

In the case of distinctive features, such as one-time pads, files should also be maintained for each pad together with other pertinent data.

f. PROCEDURE. A file on the meanings of noninternational procedure signs and signals.

g. PERSONALITIES. All personalities appearing in traffic or chatter together with the connection in which they were mentioned. Personalities derived from other sources can be added to this file but they should be so marked.

h. ORDER OF BATTLE. All order of battle identifications originating with traffic analysis plus that available from other sources.

i. NET, GROUP, AND LINK. A running record should be kept on each net or, where necessary, group or link which will act as a history and also include the basic data for station identifications as to location and order of battle.

REF ID:A58489

j. Collateral Materials. Appropriate files should be maintained for all collateral materials. In the case of direction-finding, information must be organized to suit the particular problem. Files, as required, should also be maintained on solved messages, captured documents, and similar items.

REF ID: A5384682

CHAPTER 4

APPLICATIONS OF TRAFFIC ANALYSIS

Section I. INTERCEPT OPERATIONS

63. Introduction

Traffic analysis plays an important role in the direction of intercept. It furnishes the basic information necessary to the intercept station for the performance of its mission; its requirements are coordinated with those of intelligence and cryptanalysis for the purpose of prescribing cover and fixing priorities; and it checks certain phases of station performance. Depending on the nature of the organization, traffic analysis may also be responsible for the specific determination of missions for the intercept stations.

64. Intercept Information

a. The elementary function of traffic analysis in intercept control is the providing of basic net data to the stations. This includes chiefly frequencies, calls, schedules, and station locations. Other information may be added as required. A sample listing follows:

Locations	*Frequencies*	*Call signs*	*Schedules*
Hoboken	10500/5030	ABC	0100; 0300;
Zanesville	11350/6125	DEF	0500; 0700;
			1700; 2100
Hoboken	10500/5030	ABC	even hours
Overton	16400/7625	GHI	
Overton	16400/7625	GHI	0900; 1100;
Zanesville	11350/6125	DEF	1300; 1900; 2300
Star Lake	8430/4175	MNO	0700; 0900;
Ticonderoga	8600/4235	PQR	1800; 2200;
Star Lake	8430/4175	MNO	0400; 0600;
Buffalo	7550/3965	STU	1900

b. Technical reports may also be furnished to the intercept station. Certain items are fundamental. For instance, in the case of a changing-call system, the elements of the system are necessary for con-

REF ID:A58489

tinuity in cover; the same is true of frequency systems, procedure signs and signals, etc. In the determination of the type of materials to be forwarded, a balance must be struck between the requirements of security and those of intercept. All information is of use to the station, but some is more essential. Thus, it should be the policy to furnish everything that is available, consonant with security. Even much data which appear irrelevant may be of value if only to indicate to the intercept station the importance placed upon its product.

65. Types of Coverage

If it were possible to cover all desired nets or links twenty-four hours a day, there would be few problems to intercept control. Because of limited facilities and operators, however, such is not the case, and it becomes necessary to draw a number of fine distinctions with regard to types of cover and the order of priorities. Thus, cover may be divided into several types according to the purpose it serves.

a. FULL TIME. This is the highest of all intercept priorities (except in special instances) and consists of complete daily monitoring of each assigned net or link on all known schedules. The number of missions included in the full time classification should be sufficiently small to permit the monitoring station to cover all of them with ease so that, unless something entirely unforeseen intervenes, intercept is assured. Full time cover should never tax the maximum facilities and personnel of the station except under unusual circumstances, since positions should be reversed for other types of cover. These positions may, of course, be switched to full time if absolutely necessary.

b. SAMPLING. Nets or links which cannot be covered on full time may be put on sampling. The net is checked at regular intervals, the intercept station listening to several missions each day and rotating them until all have been monitored when the list repeats. This method yields some traffic on a variety of nets and enables the traffic analyst to keep abreast of current developments.

c. SEARCH. This mission consists of a search through a frequency band or bands for new transmitters and for changes of wave lengths. In the early stages of traffic analysis, this mission is of first importance since it serves to outline what is on the air.

d. PRELIMINARY CHECK. New frequencies discovered on search must be followed up to ascertain their genuineness and desirability. To accomplish this, they are placed on preliminary check, actually an extension of the search mission. If proved valuable, these links are then transferred to either full time or sampling.

e. SPECIAL CHECK. Special check is the complete cover of a net or link for a limited period of time. The check may serve a variety of

REF ID: A584682

purposes such as whether the link is still active, or what its schedules are, or whether it can be heard at the monitoring station.

66. Factors in Assignment

The main considerations in the assignment of missions to specific intercept stations are:

a. The ability of the station to hear at the times desired.

b. The availability of positions and personnel for coverage at the station.

c. The most economic use of the station's time. This involves the problem of the common transmitter which makes it desirable to assign an entire net, where possible, to one station. For example, in the net shown in figure 47 both the A–B and A–C link should be assigned

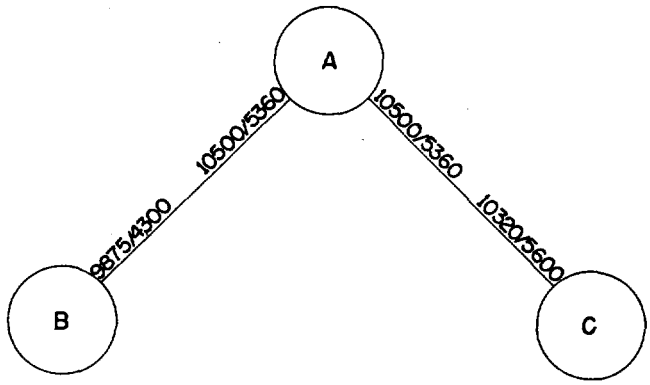


Figure 47.

to the same station, for by covering A throughout the day the activities of the net can be followed. On the other hand, if the intercept unit can hear A and B, but not C, it would become necessary to split the assignment. A second consideration in following this procedure is that the common transmitter arrangements tend to spread out until they include more links than can be handled at a single station. For example, C works another station on 10320/5600, B does likewise on 9875/4300, etc. Thus, a compromise assignment must often be devised.

d. The communication facilities between the station and the central analysis agency. In many instances, it is of prime importance that traffic arrive at a central point for analysis within the shortest possible time. For this reason assignments are sometimes made to the station which, though unable to provide the best cover, can forward the traffic the fastest.

REF ID: A584682

67. Factors in Priorities

The determination of priorities rests on the threefold requirements of intelligence, cryptanalysis, and traffic analysis. The traffic analysis needs are:

a. INTELLIGENCE. Traffic analysis, on its own, contributes to the intelligence picture and consequently is interested in seeing to it that the nets which yield the major portion of traffic analysis intelligence are adequately covered.

b. ANALYSIS OF RADIO OPERATIONS. In the study of certain elements of radio operations, intensive cover may be found valuable for limited periods of time, for example, the defining of schedules on a given net. Special check may be used to this end.

c. NET RECONSTRUCTION. Traffic analysis must maintain an up-to-date picture of all radio nets for the benefit of intercept control personnel regardless of the needs of intelligence and cryptanalysis (because those needs may change from time to time), and information must be available to permit the immediate assumption of coverage. In the reconstruction of nets of little current significance, or where the significance is unknown, special check is useful. Where nets have already been reconstructed and it is merely desired to watch them for changes, sampling cover is satisfactory.

68. Interpretation of Requirements

Besides making its own demands on intercept, traffic analysis frequently interprets the requirements of intelligence and cryptanalysis in terms of links and nets. For example, intelligence expresses interest in a given area; traffic analysis knows what links or nets to monitor in order to blanket the area. Or cryptanalysis wants more traffic in a given system, a certain routine message, or a type of isolog; traffic analysis knows what nets or links carry large portions of this traffic.

69. Station Performance

a. In order to insure proper performance by the intercept station and to check on the fitness of the assignment, coverage results are continually evaluated.

b. If a serial number, relative to the sending station, is available, it may be analyzed for missed traffic. Forms can be devised for the simple maintenance of this data which, in turn, can be obtained from the intercept operator's log. Other features, such as message center serials, may also be employed to check for missed traffic though care must be exercised in making use of them. Incidentally, there is a tendency to place emphasis on the volume of traffic copied at a station as a gauge of its efficiency. This attitude is to be discouraged since

REF ID: A684682

it is often necessary to monitor nets or links which yield little traffic, but do carry cryptographic systems of great cryptanalytic or intelligence value, or possess useful traffic analysis features.

Section II. APPLICATIONS TO CRYPTANALYSIS

70. Introduction

a. The relationship between traffic analysis and cryptanalysis is not easily defined. Often an arbitrary line must be drawn between them when it is desired to keep the functions separate, but it will be found necessary, whatever the distinctions made, for the cryptanalyst to be grounded in traffic analysis and the traffic analyst in cryptanalysis. This arises from the basic concept of traffic analysis and cryptanalysis as closely related processes with traffic analysis furnishing the frame of reference within which cryptanalysis is performed. The material supplied by traffic analysis falls into four main categories:

(1) General background information.
(2) Crib messages.
(3) Isologs.
(4) Chatter.

b. It should be borne in mind by the traffic analyst that the requirements of the cryptanalyst vary according to the stage of solution. At times, for example, an isolog may be of great value, at other times it may be of no use at all, and at still others it may be of potential use pending the development of the problem. Therefore the traffic analyst should gear his production in this field to the needs of cryptanalysis.

71. General Background Information

Traffic analysis furnishes a large amount of routine information relative to communication features which assist the cryptanalyst. Some of the main items are—

a. Routings. The knowledge of the origin and destination of traffic is fundamental.

b. Identification of Systems. Traffic analysis contributes to the identification of cryptographic systems where discriminants do not form an obvious guide and assists in the sorting of traffic into homogeneous groups.

c. Use of Systems. Through discovering the use of systems, and any peculiarities relative to it, traffic analysis aids the cryptanalytic processes. Specific applications, of course, depend on the nature of the system and the externals available.

RECD 10 : 2684682

72. The Crib Message

a. DEFINITION. When it is possible to assume portions of the underlying plain text through the recognition of external characteristics, a message may be termed a crib message. Crib messages may be divided into two main groups.

(1) Messages which display a direct external-internal relationship, as the correlation of an internal signature with the external originator.

(2) Messages which are proforma reports. These arise out of the command function which necessitates the rendering of reports both up and down channel. They are usually formalized to insure completeness and thus present several portions of predictable plain text. Reports are of two types: those periodically filed which are called routines, and those which are forwarded as the situation requires.

b. IDENTIFICATION OF CRIB MESSAGES. (1) *Use of originator or destination.* If traffic contains internal addresses or signatures, they may be assumed by a knowledge of order of battle in relation to the message routings. Thus, messages originating at Dallas, known to be the location of the 14th Division, may contain the "14th Division", its commanding officer, or one of its subordinate units in the signature position. The possibility of several units at a location should not be overlooked.

(2) *Use of serial number range.* The serial number range may be tied to an internal originator, and the signature on all traffic in the series may be predicted.

(3) *Use of other features.* In the study of internal originators and addresses, other features, such as cryptographic system, relationships between preamble originators and destinations, etc., should be correlated with the above. For example, a specific originator may be defined by a combination of routing origin, serial range, and cryptographic system.

(4) *Use of external patterns.* In the case of report messages, these can often be distinguished by the characteristics of the traffic which chiefly include—

(*a*) *Destinations.* Because the report is regularly rendered to specific people, the destinations will furnish one peculiarity of the message. If order of battle is known, the relationship between the originator and the destinations may be explained and it may even be found possible to identify the nature of the report. When the routine pattern has been established, the order of battle must be watched for changes which will result in alterations of the pattern.

Note. Crib messages bear a very direct relationship to the military situation and the order of battle since they are, particularly in the report type, instrument of the command process. Thus, a detailed knowledge of enemy dispositions and movements is essential to the study of crib traffic.

REF ID: A5384682

(*b*) *Cryptographic system.* Reports usually pass in the same system. But, where a change does take place and it can be recognized, the crib may assist in a solution of the new system.

(*c*) *Serial number range.* Because the same unit generally originates the same report, characteristic serial number ranges may be of value.

(*d*) *File date and time.* Reports which are routine in nature often exhibit a periodicity in the file date and time. For example, a ten-day report will be filed every tenth day, or a daily report as of 1700 will usually carry a file time after 1700 of that day.

(*e*) *Message length.* Because of the stereotyped nature of a report, the group count may show some consistency. In many cases, however, the length will be determined by the amount of information to be filled in, so while the message length acts as a guide, lack of regularity in this respect does not rule out the possibility of a genuine crib message existing.

(5) *Use of solved messages.* The reading of messages often produces crib traffic not previously suspected. This traffic should be studied and its characteristics noted to aid in future solution. Furthermore, it may be assumed that, if one unit originates a report, the same report is required of all other similar units. A check with order of battle will reveal the location of these other units and the specific traffic can be studied. For instance, a report may be observed from an oil depot to headquarters. This suggests that other oil depots also originate a similar report. These depots are then located and their traffic examined for the proper external characteristics as indicated on the decode.

73. The Isolog

a. DEFINITION. An isolog exists where the underlying plain text is encrypted in two different systems. There are many types of isologs depending on the nature of the cryptographic system, and it is hardly possible in this text to explore all the likely variations. Isologs arise from the cryptonets which, in turn, bear a close relationship to the order of battle. They are caused in three main ways:

(1) *The relay isolog.* When a message is relayed from one cryptonet to another, an isolog is likely. In figure 48, a message passed from A to C is reenciphered at B who holds both systems I and II. This type of isolog is usually formed by traffic passing up and down channels where reencipherment is necessary into simpler and simpler systems, the more forward the unit.

(2) *The book-message isolog.* Messages which are to be sent to a number of recipients in different cryptonets must be enciphered in different systems. In figure 48, for instance, if B wants to send the same message to A and C, the appropriate system is used for each.

REF ID:A58489

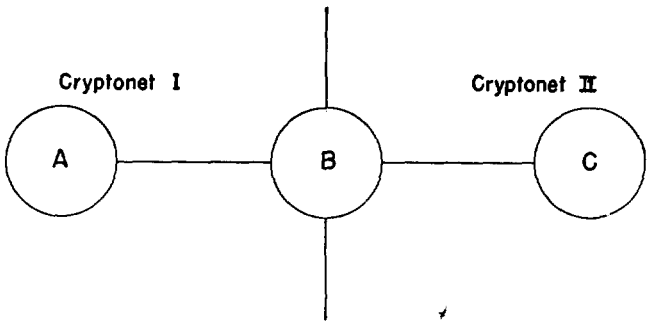


Figure 48.

(3) *Cryptographic error.* At times the code clerk will encipher a message in the wrong system. This will be refused by the receiver and the originator will reencipher in the correct system, yielding an isolog.

b. Identification of Isologs. (1) *Mechanical approach.* Isologs may be found by sorting traffic by originator and then looking for similar group counts and file dates and times. Where the two systems involved are not radically different in makeup, group counts should be close. Likewise, file dates and times, under most circumstances, will be similar.

(2) *Use of cryptonets.* A knowledge of cryptonets often simplifies the search for isologs. Certain locations, because they are in several nets, will be predisposed to the transmitting of this material. For instance, in the group of cryptonets shown in figure 49, the logical

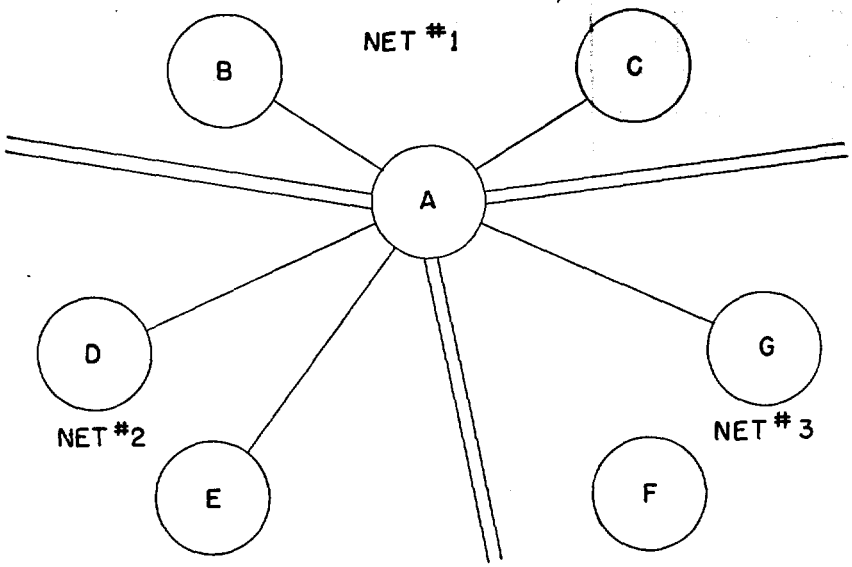


Figure 49.

REF ID:A684682

traffic to study for isologs would be messages received and transmitted by station A. Order of battle changes should be carefully followed for the cryptonets are formed by units, not radio stations, and the movement of a unit often means that a new location must be taken into account.

(3) *Use of refused traffic.* When messages are originally sent in the wrong system they will be refused or serviced, sometimes in the clear. This is a signal to watch for a retransmission of the traffic in its correct version. For this reason alone, it is important for the traffic analyst to be thoroughly familiar with procedure and the methods of servicing both encrypted and plain traffic.

74. Chatter

The study of chatter occasionally produces information of cryptanalytic value. Some of this material may be simply a discussion in the clear of cryptographic features by the radio operators. In other instances, the derivation of information may require some analysis.

Section III. APPLICATIONS TO INTELLIGENCE

75. Introduction

a. It is one of the chief objectives of traffic analysis to produce direct intelligence. Seldom will this be "pure" traffic analysis intelligence, but rather it will represent the fusing of traffic analysis data with material from other sources. In some cases, traffic analysis will furnish the initial indication; in others it will act as confirming evidence. The ability of traffic analysis to contribute to order of battle is based on the necessity for communication between military units and the fact that these communications are expressive of the enemy's dispositions and intentions.

b. The problem breaks down into three parts—

(1) Determination of order of battle relationships.
(2) Determination of movement.
(3) Identification of units.

76. Determination of Order of Battle Relationships

a. NET STRUCTURE. The net structure is one of the chief keys to the study of order of battle relationships. Methods of utilizing this element are covered in paragraph 57.

b. CONTACT RELATIONSHIPS. (1) *Traffic associations.* A study of the traffic contacts of any one point gives some indication of the nature and the echelon of the unit since every message passed implies a relationship between the sender and the recipient. In order to use

REF ID:A58489

this technique, some of the factors must be identified and the general principles of the enemy order of battle known. For example, if the following set of contacts are recorded over a period of time, and B, C, and D are all air transport units, it is likely that A is also—

Location A

To B	43 messages
To C	29 messages
To D	12 messages
From B	38 messages
From C	15 messages
From D	3 messages

Of course, other factors must be considered and these may alter the conclusion. In some orders of battle, for instance, certain of the air transport units may come under the command of an Army unit and A may represent this Hq. Thus, hasty interpretations relative to traffic associations cannot be made, and the use of all available collateral material is necessary. It may be noted, for example, that certain types of traffic associations are characteristic of units at divisional level. These associations may involve heavy traffic with Army Hq., somewhat lighter traffic with Army group, and a little traffic with characteristic points in the homeland. Similar patterns of other locations may indicate the presence of a division. There are so many variations to this type of analysis, and it is so dependent on the order of battle concerned, that it is not possible to develop the problem completely here, but the analyst's ingenuity should suggest the many applications.

(2) *Book messages.* Book messages are of particular interest because it is likely that some relationship exists between the various recipients which causes them to receive the same message. Some inferences can be made if something is known of any of the elements, such as the originator, a few of the recipients, or the use of the cryptographic system. A message, for example, passes from A to B, C, and D. A is an Army Hq., and B and C have been identified as divisional locations. Then it is probable that D is the third division of the Army. On the other hand, if the cryptographic system involved is one used by water transport units, it may be that D is included as a water transport unit which is handling the movement of some men for the two divisions.

c. Cryptographic Systems. If a cryptographic system is associated with a certain type of unit or with a definite unit and its subordinates, it will serve as an identification. For example, a system may be employed only by headquarters of Army or higher. Thus, every location sending in this system is probably Army or higher. Receiving in a system cannot be regarded as good evidence unless

REF ID:A58489

it happens in some volume, because of the possibility of a sender's error. To send in a system it must definitely be held, but receiving in it only implies that it is held. Systems restricted to Air Force, or supply, etc., may similarly be used to infer the nature of the unit at the location under study.

d. PATTERN OF SIGNAL FEATURES. These patterns may be of any type and concern almost any signal item. Three-letter calls, for instance, may only be assigned to Air Force units, or the manner of assignment may reflect the echelon of command. The same holds true for routing codes. Serial numbers which are 5-digit may be used by higher units, while 4-digit are reserved for division or below. Here again the possibilities must be developed to fit the individual case.

e. VOLUME OF TRAFFIC. The volume of traffic originated and received by any one point is indicative of its importance. Consideration, however, must be given to coverage facilities and assignments so that the traffic counts are not unduly weighted.

f. CHATTER. Security breaches involving units or clues to units occur occasionally, and chatter should be carefully scanned for them.

77. Determination of Movement

a. CHANGES IN NET STRUCTURE. It is apparent that most changes in net structure result from a more fundamental change in order of battle. Items to be noted include:

(1) Appearance of new stations on the net which often indicates the addition of a new unit.

(2) Disappearance of old stations which may mean the deactivation or move of an old unit.

(3) Moves of radio stations which usually denote the redeployment of the using unit. In moves of this sort, there is often a period of several days, between the closing of the old station and the opening of the new, when the unit will be off the air.

b. CHANGES IN CONTACT RELATIONSHIPS. (1) *Traffic Associations.* Any change in the traffic associations of a location should be carefully examined as it may indicate a resubordination or the move of a unit. For example, Army HQ at A regularly sends traffic to a division HQ at B. This contact later changes, A to C, indicating the move of Army HQ to C or else the division to a different Army if A continues to show the characteristics of an Army Hq.

(2) *Book messages.* Changes in the pattern of recipients of book messages indicate underlying order of battle changes. This is particularly applicable in the case of routine traffic where a distinguishable message passes regularly to several locations. If, for instance, a routine situation report sent daily from A to B, C, and D, changes to B, C, and E, it may be assumed that the unit at D has shifted to E.

c. CHANGES IN TRAFFIC VOLUMES. Changes in the traffic volumes

REF ID:A58489

handled at a point indicate some sort of activity though other techniques must be employed to determine the nature of the activity. In order to watch for changes, a standard of traffic volume into and out of each location is established as normal. Any rises or drops suggest changes in the situation. For example, a location handling an average of three or four messages per day suddenly jumps to 50. It is apparent that units are moving in the vicinity, that preparations are under way for a move, or that it has assumed a more important role. And the possibility that it may be caused by the use of control traffic for the purpose of deceiving the analyst should not be overlooked. As a corollary to this, changes in the volumes of precedence traffic, or in the usual file times, may also be of significance.

d. Moves of Serial Ranges. A message or signal center serial range, which is sufficiently distinctive, may be used as an indication of unit moves. For instance, an Army located at A is employing message center serials running 563–581 on the 10th. On the 12th, messages with serials 585–593 are observed originating at B, suggesting the Army's move to B.

e. Moves of Cryptographic Systems. Similar to the move of serial ranges, the move of a characteristic cryptographic system often signifies an order of battle change. A one-time pad, for instance, held only by a certain division and appearing on messages out of location A, suddenly is noted out of location B.

78. Identification of Units

The initial identification of units usually does not result from traffic analysis. Rather traffic analysis furnishes the means for following a unit about, once it has been identified. But, through the study of net, contact, and cryptographic associations (and the use of other signals features when applicable) it is often possible to define the nature and the echelon of a unit at a given location, and in some cases to name it. Chatter, also, may furnish the specific designations of units through breaches of security.

79. Conclusion

The traffic analysis techniques discussed in this manual require considerable study. It is difficult to cover a subject of this type, where so many individual bits and pieces must be fitted together, in text form since, in order to convey effectively the concept of traffic analysis, no one part should be presented before the other but rather the whole presented at once. For this reason, the text should be read and re-read. It is further to be noted that this manual is chiefly a theoretical text, that the field is still expanding, and that it is the task of the individual analyst to devise the applications best suited to his specific problems.

REF ID:A58489

APPENDIX

REFERENCES

FM 7–24	Communication in the Infantry Division.
FM 11–22	Signal Operations in the Corps and Army.
FM 17–70	Signal Communications for Armored Units.
FM 24–6	Radio Operators Manual, Army Ground Forces.
FM 24–10	Combined Radiotelegraph (W/T) Procedure.
FM 24–16	Signal Orders, Records and Reports.
FM 24–17	Signal Center and Message Center Procedure.
FM 24–18	Radio Communication.
TM 1–465	Air-Ground Communication.
TM 11–454	The Radio Operator.
TM 11–455	Radio Fundamentals.
TM 11–462	Signal Corps Reference Data.
TM 11–484	Elementary Military Cryptography.
TM 11–485	Advanced Military Cryptography.
JANAP 122	Joint Communication Instructions—Part II—Security.
JANAP 127	Joint Communication Instructions—Part VII—Joint Tape Relay Procedures.
JANAP 143	Communication Security.

U. S. GOVERNMENT PRINTING OFFICE : 0—1950

This Page Is Intentionally Left Blank

BY ORDER OF THE
SECRETARY OF THE AIR FORCE

AIR FORCE HANDBOOK 14-133

27 SEPTEMBER 2017

Intelligence

INTELLIGENCE ANALYSIS

ACCESSIBILITY: Publications and forms are available on the e-Publishing website at **www.e-Publishing.af.mil** for downloading or ordering.

RELEASABILITY: There are no releasability restrictions on this publication.

OPR: AF/A2OA

Certified by: AF/A2O
(Brig Gen Aaron M. Prupas)
Pages: 104

This Air Force Handbook (AFH) is the reference guide for conducting intelligence analysis as prescribed by Air Force Policy Directive (AFPD) 14-1, *Intelligence, Surveillance, and Reconnaissance (ISR) Planning, Resources and Operations* and supports the operational requirements and processes outlined under Air Force Instruction (AFI) 14-133, *Intelligence Analysis* and AFI 14-134, *Intelligence Analysis Production and Requirements Management*. This publication provides the definitions, guidelines, procedures and tools for intelligence analysis operations. It has application and use for Regular Component, Air Force Reserve (AFR), Air National Guard (ANG), and Department of the Air Force (AF) Civilians, except where noted otherwise. Ensure that all records created as a result of processes prescribed in this publication are maintained in accordance with (IAW) Air Force Manual (AFMAN) 33-363, *Management of Records*, and disposed of IAW the Air Force Records Disposition Schedule (RDS) in the Air Force Records Information Management System (AFRIMS). Refer recommended changes and questions about this publication to the Office of Primary Responsibility (OPR) using the AF Form 847, *Recommendation for Change of Publication*; route AF Forms 847 from the field through the appropriate functional chain of command. This publication may be supplemented at any level, but all direct supplements are routed to the OPR of this publication for coordination prior to certification and approval. Major Commands (MAJCOMs) need to provide a copy to the OPR upon publication. The use of the name or mark of any specific manufacturer, commercial product, commodity, or service in this publication does not imply endorsement by the AF.

Chapter 1— OVERVIEW **5**

1.1. Purpose 5

1.2. Intelligence Analysis 5

1.3. Operational Viewpoint-1 (OV-1). 7

Figure 1.1. AF Intelligence Analysis OV-1. 7

Chapter 2— AF INTELLIGENCE ANALYSIS ENTERPRISE **9**

2.1. Analyst Airmen. 9

2.2. AF Intelligence Analysis Enterprise (AFIAE) 9

Figure 2.1. AFIAE. 9

2.3. Analysis Spectrum 10

Figure 2.2. AF Spectrum of Intelligence Analysis. 11

2.4. Characteristics 11

Table 2.1. Layers of Analysis. 12

Figure 2.3. Layered, Distributed, and Mutually Supporting Nature of AFIAE. 14

Chapter 3— THE NATIONAL INTELLIGENCE ANALYSIS COMMUNITY AND THE AIR FORCE **15**

3.1. The Intelligence Community. 15

3.2. Intelligence Analysis and the Joint Intelligence Process. 16

Figure 3.1. Joint Intelligence Process. 17

3.3. IC Funding. 18

3.4. Quality Analysis Programs 18

3.5. AF National Tactical Integration (AF NTI) 18

Chapter 4— ANALYSIS FUNDAMENTALS–ACTIVITIES, TENETS, & STANDARDS **20**

4.1. AF ISR Capabilities 20

Figure 4.1. Enduring GIISR Capabilities. 20

4.2. AF Intelligence Analysis Activities 20

Figure 4.2. AF Intelligence Analysis Activities. 21

Figure 4.3. AF Intelligence Analysis Continuum. 22

4.3. AF Intelligence Analysis Tenets. 22

4.4. AF Standards of Intelligence Analysis 23
4.5. Beyond the Checklist 24
4.6. AF Analytic Ombuds 25
Chapter 5— ANALYSIS SKILLS AND TRADECRAFT 26
5.1. Overview 26
Figure 5.1. Transforming Data to Decisions. 26
Figure 5.2. Relationship and Role of Intelligence Analysis Skills and Tradecraft. 27
5.2. Skills and Tradecraft Fundamentals 28
Figure 5.3. Fundamental Skills and Tradecraft of the Analysis Process. 29
Figure 5.4. SATs. 31
5.3. Key Analysis Concepts. 35
Figure 5.5. Data Analytics Framework. 36
Figure 5.6. Traditional Model for Target Discovery. 38
Figure 5.7. ABI/OBP Integrated Model for Target Discovery. 39
5.4. Additional Tradecraft Resources. 39
Chapter 6— REQUIREMENTS AND PRODUCTION 40
6.1. Intelligence Requirements and Analytic Focus. 40
6.2. Intelligence Production 42
Figure 6.1. Requirement–Production Cycle. 42
6.3. Request for Information (RFI) and Analysis/Production Process 43
Figure 6.2. RFI and Analysis/Production Process. 43
Figure 6.3. RFI and Analysis/Production Process across the AFIAE. 44
6.4. Acquisition Intelligence 44

Attachment 1— GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION 46

Attachment 2— PRODUCT AND SERVICE LINES 58

Attachment 3— COMMON ANALYSIS LESSONS 61

Attachment 4— SAMPLE STANDARDS EVALUATION METHODOLOGY 65

Attachment 5— AF ISR SAT TRADECRAFT GUIDE 69

Attachment 6— IC, DOD, AND MILITARY SERVICE REFERENCES 88

Attachment 7— ONLINE RESOURCES FOR ANALYSIS SKILLS AND TRADECRAFT. 92

Attachment 8— ANNOTATED BIBLIOGRAPHY 94

Chapter 1

OVERVIEW

1.1. Purpose.

1.1.1. The responsibilities of the intelligence analyst have never been more important. The increasingly complex global environment demands analyst Airmen be steeped in tradecraft fundamentals, conversant on the Intelligence Community (IC) and other service capabilities, and prepared to tailor their analysis skills to the operational challenge at hand. The purpose of this non-directive publication is to help guide every analyst Airman in answering this call. It provides reference and instructional material for the analyst Airman working in the air, space, and/or cyber domains—whether junior or seasoned; officer, enlisted, or civilian; regular AF, reserve or guard; and serving AF, joint, national, or combined missions. The content of this publication is intentionally broad in nature, ranging from foundational doctrine and tactics, techniques, and procedures (TTPs) to analysis applications and lessons learned.

1.1.2. The long-term intent for this publication is to have it reside as a series of interactive and up-to-date web pages online, with links to IC and AF directives, templates, checklists, and other references. The online version will serve as a useful tool for the analyst Airman to quickly link to their specific analysis topic of interest. Upon publication of this handbook, the AF intends to initiate steps to transition this document to an online, interactive version.

1.1.3. The publication is organized with foundational information in six main chapters followed by useful lists, lessons learned, criteria, forms, guides, and an annotated bibliography in the attachments to aid analyst Airmen in their day-to-day missions. This document also includes links to appropriate websites with additional support material.

1.2. Intelligence Analysis. Intelligence analysis is a cognitive capability—both art and science—applying tools, judgments, processes, and tradecraft to data and information to create and deliver new intelligence, insights, and knowledge, with the goal of providing decision advantage to commanders, decision makers, and intelligence customers. Analysis is foundational to ISR, a key capability of ISR, a core competency in ISR, and integral to Global Integrated ISR (GIISR).

1.2.1. Intelligence as a Foundation. Analysis is a significant capability that extends across all AF ISR Enterprise activities in support of the full range of military operations and assigned national security missions. According to AF/A2's vision for the future of AF Intelligence, *AF ISR 2023: Delivering Decision Advantage*, a "fundamental job of AF ISR Airmen is to analyze, inform, and provide commanders at every level with the knowledge they need to prevent surprise, make decisions, command forces, and employ weapons." AF intelligence analysis provides unique capabilities to focus on and address AF mission requirements. These same unique capabilities, coupled with an Airman's distinctive air/space/cyber perspective, serve to complement and fully integrate with analysis that supports broader defense and national mission requirements.

1.2.2. Intelligence Analysis as a Capability. Analysis is one of four enduring AF ISR capabilities, the other three being Collection Operations, Targeting, and Operations

Integration. **Note**: Refer to the *AF Future Operating Concept: A View of the AF in 2035*. The AF delivers intelligence analysis capability to meet Combatant Command (CCMD) and service needs. As with any other capability area, intelligence analysis is supported by the full range of Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy (DOTMLPF-P).

1.2.2.1. Doctrine. Doctrinal considerations include analysis fundamental principles; analysis policy and procedures; common lexicon and terminology; recognized TTPs; and shared best practices and lessons learned.

1.2.2.2. Organization. AF ISR organizations range from the tactical to the strategic level, operating in a layered, distributed, and mutually supporting construct. AF initiatives to develop the intelligence analysis capability additionally impact the presentation of analyst Airmen to joint organizations such as combatant commands, joint task forces, and national analysis entities.

1.2.2.3. Training. Considerations include initial, mission, and continuation training; AF Specialty Code (AFSC) entry-, intermediate-, and advanced-level courses; and associated certification.

1.2.2.4. Materiel. Materiel concerns involve tools, technologies, systems, and architectures necessary to equip, operate, maintain, and support analysis activities.

1.2.2.5. Leadership and Education. The attention and priority of leadership is essential to growing the analysis capability. Additionally, undergraduate- and graduate-level education opportunities inside and outside of the AF play a major role.

1.2.2.6. Personnel. Planning and resourcing for qualified personnel are required to effectively conduct analysis missions.

1.2.2.7. Facilities. Cleared and adequately equipped buildings and other structures are required to conduct analysis.

1.2.2.8. Policy. Codified direction and guidance with clearly defined roles, responsibilities, processes, and terminology are fundamental to unity of effort across the AF ISR enterprise.

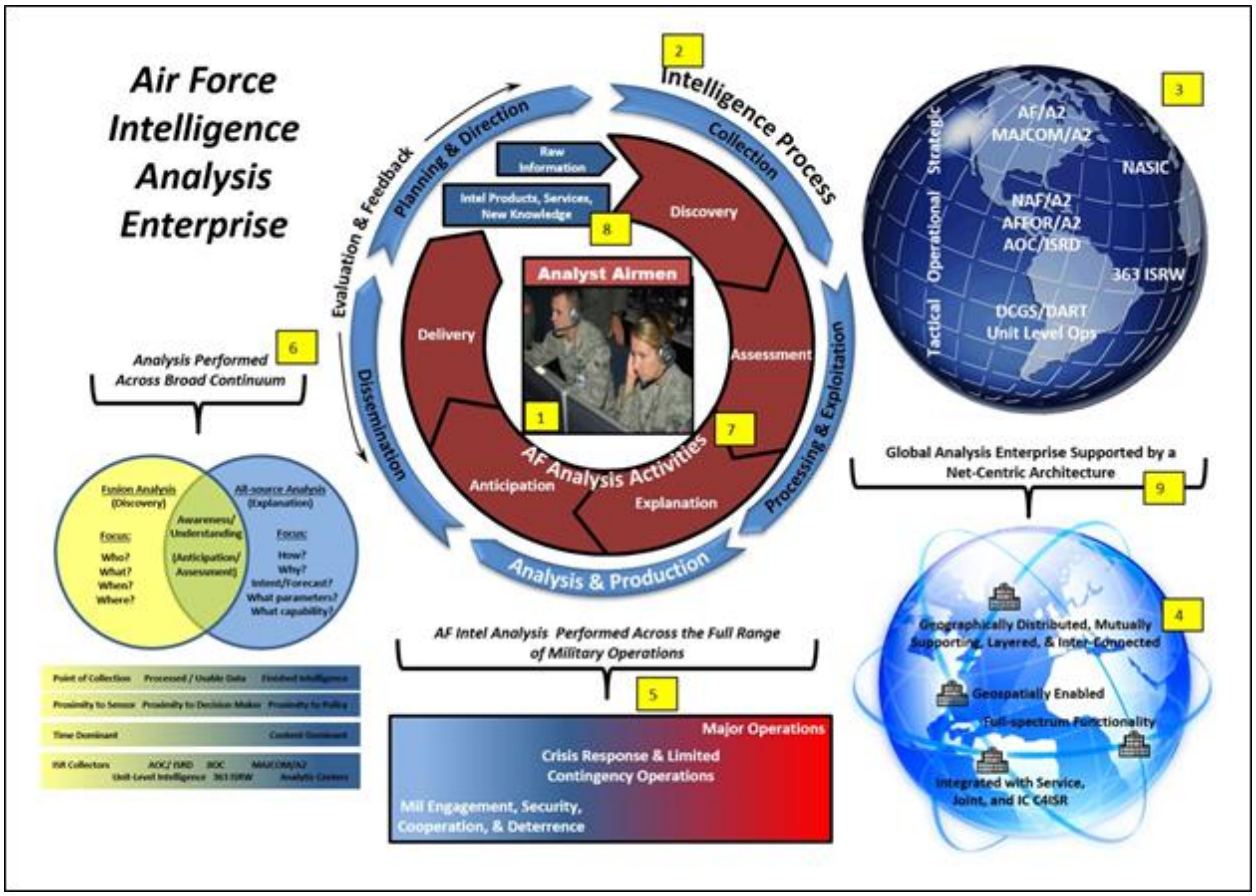
1.2.3. Intelligence Analysis as a Core Competency. ISR core competencies are the primary knowledge, skills, abilities, and behaviors required to perform AF ISR missions and ultimately enable decision advantage. The AF strives to collectively maintain sufficient expertise in its competencies. Because analysis is critical to and a driving factor in the other three enduring capabilities, all AF ISR professionals train in, maintain, and exercise, at a minimum, basic analytical capabilities and critical thinking skills wherever they are assigned. Additional information on this subject can be found in Career Field Education and Training Plan (CFETP) 14NX, Parts I and II, *AFSC 14NX Intelligence Officer Career Field Education and Training Plan* and CFETP 1N0X1, Parts I and II, *AFSC 1N0X1 All Source Intelligence Analyst Career Field Education and Training Plan*.

1.2.4. Intelligence Analysis and Global Integrated ISR (GIISR). As of 2017, GIISR is one of the AF's five enduring core missions as identified in strategic guidance, including the *AF Future Operating Concept* and the *USAF Strategic Master Plan*. A key strategic AF vector is to maintain a robust and flexible GIISR capability, supported by big data analytics. AF

strategic guidance highlights the need for the service to deepen its assessment of potential adversaries, professionalize ISR analysis, and restore analytic competencies. In turn, AF ISR vision and strategic planning establish analysis as one of five priorities for ISR and tie the AF's mandate to deliver decision advantage to its ability to provide world-class, multi- and all-source intelligence across all domains. Accurate, timely, relevant intelligence analysis is not only integral to operations, but in many ways drives military operational decisions.

1.3. Operational Viewpoint-1 (OV-1). Figure 1.1, *AF Intelligence Analysis OV-1*, offers a high-level depiction of AF intelligence analysis. The OV-1 describes analysis operations, capabilities, and activities within the greater AF ISR Enterprise and explains how analysis supports GIISR operations. Together, analyst Airmen and the AF Intelligence Analysis Enterprise (AFIAE) ensure mission success and decision advantage now and into the future. Subsequent chapters of this publication explain in more detail the various elements of the OV-1.

Figure 1.1. AF Intelligence Analysis OV-1.



1.3.1. As indicated by Item 1 in Figure 1.1, at the heart of AF intelligence analysis is the cadre of officer, enlisted, and civilian ISR professionals who are trained in intelligence analysis and production. These analyst Airmen apply critical thinking and advanced analytical skills to turn information and raw data into timely, actionable, and relevant intelligence products and services, leading to improved knowledge.

1.3.2. Analyst Airmen perform their missions within the framework of the overall joint intelligence process of Planning and Direction, Collection, Processing and Exploitation,

Analysis and Production, Dissemination and Integration, and Evaluation and Feedback (PCPAD), as Item 2 of Figure 1.1 illustrates.

1.3.3. Item 3 in Figure 1.1 indicates that AF intelligence analysis is nested within the larger AF ISR Enterprise, a Total Force construct extending from squadron to headquarters level and ranging from tactical to strategic focus.

1.3.4. As depicted in Item 4 of Figure 1.1, analyst Airmen and the AF ISR Enterprise are mutually supporting; unified in policy, authorities, tenets, and strategy; and skilled in employing tools that enable AF, joint, and IC operations.

1.3.5. Analyst Airmen are trained in the art and science of analytical tradecraft and apply common tenets and standards across the full range of military operations, from major theater warfare to humanitarian assistance and disaster relief, as depicted in Item 5 of Figure 1.1.

1.3.6. To support these operations, analyst Airmen engage in various types of analysis, ranging from fusion analysis to all-source analysis (ASA), as shown in Item 6 of Figure 1.1. Fusion analysis entails quickly melding new information with already established baseline knowledge to meet specific operational needs. Comprehensive ASA is often less time sensitive and more focused on studying and understanding long-term trends and maintaining a depth of knowledge on a given subject. Each organization within the AF ISR Enterprise conducts analysis across this continuum - at varying levels based on key intelligence questions and customer requirements - to fill a gap in knowledge, or a need to improve understanding of the threat environment and/or adversary capabilities.

1.3.7. Common analysis activities performed across the AF ISR enterprise include Discovery, Assessment, Explanation, Anticipation, and Delivery, which operate in parallel with the PCPAD process, as depicted in Item 7 of Figure 1.1. Analyst Airmen identify relevant information in support of ongoing operations and requirements, classify and categorize information, and create estimates of capabilities and impacts.

1.3.8. As Item 8 of Figure 1.1 indicates, the derived knowledge is used to create descriptions in greater context to provide indications and warning regarding a specific problem set. Intelligence products and services are developed, tailored, and presented according to key intelligence questions or customer requirements.

1.3.9. As shown in Item 9 of Figure 1.1, the AF intelligence analysis concept and the AF ISR Enterprise are interconnected by both a net-centric architecture and analytic toolsets that ensure critical interface among AF operational elements, Joint, and IC analysts, thereby ensuring access to all relevant data in a geographically-enabled and integrated manner.

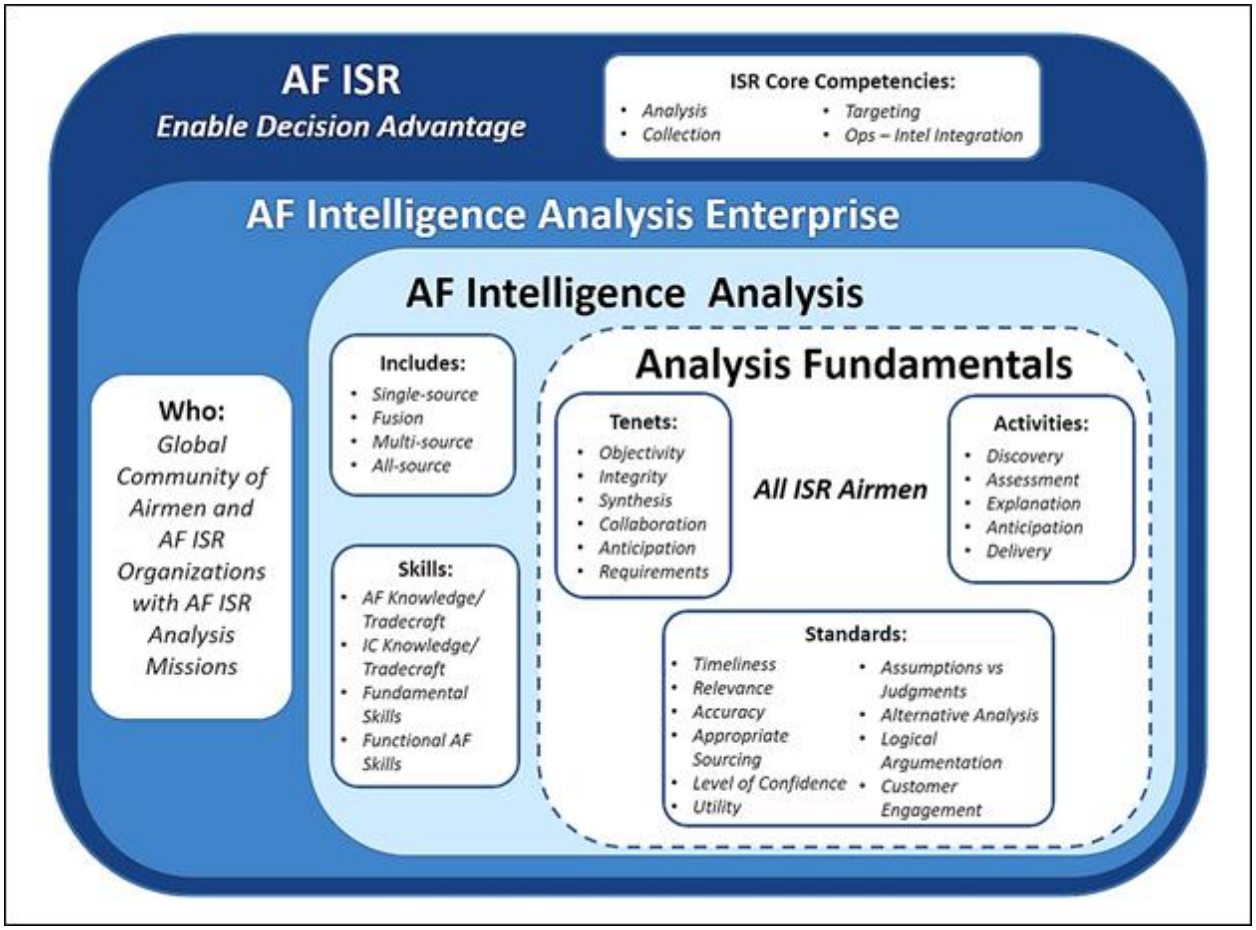
Chapter 2

AF INTELLIGENCE ANALYSIS ENTERPRISE

2.1. Analyst Airmen. An analyst Airman is an AF ISR professional who is skilled and qualified in tradecraft to perform the core competency of intelligence analysis across the air, space, or cyberspace domains. Certification criteria and programs vary based on unit and mission requirements. Analyst Airmen are bound by the professional standards for analysis established by the IC, and supplemented by AF standards and mission qualifications of the assigned ISR unit. Whether ISR professionals are analyst Airmen depends more on what they do than where they sit.

2.2. AF Intelligence Analysis Enterprise (AFIAE) . The enterprise is defined as the global community of analyst Airmen and the AF ISR organizations that employ the core competency of intelligence analysis. Figure 2.1, *AFIAE*, depicts how the AFIAE, intelligence analysis, and analysis fundamentals fit within the larger AF ISR Enterprise. Refer to **Chapter 4** for a detailed explanation of analysis fundamentals. Although not shown in Figure 2.1, the AF ISR Enterprise resides within the IC Enterprise. As a member of the IC, the AF contributes to IC analysis and production and also receives analysis and production support from other IC organizations.

Figure 2.1. AFIAE.



2.3. Analysis Spectrum . Analyst Airmen employ fundamental tenets, standards, and activities to perform analysis across a broad continuum for mission accomplishment. On one end of the analysis continuum are fusion and single-source analysis, with emphasis on timeliness over completeness. On the other end of the spectrum is comprehensive ASA, with less emphasis on rapidity, and greater emphasis on analytic content, depth, trends, technical, and other subject-matter expertise. This spectrum is depicted in Figure 2.2, *AF Spectrum of Intelligence Analysis*.

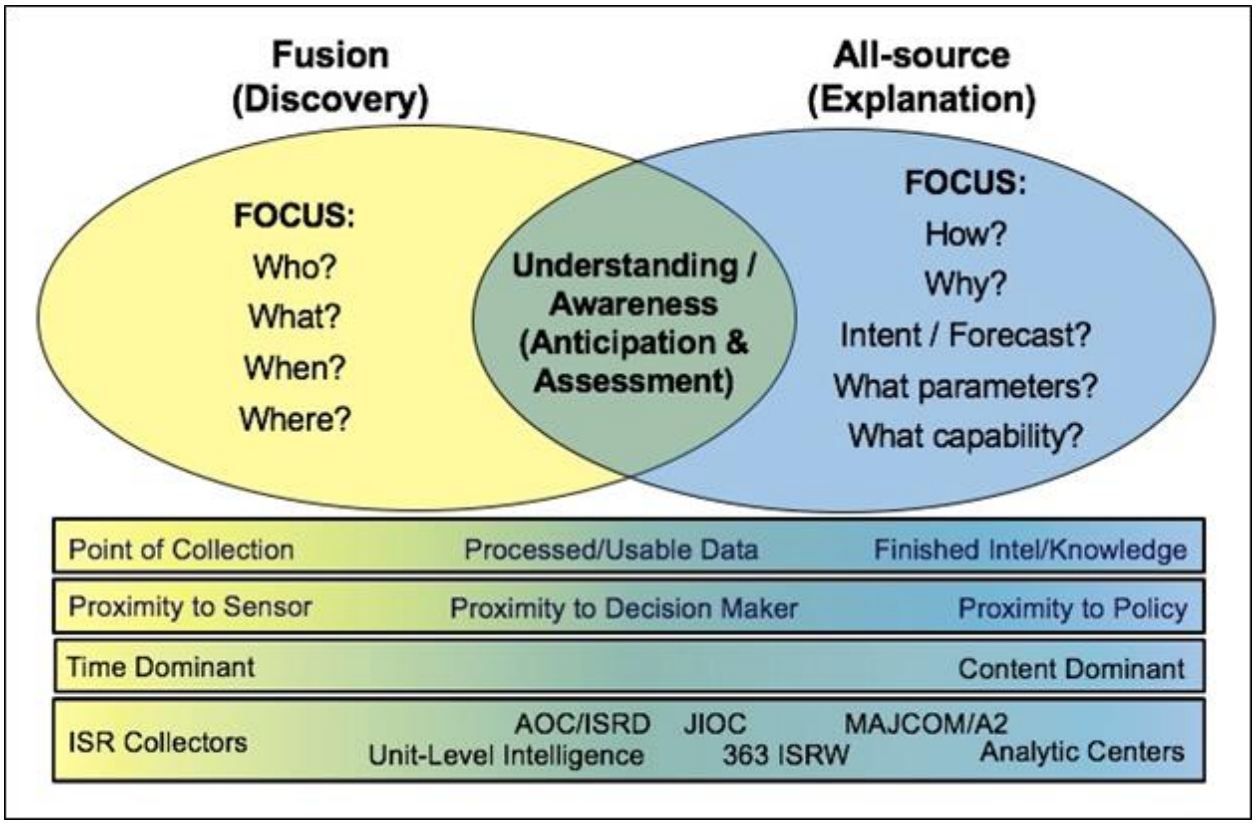
2.3.1. Single-Source Analysis (also called Exploitation). Intelligence analysis that employs a single source or expertise in a functional area to characterize events, people, or things. Such analysis is limited to describing, rather than evaluating, the topic of a particular analysis due to restrictions inherent in single-source intelligence collection, precluding the ability to provide fully contextualized intelligence assessments.

2.3.2. Fusion Analysis. Analysis in a time-sensitive environment in close proximity to the point of collection that entails quickly melding new information with baseline knowledge to meet a specific operational need. **Note:** Proximity does not refer to physical or geographic location but rather functional proximity to the collection step in the intelligence process (for example, a Distributed Common Ground System (DCGS) Analysis and Reporting Team (DART) at Beale AFB may conduct fusion analysis of an operational area on the opposite side of the globe). Emphasis is on the process of managing information and on timeliness over completeness. Fusion analysis generally has three components: 1) it usually includes more than one source; 2) it is time critical; and 3) it is performed to meet a commander's requirements or specific operational need.

2.3.3. Multi-Source Analysis (also called Multi-Intelligence (INT) Analysis). Intelligence analysis that makes use of more than one source when access to additional potential sources is limited by reasons of timeliness, system access, location, or security levels.

2.3.4. All-Source Analysis (ASA). Intelligence analysis that employs all available sources of data and information to enable the creation of new intelligence and knowledge.

Figure 2.2. AF Spectrum of Intelligence Analysis.



2.3.5. At the far left of the graphic, intelligence analysis units, such as AF DARTs, provide near-real-time (NRT), multi-source fusion analysis closest to the point of collection to improve collection, perform dynamic targeting, and support tactical warfighters. Moving to the right across the spectrum, the Air Operations Centers' (AOCs) ISR Divisions (ISRD), Joint Intelligence Operations Centers (JIOCs), and IC organizations provide multi-source and ASA with fewer time constraints and in close proximity to strategic-level commanders and decision-makers to facilitate battlespace awareness, operations planning and sustainment, and policy decisions. Since the late 1990s, changes in technology, operational needs, and CCMD requirements have blurred the once distinct lines of this analysis spectrum. Today AFIAE organizations have evolved to delivery across the spectrum – rather than delivering within any single niche.

2.4. Characteristics of the AF Intelligence Analysis Enterprise (AFIAE).

2.4.1. Layered. Intelligence analysis capabilities reside at multiple levels of command—unit, (squadron, group, wing), Numbered AF (NAF), MAJCOM, and AF-level. Additional levels, including joint and Department of Defense (DoD), exist beyond the AF. Table 2.1, *Layers of Analysis*, identifies the various layers of analysis organizations along with their general analytical focus, typical customers, and timeliness, as modern processes and technologies enable organizations to extend their focus and timelines outside traditional norms. While representative, this table is not a complete listing of all AF analysis organizations.

Table 2.1. Layers of Analysis.

Organization	Focus	Customer	Timeline
CSA (DIA, NSA, NGA, NRO)	Strategic	National leadership, DoD, IC	Days/Months; Mission dependent RT/NRT
CCMD JIOC/JTF	Strategic/Operational	CCMD, Joint forces	Days/Months
Service Intelligence Center (NASIC)	Strategic/Operational/ Tactical	National leadership, CCMD, JTF, DoD, IC, AF all levels, acquisition community	Hours/Days/Months
MAJCOM/A2	Strategic/Operational	MAJCOM staff and supported units	Days/Months
Acquisition Centers	Strategic/Operational	AF/IC leadership, MAJCOMs, acquisition program/project mgrs	Days/Months
NAF/A2, AFFOR/A2, AOC ISR Division	Operational/Tactical	CCMD, JTF/Joint forces, AF NAF and below units	Hours/Days
ISRW	Operational/Tactical	NAF and below units	Hours/Days/Months
DCGS	Operational/Tactical	CFACC, JTF, DoD, IC, AF units	RT/NRT to 72 Hours
Unit Level Intel & RPA SOC	Tactical	AF and other service units	RT/NRT to 72 Hours

AF: Air Force
A2: Director of Intelligence
AFFOR: Air Force Forces
AOC: Air Operations Center
CCMD: Combatant Command
CFACC: Combined Forces Air Component Commander
CSA: Combat Support Agency
DCGS: Distributed Command Ground System
DIA: Defense Intelligence Agency
DoD: Department of Defense
IC: Intelligence Community
ISR: Intelligence, Surveillance & Reconnaissance
ISRW: ISR Wing
JIOC: Joint Intelligence Operations Center
JTF: Joint Task Force
MAJCOM: Major Command
Mgrs: Managers
NAF: Numbered Air Force
NASIC: National Air and Space Intelligence Center
NGA: National Geospatial-Intelligence Agency
NRO: National Reconnaissance Agency
NRT: Near-real-time
NSA: National Security Agency
RPA: Remotely Piloted Aircraft
RT: Real-time
SOC: Squadron Operations Center

2.4.1.1. Starting at the bottom of Table 2.1, unit-level intelligence organizations focus on tactical analysis needs (e.g., location, movement, and readiness of enemy forces) for their tactical-level customers in the AF and other services. Unit-level intelligence organizations typically operate under short timelines from real-time or NRT to several days out.

2.4.1.2. DCGS units are tactically and operationally focused. Within each DCGS unit, the DART conducts analysis for their respective CFACC as well as other IC and DoD customers. DARTs operate in a time sensitive environment but can support the customer up to the operational level of ISR planning. Their main emphasis is fusion analysis.

2.4.1.3. ISR wings provide both operational and tactical level intelligence analysis, with timelines ranging from hours to months. In particular, the 363 ISR Wing (ISRW) is dedicated to providing all-source analysis and targeting intelligence to NAFs and below across the entire AF.

2.4.1.4. NAF/A2s, AF Forces (AFFOR)/A2, and AOC ISRDs are operationally and tactically focused in support of their associated CCMD, their joint task force (JTF), and/or their units. Their typical timelines are hours to days.

2.4.1.5. Intelligence offices within Acquisition Centers, such as the Space and Missile Systems Center (SMC), AF Life Cycle Management Center (AFLCMC) and AF Research Laboratory (AFRL), provide both strategic and operational intelligence for acquisition program managers, project managers, MAJCOMs, and AF/IC leadership, with timelines that range from days to months.

2.4.1.6. MAJCOM/A2s provide strategic and operational analyses for their MAJCOM staff and supported units, usually ranging from days to months. The Air Mobility Command (AMC)/A2 is unique in that its Air Intelligence Squadron (AIS) and the 204th Intelligence Squadron (ANG) provide direct analytic support to 18 AF and subordinate units in the conduct of their rapid global mobility missions. Additionally, U.S. Air Forces in Europe & Air Forces Africa (USAFE-AFAFRICA) and Pacific Air Forces (PACAF) are unique as Component MAJCOMs (C-MAJCOMs) in that they have the responsibility of analytically representing the Joint Force Air Component Commander to the Joint Force Commander.

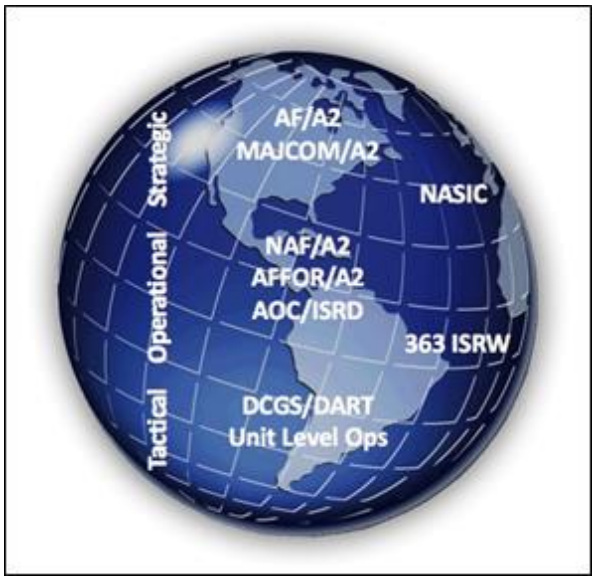
2.4.1.7. The National Air and Space Intelligence Center (NASIC**)** conducts strategic, operational, and tactical analysis for a broad range of customers in the AF, DoD, and IC as well as and including national leadership and the acquisition community. Their timelines extend from short-term to long-term, depending on the customer's needs. Whereas the 363 ISRW is the primary AF organization that conducts tactical intelligence analysis, NASIC is the primary AF organization focused on strategic intelligence. Both the 363 ISRW and NASIC provide significant analysis at the operational level, as well. Further, while other AF layers conduct analysis as part of their mission, analysis is a primary mission of the 363 ISRW and NASIC.

2.4.1.8. Joint intelligence organizations at CCMDs and JTFs conduct strategic and operational analysis in support of their respective regional and functional commands. The timelines of their analysis range from days to months.

2.4.1.9. Combat Support Agencies (CSAs) focus primarily on strategic analysis for national leadership, DoD, and the IC. Although they usually operate on timelines ranging from days to months, they also provide real-time and near-real-time analysis as requirements dictate.

2.4.2. Distributed and Mutually Supporting. In addition to being layered, analysis responsibilities are distributed across geographic regions and functional areas in the AF (see Figure 2.3, *Layered, Distributed, and Mutually Supporting Nature of AFIAE*). Analysis organizations in every layer and every region/function are interconnected and have access to each other. Organizations collaborate and share expertise to ensure the most accurate, timely analysis is provided to answer intelligence requirements. The mutually supporting nature of the AFIAE includes enterprise partners, such as the AF Office of Special Investigations (AFOSI).

Figure 2.3. Layered, Distributed, and Mutually Supporting Nature of AFIAE.



Chapter 3

THE NATIONAL INTELLIGENCE ANALYSIS COMMUNITY AND THE AIR FORCE

3.1. The Intelligence Community. The IC is a coalition of 17 agencies and organizations, including the Office of the Director of National Intelligence (ODNI), within the Executive Branch that work both independently and collaboratively to gather and analyze the intelligence necessary to conduct foreign relations and national security activities. See Attachment 6, Table A6.1, *Members of the IC*, for a complete list of IC organizations.

3.1.1. The Director of National Intelligence (DNI) has overall responsibility for intelligence support to the President and the day-to-day management of the IC. AF analysis falls under the governance and direction of the DNI. The AF is an active participant in governance and oversight forums and follows the analytical priorities, standards, processes, and procedures established by the IC. The DNI issues guidance for analysis and production through IC Directives (ICDs), IC Standards (ICSs), DNI memorandums, and other directive documents. The IC documents that most often impact AF analysis are identified in Attachment 6, Table A6.2, *Common IC and DoD Analysis References*.

3.1.2. DoD Intelligence.

3.1.2.1. The Secretary of Defense (SecDef) is responsible for the DoD portion of the IC. The Under Secretary of Defense for Intelligence (USD(I)) serves as the senior defense intelligence, counterintelligence, and security official below the SecDef and Deputy SecDef. For defense intelligence analysis the USD(I):

3.1.2.1.1. Provides oversight and direction for analysis capabilities to ensure effective support to the DoD mission.

3.1.2.1.2. Ensures analysis is aligned with IC and DoD analytical concepts, methodologies, and priorities.

3.1.2.1.3. Establishes DoD all-source analysis policy and oversees the implementation of DoD all-source analysis plans, programs, and performance.

3.1.2.1.4. Provides strategic guidance to the Defense Intelligence All-Source Analysis Enterprise (DIAAE), the collective set of all DoD organizations that execute all-source analysis activities in production of defense intelligence.

3.1.2.1.5. Develops and maintains the consolidated set of Defense Intelligence priorities that guides DIAAE analysis and reflects the intelligence needs of all Defense Intelligence consumers.

3.1.2.1.6. Establishes the DIAAE Board of Governors (BOG), a body of representatives from the DIAAE organizations that provides a forum for addressing issues, improving transparency, implementing strategies, and making resource recommendations across the DIAAE.

3.1.2.2. The AF participates in the DIAAE BOG and other DoD analysis forums and adheres to DoD analysis-related policies. Within the DoD, the agency with the largest responsibility for promulgating ASA guidance is the Defense Intelligence Agency (DIA).

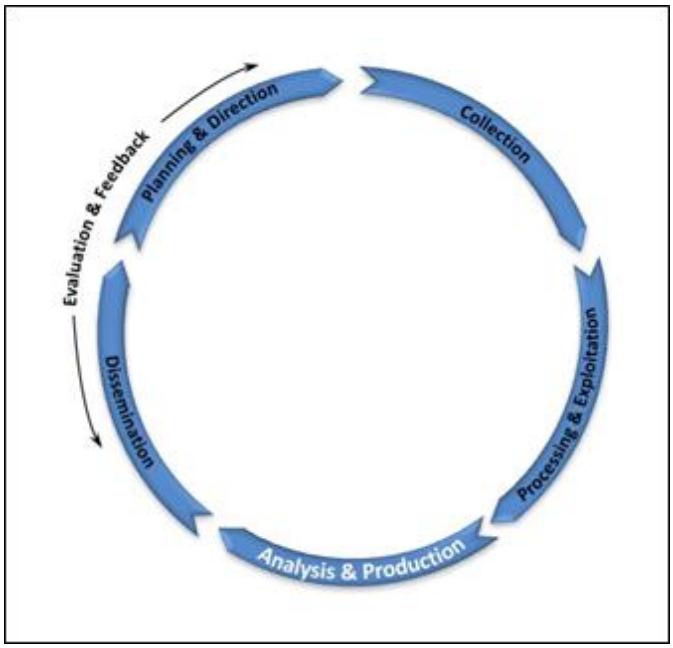
DIA governs ASA responsibilities, policies, priorities, and relationships across the DoD IAW DoD Instruction (DoDI) 3115.17 and as the DoD Functional Manager for ASA. Additionally, DIA manages the Defense Intelligence Analysis Program (DIAP), with the primary goal of maximizing enterprise efficiencies through clearly defined ASA and production responsibilities among DIA, CCMDs, and service intelligence centers.

3.1.2.3. In addition to ASA and production conducted within the DIAP, the AF conducts single-source analysis, e.g., signals intelligence, human intelligence, geospatial intelligence, etc., that is additionally governed by directives established by respective lead DoD agencies. AF production that supports these single-source disciplines adheres to AF guidance as well as standards set forth by the respective DoD lead agencies. Further, the DoD has established overarching policy related to acquisition intelligence, to which the AF adheres. If a conflict arises between the AF and IC agency guidance, IC guidance takes precedence. See Attachment 6, Table A6.2, *Common IC and DoD Analysis References*, for a list of common DoD analysis-related documents.

3.1.3. Military Services. Each military service has a senior intelligence officer (SIO) that oversees intelligence policy, planning, programming, and activities on behalf of the service chief. The AF SIO is the Deputy Chief of Staff (DCS) for ISR, also known as the AF/A2. Each service is authorized one service intelligence center, also called an intelligence analysis center. The AF's service intelligence center is NASIC. The AF has assigned the Air Combat Command (ACC) as its lead MAJCOM for the GIISR capability, which includes intelligence analysis. Similarly, other military services have assigned significant analysis responsibilities to various organizations. All services routinely reach out to each other for service-unique expertise and collaboration in addressing analysis requirements. Refer to Attachment 6, Table A6, *Major Intelligence Analysis Entities of the Military Services*, and Table A6.4, *Common Analysis Organizations*, for a breakdown of the major intelligence analysis entities in each military service and a list of service and other government agencies organized according to the primary analysis they conduct.

3.2. Intelligence Analysis and the Joint Intelligence Process. As highlighted in Joint Publication (JP) 2-0, *Joint Intelligence*, the intelligence process is comprised of six interrelated categories, collectively referred to as PCPAD. Refer to Figure 3.1, *Joint Intelligence Process*, for a graphic depiction of the PCPAD cycle. The PCPAD process is universally recognized throughout the IC and linked to the DoD Joint Capability Area (JCA) of Battlespace Awareness. JCAs provide a common framework for defining needs, analyzing operational gaps, and conducting planning and, by extension, programming for DoD capabilities.

Figure 3.1. Joint Intelligence Process.



3.2.1. Planning and Direction is dependent on the ability to synchronize and integrate the activities of collection, processing, exploitation, analysis and dissemination resources to meet Battlespace Awareness information requirements. Planning and direction activities include, but are not limited to: the identification and prioritization of intelligence requirements; the development of concepts of intelligence operations and architectures required to support the commander's mission; tasking subordinate intelligence elements for the collection of information or the production of finished intelligence; submitting requests for additional capabilities to higher headquarters; and submitting requests for collection, exploitation, or all-source production support to external, supporting intelligence entities. Planning and direction occurs continuously and allows for the prioritization of intelligence support across all ongoing operations and simultaneous planning efforts.

3.2.2. Collection is the ability to gather data and obtain required information to satisfy requirements. Collection is managed by collection managers, whose duties include identifying the most appropriate available assets and then tasking those assets to conduct collection missions. Collection managers also develop and coordinate sensor employment guidance, exercise authoritative control of specific collection operations, revise collection activities as required, monitor the overall satisfaction of requirements, and assess the effectiveness of the collection plan to satisfy the original and evolving intelligence need.

3.2.3. Processing and Exploitation involves the transformation of collected information into formats suitable for further analysis and/or action by man or machine. During processing and exploitation, raw collected data are converted into forms that can be readily used by commanders, decision-makers at all levels, intelligence analysts, and other consumers. Processing and exploitation includes first-phase imagery exploitation, data conversion and correlation, document and media translation, and signal decryption, as well as reporting the results of these actions to analysis and production elements.

3.2.4. Analysis and Production involves the integration, evaluation, and interpretation of information obtained from available sources to develop intelligence and forecast the future state to enable situational awareness and provide new knowledge/actionable information. The AF has identified five activities that occur within this category of the PCPAD process: Discovery, Assessment, Explanation, Anticipation, and Delivery. See **Chapter 4** for a description of each, along with an explanation or how it relates to broader AF ISR activities, and the tenets and standards to which analyst Airmen adhere in order to carry out these five analysis activities.

3.2.5. Dissemination and Integration focuses on the ability to present, distribute, or make available to military and national decision-makers the intelligence, information and environmental content and products that enable understanding of the operational/physical environment. Personal, networked, and database data transfers are all means of dissemination. The diversity of dissemination paths requires a high degree of communications and system interoperability among joint and multinational forces, component commands, DoD organizations, and the interagency community.

3.2.6. Evaluation and Feedback occur continuously throughout the intelligence process. It requires a collaborative dialogue among intelligence planners, collection managers, collectors, analysts, intelligence systems architects, and customers. The intent of evaluation and feedback is to identify potential problems as early as possible to minimize information gaps and mitigate capability shortfalls.

3.2.7. Although “analysis” is specifically identified in the Analysis and Production category of PCPAD, most intelligence analysts agree that analysis takes place in all categories of the joint intelligence process.

3.3. IC Funding. The National Intelligence Program (NIP), administered by the DNI, provides guidance and funding for a broad range of ISR activities within the IC. NIP is divided into sub-programs, including the General Defense Intelligence Program (GDIP) for ASA and other specific intelligence activities, the Consolidated Cryptologic Program (CCP) for signals intelligence activities, and the National Geospatial-Intelligence Program (NGP) for geospatial intelligence activities. Some AF intelligence organizations receive funding through these NIP sources for certain single-source and ASA missions and are required to adhere to the analysis and production guidelines and standards associated with the funding. However, the majority of AF analysis activities, particularly at and below wing level, are funded through the Military Intelligence Program (MIP) for mission execution. For details, refer to ICD 104, *National Intelligence Program (NIP) Budget Formulation and Justification, Execution, and Performance Evaluation* and DoDD 5205.12, *Military Intelligence Program (MIP).*

3.4. Quality Analysis Programs . The IC and AF offer a variety of analyst enrichment opportunities to broaden and deepen an analyst's experience and expertise. Some examples include the AF Quality of Analysis Program, DNI Quality of Analysis Program, National Intelligence University, DIA's Intelligence Community Advanced Analytical Program, and the AF Institute of Technology.

3.5. AF National Tactical Integration (AF NTI) . The AF NTI program integrates U.S. Signals Intelligence (SIGINT) System resources with theater air and space components to ensure seamless support. The AF NTI team shifts the focus of national SIGINT performance from discovering and reporting data to collaboratively generating actionable intelligence for the Joint

Force Air Component Commander. The AF NTI team capitalizes on data acquisition capabilities, existing databases and datalinks of multiple national SIGINT sources, and access to AF analysts in the AOC, National Cryptologic Centers, and AF intelligence production organizations (e.g., NASIC). While the program remains predominately SIGINT focused, the AF NTI enterprise also has the ability to leverage all AF ISR capabilities. **Note**: Refer to AF ISR Agency Instruction (AFISRAI) 14-153 Volume 3, 480 ISRW Supplement, *Air Force Distributed Common Ground System (AF DCGS) Operations Procedure*s.

Chapter 4

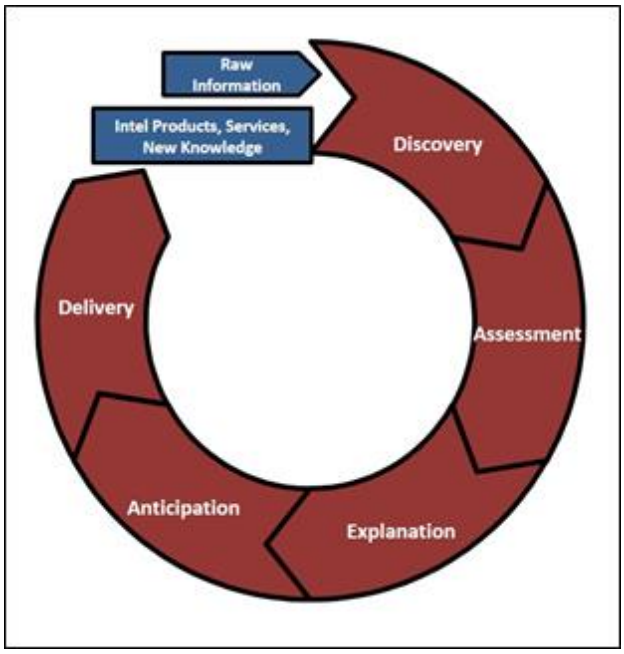
ANALYSIS FUNDAMENTALS–ACTIVITIES, TENETS, & STANDARDS

4.1. AF ISR Capabilities . The AF *GIISR Core Function Concept* highlights five enduring core capabilities (refer to Figure 4.1, *Enduring GIISR Capabilities*) that directly support the JCA of Battlespace Awareness. As previously mentioned, this JCA delineation is key for defining analysis-specific needs, analyzing gaps, and for planning and programming against AF analytic requirements. Similar to the joint PCPAD intelligence process discussed in **Chapter 3**, analysis is an essential and integral component of each of the five enduring GIISR capabilities.

Figure 4.1. Enduring GIISR Capabilities.

4.2. AF Intelligence Analysis Activities . As depicted in Figure 4.2, *AF Intelligence Analysis Activities*, analyst Airmen commonly perform five activities in support of the GIISR enduring capabilities mentioned above.

Figure 4.2. AF Intelligence Analysis Activities.



4.2.1. Discovery is the ability to research, select, manipulate, and correlate data from multiple sources to identify information relevant to ongoing operations and requirements. Discovery is about researching, better organizing, and using the data we already possess; it is also about finding previously hidden patterns and anomalies.

4.2.2. Assessment is the ability to provide focused examination of data and information about an object or an event, to classify and categorize it, and to assess its reliability and credibility in order to create estimates of capabilities and impacts. Assessment is how intelligence determines what our consumers ought to be concerned with.

4.2.3. Explanation is the ability to examine events and derive knowledge and insight from the interrelated data in order to create descriptions and propose significance in greater context. Explanation is how intelligence provides consumers with narrative stories, relates events to broader situations, and identifies the core of "what is going on."

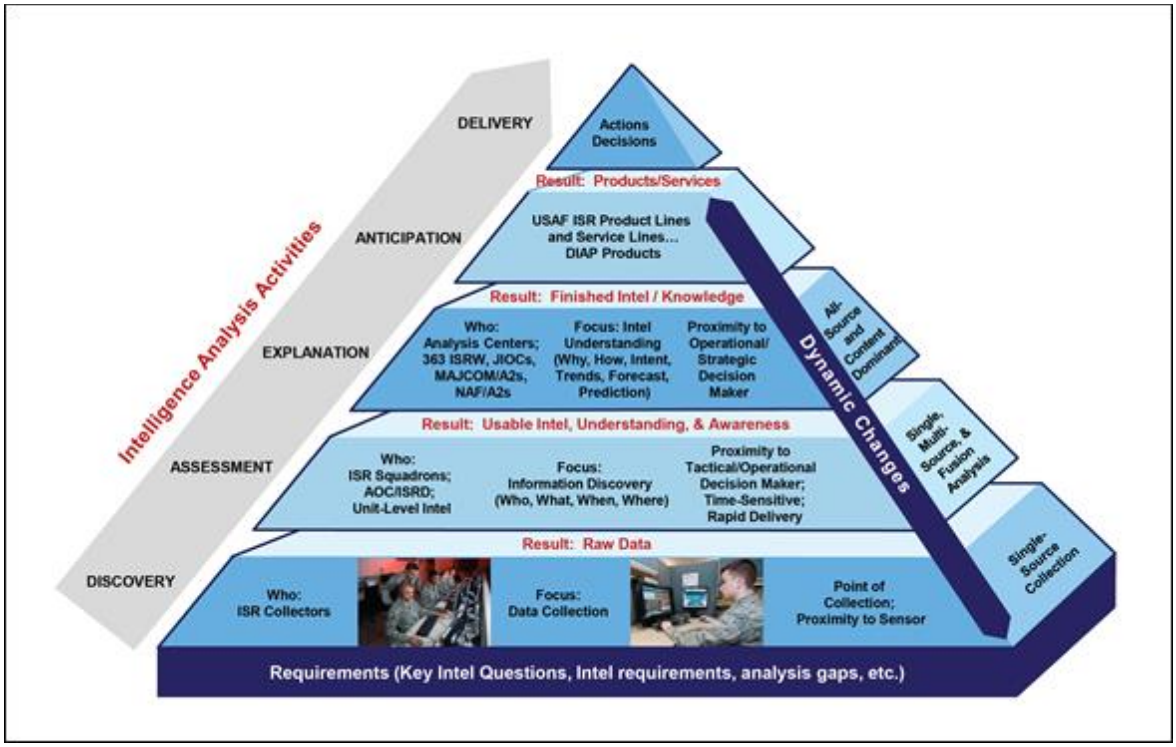
4.2.4. Anticipation is the ability to warn and describe future states of the environment based on the manipulation and synthesis of past and present data. Anticipation includes near-term warning and longer-term forecasting to alert and prepare decision makers for events that could be relevant to their responsibilities.

4.2.5. Delivery is the ability to develop, tailor, and present intelligence products and services according to customer requirements and preferences. Delivery is about classic intelligence products—from tactical reports to in-depth intelligence estimates—and a myriad of intelligence services, ranging from interactive displays and operational pictures, to multimedia crew threat briefings and tablet-embedded, dynamic intelligence assessments, enabling real-time analyst response to requests for information. Delivery is often referred to as production and/or dissemination.

4.2.6. As Figure 4.3, *AF Intelligence Analysis Continuum*, depicts, analysis activities take place across a continuum within the AF, starting with the development of requirements;

progressing through data collection, information discovery, and intelligence understanding; and culminating in services and products that impact commanders' decisions and military actions.

Figure 4.3. AF Intelligence Analysis Continuum.



4.3. AF Intelligence Analysis Tenets. AF tenets of analysis derive from and support IC, joint intelligence, and broader ISR principles, while simultaneously emphasizing analysis attributes of particular interest and priority within the AF. These are the overarching principles held to be true and in common by AF ISR professionals. Collectively, these six tenets cover the most important beliefs about AF intelligence analysis. According to AFI 14-133, while effort should be taken to apply all of these tenets, situations may dictate not all of them being used. The following descriptions are excerpts from AFI 14-133.

4.3.1. Objectivity. Analysis should be based on fact and be clear and truthful about what is *known versus what is judged*. It should *not be distorted by emotion or personal or organizational bias* and shall *be independent of command or political considerations*. Further, it should clearly delineate underlying intelligence, assumptions, and judgments. Analysts should address alternative perspectives and contrary information and avoid being unduly constrained by previous judgments.

4.3.2. Integrity. While closely linked to objectivity, integrity involves a broader focus on all activities, standards, and processes associated with AF intelligence analysis. Integrity calls for *complete honesty* and *reliability in analysis* combined with firm adherence to a code of *professional ethics* and *tradecraft standards* such as *accuracy, timeliness,* and *customer responsiveness*. Integrity includes explaining changes in previous analytic judgments, as well as addressing significant differences in judgment among various U.S. analytic elements.

As stated in JP 2-0, integrity is "the cardinal element in intelligence analysis and reporting, and the foundation on which credibility with the intelligence consumer is built."

4.3.3. Synthesis. AF intelligence analysis requires analysts to *use all available sources of information to maximize completeness*. Analysts should also identify information gaps and, where they exist, they should coordinate with collectors to develop access and collection strategies. Synthesis requires well-honed tradecraft skills, including critical thinking, alternative analysis, and the ability to take the perspective of the adversary. Compatible, service-oriented information technology architectures and tools are also key to facilitating synthesis.

4.3.4. Collaboration. Analysts must *actively solicit opinions and assessments from other analysts and seek to share ideas*. Data, information, and intelligence must be broadly accessed and shared. *Collaboration* should take place internally within the AFIAE, across the IC, and with allies, academia, and other entities outside the IC, when feasible. *Effective collaboration facilitates maximum synthesis*.

4.3.5. Anticipation. Analysis is far more than trend assessment; its true *value resides in warning* and forecasting to be relevant to *decision making, warfighting, operations,* and *acquisition*. Because *information gaps routinely limit our ability to predict with complete accuracy,* it is incumbent on analysts to effectively apply tradecraft standards such as alternative analysis, levels of confidence, assumptions vs. judgments, and appropriate sourcing. Intelligence warning and forecasting are not exact; however, analysts should utilize the most recent data/information for all warning or forecast-related analysis.

4.3.6. Requirements. The AF intelligence analysis mission is motivated by *continuous engagement with customers* to comprehend dynamic needs. Customer requirements can be solicited from a variety of sources such as: understanding their operations; holding working groups or technical exchanges with them; anticipating and listening to their questions; responding to feedback; and addressing documented need statements and derivative data needs. Effectively meeting analysis mission requirements demands an effective balance of customer familiarity, interpreted needs, collaboration, and analytical judgment.

4.4. AF Standards of Intelligence Analysis . The AF has established ten standards by which it measures and assesses analytic excellence and readiness. AF tradecraft standards align with IC standards; however, the AF incorporates two additional attributes: timeliness and customer engagement. AF standards also are in parallel with joint intelligence and GIISR guidance. These standards are used by the AF ISR Enterprise to conduct analysis operations and are integrated into AF Inspection System criteria. Attachment 4 contains a sample methodology and form to evaluate these standards. The following descriptions are excerpts from AFI 14-133. Refer to the AFI for additional details.

4.4.1. Timeliness. Analysis *must be timely* to impact planning, mission objectives, operations and otherwise aid in commanders' decisions. The aim is to deliver information and knowledge at the earliest time and place to enable customers to effectively make decisions and take action.

4.4.2. Appropriate Sourcing. Analysis *cites all sources used,* when feasible, and includes an *objective assessment of the quality, credibility, and reliability of the underlying sources*.

4.4.3. Accuracy. Analysis will *make the most accurate judgments and assessments possible*, based on the intelligence available and in light of known information gaps. A retrospective assessment of the accuracy of a judgment will help identify biases and other potential tradecraft errors for correction in future analysis.

4.4.4. Level of Confidence. To help qualify accuracy and to present analysis in a uniform and consistent manner across the AF, analysts will *indicate the degree of confidence/certainty* associated with analytic judgments and conclusions to the best of their ability, given currently available intelligence. AFI 14-133, Table 3.1, *Confidence Levels in Analytic Judgment*, provides guidance for analysts to use in assigning levels of confidence/certainty.

4.4.5. Assumptions vs. Judgments. Analysis *clearly distinguishes among underlying intelligence, analyst assumptions, and analyst judgments*.

4.4.6. Alternative Analysis. Analysis will *incorporate plausible alternative assessments,* judgments, or hypotheses, *particularly when major judgments contend with significant uncertainties, complexity, or a lack of available intelligence*, or when low probability events could produce high impact results. Whenever possible, analysis should be vetted through at least one other intelligence professional to minimize individual analyst bias.

4.4.7. Relevance. *Analysis is key to decision making*, warfighting, and acquisition efforts. Analysts should make every effort to ensure products and services fulfill the customer's intent and request, while also ensuring products and services are available to others for use beyond the original intent.

4.4.8. Logical Argumentation. Analysis will employ coherent and logical reasoning techniques, be supported by all key relevant information, and be internally consistent.

4.4.9. Utility. AF analytic products and services will *use formats* (written, verbal, visual, etc.) *that best enable understanding by the customer*. Intelligence analysis will be disseminated at the lowest classification and widest releasability levels without jeopardizing its usefulness to the customer.

4.4.10. Customer Engagement. Analysis should fully address customer requirements within time constraints and in a manner most useful. Analyst Airmen will be responsive to customer feedback. While challenging to evaluate, this tradecraft standard is foundational to AF intelligence analysis.

4.5. Beyond the Checklist . The list of analysis activities, tenets, and standards lend themselves to a checklist mentality. This is especially true with the standards, that are the criteria by which the AF evaluates analytical readiness. However, it is vital to remember that intelligence analysis is ***not just a science but also an art***. Following good tradecraft practices aids in developing a sound analytic process and foundation. However, the analyst cannot become paralyzed in making an assessment if all the tradecraft pieces do not fully align. Mistakes will be made – have been made – but we cannot fail to provide decision makers with our best assessment based on what information we had at the time. The analyst Airman learns the fundamentals but then spends many hours of intense effort honing and refining application of the fundamentals in the determined pursuit of excellence. Analysts need to express interest in the analysis activities and be eager to revisit any or all of them for the sake of providing more accurate, mission-relevant analysis for each customer requirement. Analysts need to embrace the

tenets and standards such that they become an intuitive and natural part of all analytical activities. Analysts, supervisors, and commanders also need to hold each other accountable to the tenets and standards.

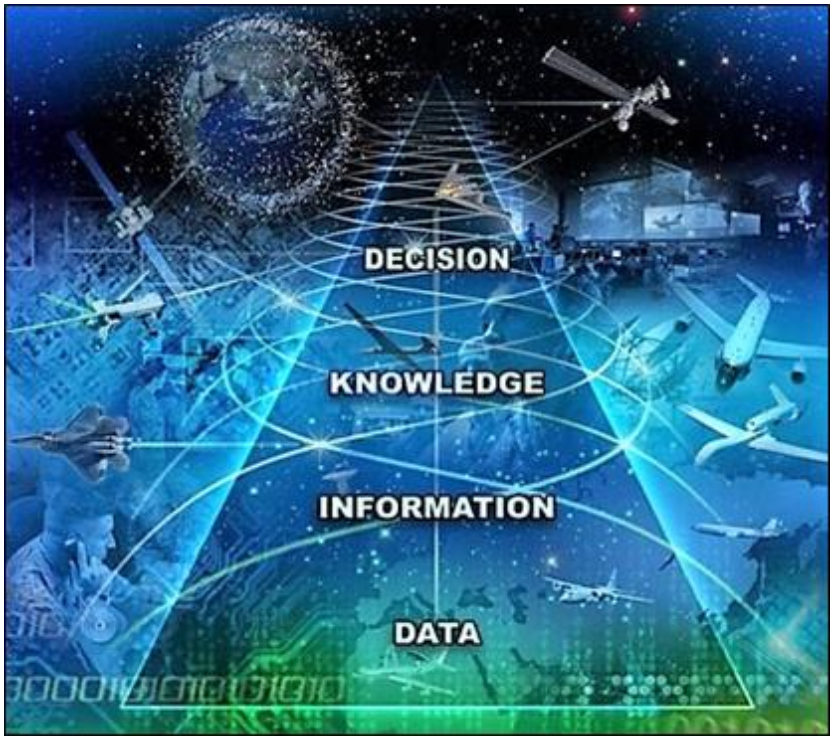
4.6. AF Analytic Ombuds . The AF Analytic Ombuds is the AF representative that responds to concerns raised by intelligence analysts about adherence to AF analysis tenets, standards, and production guidelines. The Ombuds addresses such concerns as lack of objectivity, bias, politicization, or other issues in applying analysis tenets and standards. The AF/A2 appoints the AF Analytic Ombuds in accordance with DNI guidance. In addition, NASIC and each MAJCOM/A2 designate an individual or office to serve as their organization's Analytic Ombuds IAW AFI 14-133.

Chapter 5

ANALYSIS SKILLS AND TRADECRAFT

5.1. Overview. Intelligence analysis is what transforms data into the information and knowledge necessary for warfighters and decision makers to decide and act (refer to Figure 5.1, *Transforming Data to Decisions*). While technology can assist and enable these transformations of data, without human cognition (people "in-the-loop") it is doomed to fail. There are things technology alone is not capable of. The things technology can do depend upon human analysts creating and updating the analytic models, databases, and displays that can be automated or made more efficient. The most basic and necessary unit in intelligence analysis is the analyst. **Note:** Attachment 7 identifies some online resources that contain additional information on analysis skills and tradecraft topics covered in this chapter.

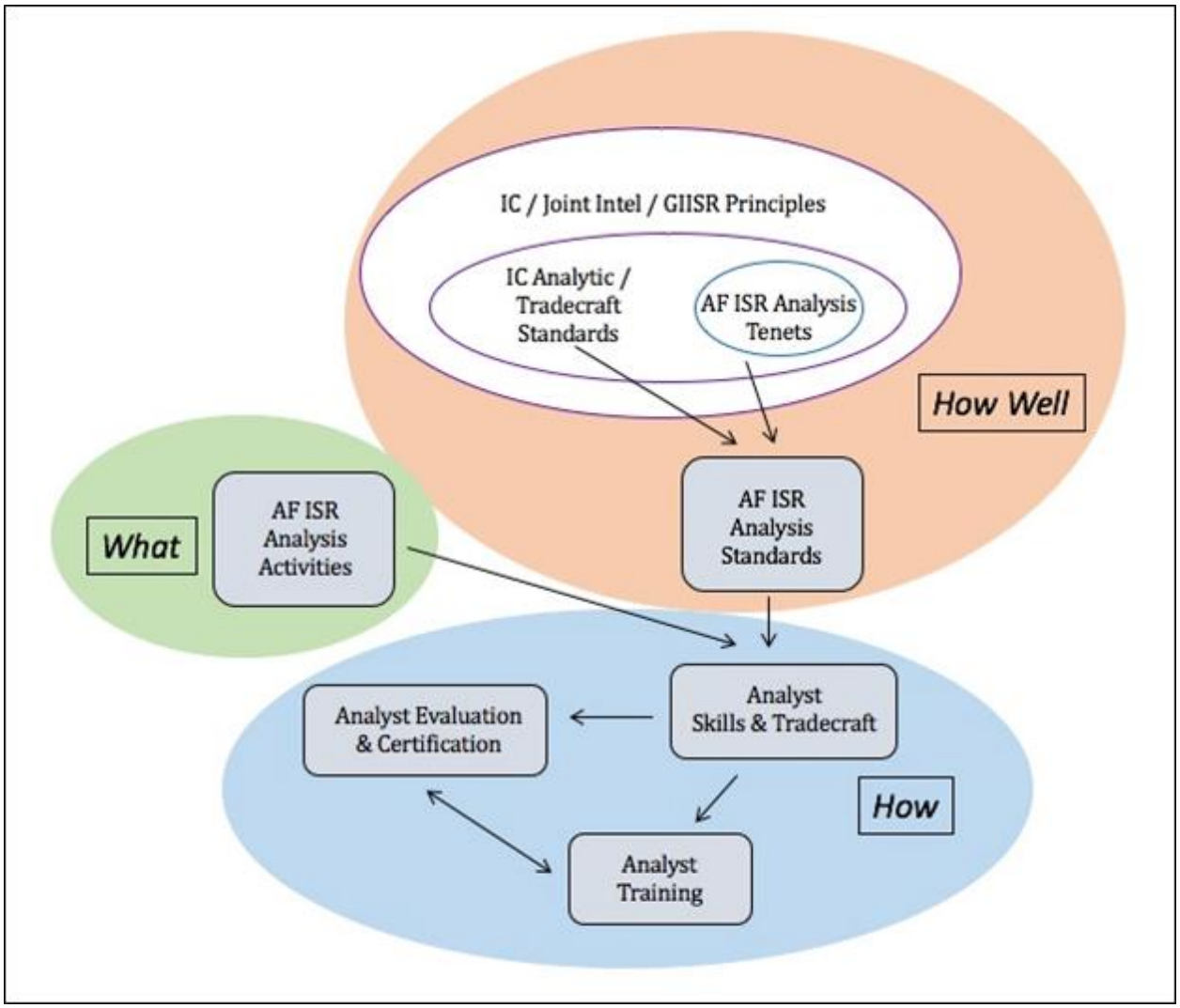
Figure 5.1. Transforming Data to Decisions.



5.1.1. Definitions and Relationships. An analysis skill is a specific ability or collection of capabilities required to competently conduct analysis that is acquired through training and/or experience. Analysis tradecraft is an established or prescribed analysis technique, practice, or systematic process. The relationship and role of intelligence analysis skills and tradecraft is illustrated in Figure 5.2, *Relationship and Role of Intelligence Analysis Skills and Tradecraft*. Whereas the five AF intelligence analysis activities (discovery, assessment, explanation, anticipation, and delivery) comprise "what" analyst Airmen do and analysis tenets/standards establish how well analysis is done, analysis skills and tradecraft are the "how" of analysis. Analysis activities, tenets, and standards drive the skills and tradecraft for which analyst Airmen need to be trained. In turn, analysis skills and tradecraft determine training, evaluation, and certification requirements. Analyst skills and tradecraft highlighted

in this publication are time-tested, repeatable, and proven effective for structured AF intelligence analysis.

Figure 5.2. Relationship and Role of Intelligence Analysis Skills and Tradecraft.



5.1.2. Analysis Transformation.

5.1.2.1. In 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act (IRTPA) in response to several commissions and hearings in the aftermath of 9/11. That act is known for establishing the ODNI; however, the act also set forth a number of tasks and objectives for the DNI to accomplish to improve intelligence and prevent or mitigate the failures that led to 9/11. It is worth highlighting that a majority of those tasks and objectives relate to the conduct of intelligence analysis: Congress directed that U.S. intelligence analysis needed to be professionalized, have set standards, and address many shortcomings in skills and tradecraft through increased guidance and training. Thomas Fingar, the first Deputy DNI for Analysis, later reflected that up until IRTPA and the subsequent transformation of analysis in the IC, analysis had largely been a craft in the IC: skills learned only on-the-job, under the tutelage of 'journeymen' and 'masters,'

where the language and processes used could differ from shop to shop, region to region, and advancement was informally recognized and locally derived. **Note:** For more information on this topic, see Thomas Fingar, *Reducing Uncertainty: Intelligence Analysis and National Security*.

5.1.2.2. This is not to say that some agencies or elements in the IC did not have more established vocabulary and tradecraft, and even so-called training and intelligence colleges, such as the CIA and DIA. However, this kind of professional approach was not widespread, and where it was present, organizations were not sharing standards or efforts. IC standards began to promulgate through DNI-approved ICDs and other policy, while shared training and vocabulary were established through collaboration, development, and sharing of IC analysis training. As these directives, policy, and training matured, efforts began to focus on defining the fundamentals of intelligence analysis as a means to true certification of all analysts in the IC. Today, these analytic standards are not only reflected in ICDs, but are standards for AF compliance, as highlighted by AFI 14-133 and associated unit Management Internal Control Toolset (MICT) Self-Assessment Communicators (SACs).

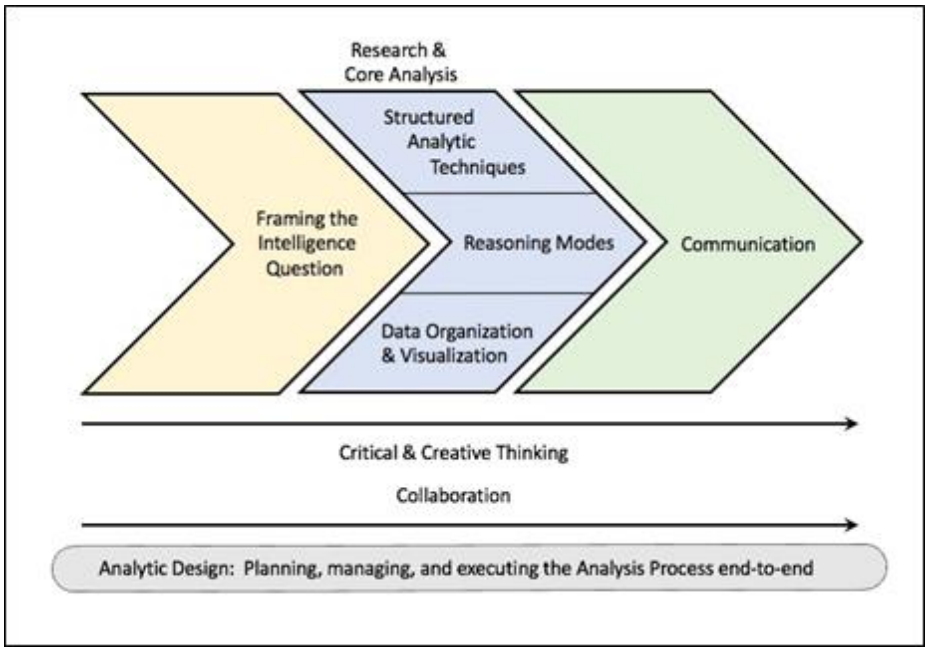
5.1.3. Analysis Certification Programs.

5.1.3.1. All-Source Analysis (ASA) Certification Program. The ASA Certification Program is a USD(I)-approved and DIA-led analysis qualification program for the DoD. The program assesses a candidate's knowledge and performance of ASA skills. The program is in the nascent stages. Initial qualification is focused on the fundamentals of intelligence analysis and open to all military and civilian intelligence analysts. The intent is for the program to expand to follow-on or higher levels of qualification. The AF ISR Force Management Division (AF/A2FD) is the AF OPR for the ASA Certification Program.

5.1.3.2. Other Certification Programs. The IC has also established certification programs for various fields of single-source analysis and activities closely linked with ASA. As one example, the Geospatial Intelligence (GEOINT) Certification Program is part of a broader USD(I) initiative to further professionalize the DoD intelligence workforce. The program applies to all cleared DoD civilian, military, and contractor practitioners in GEOINT-related work roles. Another example is the DoD Collection Management Certification Program, which ensures that collection managers possess the knowledge and skills associated with the competencies necessary to successfully carry out DoD collection management functional tasks.

5.2. Skills and Tradecraft Fundamentals. While analysis skills and tradecraft are taught in varying forms and emphasis across the IC and in AF entry and advanced training for core AF intelligence AFSCs (14N, 1NX, 9SX, 1A8X, and 0132), all AF intelligence analysts require competency in these areas. Figure 5.3, *Fundamental Skills and Tradecraft of the Analysis Process*, portrays the fundamental skills and tradecraft associated with the analysis process. Although the figure suggests an alignment, the order in which the analyst Airman applies the skills and tradecraft techniques varies depending on the requirement and is not as important as ensuring all skills and tradecraft are considered. This section will describe each of these areas.

Figure 5.3. Fundamental Skills and Tradecraft of the Analysis Process.



5.2.1. Critical and Creative Thinking.

5.2.1.1. Critical thinking is considered to be a foundational AF analysis skill. AFI 14-133 defines it as the intellectually disciplined process of actively and skillfully conceptualizing, applying, analyzing, synthesizing, and/or evaluating information gathered from or generated through observation, experience, reflection, reasoning, or communication, as a guide to belief and action. The concept of critical thinking and its associated improvements to coherent cognition arose from the philosophy departments of schools and universities in the mid-1990s. Many observers feel it was because managers and leaders across the private, commercial, and government worlds began demanding people who could "think better and deeper." **Note:** See Peter A. Facione, *Critical Thinking: What It is and Why it Counts*, p. 3. Critical thinking may be better understood by contrasting it with "normal" thinking. In everyday thinking, people often find themselves with a central thought but are distracted by other thoughts or topics as they occur either physically or mentally. They strive to get to a destination, but may wander and stall before reaching it, with little recognition of where they have been. In contrast, with critical thinking, conscious effort occurs to focus on a particular thought and additionally be "critical" (the origin of the phrase) or reflective and purposeful, using more rigorous reasoning. Reflective reasoning—thinking about how we think, or metacognition—is the key difference between normal and critical thinking.

5.2.1.2. The need for critical thinking in analysis is often paired with another adjective: "creative." Creativity has always been difficult to define, but in the context of intelligence analysis, the 9/11 Commission report abounds with calls for U.S. analysts to have more imagination: to be able to link disparate happenings and facts, to see a "bigger picture," to envision alternatives which are not spelled out. In rigorous thinking, creativity is often associated with "abductive" reasoning: the process of generating a novel hypothesis to explain given evidence that does not readily suggest a familiar

explanation. **Note:** See section 5.2.4 for additional information on reasoning. Creativity "characterizes the analyst's ability to come to a conclusion spontaneously, often without a sense of having consciously taken definable steps to get there. While the abduction process may not be easily defined or taught, it may be encouraged by providing analysts with a wide array of research material and experiences, and by supporting the expenditure of time and energy on creative thinking." **Note:** See Lisa Krizan, *Intelligence Essentials for Everyone*, pp. 31-32, and LCDR William G. Schmidlin, *Zen and the Art of Intelligence Analysis.*

5.2.1.3. Both critical and creative thinking are supported in intelligence analysis by the application of methods known as Structured Analytic Techniques (SATs) and an understanding of analytic reasoning and the role of biases, addressed below.

5.2.2. Framing the Intelligence Question. A well-framed intelligence question is the most important factor in assuring the overall quality of intelligence analysis, helping analysts to anticipate emerging trends and developments and focus efforts on addressing issues most relevant to consumers of intelligence. The question drives information discovery, the selection of analytic approaches and methods, and ultimately the analytic message conveyed to intelligence consumers. Successfully framing the intelligence question consists of clearly articulating the key intelligence issues and deconstructing the question to identify the primary factors to be considered in answering the question. A well-framed question also requires the analyst to have an adequate understanding of air/space/cyber power and the missions the analyst directly supports. Framing the question includes identifying intelligence gaps, understanding the information base, and knowing how to drive collection.

5.2.2.1. Intelligence Gaps. An intelligence gap is information that is needed to appropriately conduct intelligence analysis and help answer an intelligence question but is absent from reporting—what we know we don't know. Identifying gaps helps focus the research and collection required to close the gaps. Moreover, awareness of intelligence gaps aids analysts in properly conveying the resulting level of confidence associated with analytic judgments.

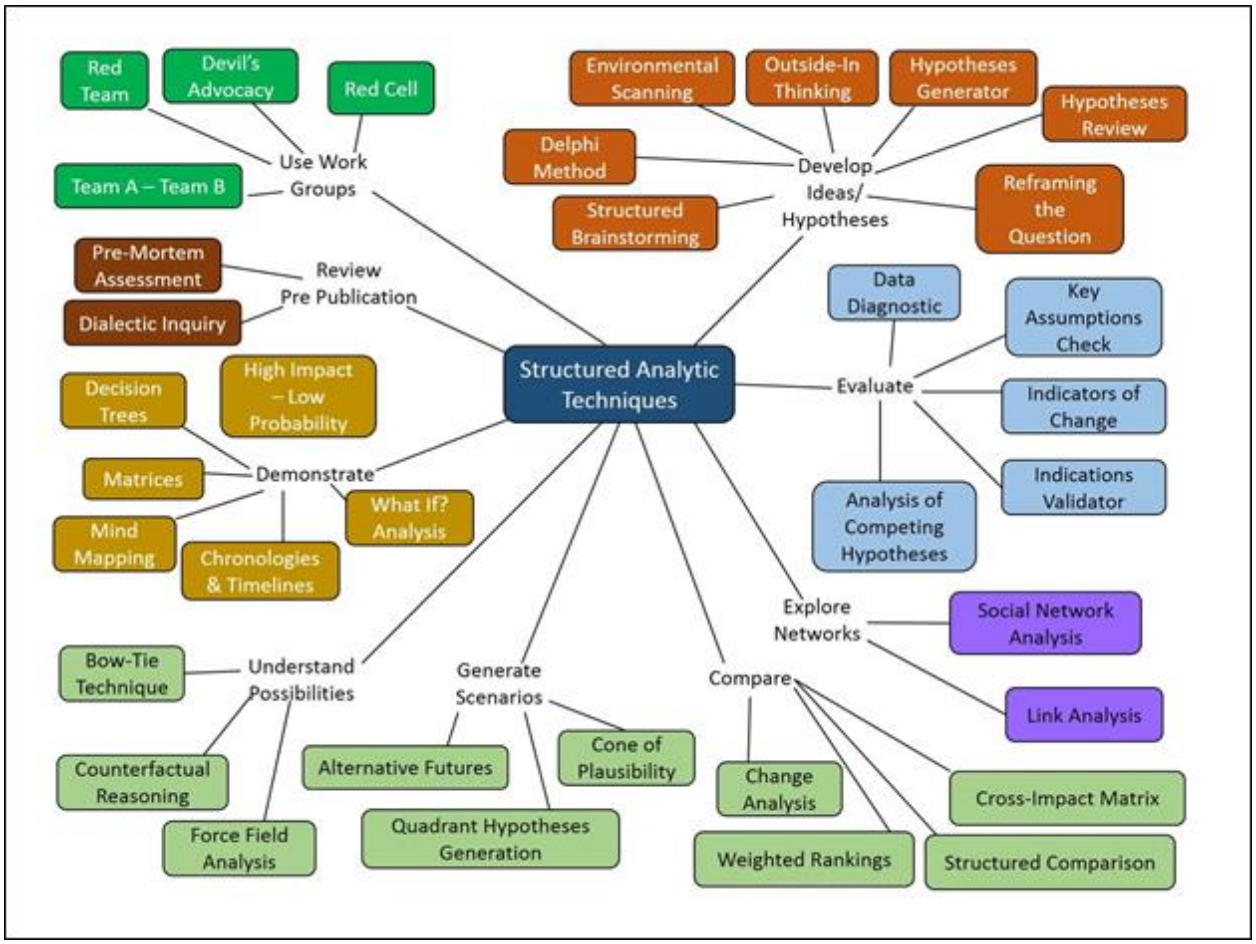
5.2.2.2. Understanding the Information Base. To effectively marshal information needed to answer intelligence questions, analysts require a solid understanding of the available information base. They need to identify what data and information is required, establish whether it is available, and determine where it can be found. In addition, they know the strengths and weaknesses of potential sources of information, are able to assess the quality of that information, in part by knowing where it comes from and how it was processed and disseminated, and understand the role analysis plays in transforming this data and information into knowledge that provides value to intelligence consumers.

5.2.2.3. Driving Collection. Analyst Airmen need to understand how information is collected and processed in the AF and more broadly in the IC to identify which sources of information are most useful in answering their intelligence questions, to assess quality and credibility, and to task collectors to collect information to fill intelligence gaps.

5.2.3. Structured Analytic Techniques (SATs). After properly framing the intelligence question, the analyst dives into the heart of the analysis process. There are several critical skills associated with this core research and analysis phase of the process, one being the application of SATs.

5.2.3.1. In *Structured Analytic Techniques For Intelligence Analysis*, Richards J. Heuer, Jr. and Randolf H. Pherson describe structured analysis as "a step-by-step process that externalizes an individual analyst's thinking in a manner that makes it readily apparent to others, thereby enabling it to be shared, built on, and critiqued by others. When combined with the intuitive judgment of subject matter experts, such a structured and transparent process can significantly reduce the risk of analytic error." **Note**: See Richards J. Heuer, Jr. and Randolf H. Pherson, *Structured Analytic Techniques For Intelligence Analysis*, p. xvi. SATs rose to prominence in intelligence analysis as part of a broad effort to transform the tradecraft following 9/11. Most SATs are not unique to intelligence analysis, but have been developed in other fields that utilize analysis. Many of these techniques, shown in Figure 5.4, *SATs*, broadly fall under the field of operations research, management tools, and general decision-making aids.

Figure 5.4. SATs.



5.2.3.2. Why are SATs important? Their application helps the analyst take a systematic approach to problem solving, mitigate bias and error, and enhance analytic credibility. SATs are useful by both individuals and teams in breaking down problems or "decomposition," generating ideas or "brainstorming," testing ideas or reviewing alternatives, and checking solutions or assessments. Structured techniques offer an effective means of applying scientific methodologies to the operational art of analysis.

Advanced analytic courses, such the AF Critical Thinking and Structured Analysis Course (CTSAC), offer focused training on SATs. Attachment 5 contains a tradecraft guide that details some of the key SATs commonly used by analyst Airmen.

5.2.4. Analytic Reasoning and Bias.

5.2.4.1. The heart of the definition for critical thinking is purposeful, reflective reasoning. Logical reasoning is defined as the process of establishing a justified belief by using premises (rules), evidence (facts), and argument (relationships). Three types of basic reasoning include:

5.2.4.1.1. Deductive reasoning—Sometimes called deductive logic, deduction is reasoning in which a conclusion is a logical consequence of the premise. A deduction moves from general rules and some evidence to particular cases.

5.2.4.1.2. Inductive reasoning—The intellectual process of drawing generalizations on the basis of observations or other evidence. Induction takes place when one learns from experience.

5.2.4.1.3. Abductive reasoning—The process of generating a novel hypothesis to explain given evidence that does not readily suggest a familiar explanation. Abductive reasoning starts from a set of accepted facts and creatively proposes their best explanation.

5.2.4.2. More recently, social scientists have helped to expand the horizons and suggest there are analytical *modes* of reasoning, most of which are familiar in description yet have significant research behind them. Reasoning is the process of forming conclusions, judgments, facts, opinions, or inferences. Reasoning assists in forming arguments based upon evidence about observed activities. It is the job of an analyst Airmen to make sense of a complicated mass of information—to understand and explain the current situation, to reconstruct the past that led to it, and to use it as the basis of predictions for the future. **Note:** See Barbara Spellman, "Individual Reasoning*"* in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, p. 117. As human beings with developed intellects, we generally may be said to have six modes of reasoning:

5.2.4.2.1. Status Quo—Making immediate judgments and inferences.

5.2.4.2.2. Authoritative—Drawing inferences from expert testimony or strong belief.

5.2.4.2.3. Comparative—Drawing conclusions from examples, cases, or analogies.

5.2.4.2.4. Empirical—Drawing conclusions from personal interaction with real evidence.

5.2.4.2.5. Scientific—Drawing casual inferences using facts, premises, and logic.

5.2.4.2.6. Market—Drawing conclusions from a structured consensus of persons.

5.2.4.3. We use many of these modes of reasoning every day, and there are analytical equivalents used in the process and mission of intelligence. However, bias remains one of the most common detractors in applying the modes of reasoning. Cognitive biases are mental errors caused by our simplified information processing strategies. When people reason, they employ various simplifying strategies and rules of thumb to ease the burden of mentally processing information to make judgments and decisions. "I always get

enchiladas at Mexican restaurants; the interstate is always faster; or I always get my news from an online news source." These simple rules of thumb may be acceptable for surviving the daily grind, but not for performing intelligence analysis. Analysts have to remain detached from normal survival biases and start fresh with each new problem.

5.2.4.4. Common types of cognitive biases include:

5.2.4.4.1. Bandwagon Effect—Tendency to believe something because many others believe it.

5.2.4.4.2. Clustering Illusion—Tendency to overvalue small runs, streaks, or clusters in large sets of data.

5.2.4.4.3. Confirmation Bias—Tendency to overvalue data supporting initial assumptions or expectations, and undervalue that which contradict.

5.2.4.4.4. Framing Effect—Tendency to draw different conclusions from the same data if it is presented differently.

5.2.4.4.5. Illusory Correlation—Belief that two events are related when they might not be.

5.2.4.4.6. Insensitivity to Sample Size—Tendency to underestimate the variation in data from small samples.

5.2.4.4.7. Mirror Imaging— Assumption that others see events and react to them just as we do.

5.2.5. Data Organization, Visualization, and Analytic Modeling.

5.2.5.1. As analyst Airmen begin to acquire information related to their intelligence question, either as part of a focused research effort or routine monitoring within their areas of responsibility, they need to employ a systematic approach to triaging and organizing information to identify trends, patterns, and relationships relevant to their intelligence question. The use of visualization techniques can assist analysts in deriving meaning from large volumes of fragmented information.

5.2.5.2. Visualization and analytic modeling are companion concepts to SATs. Effective visualization helps the analyst Airman analyze and reason about data and evidence. Analytic models can often help capture and expose knowledge, focus collection on the right needs, and apply analytics to the right questions. Visualization and analytic modeling apply to both the analytic process itself, and the delivery of information to consumers. Their importance was a key factor in establishing the analytic tradecraft standards of "effective visual information" by the IC and "utility" by the AF.

5.2.5.3. Like analysis, visualization and analytic modeling are both art and science. The advent of big data and data analytics has begun to emphasize the science and created the field known as data science. Data scientists find, interpret, and merge rich data sources; ensure consistency of data sets; create visualizations to aid in understanding data; build mathematical models using the data; and present and communicate data insights and findings to specialists, scientists and non-technical audiences.

5.2.6. Communication. Effective communication is essential to the craft of intelligence and even the best intelligence analysis falls short if communicated poorly. Consumers often

judge the validity of analysis by the quality of how it is communicated. The importance of communication is underscored by ICDs 203, 206, and 208 and AFI 14-133, which prescribe standards and principles for dissemination and require annual assessments for compliance. Analysts use multiple vehicles and formats to communicate their assessments to consumers.

5.2.6.1. Analytic Writing. Well-written products share a common set of attributes. First and foremost, good intelligence writing is analytic. That means, it does not simply report events; it explains the significance of those events and much more. Intelligence assessments are structured so that busy consumers can quickly grasp the main message and underlying reasoning, and be clear, precise, and convincing. In particular, analysts minimize the chance for misinterpretation of the findings, the certainty behind them, or how they were arrived at. Even the best analysis, if presented poorly, could cause the customer to question its credibility.

5.2.6.2. Visuals. Whereas data visualization during core research and analysis helps the analyst to "discover" the story, visualization for presentation helps "tell" the story. Visual presentation uses graphics—from charts and graphs to maps and complex tables, and both hardcopy and digital—to make relationships between data more easily understood.

5.2.6.3. Briefings. Briefings are a key mechanism for communicating analytic judgments to customers and can foster two-way communications to ensure that customer intelligence questions are addressed. Effective briefings consist of a well-organized, clear message relevant to the target audience; appropriate, tailored visual aids to reinforce the message; and a presentational style that keeps the audience focused on the message. Briefing is a skill that is honed through practice.

5.2.6.4. Multimedia Products. Significant innovations in multimedia tools have emerged that make possible sophisticated products that go beyond static graphical presentations. Multimedia products are generally either interactive or use full-motion video or animated web graphics to display content. Some techniques are particularly useful for depicting changes in data over time or comparing complex or multivariate data by allowing users to choose which variable they want to see. Despite these different ways to communicate analysis, the fundamentals remain the same: analysts need to present their analysis with clarity and sound logic.

5.2.7. Collaboration.

5.2.7.1. Similar to critical and creative thinking, collaboration is a skill that extends across the entire analysis process. Effective intelligence analysis depends on strong interpersonal relationships among analysts within and across intelligence agencies and the way the analysts relate to collectors, customers, and other experts within and outside the IC. Analysts are expected to collaborate and team to tackle complex intelligence questions, coordinate analytic products, and engage in regular discussions with colleagues that explore and challenge analytic judgements and prevailing assumptions. As one of the six AF intelligence analysis tenets, collaboration is considered a fundamental attribute and priority in AF analysis. Further, collaboration is the catalyst to every IC member's responsibility to "provide, discover, and request" as mandated in ICD 501.

5.2.7.2. An important aspect of collaboration and teaming is analytic outreach, which ICD 501 defines as the open, overt, and deliberate act of an IC analyst engaging with an individual outside the IC to explore ideas and alternate perspectives, gain new insights, generate new knowledge, or obtain new information. Outside experts include those in academics, business, non-governmental organizations, scientists, and others. Various methods of analytic outreach include conferences, seminars, exchanges, sabbaticals, and the building of trusted professional relationships.

5.2.7.3. Skills required for effective collaboration include employing tools to facilitate scheduling, access to data, and the sharing of analysis; effective team management practices; social networking techniques; constructive criticism—both giving and receiving; and interpersonal skills. Analysts need to also be aware of and take measures to avoid impediments to teaming, especially the "What's in it for me?" mindset. A study of the collaboration environment in the IC in 2007 identified six imperatives to help overcome such mindsets: mission criticality, mutual benefit, mutual trust, common understanding through common lexicon and transparent rules of the road, access and agility to identify collaborators and form collaborative communities, and incentives. **Note:** Derived from Integrated Concepts Development Office, *Achieving a Robust Collaborative Environment*.

5.2.8. Analytic Design. Analytic design is the activity of planning, managing, and executing the analysis process end-to-end—from the development of the right intelligence question, research, and core analysis to the crafting of an assessment that captures and communicates analytic insight for customers. Although analytic design is described last in this chapter's list of skills and tradecraft, it takes place up-front and then continues throughout the analysis process. In analytic design, the analyst outlines the plan for framing the question, applying SATs, reasoning and mitigating biases, organizing and visualizing data, communicating the analysis, collaborating with all applicable entities, and employing critical and creative thinking skills. Then, as the plan is put into action, the analyst revisits and revises the plan, as needed, to comprehensively address the requirement. More information on this subject is available at the following site: *ICAT-G/Products Analytic Design Portal*, Joint Worldwide Intelligence Communications System (JWICS) Caution-url: **https://intellipedia.intelink.ic.gov/wiki/Portal:IC_Analytic_Tradecraft_Gateway/Analytic_Design**.

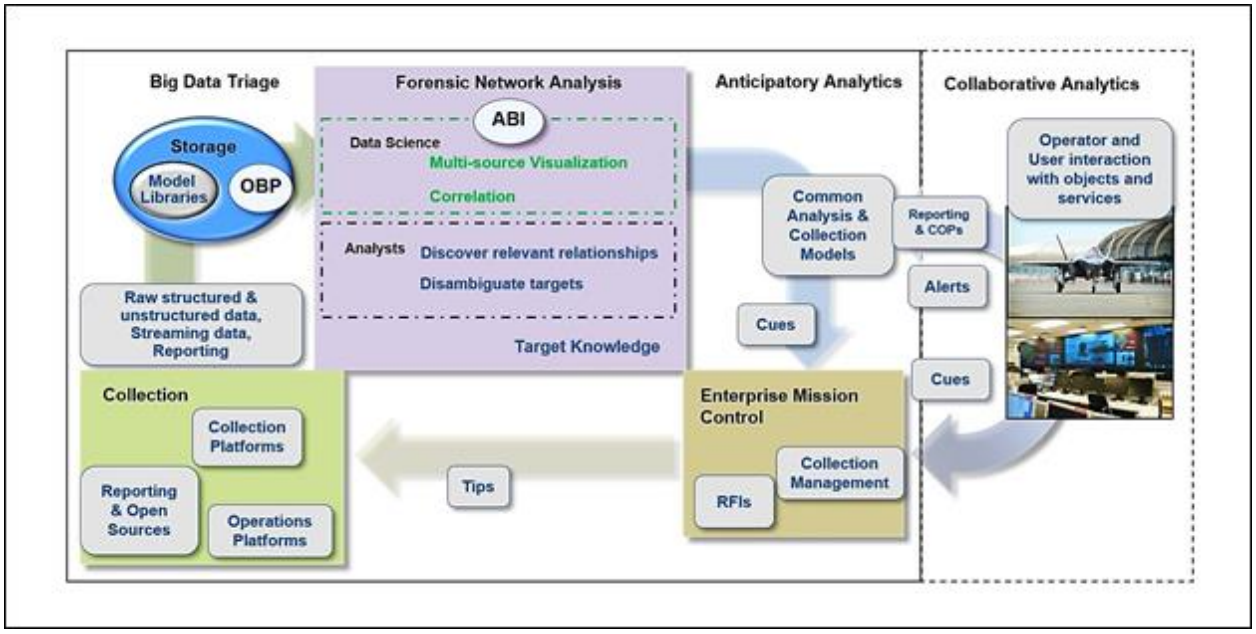
5.3. Key Analysis Concepts.

5.3.1. Big Data, Data Analytics and Data Science.

5.3.1.1. According to the *AF Future Operating Concept: A View of the AF in 2035*, the term big data describes large volumes of high-velocity, complex, variable data that require advanced techniques and technologies to enable the capture, conditioning, reliability, storage, distribution, management, and analysis of the information. The significance of big data extends beyond the sheer volume, complexity, and diversity of data; it is profoundly changing the way we think about data and creates new knowledge and information. **Note**: Paul B. Symon and Arzan Tarapore, "Defense Intelligence Analysis in the Age of Big Data," *Joint Forces Quarterly*, p. 4. Big data is driving us from a perspective of "causation" to one of "correlation." Rather than the traditional perspective of analyzing discrete amounts of data to understand the past cause and effect

(the why) and use that as a predictor of future behavior, data analytics enables analysts to harness the massive amounts of data available to draw correlations and use patterns of life (the what) as a predictor of future behavior, even if we do not understand "the why." **Note**: Kenneth Neil Cukier and Viktor Mayer-Schoenberger, "The Rise of Big Data: How It's Changing the Way We Think about the World," *Foreign Affairs*. Figure 5.5, *Data Analytics Framework*, depicts a general framework for data analytics.

Figure 5.5. Data Analytics Framework.



5.3.1.2. Data Science is at the heart of adapting the AF ISR Enterprise to the evolving big data environment. It can generally be described as the practice of exploiting and deriving valuable insights from data. This involves extracting knowledge from data sets that may be small, large, structured, multi-modal, multi-lingual, semi-structured or unstructured. Since data science is an inherently technical and specialized field, it is best performed by individuals trained and qualified in the complex and specialized nature of the work. As the DCS for ISR White Paper, *Data Science and the USAF ISR Enterprise* conveys, rather than train analyst Airmen to be data scientists, the AF approach is to develop a force of ISR professionals, operators, and knowledge managers that understand and leverage the capabilities that data scientists bring to the fight. Figure 5.5 highlights the role of data science relative to analysts in the process of data analytics.

5.3.1.3. The implications of big data, data analytics, and data science for intelligence analysis cannot be overstated. In recognition of this, the IC has embarked on a number of analytic modernization initiatives to exploit emergent big data capabilities, improve intelligence integration, and accelerate intelligence decision cycles. Two major initiatives are object-based production (OBP) and activity-based intelligence (ABI).

5.3.2. Object-Based Production (OBP).

5.3.2.1. Traditionally, analysts spend a great deal of time and effort assembling, collating, and parsing diverse data sources that pertain to a given intelligence problem.

As Figure 5.5 illustrates, OBP is a framework for organizing and sharing information. It is defined as the act of organizing intelligence around objects of interest—not by collection or data type—which allows users to aggregate intelligence information from across multiple intelligence domains and associate it with particular objects of interest. All intelligence that relates to something that physically exists in the real world is assembled and made centrally available as an object that all collectors, producers, and consumers can access. Objects include physical things (e.g., ships, buildings, vehicles, persons, and political boundaries), as well as abstract things (e.g., events and issues). The intent of OBP is to provide a consolidated perspective about the behavior of objects and their interaction with one another.

5.3.2.2. Traditionally, the output of each intelligence discipline is assembled by an analyst in order to understand the who/what/where/when of the object. The OBP alternative enables analysis to be directly attached to the object in question to allow delivery of complete find, fix, and track information direct to operational users. Thus, intelligence analysis is not stove-piped or the end result of a linear process. Instead, in this synthetic model, known information is dynamically assembled within the intelligence process. Automatic exploitation systems and manual intelligence analysis work in tandem to dynamically populate a shared community of objects that all analysts have access to. The result is that analysts can better understand intelligence activity by more clearly identifying and managing intelligence gaps and spending less time assembling information.

5.3.3. Activity-Based Intelligence (ABI).

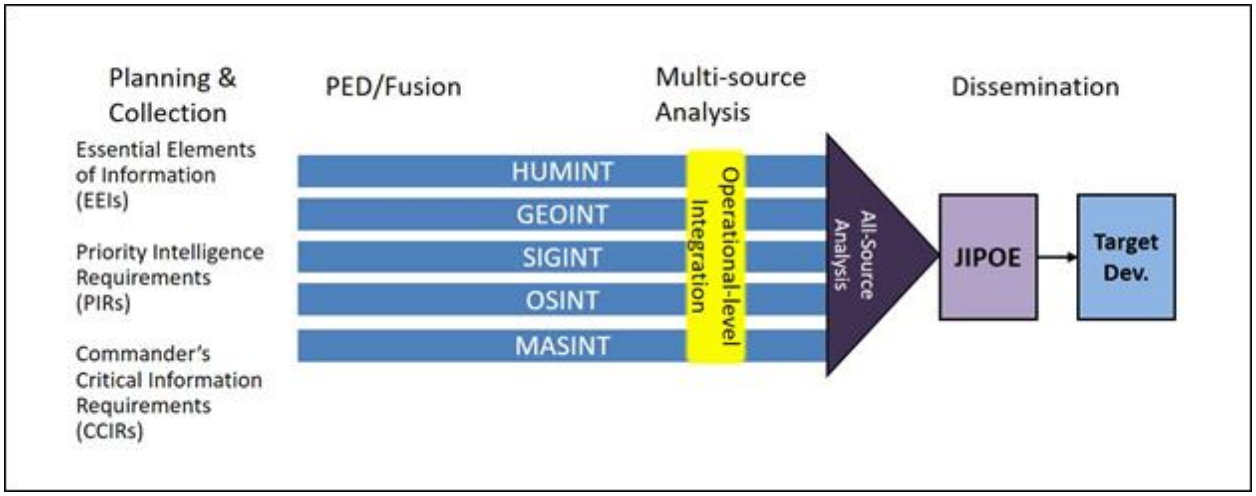
5.3.3.1. ABI emerged from the experiences of analysts working dynamic targets and analytic problems. It centers on the discovery and association of unknown activities. DIA, the National Geospatial-Intelligence Agency (NGA), and the National Security Agency (NSA) describe ABI as an analytic method applied to structured data from all sources, to discover objects (e.g., high-value target location), relationships (e.g., supplier/consumer), or behaviors (e.g., pattern of life) by resolving significant activity.

5.3.3.2. NGA has delineated four ABI tenants that apply to a variety of missions and problem-sets: 1) geo-reference to discover; 2) integration before exploitation; 3) data neutrality; and 4) sequence neutrality. As geo-referenced activity becomes the starting point of discovery, that allows for the rapid integration of multi-INT data and allows for analysis without data-source or sequence biases presented by the traditional linear collection process. Successful ABI analysis relies heavily on geo-referenced data that did not lend itself to an immediate application when it was collected, but eventually enhanced the larger context or provided more accurate characterization and understanding of data collected at a later date.

5.3.3.3. As ABI and OBP have grown to become IC-wide methodologies, NGA has advocated and developed a concept called Structured Observation Management (SOM). SOM is the practice and method of organizing and sharing multi-sensor data that is not focused on objects (e.g., activities or events), in order for the resulting data to be consistent with, and in support of, both ABI and OBP processes. It can be thought of as a 'bridge' between the new analytic processes of OBP and ABI.

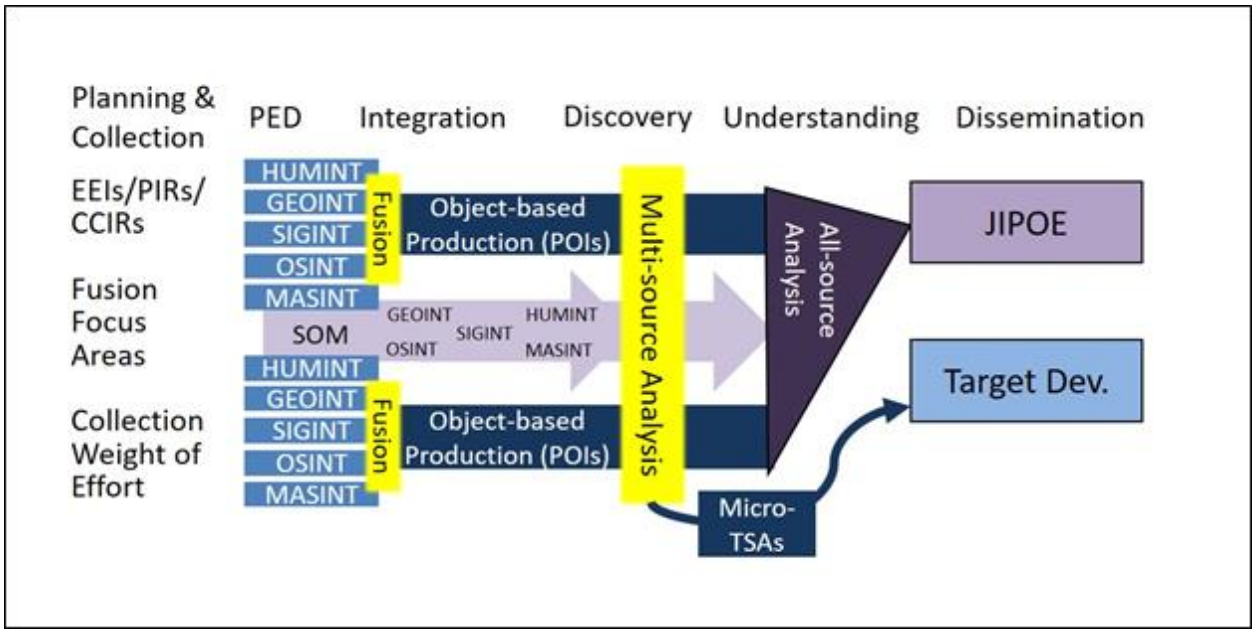
5.3.3.4. AF ISR analysts need to innovate to implement ABI in our mission sets. One such effort is Scoped Activity-based Intelligence for Nodal Targeting (SAINT), an ACC-developed capability that operationalizes ABI, predominantly in support of deliberate targeting. SAINT's strength lies in the rapid fusion of data and information to create multi-source intelligence as early in the intelligence cycle as possible, and close to the point of collection in order to enable collection refinement. Figure 5.6, *Traditional Model for Target Discovery*, depicts the traditional model of a linear production chain that combines to contribute to content-dominant analysis, a time-consuming approach to Joint Intelligence Preparation of the Operational Environment (JIPOE) and ultimately target development. In contrast, Figure 5.7, *ABI/OBP Integrated Model for Target Discovery*, highlights the SAINT construct, in which OBP enables fusion analysis and micro-target system analyses (TSAs) in a time-dominant environment. This model makes possible a symbiotic analysis/collections relationship to support strategic, operational, and tactical objectives simultaneously.

Figure 5.6. Traditional Model for Target Discovery.



Note: Source is Michael Kreuzer and Denis Dallaire, *Targeting the Islamic State: Activity-based Intelligence Empowering Air Force Targeting*.

Figure 5.7. ABI/OBP Integrated Model for Target Discovery.



Note: Source is Michael Kreuzer and Denis Dallaire, *Targeting the Islamic State: Activity-based Intelligence Empowering Air Force Targeting*.

5.4. Additional Tradecraft Resources.

5.4.1. IC Analytic Tradecraft Gateway (ICAT-G). The ICAT-G serves as a repository for the ICs collective knowledge of the analytic process, methods and techniques, and best practices. It is a useful, comprehensive reference aid for analysts and a valuable resource for analytic training. It is located on JWICS at Caution-url: **https://intellipedia/intelink.ic.gov/wiki/ICAT-G**.

5.4.2. Online Critical Thinking and Analysis Environment (OCTANE). OCTANE is a 25 AF online initiative for analysts to find mentors and exchange information through an analyst mentor network, practice tradecraft, compete with peers through IntelTrivia, and download free applications and games for use on mobile devices. The OCTANE site is on the Nonsecure Internet Protocol Router Network (NIPRNet) at **https://www.25afoctane.com**.

5.4.3. Center for Marine Expeditionary Intelligence Knowledge (CMEIK). The CMEIK is dedicated to advancing analytic tradecraft across the Marine Corps intelligence enterprise. The CMEIK offers courses, tradecraft notes, and video podcasts on a variety of analysis topics that are applicable to all military services. Several examples include a writing guide, SAT pocket guide, intelligence preparation of the battlespace template, and a collaboration page. CMEIK information is available on the SECRET Internet Protocol Router Network (SIPRNet) at Caution-url: **www.mcia.usmc.smil.mil/cmeik**.

Chapter 6

REQUIREMENTS AND PRODUCTION

6.1. Intelligence Requirements and Analytic Focus.

6.1.1. Questions, Requirements, and Customers.

6.1.1.1. Intelligence analysis and production are driven by leading questions or requirements for intelligence to fill a gap in knowledge or understanding of the environment, adversary capabilities, centers of gravity, or intentions. Questions may be more formal, such as Key Intelligence Questions (KIQs) from AF and IC Programs of Analysis (PoAs), or more informal, such as those that stem from direct, near-term support to operations. All questions are based on an intelligence organization's relationship with its customer and an understanding of customer needs.

6.1.1.2. Intelligence analysis and production are also driven by priorities at all levels of command, from the President of the United States down to the tactical level of operations. At the national- and IC-level, this primarily manifests itself in the National Intelligence Priorities Framework (NIPF).

6.1.2. National Intelligence Priorities Framework (NIPF**)**. Published annually and reviewed quarterly, the NIPF is the primary mechanism to establish, manage, and communicate national intelligence priorities. Guidance from the President and National Security Advisor determines overall priorities. Secretaries and cabinet-level heads of departments and agencies provide formal input to NIPF development. The DNI is responsible for developing and managing the NIPF. All IC activities, including those of the AF, adhere to the NIPF priorities. **Note:** See ICD 204, *National Intelligence Priorities Framework*, for NIPF policy and responsibilities.

6.1.3. Programs of Analysis (PoAs).

6.1.3.1. Per DNI direction, each IC member publishes an annual PoA to provide comprehensive analysis and production focus for their organization. Collectively, the IC PoAs offer a framework for collaboration with customers, stakeholders, and IC partners. The DNI has directed each IC organization to annually publish a PoA to provide comprehensive intelligence analysis and production focus for their organization.

6.1.3.2. The AF ISR PoA (AFISRPoA) is organized into broad, overarching analytic categories, each with multiple KIQs that represent the most pressing analysis required in each category. AF analysis organizations use these categories and KIQs to guide their analytic focus.

6.1.3.3. All PoAs are to reference NIPF priorities when possible. Additionally, a new DoD Integrated Defense Intelligence Priorities (IDIP) process is being implemented to identify and describe intelligence priorities for the diverse set of DoD customers: policy, operations, and acquisition. The IDIP is the DoD intelligence inject into the NIPF and provides an additional layer of data with traceability to analytic stakeholders. Analysts reference both the NIPF and IDIP for understanding of analysis and production priorities, and reference these priorities, when feasible, in development of respective AF intelligence products and services. Additionally, the IDIP can be used by analysts to help

frame internal resource and planning discussions across the Planning, Programming, Budgeting, and Execution (PPBE) cycle.

6.1.3.4. AFI 14-134 directs development of the AFISRPoA and sub-echelon PoAs for NASIC, and the 363 ISRW via 25 AF and ACC. The intent is for every major AF ISR production element to eventually develop its own PoA to focus on analysis priorities and production. The desired end-state resulting from the AFISRPoA and subordinate level PoAs would be a more unified AF ISR analysis and production enterprise.

6.1.3.5. JWICS Intellipedia lists and provides access to all AF and IC PoAs. A listing of associated AF ISR and IC PoAs resides on JWICS Intellipedia at Caution-url: **https://intellipedia.intelink.ic.gov/wiki/Programs_of_Analysis**. Analysts reference and leverage KIQs that are specific to their analysis mission area, enabling them to work toward common AF and IC goals, improve efficiency through elimination of redundant analytic efforts, and expand their collaboration both within and outside the AF.

6.1.4. Across the AF, DoD, and IC, various terms are used when referring to an intelligence question and/or requirement, including request for information (RFI), request for support (RFS), intelligence need, intelligence requirement, KIQ, and production requirement (PR). Henceforth, this publication will use RFI to refer to all types of intelligence questions and/or requirements. RFIs range from informal to formal and from verbal to formally documented requests. They originate from an intelligence customer (also called an intelligence consumer), which includes but is not limited to, operational units, acquisition organizations, national policy makers, other intelligence elements throughout the AF, DoD, and IC, and counterintelligence units, such as AFOSI. While RFIs may be explicitly stated, analysts anticipate and help shape RFIs, based on known mission needs and a thorough understanding of operations. Supervisors help ensure their analysts are able to engage with the customer, as needed.

6.1.5. Requirements deemed most important to mission accomplishment are identified as priority intelligence requirements (PIRs). By definition, these are the critical requirements that must be satisfied for a commander and staff to understand an adversary and the operational environment in order to successfully plan and conduct a mission. PIRs are general statements of intelligence need, such as, "What is the operational status of the adversary's integrated air defense system?" or "What terrorist groups are active within the area of interest?" PIRs provide the framework for prioritization of all GIISR operations within a CCMD. PIRs, combined with a commander's friendly force information requirements (FFIRs), constitute the commander's critical information requirements (CCIRs).

6.1.6. PIRs drive the development of detailed essential elements of information (EEIs). EEIs further define the commander's PIRs by outlining specific information requirements, such as, "What is the current location of the adversary SA-20 battalion?" The designation of PIRs and EEIs help ensure efforts are focused on critical information needed to support warfighters.

6.1.7. Priority requirements in acquisition intelligence are identified as critical intelligence parameters (CIPs). A CIP is a factor that defines the threshold at which the performance of a foreign system/capability would likely degrade or nullify the effectiveness of an acquisition program or details of a developmental U.S. system, the disclosure of which could allow an

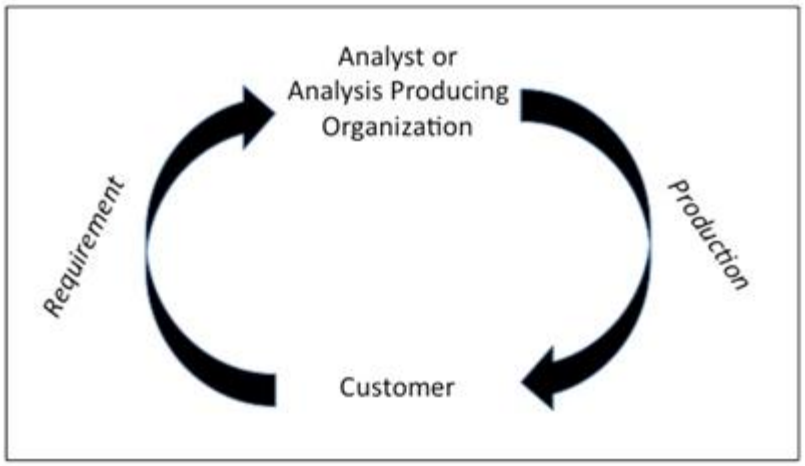
adversary to effect countermeasures to degrade mission effectiveness of the system, if it were to be fielded. CIPs are a key concept for an operational MAJCOM's requirements process/documents, as well as for an acquisition program. They are essentially a PIR for new capabilities going through the requirements and acquisition systems.

6.2. Intelligence Production .

6.2.1. Intelligence production is the development, tailoring, and presentation of intelligence knowledge via products and/or services that meet or address customer requirements. Production is an all-encompassing term that ranges from formal, published products on one end of the spectrum (e.g., a formal intelligence summary) to informal, impromptu updates on the other end (e.g., a location update on a tactical threat as a pilot steps to the aircraft). In some cases, analysts tailor existing intelligence to answer customer requirements. In other cases, analysts perform analysis on existing data, information, and intelligence to create new intelligence and knowledge. Still, in other cases analysts request collection of new data to consider in their analysis.

6.2.2. Ultimately, production culminates in at least one intelligence output for a customer, bringing the cycle full-circle, as depicted in Figure 6.1, *Requirement–Production Cycle*. An output may be an intelligence product or an intelligence service.

Figure 6.1. Requirement–Production Cycle.



6.2.3. An intelligence product is defined as tangible information in written, visual, digital, and/or verbal form that: 1) conveys information of intelligence value (e.g., written assessment, threat map, targeting materials, database, etc.); or 2) facilitates the accomplishment of an intelligence mission (e.g., assessment checklists, training folders, etc.). This definition is sufficiently broad to capture products that both directly and indirectly contribute to mission accomplishment, including those associated with intelligence analysis. The IC has established certain standards that products should meet. See Attachment 4 for a sample methodology and form to evaluate product standards.

6.2.4. An intelligence service is defined as assistance provided to another entity during the performance of ISR support, including: 1) the actual action of delivering or conveying intelligence to a user (e.g., presenting a briefing, tipping and cuing, collaboration, threat modeling, etc.); and 2) the process of enabling an ISR mission (e.g., exercise planning, skill

knowledge training, security clearance indoctrination, etc.). Some intelligence services result in additional intelligence products. Similar to intelligence products, this definition includes services associated with all categories of ISR mission accomplishment, one being intelligence analysis.

6.2.5. AF products and services are grouped into 14 product lines and 14 service lines. See Attachment 2 for descriptions of each product and service line.

6.3. Request for Information (RFI) and Analysis/Production Process . AFI 14-134 establishes and details the AF RFI and analysis/production process. Figure 6.2, *RFI and Analysis/Production Process*, illustrates the basic RFI flow that occurs at each organizational level. Figure 6.3, *RFI and Analysis/Production Process across the AFIAE*, depicts the flow across the whole analysis enterprise. The RFI and analysis/production process operationalizes the layered, distributed, mutually supporting AFIAE. It is the construct through which AF intelligence entities address customer requirements, share analytic findings, tap into analysis expertise across the IC, and collaborate on production. It is the mechanism that enables the AFIAE to achieve decision advantage. Refer to AFI 14-134, **Chapter 3** for specifics on the RFI process, categorization, tracking, and timelines.

Figure 6.2. RFI and Analysis/Production Process.

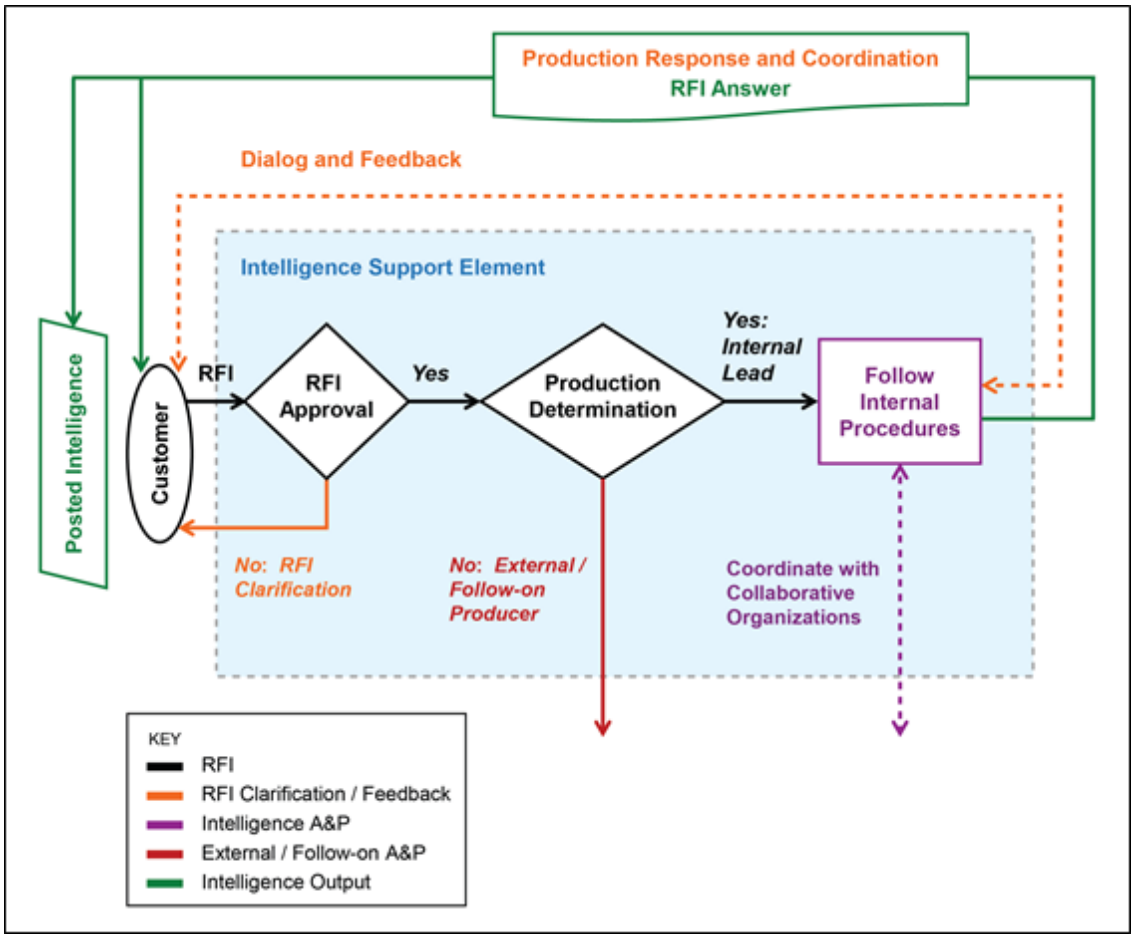
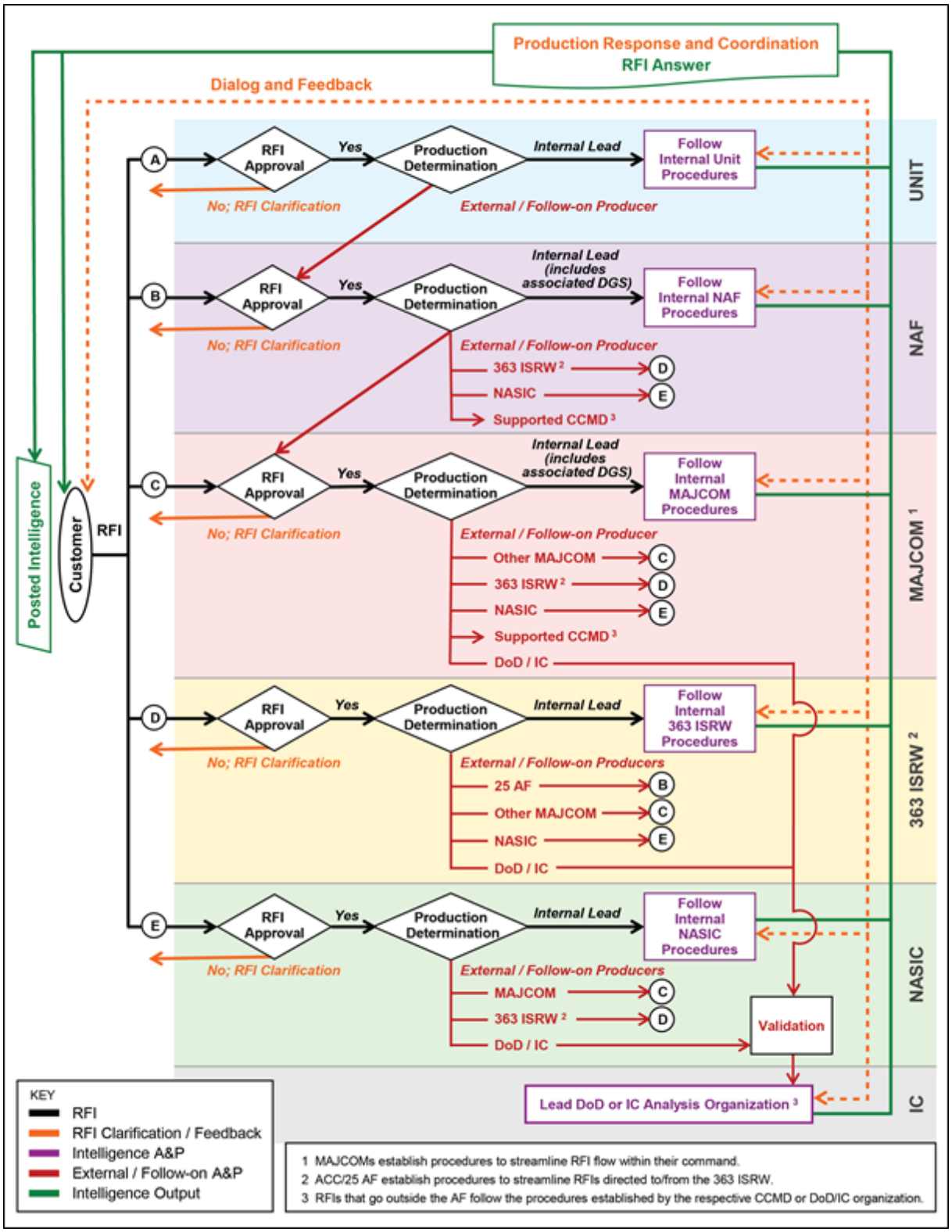


Figure 6.3. RFI and Analysis/Production Process across the AFIAE.



6.4. Acquisition Intelligence Production. Intelligence analysis and production are integral to the entire life cycle process of requirements definition, acquisition, and sustainment of weapon

systems. Acquisition customers require the production of specific threat assessments and potentially unique forms of data to support research, development, test and fielding of warfighting capabilities. Acquisition intelligence analysts support acquisition programs and initiatives by helping to identify and document intelligence dependencies (such as Intelligence Mission Data [IMD], modeling and simulation, etc.) that provide critical input to intelligence production efforts and the development of product/service requirements. As part of threat support to acquisition, NASIC and other service intelligence centers continually monitor and produce intelligence on adversary capabilities deemed critical to operational success for the developing capability. In partnership, acquisition intelligence specialists, operational command intelligence planners, and service intelligence center analysts provide direct support to acquisition decision processes, as defined in the *DIAP Users Guide* and DoD directives and instructions. These documents provide additional guidance for specific requirements and resourcing activities.

VERALINN JAMIESON, Lt Gen, USAF
Deputy Chief of Staff, Intelligence,
Surveillance, and Reconnaissance

Attachment 1

GLOSSARY OF REFERENCES AND SUPPORTING INFORMATION

References

Activity-Based Intelligence: Methods, Origins, Future, RAND, PR-1157-USCA, August 2014

ACWG Charter, 13 February 2015

AF Future Operating Concept: A View of the AF in 2035, September 2015, **http://www.af.mil/Portals/1/images/airpower/AFFOC.pdf**

AFCO-CFA Intellipedia Page, **https://intellipedia.intelink.gov/wiki/Air_Force_Cryptologic_Office_(AFCO)/CFA_Advanced_Analysis_and_Training**

AFI 33-360, *Publications and Forms Management*, 1 December 2015

AFI 90-1601, *Air Force Lessons Learned Program*, 18 December 2013

AFISRAI 14-153 Volume 3, 480 ISRW Supplement, *Air Force Distributed Common Ground System (AF DCGS) Operations Procedure*s, 5 February 2014

AFMAN 33-363, *Management of Records*, 1 March 2008

AFPD 14-1, *ISR Planning, Resources, and Operations*, 2 April 2004

ASA Certification site, JWICS Caution-url: **https://intelshare.intelink.ic.gov/sites/asacertification**

Center for Marine Expeditionary Intelligence Knowledge (CMEIK) site, SIPRNet Caution-url: **www.mcia.usmc.smil.mil/cmeik**

Assistant Director of National Intelligence (A/DNI) for Systems and Resource Analysis, *FY2017-2021 Major Issue Study Final Report Activity-Based Intelligence (ABI) Way Ahead*, May 2015

CFETP 14NX, Parts I and II, *AFSC 14NX Intelligence Officer Career Field Education and Training Plan*, 13 February 2013

CFETP 1N0X1, Parts I and II, *AFSC 1N0X1 All Source Intelligence Analyst Career Field Education and Training Plan*, 26 September 2016

DDII Analytic Integrity and Standards Group, *Applying the Intelligence Community's Analytic Tradecraft Standards: A Guide to Best Practices*, 2nd edition, September 2015

DDII Analytic Integrity and Standards Group, *Multi-INT Collection Source Description Guide: A Tradecraft Working Aid*, July 2005

DIA-01-1309-510, *DIA Style Manual for Intelligence Production 2017*, JWICS Caution-url: **https://intelshare.intelink.ic.gov/sites/ddii/mid/AIS/default.aspx**

DIAD 5000.200, *Intelligence Threat Support for Major Defense Acquisition Programs*, 1 Feb 2013

DIAI 5000.002, *Intelligence Threat Support for Major Defense Acquisition Programs*, 1 Feb 2013

DIAP Users Guide, January 2016

DNI Memorandum, *All-source Analysis Improvements*, 25 Aug 2015

DNI Memorandum, *Principles of Intelligence Transparency for the Intelligence Community*, 15 Jan 2015

DNI, *Principles of Intelligence Transparency for the Intelligence Community*, January 15, 2015

DoDD 5000.01, *The Defense Acquisition System*, May 12, 2003

DoDD 5105.21, *Defense Intelligence Agency (DIA)*, March 18, 2008

DoDD 5143.01, *Under Secretary of Defense for Intelligence (USD(I))*, October 24, 2014

DoDD 5205.12, *Military Intelligence Program*, November 14, 2008

DoDD 5250.01, *Management of Intelligence Mission Data (IMD) in DoD Acquisition*, January 22, 2013

DoDI 3115.17, *Management and Oversight of DoD All-Source Analysis*, November 16, 2016

DoDI 5000.02, *Operation of the Defense Acquisition System*, January 7, 2015

DoD Manual (DoDM) 3305.02, *DoD Collection Management Accreditation and Certification*, November 21, 2012

GEOINT Professional Certification site, **https://www.nga.mil/Careers/Pages/GEOINT-Professional-Certification.aspx**

IC Analysis Tradecraft Gateway, JWICS Caution-url: **https://intellipedia/intelink.ic.gov/wiki/ICAT-G**

IC Programs of Analysis, JWICS Caution-url: **https://intellipedia.intelink.ic.gov/wiki/Programs_of_Analysis**

ICD 104, *National Intelligence Program (NIP) Budget Formulation and Justification, Execution, and Performance Evaluation*, 30 April 2013

ICD 191, *Duty to Warn*, 21 July 2015

ICD 205, *Analytic Outreach*, 28 August 2013

ICD 208, *Maximizing the Utility of Analytic Products*, 9 January 2017

ICD 209, *Tearline Production and Dissemination*, 6 September 2012

Integrated Concepts Development Office, *Achieving a Robust Collaborative Environment*, May 2007

JLLIS Database, SIPRNet Caution-url: **https://www.jllis.smil.mil**

Johnston, Cathy, *Modernizing Defense Intelligence: Object Based Production and Activity Based Intelligence*, Briefing for DIA, 27 June 2013

Joint Capability Areas: JCA 2010 Refinement, 8 April 2011

Kreuzer, Michael, and Denis Dallaire, *Targeting the Islamic State: Activity-based Intelligence Empowering Air Force Targeting*, The Mitchell Institute for Aerospace Power, September 2016

National Intelligence Analysis Board, *Integrating the Analytic Enterprise*, October 2015

National Intelligence Priorities Framework, JWICS Caution-url: **https://intellipedia.intelink.ic.gov/wiki/NIPF**

NGA, *Activity-Based Intelligence (ABI) Concept of Operations: A 2015 Strategic Initiative*, Ver. 4.0, August 2015

NGA Briefing, *Object-Based Production (OBP) and Activity Based Intelligence (ABI)*, 19 November 2015

NGA Briefing, *Object Based Production (OBP) Basics*, 1 Nov 2013

ODNI Systems & Resource Analyses, *ABI Way Ahead*, JWICS Caution-url: **https://intelshare.intelink.ic.gov/sites/sramis/abi/default.aspx**

Online Critical Thinking and Analysis Environment (OCTANE), **https://www.25afoctane.com**

Quellfire Documentation, JWICS Caution-url: **https://intelshare.intelink.ic.gov/sites/quellfire/SitePages/ProgramDocumentation.aspx**

QUELLFIRE Object-Based Production Concept of Operations, V1.0, May 2013

QUELLFIRE Program Manager Briefing, *Changing the Way the Intelligence Community Shares Information: Object-based Production*, 20 February 2013

Schmidlin, LCDR William G, *Zen and the Art of Intelligence Analysis*, Joint Military Intelligence College, July 1993

Spellman, Barbara, "Individual Reasoning" in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, Baruch Fischhoff and Cherie Chauvin, Washington D.C., National Academies Press, 2011

Universal GEOINT Certification Program site,**https://usgif.org/certification**

USAF Strategic Master Plan, May 2015, **http://www.af.mil/Portals/1/documents/Force%20Management/Strategic_Master_Plan.pdf**

USD(I) Memorandum, *Strengthening Defense Intelligence Analysis*, May 21, 2016

Adopted Forms

AF Form 847, *Recommendation for Change of Publication*

Abbreviations and Acronyms

A/DNI—Assistant Director of National Intelligence

A&P—Analysis and Production

A2—Director of Intelligence

A2/AD—Anti-Access/Area Denial

ABI—Activity-Based Intelligence

ACC—Air Combat Command

ACIC—Army Counterintelligence Center

ACWG—Analysis Capability Working Group

AF—Air Force

AF NTI—Air Force National Tactical Integration

AFCO-CFA—Air Force Cryptologic Office Advanced Analysis & Training Branch

AFFOR—Air Force Forces

AFH—Air Force Handbook

AFI—Air Force Instruction

AFIAE—Air Force Intelligence Analysis Enterprise

AFISRAI—Air Force Intelligence, Surveillance, and Reconnaissance Agency Instruction

AFISRPoA—Air Force Intelligence, Surveillance, and Reconnaissance Program of Analysis

AFLCMC—Air Force Life Cycle Management Center

AFLLP—Air Force Lessons Learned Program

AFMAN—Air Force Manual

AFOSI—Air Force Office of Special Investigations

AFPD—Air Force Policy Directive

AFR—Air Force Reserve

AFRIMS—Air Force Records Information Management System

AFRL—Air Force Research Laboratory

AFSC—Air Force Specialty Code

AGILE—Advanced Global Intelligence Learning Environment

AIS—Air Intelligence Squadron

AMC—Air Mobility Command

AN—Anticipation

ANG—Air National Guard

AOC—Air Operations Center

AOR—Area of Responsibility

AS—Assessment

ASA—All-Source Analysis

BDA—Battle Damage Assessment

BOG—Board of Governors

Btn—Battalion

C-MAJCOM—Component MAJCOM

CAIAC—Civil Aviation Intelligence Analysis Center

CCIR—Commander's Critical Information Requirement

CCMD—Combatant Command

CCP—Consolidated Cryptologic Program

CFACC—Combined Forces Air Component Commander

CFETP—Career Field Education and Training Plan

CFLI—Core Function Lead Integrator

CGCIS—Coast Guard Counterintelligence Service

CGIS—Coast Guard Investigation Service

CIA—Central Intelligence Agency

CID—Criminal Investigation Command

CIP—Critical Intelligence Parameter

CMEIK—Center for Marine Expeditionary Intelligence Knowledge

CSA—Combat Support Agency

CTSAC—Critical Thinking and Structured Analysis Course

CY—Calender Year

CYBERCOM—Cyber Command

DART—Distributed Common Ground System Analysis and Reporting Team

DCGS—Distributed Common Ground System

DCS—Deputy Chief of Staff

DDII—Deputy Director of National Intelligence for Intelligence Integration

DE—Delivery

DEA—Drug Enforcement Agency

DHS—Department of Homeland Security

DI—Discovery

DIA—Defense Intelligence Agency

DIAAE—Defense Intelligence All-Source Analysis Enterprise

DIAD—DIA Directive

DIAI—DIA Instruction

DIAP—Defense Intelligence Analysis Program

DIRINT—Director of Intelligence

DNI—Director of National Intelligence

DoD—Department of Defense

DoDD—Department of Defense Directive

DoDI—Department of Defense Instruction

DoDM—Department of Defense Manual

DOE—Department of Energy

DOS—Department of State

DOTMLPF-P—Doctrine, Organization, Training, Materiel, Leadership and Education, Personnel, Facilities, and Policy

EEI—Essential Element of Information

EVE—Evaluation of Evidence

EX—Explanation

FAC—Framework for Analytic Cognition

FBI—Federal Bureau of Investigation

FFIR—Friendly Force Information Requirements

GDIP—General Defense Intelligence Program

GEOINT—Geospatial Intelligence

GIISR—Global Integrated Intelligence, Surveillance, and Reconnaissance

HPW—Human Performance Wing

HUMINT—Human Intelligence

IAW—In Accordance With

IC—Intelligence Community

ICAT-G—Intelligence Community Analytic Tradecraft Gateway

ICC—Intelligence Coordination Center

ICD—Intelligence Community Directive

ICS—Intelligence Community Standard

ID—Identification

IDIP—Integrated Defense Intelligence Priorities

IMD—Intelligence Mission Data

INSCOM—Intelligence and Security Command

INT—Intelligence

IRTPA—Intelligence Reform and Terrorism Prevention Act

ISR—Intelligence, Surveillance, and Reconnaissance

ISRD—Intelligence, Surveillance, and Reconnaissance Division

ISRW—Intelligence, Surveillance, and Reconnaissance Wing

ISSO—Intelligence Systems Support Office

JCA—Joint Capability Area

JCS—Joint Chiefs of Staff

JIDA—Joint Improvised-Threat Defeat Agency

JIOC—Joint Intelligence Operations Center

JIPOE—Joint Intelligence Preparation of the Operational Environment

JLLIS—Joint Lessons Learned Information System

JLLP—Joint Lessons Learned Program

JP—Joint Publication

JTF—Joint Task Force

JWICS—Joint Worldwide Intelligence Communications System

KIQ—Key Intelligence Question

LL—Lessons Learned

MAJCOM—Major Command

MASINT—Measurement and Signature Intelligence

MCIA—Marine Corps Intelligence Activity

Mgrs—Managers

MICF LANT—Maritime Intelligence Fusion Center Atlantic

MICF PAC—Maritime Intelligence Fusion Center Pacific

MICT—Management Internal Control Toolset

MIP—Military Intelligence Program

MOM—Motive, Opportunity and Means

MOSES—Manipulability of Sources

MQT—Mission Qualification Training

MSIC—Missile and Space Intelligence Center

NAF—Numbered Air Force

NAI2O—National Aviation Intelligence Integration Office

NASIC—National Air and Space Intelligence Center

NCIS—Naval Criminal Investigative Service

NCTC—National Counterterrorism Center

NGA—National Geospatial-Intelligence Agency

NGIC—National Ground Intelligence Center

NGP—National Geospatial-Intelligence Program

NIP—National Intelligence Program

NIPF—National Intelligence Priorities Framework

NIPRNet—Nonsecure Internet Protocol Router Network

NOFORN—Not Releaseable to Foreign Nationals

NRO—National Reconnaissance Office

NRT—Near-real-time

NSA—National Security Agency

NSC—National Security Council

NTI—National Tactical Integration

OBP—Object-Based Production

OCTANE—Online Critical Thinking and Analysis Environment

ODNI—Office of the Director of National Intelligence

ONI—Office of Naval Intelligence

OPR—Office of Primary Responsibility

OSINT—Open-Source Intelligence

OV-1—Operational Viewpoint-1

PACAF—Pacific Air Forces

PCPAD—Planning and Direction, Collection, Processing and Exploitation, Analysis and Production, Dissemination and Integration, Evaluation and Feedback

PED—Processing, Exploitation, and Dissemination

PIR—Priority Intelligence Requirement

PoA—Program of Analysis

POP—Past Opposition Practices

PPBE—Planning, Programming, Budgeting, and Execution

PR—Production Requirement

RDS—Records Disposition Schedule

RDT&E—Research, Development, Test, and Evaluation

RFI—Request for Information

RFS—Request for Support

RPA—Remotely Piloted Aircraft

RT—Real-time

SAC—Self-Assessment Communicator

SAINT—Scoped Activity-based Intelligence for Nodal Targeting

SAT—Structured Analytic Technique

SecDef—Secretary of Defense

SIGINT—Signals Intelligence

SIO—Senior Intelligence Officer

SIPRNet—SECRET Internet Protocol Router Network

SMC—Space and Missile Systems Center

SOC—Squadron Operations Center

SOM—Structured Observation Management

TRANSCOM—Transportation Command

TS/SCI—TOP SECRET/Sensitive Compartmented Information

TSA—Target System Analysis

TTPs—Tactics, Techniques, and Procedures

USA—U.S. Army

USAF—U.S. Air Force

USAFE-AFAFRICA—U.S. Air Forces in Europe & Air Forces Africa

USCG—U.S. Coast Guard

USD(I)—Under Secretary of Defense for Intelligence

USMC—U.S. Marine Corps

USN—U.S. Navy

Terms

Abductive Reasoning—The process of generating a novel hypothesis to explain given evidence that does not readily suggest a familiar explanation. Abductive reasoning starts from a set of accepted facts and creatively proposes their best explanation.

AF Intelligence Analysis Enterprise (AFIAE)—The global community of analyst Airmen and the AF ISR organizations that employ the core competency of intelligence analysis.

All-Source Analysis—Intelligence analysis that employs all available sources of data and information to enable the creation of new intelligence and knowledge.

Analysis Center—An organization with a predominant mission of all-source analysis. Analysis centers provide timely, accurate, and relevant intelligence analysis to support national and defense policymakers, warfighters, and the acquisition community.

Analysis Skill—A specific ability or collection of capabilities required to competently conduct analysis that is acquired through training and/or experience.

Analysis Tradecraft—An established or prescribed analysis technique, practice, or systematic process.

Analyst Airman—An AF ISR professional who is skilled and certified in tradecraft to perform the core competency of intelligence analysis.

Analytic Ombuds—Representative that is responsible for addressing organizational concerns regarding lack of objectivity, bias, politicization, or other concerns in the application of analysis and production standards.

Analytic Production Steward—Senior AF official designated to represent the analysis and production activities that their respective element is authorized to conduct, and to make determinations regarding the dissemination to or retrieval by authorized personnel of analysis produced by that activity.

Best Practice—A method or technique that has consistently shown results superior to those achieved with other means.

Big Data—A concept used to describe the explosion of available data as a result of the information environment.

Counterintelligence—Information gathered and activities conducted to identify, deceive, exploit, disrupt, or protect against espionage, other intelligence activities, sabotage, or assassinations conducted for or on behalf of foreign powers, organizations, or persons or their agents, or international terrorist organizations or activities.

Counterintelligence Analysis—The process of examining and evaluating information to determine the nature, function, interrelationships, personalities, and intent regarding the intelligence capabilities of a Foreign Intelligence Entity.

Covered Analytic Product—A subset of disseminated analytic products or services that is officially designated by the respective IC element as falling under the authority of ICD 206.

Critical Intelligence Parameter—A factor which clearly defines the threshold at which the performance of a foreign system/capability will likely compromise the program / mission effectiveness of the U.S. system.

Critical Thinking—The intellectually disciplined process of actively and skillfully conceptualizing, applying, analyzing, synthesizing, and/or evaluating information gathered from, or generated through observation, experience, reflection, reasoning, or communication, as a guide to belief and action.

Deductive Reasoning—Reasoning where a conclusion is a logical consequence of the premise. A deduction moves from general rules and some evidence to particular cases.

Defense Intelligence All-Source Analysis Enterprise (DIAAE)—The collective set of all DoD organizations that execute all-source analysis activities in production of defense intelligence.

Defense Intelligence All-Source Analysis Enterprise Board of Governors (DIAAE BOG)—A body comprised of representatives of the organizations of the DIAAE that provides a forum for issue identification and resolution; improving transparency and synchronization across the DIAAE; implementing DIAAE strategies and processes; providing support to the DoD Functional Manager for All-Source Analysis; and making resource recommendations based on changes to priorities and emerging requirements.

Essential Element of Information (EEI)—A specific information requirement that supports a more general Priority Intelligence Requirement (PIR).

Fusion Analysis (also called Time-Dominant Fusion)—Analysis in a time-sensitive environment in close proximity to the point of collection that entails quickly melding new information with baseline knowledge to meet a specific operational need. Emphasis is on the process of managing information and on timeliness over completeness.

Inductive Reasoning—The intellectual process of drawing generalizations on the basis of observations or other evidence. Induction takes place when one learns from experience.

Intelligence Analysis—A cognitive activity–both art and science–applying tools, processes, tradecraft, methods, and judgements to data and information to create and deliver new intelligence, insights, and knowledge, with the goal of providing a decision advantage to commanders and decision makers.

Intelligence Customer (also called Intelligence Consumer)—A requestor or user of intelligence, including an operational unit, an acquisition organization, a national policy maker, or an intelligence organization.

Intelligence Production—The development, tailoring, and presentation of intelligence knowledge via products and/or services that address customer requirements.

Intelligence Requirement—(also called Request for Information, Production Requirement, Request for Support, or Key Intelligence Question)—A need for intelligence to fill a gap in knowledge or understanding of the environment, adversary capabilities, centers of gravity, or intentions.

Intelligence Support Element—An AF intelligence organization at any echelon whose focus is on providing intelligence for AF planning, operation, or decisions.

ISR Activity—A task undertaken by a member of the ISR community that is associated with the accomplishment of an intelligence mission. An ISR Activity could result in one or more intelligence outputs. ISR Activities do not include tasks carried out by ISR personnel that are unrelated to a specific intelligence mission, such as security force augmentation, honor guard duty, professional military education, or physical training.

ISR Output—The result of an ISR Activity. An output is categorized as either an ISR product or an ISR service. Single or multiple outputs may derive from one activity, or one output could be derived from multiple Activities. All outputs relate directly or indirectly to the accomplishment of an intelligence mission.

ISR Product—A specific type of output from an ISR activity that consists of tangible information in written, visual, digital, and/or verbal form that conveys information of intelligence value (e.g., written assessment, threat map, and targeting materials) or facilitates the accomplishment of an intelligence mission (e.g., ISR program element code build, self-assessment checklist, or training folder).

ISR Service—A type of output from an ISR Activity. Assistance provided to another entity during the performance of an ISR mission: (1) the actual action of delivering or conveying intelligence to a user (e.g., presenting a briefing, tipping and cuing, collaboration, or threat modeling), or (2) the process of enabling an ISR mission (e.g., exercise planning, skill

knowledge training, or security clearance indoctrination). Some ISR Services result in additional ISR Products.

Key Intelligence Question—A strategic, high-level question that states the primary unknown, or information need, about an intelligence issue or problem, which subsequently drives intelligence analysis and/or production within an organization.

Lead/Designated Producer—The primary analysis and production organization responsible for integrating collaborative analysis with its own to provide a comprehensive and accurate intelligence product or service to a customer.

Lesson Learned—An observation that, when validated and resolved, results in an improvement in military operations or activities at the strategic, operational, or tactical level and in long-term, internalized change to an individual or an organization.

Multi-Source Analysis (also called Multi—INT Analysis)—Intelligence analysis that makes use of more than one source when access to additional potential sources is limited by reasons of timeliness, system access, location, or security levels.

Priority Intelligence Requirement (PIR)—A critical requirement that a commander and staff need to understand the adversary or operational environment to conduct the mission. A PIR is typically comprised of multiple, specific Essential Elements of Information (EEIs).

Production Response—An agreement between a lead/designated producer and a customer for the production of intelligence, containing sufficient detail to permit customer acceptance, rejection, or modification of the proposed intelligence output.

Service Intelligence Center—The analysis center designated for each military service. The AF has designated NASIC as the service intelligence center for the AF.

Single-Source Analysis (also called Exploitation)—Intelligence analysis that employs a single source or expertise in a functional area to characterize events, people, or things. Such analysis is limited to describing, rather than evaluating, the topic of a particular analysis due to restrictions inherent in single-source intelligence collection, precluding the ability to provide fully contextualized intelligence assessments.

Attachment 2

PRODUCT AND SERVICE LINES

A2.1. As Table A2.1, *Product and Service Line Categories*, illustrates, AF products and services are grouped into 14 product lines and 14 service lines, which can be further classified into four general categories: awareness; mission-specific; representation; and enabling. Sections A2.2 and A2.3 describe each product and service line.

Table A2.1. Product and Service Line Categories.

Category	Product Lines	Service Lines
Awareness	Intelligence Assessment Threat Study Intelligence Summary Intelligence Report Intelligence Alert	Analysis Situational Awareness Collaboration Intelligence Supportability Analysis
Mission Specific	Mission Document Targeting Document Requirement	Mission Operations Targeting Mission Readiness Operational Mission Training Requirements Management
Representation	Database Briefing Display Model	
Enabling	Policy, Plan or Program Mission Support Document	ISR Professional Training Policy, Planning, and Programming Force Management ISR Systems Security

Notes:
1. Some Product and Service Lines have similar labels. A good rule of thumb in distinguishing between them is that a Product Line is focused on a tangible output while a Service Line is focused on the action, process or function that results in the Product Line.
2. Product Lines include sanitized and releasable versions of products.
3. The scope, focus, and window of analysis decrease from Assessments to Alerts.
4. The Enabling category includes those products and services that indirectly contribute to substantive intelligence but, in and of themselves, do not have a primary purpose of

substantive intelligence.

A2.2. ISR Product Lines.

A2.2.1. **Intelligence Assessment** –Strategic, longer-term, analytical publication; focused on future capabilities and intentions; usually broad in military and/or political scope.

A2.2.2. **Threat Study** –Longer-term analysis that is more narrowly scoped than an assessment; usually focused on a threat system or category of threat systems; generally strategic or operational in scope.

A2.2.3. **Intelligence Summary** –Roll-up historical analysis of multiple events or missions; shorter timeframe than an assessment or a study (e.g., daily or weekly summary).

A2.2.4. **Intelligence Report** –Analysis from a single event or mission; includes results from a single-source intelligence collection; often associated with mission results; generally tactical or operational in scope.

A2.2.5. **Intelligence Alert** –High priority intelligence update with potential urgency and/or mission impact; usually focused on a singular threat or data point.

A2.2.6. **Database** –Systematically arranged collection of data, structured for convenient access and manipulation, generally in a computer.

A2.2.7. **Policy, Plan or Program** –Official ISR policy; guidance; plans; TTPs; research, development, test, and evaluation (RDT&E) efforts; agreements; and resourcing data, to include PPBE-related documentation.

A2.2.8. **Mission Document** –Text-based materials associated with conducting an ISR-specific mission or other air/space/cyber operational mission; does not include target materials.

A2.2.9. **Targeting Document** –Text-based analysis, reports, lists, or publications associated with targeting, weaponeering, or battle damage assessment (BDA); includes hard copy and soft copy formats; does not include target briefings or stand-alone target graphics.

A2.2.10. **Requirement** –A need for intelligence information, such as a request for information, a collection need, and essential mission information.

A2.2.11. **Mission Support Document** –Text-based materials that assist in the accomplishment of some enabling activities, such as training, exercises, conferences, security, and continuity.

A2.2.12. **Briefing** –Graphic-based presentation that is usually delivered verbally. Often times, a briefing is developed to visually summarize and verbally present the results of a text-based product (e.g., assessment, study, target document or mission support document). The most common form of a briefing is a Microsoft PowerPoint presentation.

A2.2.13. **Display** –Visual representation of analysis. Formats include maps, charts, videos, graphics, and diagrams. Displays are often incorporated into briefings or text-based products.

A2.2.14. **Model** –Physical representation of a threat or threat system or artificial representation of how a threat system will perform in actual operations.

A2.3. ISR Service Lines.

A2.3.1. **Analysis** –Services associated with the evaluation, interpretation, and often times integration of intelligence from available data sources and types. Includes the conduct of single-source, multi-source, and all-source analysis.

A2.3.2. **Mission Operations** –Services associated with the conduct of air/space/cyber operational missions, including ISR collection and processing, exploitation, and dissemination (PED) missions.

A2.3.3. **Situational Awareness** –Services provided to assist leadership and operators, including other ISR professionals, in comprehensively understanding the threat environment in which they are focused.

A2.3.4. **Intelligence Supportability Analysis** –The process by which intelligence, acquisition, and operations analysts identify, document and plan for requirements, needs, and supporting intelligence infrastructure necessary to successfully acquire and employ AF capabilities.

A2.3.5. **Targeting** –Services associated with the development of target materials, weaponeering, and BDA.

A2.3.6. **Mission Readiness** –Services that support the preparedness or capability of ISR or operational units to carry out their assigned missions.

A2.3.7. **ISR Professional Training** –Services involving the training and education of ISR personnel in ISR-related skills and tradecraft. Includes Mission Qualification Training (MQT) of ISR personnel.

A2.3.8. **Operational Mission Training** –Services associated with *threat-related* training of operational mission crews. Includes threat training for ISR personnel assigned to operational crews, such as cyber defense mission crews.

A2.3.9. **Requirements Management** –Services focused on managing ISR capability needs, requests for intelligence, and requests for assistance, forces, resources, or essential mission information.

A2.3.10. **Policy, Planning, and Programming** –Services involving the development of ISR policy, guidance, plans, TTPs, RDT&E efforts, agreements, and resource management, to include PPBE support.

A2.3.11. **Force Management** –Services associated with governing or guiding ISR manpower and personnel.

A2.3.12. **ISR Systems** –Services involving the establishment, accreditation, maintenance, and employment standards of ISR information technology systems.

A2.3.13. **Security** –Services associated with the protection, sanitization, and disclosure of classified information and with the establishment/maintenance of classified facilities.

A2.3.14. **Collaboration** –Services that explicitly facilitate the sharing of information both within and outside of the ISR community. While all Services involve "sharing information" to a certain extent, the Services in this Service Line are functions whose primary purpose is to share or exchange information.

Attachment 3

COMMON ANALYSIS LESSONS

A3.1. Table A3.1, *Common Analysis Lessons,* captures some of the general considerations broadly accepted across the AF ISR Enterprise and proven effective in improving analysis capabilities throughout time. Key sources for the lessons in this table include subject matter experts with extensive operational and tactical experience, various AF/A2 reviews of intelligence analysis, and a study by RAND Corporation. The table is organized by chapters in this handbook. The identification (ID) column refers to the AFH chapter associated with each lesson along with a unique alpha designator. To the right of the lessons are five columns that correspond to the five analysis activities: Discovery (DI), Assessment (AS), Explanation (EX), Anticipation (AN), and Delivery (DE). Those five columns indicate the primary (large, bold, upper-case X), secondary (standard, upper-case X), and tertiary (lower-case x) analysis activities associated with each lesson.

Table A3.1. Common Analysis Lessons.

ID	LESSON	ANALYSIS ACTIVITIES				
Chp 2	**AF Intelligence Analysis Enterprise (AFIAE)**	**DI**	**AS**	**EX**	**AN**	**DE**
2A	Increase your knowledge of different analytic and PED organizations to best understand AF ISR capabilities, enhance your network, and improve your tradecraft.	**X**	x	x		
2B	Be knowledgeable of air/space/cyber power strategy and theater objectives to help your assessment of developments.		**X**			
2C	Understand the larger context of the theater, problem set, or operation in which you are focused—applies to all analysts.	**X**				
2D	Check with area of responsibility (AOR) analysts to help collaborate your assessment of activities in that theater.		**X**			
2E	Coordinate with theater-specific and 363 ISRW targeteers for full understanding of your target and assessments.		**X**			
2F	Become familiar with different theaters to widen your expertise.			**X**		
2G	Continually balance timely notification to decision makers in support of operations against more in-depth and deliberate analysis/assessments.				**X**	
Chp 3	**IC and other Military Service Capabilities**	**DI**	**AS**	**EX**	**AN**	**DE**
3A	Gain Joint experience at a regional JIOC for improved & integrated analysis.			**X**	X	
3B	Seek out assignments in or deployments to an operational AOR to deepen and broaden your analysis expertise.			**X**	X	

3C	Be aware of U.S. military and theater capabilities and those of coalitions to enhance your analysis.			**X**		
3D	Prepare for future operations in a communications-contested environment; use/build resident capabilities prior to any deployment or operation.	x	x	x	**X**	x
3E	Enhance your Open-Source Intelligence (OSINT) expertise and understanding of IC-wide OSINT capabilities and organizations to leverage during crisis operations and to enhance your analytic prowess.	**X**				
3F	Improve your network with special operations ISR personnel for enhanced interface in-theater.		**X**	x	X	
Chp 5	**Analysis Skills and Tradecraft**	**DI**	**AS**	**EX**	**AN**	**DE**
5A	Leverage IC and joint programs that train, develop, and/or equip analysts to properly use tradecraft and provide better analysis.	x	x	**X**	X	x
5B	Participate in AF and Joint exercises to help sharpen analytic and joint awareness skills prior to an operational deployment.		x	**X**	X	
5C	Expand expertise and analytic skills beyond traditional warfare constructs to also be familiar with irregular warfare and non-traditional enemies.	**X**	x	x		
5D	Develop a network for improved collaboration/Red Teaming in different theaters.		x	**X**	X	
5E	Leverage theater and target-specific linguists as a good source to Red Team analysis, especially given adversary insights.		x	**X**	X	
5F	Leverage expertise and skills from multiple disciplines including scientists, engineers, space and cyber professionals, meteorologists, and the medical community for effective intelligence analysis.	x	x	**X**	X	
5G	Understand knowledge management, data science, and big data analytic concepts and principles for improved data aggregation.			**X**	X	
5H	Don't become influenced/infatuated with a particular sensor or source; cross-reference/check with multiple sources.	**X**				
Chp 6	**Analysis Requirements and Production**	**DI**	**AS**	**EX**	**AN**	**DE**
6A	Educate customers on AF ISR capabilities so they can help provide the best analysis possible to meet existing requirements.					**X**
6B	Understand what products are currently available and who is already working on/analyzing similar requirements to ensure unity of purpose and avoid duplication of effort.	**X**				
6C	Understand basic acquisition-/IMD-related intelligence requirements to help better align assessments in support		**X**			

	of respective customers.					
6D	Prepare now for the operations and warfare of tomorrow; expect contingency operations to occur in your area of analytic expertise and pre-plan against your analytic target with pre-positioned RFIs, target identification, etc.	x			**X**	
6E	Coordinate/interface often with resident collection managers on assessments and proposed collection strategies.	x	**X**		X	
6F	Enhance your ability to assess risks associated with commander estimates and plans (e.g., operational plans, contingency plans, etc.) for improved utility and interface with traditional operations.		**X**			
6G	Always consider the commander's intent, end state, definition of success, and the potential adversary centers of gravity when performing analysis.			x	**X**	
6H	Develop the analysis/assessment then take a final "step back" to review again from a strategic mindset and perspective.		x	**X**		
6I	Strive to produce assessments that are releasable and only make products/services “Not Releaseable to Foreign Nationals (NOFORN)” or caveated when required.					**X**

Notes:
1. The list is not intended to be comprehensive or all inclusive, nor is it intended to serve as a checklist that analyst Airmen are expected to meet. The aim is for analyst Airmen and analysis organizations across the AF to refine and expand the list over time.
2. Key sources for the lessons learned in this table include subject matter experts, various AF/A2 reviews of intelligence analysis, and a study by RAND Corporation: Brien Alkire, et al., *Leveraging the Past to Prepare for the Future of Air Force Intelligence Analysis*, RR-1330-AF.

A3.2. Some of the intelligence analysis lessons in Table A3.1 have been formally documented in some form or fashion via the AF Lessons Learned (LL) Program (AFLLP). The AFLLP exists to enhance readiness and improve combat capability by capitalizing on the experiences of Airmen and organizations. A lesson learned is an observation that, when validated and resolved, results in an improvement in military operations or activities at the strategic, operational, or tactical level and in long-term, internalized change to an individual or an organization. The AFLLP is part of the larger Joint Lessons Learned Program (JLLP). The Joint LL Information System (JLLIS) is used to track and disseminate LLs throughout the AF, DoD, and IC. JLLIS allows AF personnel to search, submit, and manage all AF Observations, Lessons Identified, After Action Reports, LLs, and other information up to TOP SECRET/Sensitive Compartmented Information (TS/SCI). The JLLIS database is located at SIPRNet Caution-url: **https://www.jllis.smil.mil**. All analyst Airmen are encouraged to register in JLLIS and enter observations that contain potential lessons into JLLIS for coordination through the AFLLP and/or inform their local chain of command as appropriate.

A3.3. In addition, several MAJCOMs actively acquire lessons learned or best practices. For example, HQ ACC/A2OO (Weapons and Tactics) has established a program to capture lessons learned, TTPs, and experience from ISR professionals returning from deployments.

Attachment 4

SAMPLE STANDARDS EVALUATION METHODOLOGY

A4.1. IAW AFI 14-133, MAJCOM/A2s and the NASIC/CC are responsible for developing a means to annually measure and assess AF intelligence analysis standards via SACs for reporting in the MICT. In addition, the DNI requires the AF to annually evaluate specified "covered products" for compliance with IC standards. Table A4.1, *IC Product Evaluation Criteria and Rating Scales*, delineates IC analytic tradecraft standards for use in assessment and "covered product" evaluations. The JWICS Advanced Global Intelligence Learning Environment (AGILE) offers computer-based training on how to conduct product evaluations. It is important to note that while AF tradecraft standards align with IC standards, the AF evaluates two additional standards: timeliness and customer engagement. Table A4.2, *Sample Tradecraft Criteria for Timeliness*, and Table A4.3, *Sample Tradecraft Criteria for Customer Engagement*, offer considerations for self-assessment on these two additional AF standards.

Table A4.1. IC Product Evaluation Criteria and Rating Scales.

Reviewer		Objective	1. Yes	2. No
Date of Review		Independent of political consideration	☐ Yes	☐ No
Product Name		Timely	☐ Yes	☐ No
Product ID Number		Based on all available sources of intelligence	☐ Yes	☐ No

1. Properly describes quality and credibility of underlying sources, data, and methodologies			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Largely lacks sourcing or describes reporting base, data, or methodologies only vaguely; **OR** ☐ Misidentifies or misrepresents cited reporting, data, or methodologies.	☐ Contains basic, generic descriptions of cited reporting, data, or methodologies; **BUT** ☐ Provides little detail on factors that may affect the quality and credibility of underlying sources, data, or methodologies.	☐ Contains at least basic, generic descriptions of cited reporting, data, or methodologies; **AND** ☐ Provides considerable detail on factors that may affect the quality and credibility of underlying sources, data, or methodologies.	☐ Satisfies "good" criteria; **AND** 1. Identifies which sources are most important to major analytic judgments; **OR** ☐ Provides additional detail about sources, data, or methodologies that provides insight into their contribution to the analysis.
Comment:			

2. Properly expresses and explains uncertainties associated with major analytic judgments			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Does not indicate levels of uncertainty associated with major analytic judgments; **OR** ☐ Indicates levels of uncertainty associated with major analytic judgments that are inconsistent with the basis ascribed to them.	☐ Indicates levels of uncertainty associated with major analytic judgments; **BUT** ☐ Does not explain their basis (e.g., by reference to strengths and weaknesses of the information base, contrary reporting, assumptions, or the nature of the judgment).	☐ Indicates levels of uncertainty associated with major analytic judgments; **AND** ☐ Explains their basis (e.g., by reference to strengths and weaknesses of the information base, contrary reporting, assumptions, or the nature of the judgment).	☐ Satisfies "good" criteria; **AND** **1.** Provides especially thorough discussion of nature and sources of uncertainties affecting major analytic judgments; **OR** ☐ Identifies indicators that, if detected, would alter levels of uncertainty associated with major analytic judgments.
Comment:			

3. Properly distinguishes between underlying intelligence information and analysts' assumptions and judgments			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)

☐ Does not distinguish among statements that convey underlying information, assumptions, and judgments.	☐ Sometimes distinguishes among statements that convey underlying information, assumptions, and judgments; **OR** ☐ Does not explicitly state assumptions that serve as linchpins of an argument or bridge key information gaps.	☐ Consistently distinguishes among statements that convey underlying information, assumptions, and judgments; **AND** ☐ Explicitly states assumptions that serve as linchpins of an argument or bridge key information gaps.	☐ Satisfies "good" criteria; **AND** 1. Identifies indicators that, if detected, could validate or refute judgments or assumptions; **OR** ☐ Explains the implications for judgments if assumptions are incorrect.
Comment:			
4. Incorporates alternative analysis			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Does not present alternatives when uncertainties, complexity, or low probability / high impact situations warrant their inclusion.	☐ Presents alternatives when uncertainties, complexity, or low probability / high impact situations warrant their inclusion; **BUT** ☐ Does not explain the evidence and reasoning that underpin them or discuss their likelihood or implications related to U.S. interests.	☐ Presents alternatives when uncertainties, complexity, or low probability / high impact situations warrant their inclusion; **AND** ☐ Explains the evidence and reasoning that underpin them; **AND** ☐ (c) Discusses their likelihood or implications related to U.S. interests.	☐ Satisfies "good" criteria; **AND** ☐ Identifies indicators that, if detected, would affect the likelihood of any identified alternatives.
Comment:			
5. Demonstrates customer relevance and addresses implications			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Provides little or no information or analysis beyond what is generally known; **OR** ☐ Does not respond adequately to a specific tasking.	☐ Provides useful information and analysis but does not address implications; **OR** ☐ Does not address an important issue or question raised by the analysis; **OR** ☐ Satisfies a specific tasking only partially.	☐ Provides useful information and analysis and addresses near-term, direct, or first-order implications; **AND** ☐ Adds value by addressing at least one of the following: trends or prospects, appropriate context, insight gained from synthesizing a large volume of information, warning of threats to U.S. interests, or factors affecting opportunities for U.S. actions (without prescribing U.S. policy); **OR** ☐ Satisfies a specific tasking fully.	☐ Satisfies "good" criteria; **AND** ☐ Assesses longer-term, indirect, or second-order implications; **OR** ☐ Provides exceptionally expert analysis (e.g., by drawing on multiple disciplines or presenting illuminating comparisons); **OR** ☐ Warns of threats in detail (e.g., by discussing specific indicators, likelihood, or imminence); **OR** ☐ Analyzes in detail factors affecting opportunities for U.S. action (e.g., by discussing risks, benefits, or possible reactions to potential U.S. actions).
Comment:			
6. Uses clear and logical argumentation			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Lacks a main analytic message; **OR** ☐ Does not support analytic judgments with relevant evidence or undermines them by using flawed logic; **OR**	☐ Presents a main analytic message; **BUT** ☐ Does not combine evidence, context, and assumptions effectively to support analytic judgments or uses weak logic; **OR**	☐ Presents a prominent and clear main analytic message; **AND** ☐ Presents clear reasoning with no flaws in logic and effectively combines evidence, context, and	☐ Satisfies "good" criteria; **AND** ☐ Addresses any inconsistent or contrary information in a way that reconciles it with analytic judgments; **OR** ☐ Demonstrates notable skill or sophistication in combining evidence, context, and assumptions convincingly to

☐ Often uses unclear language or uses a structure that is not easily understood.	☐ Sometimes uses unclear language or a structure that at times is not easily understood.	assumptions to support analytic judgments; **AND** ☐ Uses clear language and a structure that displays a logical flow appropriate for the argument being presented.	support analytic judgments.
Comment:			

7. Explains change to or consistency of analytic judgments			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Does not note or explain that a major analytic judgment differs from previous production.	☐ Does not note that a major analytic judgment is consistent with previous production; **OR** ☐ Notes how a major analytic judgment compares with previous production but does not explain how new information or reasoning supports changing or maintaining an existing analytic line.	☐ Notes how a major analytic judgment compares with previous production and explains how new information or reasoning supports changing or maintaining an existing analytic line.	☐ Satisfies "good" criteria; **AND** ☐ Highlights and explains how a major analytic judgment compares with judgments on the topic held within the U.S. intelligence community, not just within the same analytic element.
Comment:			

8. Makes accurate judgments and assessments			**Harvest Date:**		
Phase 1			**Phase 2:** Often accuracy cannot be evaluated until a later date. Establish a "harvest" date to revisit the assessment to evaluate Phase 2.		
☐ Unclear	☐ Conditioned	☐ Unconditioned	☐ Accurate	☐ No Accurate	☐ Indeterminate
☐ Judgment or assessment is not expressed clearly.	☐ Judgment or assessment is expressed clearly and is conditioned (e.g., by an "if/then" statement).	☐ Judgment or assessment is expressed clearly and is not conditioned (e.g., by an "if/then" statement).	☐ Judgment or assessment is found to be accurate.	☐ Judgment or assessment is found to be not accurate.	Accuracy could not be determined for any of several reasons: ☐ Nature of judgment or assessment prevented assessment of accuracy. ☐ Data needed to assess accuracy were not found. ☐ Irreconcilable views among evaluators prevented agreement on a final assessment of accuracy.
Comment:					

9. Incorporates effective visual information where appropriate			
☐ Poor (0)	☐ Fair (1)	☐ Good (2)	☐ Excellent (3)
☐ Does not use visual information when its use would have substantially complemented or enhanced an analytic product; **OR** ☐ Presents visual information that is inconsistent with or not pertinent to the text of an analytic product, or that confuses or detracts from an analytic product's presentation.	☐ Presents visual information that is pertinent to an analytic product; **BUT** ☐ Does little to clarify (illustrate, summarize, or provide greater detail), complement, or augment data or analytic points in an effective manner that enhances customer understanding of a product's analysis.	☐ Presents visual information that is pertinent to an analytic product; **AND** ☐ Clarifies (illustrates, summarizes, or provides greater detail), complements, or augments data or analytic points in an effective manner that enhances customer understanding of a product's analysis.	☐ Satisfies "good" criteria; **AND** ☐ Takes particularly effective advantage of visual presentational methods to convey data or analytic points in a way that enhances a product's value by making complex issues more understandable, adding insight or perspective, increasing knowledge retention, or highlighting trends, drivers, or indicators.
Comment:			

General Comments:
If an evaluator determines that a standard is **not applicable**, *it should be noted, with a justification, in the comment box.*

Table A4.2. Sample Tradecraft Criteria for Timeliness.

1. Poor (0)	2. Fair (1)	3. Good (2)	4. Excellent (3)
5. ISR element fails to provide analysis products and services in sufficient time to impact planning, operations, and decision-making	6. ISR element timeliness in providing analysis products and services marginally impacts planning, operations and decision-making	7. ISR element provides analysis products and services in sufficient time to impact planning, operations, and decision-making	8. ISR element provides analysis products and services at the earliest time and place to enable decision advantage and create significant mission and capability opportunities
Comment:			
Note: AF intelligence analysis is timely to impact planning, mission objectives, operations and to otherwise aid in commanders' decisions. Analysts are responsible for engaging with customers and end-users of intelligence to understand what they need and when they need it in order to deliver information and knowledge at the earliest time and place to enable customers to effectively make decisions and take action. Timeliness is about ensuring awareness, creating opportunities, and enabling warfighting decision advantage.			

Table A4.3. Sample Tradecraft Criteria for Customer Engagement.

1. Poor (0)	2. Fair (1)	3. Good (2)	4. Excellent (3)
1. ISR element has limited engagement with the customer to understand their requirements or seek feedback on product/service timeliness or utility	2. ISR element requests and responds to customer feedback for some, but not all, products and services	3. ISR element requests and responds to customer feedback for all products and services	4. ISR element satisfies "good" criteria; **AND** 5. Regularly engages with the customer to anticipate their requirements by understanding their operations, listening to their questions and concerns, and identifying intelligence needs to support documented capabilities and concepts; **AND** **6.** Has a formal engagement program established
Comment:			
Note: Analysis fully address customers' requirements within the time constraints and in a manner most useful. Analyst Airmen are responsive to customer feedback. While challenging to evaluate, this tradecraft standard is foundational to AF intelligence analysis.			

Attachment 5

AF ISR SAT TRADECRAFT GUIDE

A5.1. The following 19 figures are excerpts from an AF tradecraft guide on SATs, developed by AFCO-CFA. The figures offer insight into some, but not all, of the key SATs used in intelligence analysis to help improve tradecraft standardization across the AFIAE.

Figure A5.1. Imagination Techniques and Indicators.

IMAGINATION TECHNIQUES AND INDICATORS

Core Techniques	Description	When to Use
Structured Brainstorming	A group process for generating new ideas and concepts	Used to stimulate new thinking and generate a range of hypotheses about an issue
Red Team	A function executed by trained, educated, and practiced team members that provide an independent capability to fully explore alternatives from the perspectives of partners, adversaries, and others	Used to fully explore alternatives in plans, operations, concepts, organizations and capabilities in the context of the operational environment
Alternative Futures Analysis	Tool to help analysts explore multiple ways a situation can develop when there is high complexity and uncertainty	Mostly used when a situation is viewed as too complex or the outcomes are too uncertain to trust a single outcome assessment
Outside-In Thinking	Analytical tool used to identify the full range of basic forces, factors and trends that would indirectly shape an issue	Used to identify all the critical, external factors that could influence how a situation will develop

Figure A5.2. Structured Brainstorming.

STRUCTURED BRAINSTORMING

A technique for stimulating new thinking. It can be applied to virtually all of the other structured analytic techniques and allows the analyst to see a wider range of factors that might bear on the topic.

Brainstorming Ground Rules

1. Never criticize an analyst's ideas
2. Allow sufficient time to brainstorm
3. Involve at least one "outsider" in the process

Divergent Thinking Phase

1. "Post-It" note exercise

Convergent Thinking Phase

1. Arrange notes by commonalities to form clusters
2. Some notes may be moved or copied as cluster form
3. Select a word or phrase that characterizes each cluster
4. Identify any notes that do not fit with others and consider them useless noise or the beginning of an idea that deserves further attention (wild cards)
5. Select one or two areas that deserve the most attention
6. Set priorities based on consensus and decide on the next steps for analysis

Figure A5.3. Red Team Analysis.

RED TEAM ANALYSIS

Function executed by trained, educated, and practiced team members to provide commanders an independent capability to fully explore alternatives in plans, operations, concepts, organizations, and capabilities in the context of the operational environment and from the perspectives of partners, adversaries, and others.

Red Team Techniques

1. Team puts themselves into the adversary's circumstance and reacts as the adversary would
2. Assessments are not coordinated with anyone outside the team
3. Develop set of "first person" questions
4. Draft policy papers in which the group makes decisions, proposes recommendations, or develops courses of action
5. Present analysis in the first-person format
6. Avoid use of caveats or qualifications
7. Focus on a prediction based on the adversary's world
8. Do not plot out all possible courses of action

Figure A5.4. Alternative Futures Analysis.

ALTERNATIVE FUTURES ANALYSIS

An imaginative technique that systematically explores multiple scenarios. This technique can be used when a situation's uncertainty and complexity require consideration of more than one outcome.

Six-Step Process

1. Develop a focused issue and intelligence question
2. Identify drivers, forces, factors, and variables that can affect the issue
3. Select the two most critical and uncertain drivers
4. Establish plausible endpoints for each driver
5. Form a futures matrix by crossing the two axes. The resulting quadrants are the basis for alternative future scenarios
6. Build narratives that describe these futures and how they might come to be (Signposts or Indicators can then be developed)

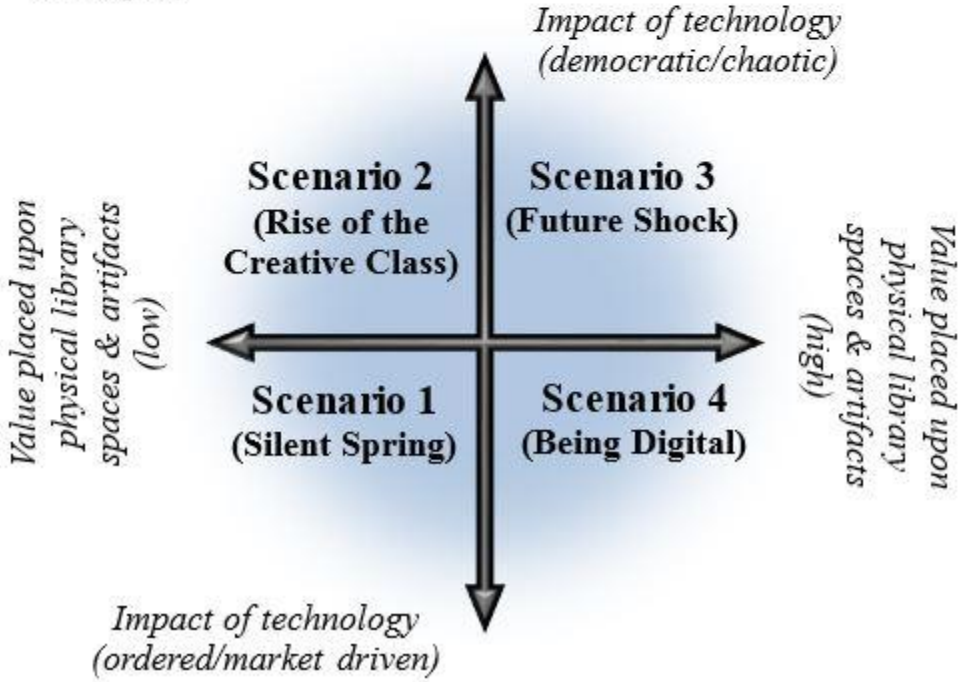


Figure A5.5. Outside-in Thinking.

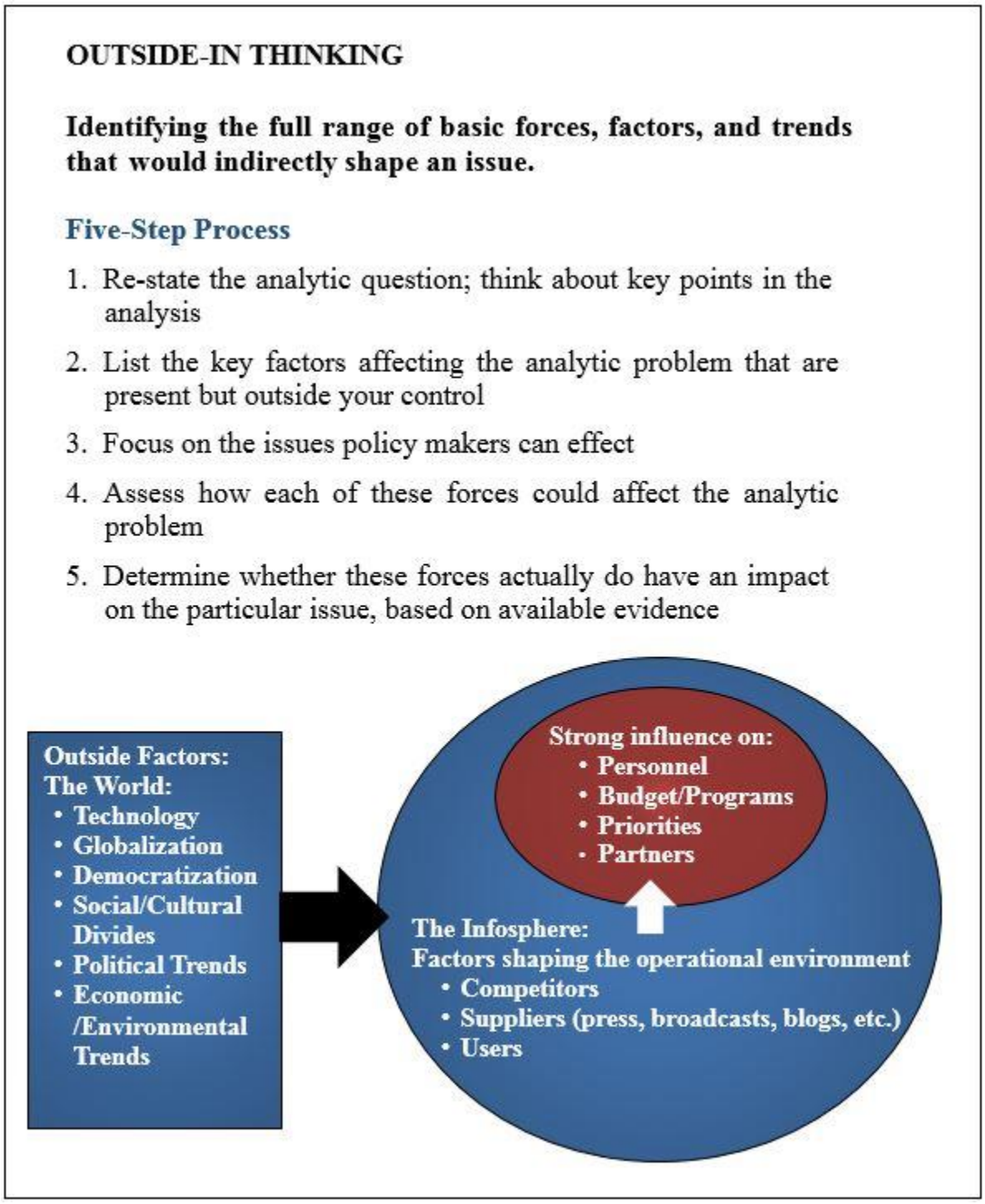


Figure A5.6. Diagnostic Techniques.

DIAGNOSTIC TECHNIQUES

Core Techniques	Description	When to Use
Key Assumptions Check	List and review the key working assumptions on which fundamental judgments rest	Most useful at the beginning of an analytic project
Quality of Information Check	Evaluate completeness and soundness of available information sources	Use to establish confidence level in analytic judgments, & ensure judgments are anchored to strong, relevant sources
Indicators or Signposts of Change	Reviewing observable events and trends to determine if a postulated situation is developing	Used to instill analytic rigor into the analytic process enhancing the credibility of analytic judgments
Deception Detection	Systematic use of checklists to determine when deception may be present and how to avoid being deceived	Used to counter adversary attempts of misinformation, concealment, and misdirection
Analysis of Competing Hypotheses	A systematic and logical approach to generate and evaluate all plausible hypotheses to solve a given problem	Any analysis where there are alternative explanations for what has happened, is happening, or is likely to happen

Figure A5.7. Key Assumptions Check.

KEY ASSUMPTIONS CHECK

A diagnostic technique that identifies hypotheses analysts have accepted to be true and that form the basis of the assumption

Four-Step Process

1. Review the analytic line on the issue; write it down for all to see and defend it orally
2. Articulate all the premises, both stated and unstated in finished intelligence, that are accepted as true for this analytic line to be valid
3. Challenge each assumption, asking why it must be true and whether it remains valid under all conditions
4. Refine the list of key assumptions to contain only those that must be true to sustain your analytic line; consider under what conditions, or in the face of what information, these assumptions might not hold

Questions to Ask

How much confidence exists that this assumption is correct?

What explains the degree of confidence in the assumption?

What circumstances or information might undermine this assumption?

Is a key assumption more likely a key uncertainty or key factor?

Could the assumption have been true in the past but be less so now?

If the assumption proves wrong, would it significantly alter the analytic line? If so, how?

Has this process identified new factors that need further analysis?

Figure A5.8. Quality of Information Check.

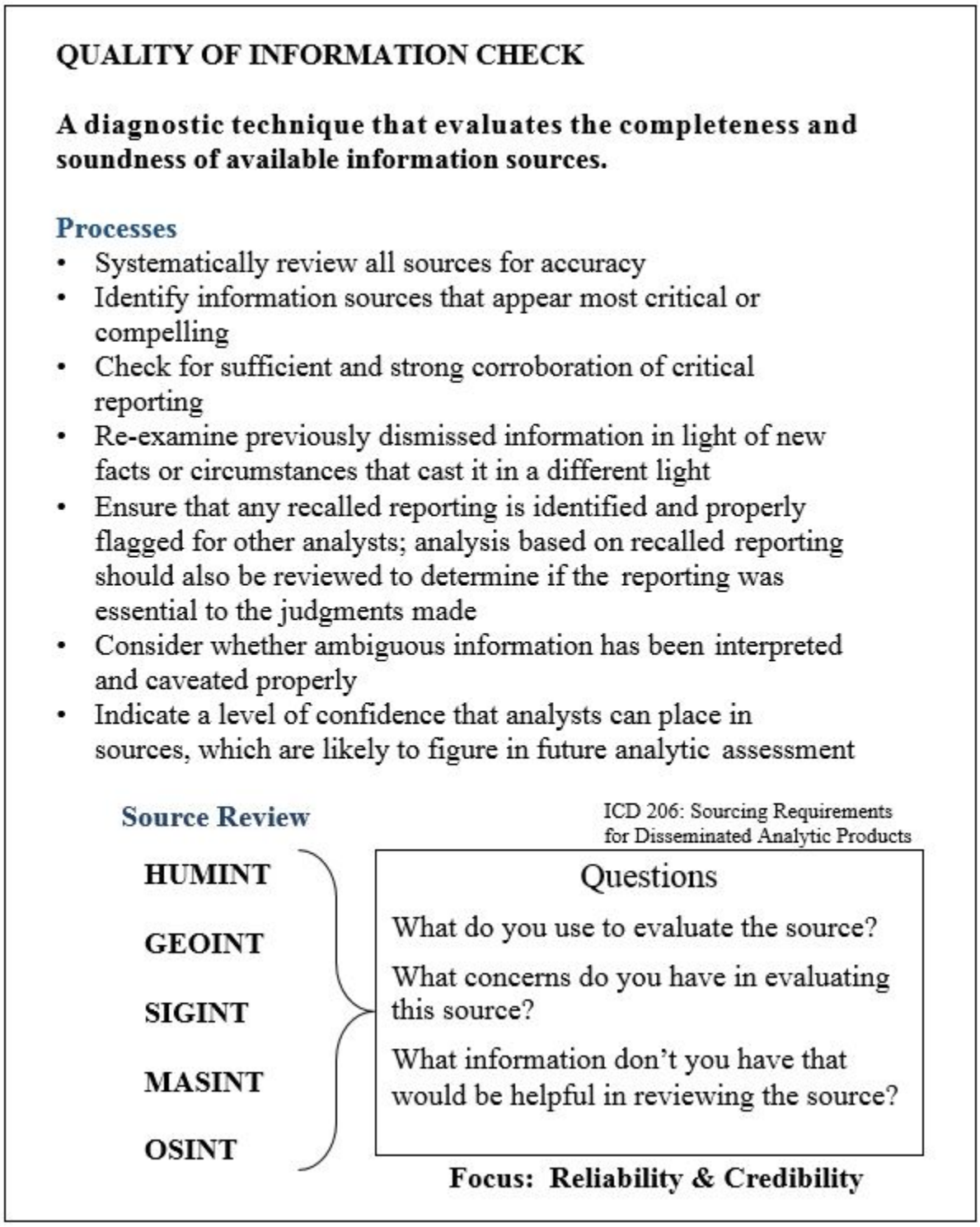


Figure A5.9. Indicators or Signposts of Change.

INDICATORS OR SIGNPOSTS OF CHANGE

Also called Signpost Analysis, this technique involves periodically reviewing a list of observable events or trends to track events, monitor targets, spot emerging trends, and warn of unanticipated change.

Indicator Technique Recommendations	
Analytic Environment	Indicator Technique
Non-Controversial • The issue is non-controversial within the IC or the policy community • Analysts and/or policymakers are uncertain about how the situation will actually evolve	• Simple lists of observables • Two contrasting lists of indicators (that would suggest a leader is growing stronger and a second list that he is growing weaker)
Somewhat Controversial • Some analysts or agencies have preferred positions or established equities to protect • The outcome has major policy or resource implications	• Use simple scales • Provide definitions for each indicator • Portray the information graphically • Revisit on periodic basis
Highly Controversial • Analysts hold strong, contrary views • Major institutional equities are at stake within the IC • The issue is highly charged within the policy community	• Provide a level of confidence for each rating • Provide a narrative description of what one would expect to observe at each level on a rating scale • List the sources of info and how important each was in establishing the rating

Figure A5.10. Deception Detection.

DECEPTION DETECTION

Diagnostic technique where analysts systematically use checklists to determine when deception actually may be present and how to avoid being deceived.

Does a foreign actor have the Motive, Opportunity and Means (MOM) to deceive?

1. Motive (What are the deceiver's goals?)
2. Channels (What means are available?)
3. Risks (What are the risks of discovery?)
4. Costs (Can deception be accomplished?)
5. Feedback (Can the deceiver monitor its use?)

Would this potential deception be consistent with Past Opposition Practices (POP)?

1. Does the deceiver have a history of deception?
2. Does this deception fit past patterns?

Is there cause for concern regarding the Manipulability of Sources (MOSES)?

1. Is the source reliable?
2. Does the source have access?
3. How good are the source's *bona fides*?
4. Is the source vulnerable to control or manipulation by the target?

What can be learned from the Evaluation of Evidence (EVE)?

1. How accurate is the source's reporting?
2. Is the whole chain of evidence available?
3. Does critical evidence check out?
4. Does evidence from one source conflict with others?
5. Do other sources of information provide corroborating evidence?
6. Is the absence of evidence unusual?

Figure A5.11. Analysis of Competing Hypotheses.

ANALYSIS OF COMPETING HYPOTHESES

Provides a systematic and logical approach to generate and evaluate plausible hypotheses to solve a given problem.

Eight-Step Process

1. Generate hypotheses
2. Gather and list evidence
3. Prepare the evidence and hypothesis matrix
4. Refine the matrix
5. Draw tentative conclusions
6. Perform sensitivity analysis
7. Report conclusions
8. Identify milestones

	Cred	Rel	H 1	H 2	H 3
Score			2	4	3
Evidence 1	H	H	C	C	C
Evidence 2	M	M	I	C	C
Evidence 3	M	M	C	C	I
Evidence 4	H	H	I	C	I
Evidence 5	M	M	I	I	C

H – High
M – Medium
L – Low

C – Consistent / Supports
I – Inconsistent / Does Not Support
N/A – Not Applicable

Figure A5.12. Focus Techniques.

FOCUS TECHNIQUES

Core Techniques	Description	When to Use
Issue Development	Used to ensure the central issues and alternative explanations of an issue or problem are identified within the scope and focus of the problem statement to aid in gathering the best answer	Used anytime analysts begin to assess a new issue or problem or begin a new research endeavor to mitigate bias toward the issue
Question Refinement	A simple technique to ensure analysts are answering the right question when responding to an intelligence requirement	Used when a consumer's intelligence requirement is not completely clear or when research begins to lead to ambiguity and confusion

Figure A5.13. Issue Development.

ISSUE DEVELOPMENT

A divergent technique that opens the mind of the analyst to substantive alternatives. Restating a problem opens it up and reveals important perspectives and issues otherwise overlooked.

Start with the initial poorly defined/stated issue

1. Paraphrase: Redefine the issue without losing the original meaning
2. 180 Degrees: Turn the issue on its head. Is the issue the one asked or the opposite of it?
3. Broaden the Focus: Instead of focusing on only one piece of the puzzle, step back and look at several pieces together
4. Narrow the Focus: Can the issue be broken down further? Take the question and ask about the components that make up the problem
5. Redirect the Focus: What outside forces impinge on this issue? Is deception involved?
6. Ask Why: Question the initial issue or question. Develop a new question based on the answer. Then question the second question and develop a new question based on that answer. Repeat this process until you believe the real problem emerges. This process is particularly effective in generating possible alternatives

End with a final refined issue

Figure A5.14. Question Refinement.

QUESTION REFINEMENT

A simple analytical technique used to ensure analysts are answering the right question when responding to a customer's intelligence requirement.

7-Step Process

1. **New Development -** Describe a change to the operating environment or security interests that result in a requirement for intelligence analysis and production.
2. **Raw Question(s) -** In response to the New Development, the immediate questions that come to mind, or that would come to mind for your customer. In relation to an event of interest, the raw questions could be, "Who did it and why?" or "What caused it?"
3. **Key Issue -** A key issue area normally includes an issue area and a geographic area. Issue areas are substantive categories of policy, strategy, or war fighting function. Key issue areas for a military operation can often be found in campaign descriptions of the lines of effort.
4. **National Interests -** The big picture must be considered thoughtfully when refining the intelligence requirement. Analysts should be able to tie assessments to U.S. security interests in general.
5. **Specific Customer Concerns -** This section of the refinery is often used to determine what questions are relevant and required to fulfill the intelligence question versus those specific requirements that might be better answered separately.
6. **Time Frame -** Answering your intelligence requirement should be targeted at a particular time, normally in the future (ex: "in the next 6 months," or "before 1 May 201X").
7. **Refined Question -** The refined intelligence question should be open-ended, requiring more than a yes or no answer, and should meet a specific customer's intelligence needs.

Figure A5.15. Contrarian Techniques.

CONTRARIAN TECHNIQUES

Core Techniques	Description	When to Use
Devil's Advocacy	Technique used to challenge a single, strongly held view or consensus by building the best possible case for an alternative explanation	Used when analysts need to provide further confidence that the current analytic line will hold up to close scrutiny
High Impact / Low Probability	Highlights a seemingly unlikely event that would have major policy consequences if it were to happen	Used when analysts believe an event is unlikely but have not given much thought to the consequences of its occurrence
What If? Analysis	A technique which assumes an event has occurred with potential (negative or positive) impact and explains how it might come about	Used to challenge a strong mindset that an event will not happen or be confidently justified
Team A / Team B Analysis	Separates teams to contrast two or more strongly held views or competing hypotheses	Used when there are two or more equally strong mind-sets held on an issue that need to be clarified (Devil's Advocacy challenges a single dominant mindset)

Contrarian: opposition or rejection of popular opinion

Figure A5.16. Devil's Advocacy.

DEVIL'S ADVOCACY

A contrarian technique for challenging a single, strongly held view or consensus by building the best-possible case for an alternative explanation.

Explicitly challenges key assumptions to see if they will not hold up under some circumstances.

Methodology

1. Outline the mainline judgment and key assumptions and characterize the evidence supporting the current analytic view
2. Select one or more assumptions—stated or not—that appear the most susceptible to challenge
3. Review the information used to determine whether any is of questionable validity, whether deception is possibly indicated, or whether major gaps exist
4. Highlight the evidence that could support an alternative hypothesis or contradicts the current thinking
5. Present to the group the findings that demonstrate there are flawed assumptions, poor quality evidence, or possible deception at work
6. Consider drafting a separate contrarian paper that lays out the arguments from a different analytic conclusion if the review uncovers major analytic flaws
7. Be sure that any products generated clearly lay out the conventional wisdom and are identified as an explicitly "Devil's Advocate" project; otherwise the reader can become confused as to the current official view on the issue

Figure A5.17. High Impact / Low Probability.

HIGH IMPACT / LOW PROBABILITY

A technique used to highlight a seemingly unlikely event that would have major policy consequences if it happened.

If there is a strongly-held view that an event is unlikely, then postulating precisely the opposite should not be difficult.

Perform the following steps to determine the effects of High Impact/Low Probability events:

1. Define the high-impact outcome clearly. This process is what will justify examining what most analysts believe to be a very unlikely development
2. Devise one or more plausible explanations for or "pathways" to the low probability outcome. This should be as precise as possible, as it can help identify possible indicators for later monitoring
3. Insert possible triggers or changes in momentum if appropriate. These can be natural disasters, sudden health problems of key leaders, or new economic or political shocks that might have occurred historically or in other parts of the world
4. Brainstorm with analysts having a broad set of experiences to aid the development of plausible but unpredictable triggers of sudden change
5. Identify for each pathway a set of indicators or "observables" that would help you anticipate that events were beginning to play out this way
6. Identify factors that would deflect a bad outcome or encourage a positive outcome

Figure A5.18. "What If" Analysis.

"WHAT IF" ANALYSIS

That "What If?" Analysis is the technique which assumes an event has occurred with potential (negative or positive) impact and explains how it might come about.

Method

1. Assume the event has happened
2. Select some triggering events that permitted the scenario to unfold to help make the "what if" more plausible; for example, analysts might postulate the death of a leader, a natural disaster, or some economic event that would start a chain of other events
3. Develop a chain of argumentation based as much on logic as evidence to explain how this outcome could have come about
4. "Think backwards" from the event in concrete ways–that is, specifying what must actually occur at each stage of the scenario is often very useful
5. Identify one or more plausible pathways or scenarios to the unlikely event; very often more than one will appear possible
6. Generate a list of indicators or "observables" for each scenario that would help to detect the beginnings of the event
7. Consider the scope of the positive and negative consequences of each scenario and their relative impacts
8. Monitor the indicators developed on a periodic basis

Figure A5.19. Team A / Team B.

TEAM A / TEAM B

Used when there may be competing and possibly equally strong mind sets held on an analytical issue; this approach helps opposing groups see the merit in each other's perspective.

Two Phases

1)Analysis Phase

1. Identify the two or more competing hypotheses or points of view
2. Form teams or designate individuals to develop the best case for each hypothesis
3. Review all pertinent information that supports their respective position
4. Identify missing information that would strengthen their hypotheses
5. Structure each argument, presenting key assumptions, key pieces of evidence, and careful articulation of the logic behind the argument

2)Debate Phase

1. Set aside time for an oral presentation of the alternative team findings; this can be an informal brainstorming session or a more formal debate
2. Have an independent jury of peers to listen to the oral presentation and be prepared to question the teams regarding their assumptions, evidence, or logic
3. Allow each team to present its case, challenge the other team's arguments, and rebut the opponent's critique of its case
4. Let the jury consider the strength of each presentation and recommend possible next steps for further research and collection efforts

Attachment 6

IC, DOD, AND MILITARY SERVICE REFERENCES

A6.1. The IC. As shown in Table A6.1, *Members of the IC*, the IC is a coalition of 17 agencies and organizations, including the ODNI, within the Executive Branch that work both independently and collaboratively to gather and analyze the intelligence necessary to conduct foreign relations and national security activities.

Table A6.1. Members of the IC.

Office of the Director of National Intelligence (ODNI)	
U.S. Air Force (USAF) Intelligence	Department of the Treasury
U.S. Army (USA) Intelligence	Drug Enforcement Agency (DEA)
Central Intelligence Agency (CIA)	Federal Bureau of Investigation (FBI)
U.S. Coast Guard (USCG) Intelligence	U.S. Marine Corps (USMC) Intelligence
Defense Intelligence Agency (DIA)	National Geospatial-Intelligence Agency (NGA)
Department of Energy (DOE)	National Reconnaissance Office (NRO)
Department of Homeland Security (DHS)	National Security Agency (NSA)
Department of State (DOS)	U.S. Navy (USN) Intelligence

A6.2. IC and DoD Reference Documents. Table A6.2, *Common IC and DoD Analysis References*, lists various IC and DoD publications that most often impact AF analysis.

Table A6.2. Common IC and DoD Analysis References.

IC
DNI *Principles of Intelligence Transparency for the Intelligence Community* ICD 191, *Duty to Warn* ICD 203, *Analytic Standards* ICD 204, *National Intelligence Priorities Framework* ICD 205, *Analytic Outreach* ICD 206, *Sourcing Requirements for Disseminated Analytic Products* ICD 208, *Maximizing the Utility of Analytic Products* ICD 209, *Tearline Production and Dissemination*
DoD
DoDI 3115.17, *Management and Oversight of DoD All-Source Analysis* DIA Directive (DIAD) 5000.200, *Intelligence Threat Support for Major Defense Acquisition*

Programs

DIA Instruction (DIAI) 5000.002, *Intelligence Threat Support for Major Defense Acquisition Programs*

DIAP Users Guide

DoD Directive (DoDD) 5000.01, *The Defense Acquisition System*

DoDD 5105.21, *Defense Intelligence Agency*

DoDD 5250.01, *Management of Intelligence Mission Data (IMD) in DoD Acquisition*

DoDI 5000.02, *Operation of the Defense Acquisition System*

A6.3. Military Services. As depicted in Table A6.3, *Major Intelligence Analysis Entities of the Military Services*, each military service has a SIO that oversees intelligence policy, planning, programming, and activities on behalf of the service chief. The AF SIO is the DCS for ISR, also known as the AF/A2. Each service is authorized one service intelligence center, also called an intelligence analysis center. The AF's service intelligence center is NASIC. The AF has assigned the ACC as its lead MAJCOM for the GIISR capability, which includes intelligence analysis. Similarly, other military services have assigned significant analysis responsibilities to various organizations. All services routinely reach out to each other for service-unique expertise and collaboration in addressing analysis requirements.

Table A6.3. Major Intelligence Analysis Entities of the Military Services.

	USAF	USA	USN	USMC	USCG
Service Senior Intelligence Officer (SIO)	Deputy Chief of Staff for ISR (USAF/A2)	Deputy Chief of Staff for Intelligence (USA/G2)	Director of Naval Intelligence (USN/N2/6)	Director of Intelligence (USMC/DIRINT)	Assistant Commandant for Intelligence (USCG/CG-2)
Service Intelligence Center	National Air and Space Intelligence Center (NASIC)	National Ground Intelligence Center (NGIC)	Office of Naval Intelligence (ONI)	Marine Corps Intelligence Activity (MCIA)	Intelligence Coordination Center (ICC)
Lead Command	Air Combat Command (ACC) 1. Core Function Lead Integrator (CFLI) for Global Integrated ISR (GIISR) **2.** Chair, Analysis Capability Working Group (ACWG)	Intelligence and Security Command (INSCOM)	N/A	N/A	N/A
Other Major Analysis Organizations	1.Intelligence Systems Support Office (ISSO) 2.363 ISRW 1.Civil Aviation Intelligence Analysis Center (CAIAC)		• Nimitz Operational Intelligence Center • Farragut Technical Analysis Center • Kennedy Irregular Warfare Center Hopper		• Maritime Intelligence Fusion Center Atlantic (MICF LANT) • Maritime Intelligence Fusion Center Pacific (MICF PAC) Coast Guard Investigative Service (CGIS)

			Information Services Center		
Counter-Intelligence Organizations	AF Office of Special Investigations (AFOSI)	Army Counterintelligence Center (ACIC)	Naval Criminal Investigative Service (NCIS)	2nd Intelligence Battalion	Coast Guard Counterintelligence Service (CGCIS)

Notes:
1. The USA service intelligence center (NGIC) falls under INSCOM. The service intelligence center in each of the other military services falls under the service SIO.
2. The AF assigns a CFLI to each of its major capabilities. The ACC Commander is the GIISR CFLI, which includes intelligence analysis. The ACC staff coordinates closely with intelligence analysis stakeholders across the AFIAE to develop, program, and advocate for intelligence analysis capabilities and requirements.
3. The ACWG serves as a cross-MAJCOM entity of analysis stakeholders responsible for supporting the development and advancement of air, space, and cyberspace intelligence analytical capabilities within the AF ISR Enterprise and across the full range of military operations. The ACWG provides a means to coordinate, assess, and synchronize AF intelligence analysis policies, tradecraft, education, training, and tools, as well as to recommend materiel and non-materiel solutions through established AF processes and offices.

A6.4. Common Analysis Organizations. Table A6.4, *Intelligence Analysis Organizations by Mission Type*, identifies IC, DoD, military service, and other government agencies organized according to the primary analysis they conduct. The table is not meant to be exhaustive; rather it provides a sampling of missions and the key analysis organizations that support them.

Table A6.4. Intelligence Analysis Organizations by Mission Type.

Air / Integrated Air Defense Systems	**Short Range Missiles**	**Med / Long Range Missiles**	**Ground**
NASIC	MSIC	NASIC	NGIC
Maritime	**Space**	**Cyber**	**Counter-IED**
ONI MCIA	NASIC NRO 14 AF	CYBERCOM NSA NASIC 24 AF 25 AF AFOSI	JIDA
Counter-terrorism	**Counter-intelligence**	**Threat Finance**	**Criminal**
NCTC DHS FBI CIA CGIS	AFOSI CIA FBI ACIC NCIS 2d Intelligence Btn CGCIS	Treasury FBI	AFOSI FBI NCIS CID CGIS
Rotary Wing	**Unmanned Systems**	**Surface-to-Air Missiles**	**Electronic Warfare Systems**
NGIC	NASIC NGIC ONI	MSIC	NASIC NGIC ONI
Rapid Air Mobility	**Global Commons**		
AMC AIS	CAIAC		

	NAI2O TRANSCOM JIOC AMC AIS MIFC LANT MIFC PAC		

Notes:
1. As the DoD functional manager for analysis, DIA provides overarching all-source analysis and/or guidance for all mission types listed.
2. The Missile and Space Intelligence Center (MSIC) is an equivalent organization to the service intelligence centers. Additionally, MSIC provides support to space analysis.
3. CYBERCOM—Cyber Command; JIDA—Joint Improvised-Threat Defeat Agency; NCTC—National Counterterrorism Center; CGIS—Coast Guard Investigation Service; Btn—Battalion; CID—Criminal Investigation Command; NAI2O—National Aviation Intelligence Integration Office; TRANSCOM—Transportation Command

Attachment 7

ONLINE RESOURCES FOR ANALYSIS SKILLS AND TRADECRAFT.

Table A7.1, *Online Resources for Skills and Tradecraft,* identifies resources that contain additional background, information, and guidance on analysis skills and tradecraft topics discussed in Chapter 5. The list reflects some of the common resources as of 2017 and is not meant to be exhaustive nor all-inclusive.

Table A7.1. Online Resources for Skills and Tradecraft.

Analysis Certification
ASA Certification site, JWICS Caution-url: https://intelshare.intelink.ic.gov/sites/asacertification
Universal GEOINT Certification Program site, https://usgif.org/certification
Critical Thinking and Reasoning
AFCO-CFA Intellipedia Page, https://intellipedia.intelink.gov/wiki/Air_Force_Cryptologic_Office_(AFCO)/CFA_Advanced_Analysis_and_Training
Foundation for Critical Thinking, *The Critical Thinking Community,* http://www.criticalthinking.org
Grimes, Geoffrey, *Scholasticism, Rationalism, and Empiricism: Epistemology and Three Western Systems of Reasoning*, http://www.distancelearningassociates.org/eng2327/BC-ReasoningSystems.htm
SATs
AFCO-CFA Intellipedia Page, https://intellipedia.intelink.gov/wiki/Air_Force_Cryptologic_Office_(AFCO)/CFA_Advanced_Analysis_and_Training
CIA, *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis*, March 2009, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf
DCS for ISR White Paper, *Data Science and the USAF ISR Enterprise,* February 2016, http://www.defenseinnovationmarketplace.mil/resources/Data_Science_and_the_USAF_ISR_Enterprise%20_White_Paper.PDF
ICAT-G/Research Portal, JWICS Caution-url: https://intellipedia.intelink.ic.gov/wiki/Portal:IC_Analytic_Tradecraft_Gateway
Lengler, Ralph, and Martin J. Eppler, *A Periodic Table of Visualization Methods*,

http://www.visual-literacy.org/periodic_table/periodic_table.html
Collaboration and Communication
AFCO-CFA Intellipedia Page, https://intellipedia.intelink.gov/wiki/Air_Force_Cryptologic_Office_(AFCO)/CFA_Advanced_Analysis_and_Training
DIA-01-1309-510, *DIA Style Manual for Intelligence Production 2017*, JWICS Caution-url: https://intelshare.intelink.ic.gov/sites/ddii/mid/AIS/default.aspx
ICAT-G/Research Portal, JWICS Caution-url: https://intellipedia.intelink.ic.gov/wiki/Portal:IC_Analytic_Tradecraft_Gateway
OPB and ABI
ODNI Systems & Resource Analyses, *ABI Way Ahead*, JWICS Caution-url: https://intelshare.intelink.ic.gov/sites/sramis/abi/default.aspx
Quellfire Documentation, JWICS Caution-url: https://intelshare.intelink.ic.gov/sites/quellfire/SitePages/ProgramDocumentation.aspx

Attachment 8

ANNOTATED BIBLIOGRAPHY

This attachment contains IC and academic resources for analyst Airmen to reference to improve their analysis aptitude. The list reflects some of the common references as of 2017 and is not meant to be exhaustive nor all-inclusive.

A8.1. Analysis Skills, Tradecraft, and Processes in the IC. The following texts focus specifically on IC analysis.

711th Human Performance Wing (HPW), ***The Framework for Analytic Cognition (FAC)***, AFRL, Wright-Patterson Air Force Base, Ohio, April 2014
This report serves as a guide to conducting intelligence analysis thoroughly while remaining sufficiently pliable to adapt to unstructured issues. It focuses on describing methods to foster analyst understanding of human-shaped capabilities and intentions for application in intelligence missions.

CIA, ***A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis,*** March 2009, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/Tradecraft%20Primer-apr09.pdf
This guide highlights several structured analytic techniques to outline and assist analysts to think about and work difficult problems associated with intelligence analysis. The primer identifies several hurdles to this process such as biases, expectations, and mental models. Ultimately, the guide aims to inform intelligence analysts about their thinking processes to increase their self-awareness and efficacy in making judgments.

Clark, Robert M., ***Intelligence Analysis: A Target-Centric Approach***, 4th edition, CQ Press, 2012
This book urges analysts to focus on the intelligence problem at hand to drive insight. It provides a thorough overview of how the intelligence analysis process works with ample examples. The book also identifies areas where intelligence analysis could/should work better.

Clark, Robert M., ***The Technical Collection of Intelligence***, CQ Press, 2010
This book examines the technical means by which advanced countries collect intelligence information (acoustic, infrared, etc.). The author describes the collection, processing, and exploitation phases of intelligence technical collection in an understandable language.

Defense Intelligence Reference Document DIA-01-1003-001A, ***Tradecraft Primer: Basic Structured Analytic Techniques***, 4th edition, 3 March 2011
This DIA handbook provides an outline of analytic methods to help intelligence analysts improve their critical thinking skills, producing more thorough, less biased judgments. The techniques provided in this text also function to build a common lexicon in the IC, fostering consistent understanding and thereby efficiency and accuracy.

Folker, Robert D. Jr., ***Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods***, Occasional Paper #7, Joint Military Intelligence College, 2000
This summary of a master's thesis compares the results of those who used a specific structured analytic technique with those who did not in preparing intelligence estimates.

Fingar, Thomas, ***Reducing Uncertainty: Intelligence Analysis and National Security***, Stanford Security Studies, 2011

The goal of this book is to inform readers from outside the IC what analysts in the IC do and how they do it. The book explains the pressures IC analysts are under (political etc.), why they often focus on worst-case scenarios, and the value of National Intelligence Estimates.

Fischhoff, Baruch, and Cherie Chauvin, ***Intelligence Analysis: Behavioral and Social Scientific Foundations***, National Academies Press, 2011

This book focuses on the human aspect of the IC and how to improve judgments made by both individual analysts and groups of analysts. The book provides an overarching perspective on the issues and processes that contribute to tough decision and judgment making.

George, Roger Z., and James B. Bruce, ed., ***Analyzing Intelligence: Origins, Obstacles and Innovation***, Washington D.C.: Georgetown University Press, 2008

This book provides a post-9/11 assessment of the state of intelligence analysis. The text offers insights into the obstacles for intelligence analysis, providing a plan to improve analytical methods, training, and approach. The book highlights adapted tradecraft, predictive analysis, and collaboration as areas needing improvement.

Grabo, Cynthia, ***Anticipating Surprise: Analysis for Strategic Warning***, University Press of America, 2002

This book, originally designed as a CIA analyst training guide, outlines the steps in the anticipatory analysis process, including discussing guidance for assessing the meaning of pieces of intelligence. In the wake of post-9/11 IC critiques, the author provides suggestions on how to improve and clarify warnings to decision makers.

Hackman, Richard J., ***Collaborative Intelligence: Using Teams to Solve Hard Problems***, San Francisco: Berrett-Koehler Publishers Inc., 2011

The book highlights the increased need and prevalence for interdisciplinary collaboration in intelligence analysis and identifies that most teams in the field often break down or prove ineffective. The author outlines six conditions leaders can employ to encourage the development, efficacy, and maintenance of teams working on intelligence analysis tasks.

Hall, Wayne Michael, and Gary Citrenbaum, ***Intelligence Analysis: How to Think in Complex Environments***, Santa Barbara, California: Praeger Security International, 2010

This book discusses the various types of advanced analysis—including anticipatory, semiotics, and link analysis—while laying out the steps of analytical problem solving: decomposition, critical thinking, analysis, recomposition, and synthesis. The book also discusses the systems of thought and how those impact an individual's analytical process and decision/judgment.

Heuer, Richards J., Jr., ***The Psychology of Intelligence Analysis***, Washington, D.C.: Central Intelligence Agency, Center for the Study of Intelligence, 1999

This collection of CIA articles spanning 1978-1986 reviews timeless concepts of cognitive psychology concerning how individuals gather and process information to shape their judgments.

Heuer, Richards J., Jr. and Randolf H. Pherson, ***Structured Analytic Techniques For Intelligence Analysis***, Washington, D.C.: CQ Press, 2014

This text identifies best practices in structured analysis to inform analysts within the intelligence field and across other disciplines.

Kent, Sherman, ***Strategic Intelligence for American World Policy***, Princeton University Press, 2015

This book was originally written and published in 1966 by Sherman Kent, who pioneered many of the methods of intelligence analysis. The book analyzes the varied aspects of what is known as "high-level foreign positive intelligence." Kent asserts that very little of it involves cloaks and

daggers. All of it is important to national survival, and should be understood by the citizens of a democracy.

Kerbel, Josh, and Anthony Olcott, *Synthesizing with Clients, Not Analyzing for Customers*, Studies in Intelligence, Vol. 54, No. 4. December 2010, https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol.-54-no.-4/synthesizing-with-clients-not-analyzing-for.html

This article discusses the challenges, purpose, and shortcomings of the separation between analysts and the policy/decision makers they inform. One purpose is to avoid politicization of analysis and mitigate confirmation biases, but the separation can also lead to unanswered questions from decision-makers or ignored reports created by the analysts but not read.

Lowenthal, Mark M., *Intelligence: From Secrets to Policy*, 6th edition, CQ Press, 2014

This text provides an introduction to the field of intelligence, from both the analyst and policymaker perspectives. This book covers all phases and domains of intelligence analysis, providing current event examples and trends to watch.

Moore, David T., *Critical Thinking and Intelligence Analysis*, 2nd edition, Books Express Publishing, 2010

This book, sponsored by the National Defense Intelligence College, establishes how critical thinking fits into intelligence analysis. The author offers input on how to teach critical thinking to analysts with the goal of integrating into the intelligence analysis process.

Moore, David T., *Sensemaking: A Structure for an Intelligence Revolution*, 2nd edition, CreateSpace Independent Publishing Platform, 2013

The goal of this book is to identify where and how to improve the IC and its processes. The text identifies problem areas, including discussions of 'wicked problems,' complexity theory, and macro-vs-micro cognition. It also proposes possible solutions.

Symon, Paul B., and Arzan Tarapore, "Defense Intelligence Analysis in the Age of Big Data," *Joint Forces Quarterly*, Vol 79, 4th Quarter 2015

This article discusses the emerging challenge of big data analytics for military intelligence communities. The article highlights that, although big data generates knowledge creation, additional tools and methods are needed to absorb, process, and analyze the vast onslaught of information.

White, Jeffrey, *Shakespeare for Analysts: Literature and Intelligence*, CreateSpace Independent Publishing Platform, 2013

This paper, originally sponsored by the Joint Military Intelligence College in 2003, advocates inclusion of Shakespeare in intelligence analysts' bookshelves. The author asserts that since analysts are concerned with human personalities within political and military leadership, analysts should use Shakespeare's work as insight into how people are motivated and pursue power.

Zegart, Amy B., *Flawed by Design: The Evolution of the CIA, JCS, and NSC*, Stanford University Press, 2000

Using an institutionalist approach, the author asserts that the CIA, Joint Chiefs of Staff (JCS), and National Security Council (NSC) are hindered from operating effectively by design. Frequent elections, the prominence of elected officials controlling these organizations, and Congressional checks foster competitive, rival organizations fighting amongst themselves to protect their own intelligence assets.

A8.2. Analysis Skills, Tradecraft, and Processes in General . Whereas section A8.1 identifies sources that specifically address IC skills, tradecraft, and processes, the following

sources apply to the discipline of analysis writ large. While the following were written with a broader academia focus, they are also relevant to IC analysis.

Bothamley, Jennifer, *Dictionary of Theories*, Barnes & Noble, 2004
This book is a composite reference that alphabetically arranges theories, laws, hypotheses, etc. from across many disciplines. It serves as a thorough annotated bibliography of well-known theories, and includes short descriptions and comments on the validity of each entry.

Cukier, Kenneth Neil, and Viktor Mayer-Schoenberger, "The Rise of Big Data: How It's Changing the Way We Think," *Foreign Affairs*, May - June 2013, https://www.foreignaffairs.com/articles/2013-04-03/rise-big-data
This article discusses the concept of big data, describing the vast and increasing amount of information that can be harnessed, processed and used to support trends and inform new knowledge. The article also cautions that big data should be used to inform but not explain everything.

Dewey, John, *How We Think*, Boston, Massachusetts: D.C. Heath and Co. Publishers, 1910
This book offers an early overview of the importance of self-awareness in thought. The author calls for a focus in "mental training" and "training of thought" to increase one's deliberateness when thinking, solving, and assessing problems.

Elder, Linda, and Richard Paul, *The Thinker's Guide to Analytic Thinking*, 2nd edition, Dillon Beach: Foundation for Critical Thinking Press, 2007
This guide describes the structures and importance of analytic thinking. The authors discuss how we reach our conclusions and judgements–viewing an idea through our biases, point of view, experiences, and assumptions. The book provides a framework for understanding how we think and how that impacts decisions.

Facione, Peter, *Critical Thinking: What It Is and Why It Counts*, Milbrae, California: Measured Reasons and the California Academic Press, 2013
This essay familiarizes readers with the key skills and habits associated with critical thinking and why practicing critical thinking is useful in their personal and social decision-making. The article identifies several of the heuristic strategies individuals are naturally inclined towards and the pros/cons and biases associated therein.

Facione, Peter, and Carol Ann Glittens, *Think Critically*, 3rd edition, Prentice Hall, Pearson Education Inc., 2015
This text introduces and practically describes critical thinking as important for making big decisions in the real-world.

Foundation for Critical Thinking, *The Critical Thinking Community*, http://www.criticalthinking.org
This website is sponsored by the Foundation for Critical Thinking, a non-profit organization that seeks to promote essential change in education and society through the cultivation of fair-minded critical thinking—thinking which embodies intellectual empathy, humility, perseverance integrity, and responsibility.

Gilovich, Thomas, *How We Know What Isn't So: The Fallibility of Human Reason in Everyday Life*, The Free Press, 1991
This book addresses the question: When can we trust what we believe, and when are these beliefs suspect? Thomas Gilovich offers a wise and readable guide to the fallacy of the obvious in everyday life. Illustrating his points with vivid examples, he documents the cognitive and social processes that distort our thoughts, beliefs, judgements, and decisions, inevitably altering our impression of reality.

Grimes, Geoffrey, ***Scholasticism, Rationalism, and Empiricism: Epistemology and Three Western Systems of Reasoning***, http://www.distancelearningassociates.org/eng2327/BC-ReasoningSystems.htm
This website discusses the basic concepts of what the author describes as three core systems of reasoning: scholasticism, rationalism, and empiricism. The author asserts all those raised in Western cultures can be binned into one of these three categories.
Jones, Morgan D., ***The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving***, Crown Business, 1998
This handbook provides fourteen tools to help individuals break down problems, enabling more efficient and informed decisions.
Kahneman, Daniel, ***Thinking, Fast and Slow***, New York: Farrar, Straus and Giroux, 2011
In this book author Daniel Kahneman describes the two systems of thinking: the intuitive (fast System 1) and the logical (thorough System 2). The text describes the identifiers of each system and how it impacts our decisions. The author provides methods to identify and prevent mental shortcuts that can cause judgement errors.
Kahneman, Daniel, Andrew Rosenfield, Linnea Gandhi, and Tom Blaser, ***Noise: How to Overcome the High, Hidden Cost of Inconsistent Decision Making***, Harvard Business Review, 2016
This article explains the difference between the concepts of "noise" and bias and provides a prescription of how leaders can test the level of "noise" in their organizations. Further, it describes steps to mitigate noise and promote analytical consistency.
Kahneman, Daniel, Paul Slovic, and Amos Tversky, ***Judgement under uncertainty: Heuristics and biases***, Cambridge University Press, 1982
This book describes the various judgment heuristics and biases. The text discusses how those biases can impact decision-making and judgments and suggests methods for identifying and overcoming these biases.
Kaplan, Abraham, ***The Conduct of Inquiry: Methodology for Behavioral Science***, Transaction Publishers, 1998
In this book the author discusses the various behavioral science disciplines and the methodologies and shortcomings of each. It provides a constructive assessment of the various standards and strategies of social research methods to guide behavioral scientists' research.
Kosko, Bart, ***Fuzzy Thinking: The New Science of Fuzzy Logic***, Hyperion, 1993
This book discusses the concept of fuzzy thinking/fuzzy logic, the principle that nothing is absolute. The author challenges the typical Western thinking that there is black and white—right and wrong, asserting that there are lots of shades of gray, with many perspectives.
Krizan, Lisa, ***Intelligence Essentials for Everyone***, Joint Military Intelligence College, June 1999
This paper provides guidance for the implementation of sound intelligence within and outside government infrastructure. The author describes the methods to employ to reach empirically-supported decisions with fewer flaws.
Laney, Douglas, et al., ***How Data Scientist Skills and Qualifications Differ from those of BI Analysts and Statisticians***, 21 October 2015
This article helps readers understand the distinction between the new data scientist career and associated skill-set and the legacy career of statisticians. Additionally, the authors describe why a statistician is not adequate for data science problems.

Lengler, Ralph, and Martin J. Eppler, ***A Periodic Table of Visualization Methods***,
http://www.visual-literacy.org/periodic_table/periodic_table.html
This online learning tool informs users on the ability to generate, understand, and apply visualizations. The site employs a didactic approach using problem-based learning techniques to foster understanding of visualization methods.
Linden, Alexander, et al., ***Organizational Principles for Placing Advanced Analytics and Data Science Teams***, 4 September 2013
With the onslaught of big data driving the need for teams of advanced analysts and data scientists in organizations of various disciplines, this article discusses where to best place these teams organizationally and the pros and cons of various locations.
Livio, Mario, ***The Equation that Couldn't be Solved: How Mathematical Genius Discovered the Language of Symmetry***, Simon & Schuster, 2006
This book attempts to explain mathematical symmetry through a "quantic" equation to non-mathematically inclined readers. The text discusses how the idea of group theory arose.
Mackay, Charles, ***Extraordinary Popular Delusions and the Madness of Crowds***, CreateSpace Independent Publishing Platform, 2013
This book studies the psychology of crowds and mass mania with historical examples such as the witch hunts. The text offers explanation as to why reasonable, intelligent individuals take on opinions in a crowd environment that they otherwise would not.
Margolis, Howard, ***Patterns, Thinking, and Cognition: A Theory of Judgement***, Chicago, Illinois: University of Chicago Press, 1987
This book discusses how pattern recognition impacts thinking and judgment. The author discusses identification of patterns, sub-patterns and when anomalies are actually part of the pattern.
Mlodinow, Leonard, ***The Drunkard's Walk: How Randomness Rules Our Lives***, Vintage, 2009
This book discusses how much of our lives are lived and guided by randomness. He introduces the concept of chaos theory, and reveals psychological illusions guiding "chance." The text presents several tools to help readers make more informed decisions in their everyday lives.
Pirsig, Robert M., ***Zen and the Art of Motorcycle Maintenance***, Bantam, 1975
In this book the author combines philosophy with the practical, real-world processes of motorcycle mechanics. Despite the title, this book prompts the reader to deep-think about critical thinking methods and more complex philosophical dilemmas, such as good-vs-evil.
Surowiecki, James, ***The Wisdom of Crowds***, Anchor Books, 2008
This book asserts that crowd-sourcing perspectives, or incorporating a range of diverse perspectives, improves problem-solving. The author identifies four necessary conditions that, when met, produce crowds that are smarter together than any one individual.
Tetlock, Philip E., and Dan Gardner, ***Superforecasting: The Art and Science of Prediction***, 1st edition, 2015
In this work, Philip Tetlock and coauthor Dan Gardner offer a masterwork on prediction, drawing on decades of research and the results of a massive, government-funded forecasting tournament. Superforecasting offers the first demonstrably effective way to improve our ability to predict the future.
Tufte, Edward R., ***The Visual Display of Quantitative Information***, 2nd edition, Cheshire, Connecticut: Graphics Press, 2001

This text covers the theory and practice used in the design and use of statistical graphics, charts and tables. It outlines the benefits and potential misrepresentation of empirical visualization methods.

A8.3. Studies and White Papers on Analysis. ***Air Force Intelligence Analysis Roles and Responsibilities Review for 2016***, September 2016

This report is a primary deliverable for the AF Analysis Plan of Action and Milestones. The report details the results of an AF-wide review of roles and responsibilities for analysis and production.

Alkire, Brien, Abbie Tingstad, Dale Benedetti, Amado Cordova, Irina Danescu, Lt Col William Fry, Brig Gen (ret.) D. Scott George, Lawrence M. Hanser, Lance Menthe, Erik Nemeth, David Ochmanek, Julia Pollak, Jessie L. Riposo, Lt Timothy Smith, Alexander Stephenson, ***Leveraging the Past to Prepare for the Future of Air Force Intelligence Analysis***, Santa Monica, California: RAND Corporation, RR-1330-AF, 2016, http://www.rand.org/pubs/research_reports/RR1330.html

This RAND report looks to the past for lessons to help inform recommendations in addressing future challenges for the AFIAE. The report identifies challenges regarding future operational pace, contextual and deep knowledge, the integration and understanding of space and cyber missions, and the growing volume of data to be analyzed.

Chang, Welton, Eva Chen, Barbara Mellers, and Philip Tetlock, "Developing Expert Political Judgment: The Impact of Training and Practice on Judgmental Accuracy in Geopolitical Forecasting Tournaments," ***Judgment and Decision Making*** 11, no. 5 (2016): 509-26

This essay tests the power of a cognitive-debiasing training module to improve probability judgments in a four-year series of geopolitical forecasting tournaments sponsored by the U.S. Intelligence Community.

Committee on Improving the Effectiveness and Efficiency of U.S. Air Force Pre-Acquisition Development Planning et al., ***Development Planning: A Strategic Approach to Future Air Force Capabilities***, National Academies Press, 2015

This book provides recommendations, informed by development planning efforts of the past, for leaders to think strategically into upcoming decades concerning where the AF may have capability gaps.

Committee on U.S. Air Force Strategic Deterrence Military Capabilities in the 21st Security Environment et al., ***U.S. Air Force Strategic Deterrence Analytic Capabilities: An Assessment of Tools, Methods, and Approaches for the 21st Century Security Environment***, National Academies Press, 2015

This book describes the analytic skills required in successful nuclear deterrence. The text also discusses how nuclear deterrence works through assurance and posture, how it can fail, and how to mitigate the risk of deterrence failure.

DCS for ISR White Paper, ***Data Science and the USAF ISR Enterprise***, February 2016, http://www.defenseinnovationmarketplace.mil/resources/Data_Science_and_the_USAF_ISR_Enterprise%20_White_Paper.PDF

This paper explores the impact of big data, the transformation of IC information technology, and how each will drive the necessity for an AF ISR strategic approach to data science.

DCS for ISR White Paper, ***Five Examples of Big Data Analytics and the Future of ISR***, November 2014

This paper describes the concept of big data and how it relates to ISR now and in the future through five examples. The paper asserts that big data is the new norm and intelligence professionals must adapt the way they employ data analytics to harness the depth of information now available.

DCS for ISR White Paper, *Revolutionizing AF Intelligence Analysis*, January 2014, http://www.defenseinnovationmarketplace.mil/resources/20140211_IntelligenceAnalysisWhitePaper_PA.pdf

This paper seeks to explain the increasing priority of analysis by identifying motivations, presenting a common lexicon, exploring key issues, and outlining the way ahead. The paper asserts that intelligence analysis is changing and increasing in prominence and therefore our analysis processes and emphasis must also adapt.

ISR Capability Planning and Analysis Process Committee on Examination of the Air Force Intelligence, *Capability Planning and Analysis to Optimize Air Force Intelligence, Surveillance, and Reconnaissance Investments*, National Academies Press, 2012

This report answers a request from the AF to assess the current AF approach to ISR corporate planning and programming. The report identifies best practices and recommends specific improvements to build-out existing tools and processes to ensure AF ISR processes can enable successful satisfaction of customer needs in accomplishing their missions.

Lin-Greenberg, Capt Erik, Krysten Young, and Col Brian Ray, *Improving Intelligence Analysis for the A2/AD Environment*, March 2015

This paper discusses the impact an Anti-Access/Area Denial (A2/AD) environment would have on the AF's ability to collect, analyze, and act on intelligence.

McClung, Lt Col Michael E., *2 Propositions Regarding Intelligence for Airpower*, Air University, 14 February 2013

This research paper provides two propositions concerning AF intelligence: 1) "the nature of intelligence for airpower is driven by the rapid evolution and expanding breadth of airpower itself" and; 2) "Analysis is the essence of intelligence for airpower, and like airpower it is broad, but targeting and threat analysis are central."

Report of USAF ISR Analysis and Production–CY 2014, 19 June 2014

This report is the result of a survey of AF ISR leaders to document AF production, including identifying production goals, focus, and areas for improvement. This survey built upon findings from a 2013 survey and further developed a baseline for comparison of the 2016 survey results.

Survey Report of USAF All-Source Intelligence Analysis, 1 August 2013

This report is the outcome of a survey to gage results and assessments of AF all-source analysis. The report asserts that if the USAF is serious about 'revolutionizing analysis,' it must concur with improved emphasis and investment.

Treverton, Gregory F., and C. Bryan Gabbard, *Assessing the Tradecraft of Intelligence Analysis*, Santa Monica, California: RAND Corporation, 2008, http://www.rand.org/content/dam/rand/pubs/technical_reports/2008/RAND_TR293.pdf

This RAND report is the result of a survey of the IC and other research to discover what constitutes intelligence analysis and how is it performed. The researchers found that "analysis" covers a range of activities that varies from organization to organization. The report concludes that to foster collaboration and shared understanding, common tools, agendas, and education curriculums should be established and shared across the community.

Treverton, Gregory F., and Jeremy J. Ghez, ***Making Strategic Analysis Matter***, Santa Monica, California: RAND Corporation, 2012, http://www.rand.org/content/dam/rand/pubs/conf_proceedings/2012/RAND_CF287.pdf
This RAND report is the result of a workshop that found that though there is not much demand for strategic analysis from policy and decision makers, there is substantial value in conducting this level of analysis.

A8.4. Analysis Scenarios and Historical Applications. Bruce, James B., and Jeffrey Martini, ***Whither Al-Anbar Province? Five Scenarios Through 2011***, Santa Monica, California: RAND Corporation, 2010, **http://www.rand.org/pubs/occasional_papers/OP278.html**

This report produced for the Marines by RAND analyzes the question, 'what does the future hold for Iraq's al-Anbar province?' The researchers play through five scenarios. The report concludes that the U.S. (and specifically the Marines) can influence some of the drivers shaping the scenario outcomes and suggests constant course of action evaluations to identify possible and probable future trajectories.

Ehlers, Robert S., Jr., ***Targeting the Third Reich: Air Intelligence and the Allied Bombing Campaigns***, University Press of Kansas, 2009
This book highlights the cooperative intelligence elements (Royal Air Force) and bombing elements (U.S. Army Air Force) of the allied forces in Europe during World War II. The text discusses the often overlooked value added by the combined intelligence-bomber efforts in crippling the German war-making capabilities.

Fukuyama, Francis, ***Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics***, Baltimore, Maryland: Brookings Institution Press, 2007
This book discusses the value, necessity, and difficulties for foreign policy analysts to anticipate wild card events (such as, the 9/11 attacks, the rapid emergence and spread of diseases like H5NI, and the collapse of communism) in world politics. The author points out that biases and political pressures often influence the prediction and likelihood assessments of these types of events. Additionally, the credibility of some assessments for the probability of these "wild cards" is questionable, with a "boy that cried wolf" tainted view.

Neustadt, Richard E., and Ernest R. May, ***Thinking in Time: The Uses of History for Decision-Makers***, 1st edition, New York: Free Press, 1986
This book provides methods decision-makers and analysts can apply from historical lessons to current decisions.

Taleb, Nassim Nicholas, ***The Black Swan: The Impact of the Highly Improbable***, 2nd edition, Random House Trade Paperbacks, 2010
This book defines and discusses "black swan" events. The author highlights the importance of considering black swans when conducting analysis and making judgments. Although rare, black swan events have occurred and may occur, with far reaching and dramatic consequences.

Vertzberger, Yaacov, ***Risk Taking and Decision Making: Foreign Military Intervention Decisions***, Stanford University Press, 1998
This book discusses the realities of risk and provides analysis of what elements impact risk judgments and preferences in individuals' decision-making. The author uses five case studies to illustrate the calculations and consequences of risks in military interventions.

Walton, Timothy, ***Challenges in Intelligence Analysis: Lessons from 1300 BCE to the Present***, Cambridge University Press, 2010

This work provides short, critical analyses of past scenarios that successfully or unsuccessfully employed intelligence analysis.

A8.5. Analysis Education and Training. Center for the Study of Intelligence, *The Future of Higher Education: Implications for Intelligence*, March 2015

This paper argues that because education models in formal education institutions have and continue to change, methods for training in the workplace must also change and adapt for new generations' learning styles.

Chang, Welton, and Philip E. Tetlock, *Rethinking the Training of Intelligence Analysts*, Taylor & Francis, 29 February 2016, http://www.tandfonline.com/doi/pdf/10.1080/02684527.2016.1147164#.V6SgAqpf3xg

This article discusses the continuing challenge of erroneous and/or incomplete intelligence assessments in the IC. The authors advocate for new training approaches for intelligence analysts that adopt a scientifically validated process, which regularly reevaluated against benchmarks.

A8.6. Deception Analysis. Barton Whaley, *Textbook of Political-Military Counterdeception: Basic Principles & Methods*, National Defense Intelligence College, 2007

This is a textbook on counterdeception. It is designed to help users think like a detective in employing analytical skills.

Godson, Roy, and James J. Wirtz, *Strategic Denial and Deception: The Twenty-First Century Challenge*, Transaction Publishers, 2008

This book considers whether globalization, proliferating communication technologies, and the dissemination of vast amounts of information make effective foreign denial and deception more or less likely.

Gooch, John, and Amos Perlmutter, *Military Deception and Strategic Surprise*, Digital Printing, 2007

The six essays in this book deal primarily with the theory of deception and strategic-level deception. They present a picture of the dynamics and potential benefits of deception. Examples of operational-level deception are mentioned in some of the essays to illustrate certain points.

Latimer, Jon, *Deception in War: The Art of the Bluff, the Value of Deceit, and the Most Thrilling Episodes of Cunning in Military History, from the Trojan Horse to the Gulf War*, The Overlook Press, 2001

This work shows how simple some tricks have been, but also how technology has increased the range and subtlety of what is possible—bogus radio traffic, virtual images, even false smells. He draws examples from land, sea, and air to show how great commanders have always had, as Winston Churchill put it, that indispensable "element of legerdemain, an original and sinister touch, which leaves the enemy puzzled as well as beaten."

A8.7. Analysis Policy and Guidance . This list is not intended to be comprehensive but rather to highlight several key resources.

AFI 14-133, *Intelligence Analysis*, 29 March 2016

As the keystone instruction for AF intelligence analysis, this publication codifies how the Air Force conducts and presents analysis capabilities in support of Global Integrated ISR and other service core functions. It establishes the standards for AF intelligence analysis and delineates the associated roles and responsibilities of AF ISR Enterprise organizations.

AFI 14-134, *Intelligence Analysis Production and Requirements Management*, 21 June 2016

This publication provides guidance and procedures on AF intelligence analysis production and requirements management in support of internal AF requirements, as an integral complement to the IC for DIAP-focused production, and in support of the annual AFISRPoA.

Air Force ISR 2023: Delivering Decision Advantage,
http://www.defenseinnovationmarketplace.mil/resources/AF-ISR_2023.pdf
This strategic document approved by AF/A2, discusses emerging and future challenges for the AF ISR Enterprise, and focuses on how the enterprise should posture to addresses these challenges while meeting enduring core missions.

Annex 2-0, ***Global Integrated Intelligence, Surveillance, and Reconnaissance***, 29 January 2015
The annex serves as an AF supplement to JP 2-0 and covers AF specific topics and perspectives on GIISR.

Commander ACC, ***GIISR Core Function Concept***, 23 Jan 2013
This document identifies five enduring core GIISR capabilities that directly support the JCA of Battlespace Awareness. Analysis is an essential and integral component of each of the five enduring capabilities.

DoDI 3115.17, ***Management and Oversight of DoD All-Source Analysis***, November 16, 2016
This instruction establishes DoD policy and assigns responsibilities for the management and oversight of DoD ASA. It also establishes the DIAAE BOG, an intergovernmental committee as the primary forum for DoD-wide analytic synchronization and integration.

ICD 203, ***Analytic Standards***, 2 January 2015
This directive establishes common analytic standards to be used across the IC to ensure clear communication among organizations.

ICD 204, ***National Intelligence Priorities Framework***, 2 January 2015
This directive establishes the NIPF as the mechanism to create, prioritize and share intelligence priorities.

ICD 206, ***Sourcing Requirements for Disseminated Analytic Products***, 22 January 2015
This directive establishes the sourcing information that must be included in covered analytic products so as to increase the credibility and transparency of intelligence analysis.

ICD 501, ***Discovery and Dissemination or Retrieval of Information within the Intelligence Community***, 21 January 2009
In pursuit of a culture of responsible sharing and collaboration across the IC, this directive establishes guidance and policies for the discovery, dissemination or retrieval of intelligence and intelligence-related information collected or analysis produced by the IC.

JP 2-0, ***Joint Intelligence***, 22 October 2013
This publication addresses the nature of intelligence and establishes the principles of joint intelligence. It is one of the base guiding documents for DoD IC organizations.

This Page Is Intentionally Left Blank

FM 34-8-2

INTELLIGENCE OFFICER'S HANDBOOK

HEADQUARTERS, DEPARTMENT OF THE ARMY

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

FIELD MANUAL
No. 34-8-2

Headquarters
Department of the Army
Washington, DC, 1 May 1998

Table of Contents

Page

PREFACE iv

CHAPTER 1 - G2/S2 ROLES AND MISSIONS 1-1
Why You Need This Handbook 1-1
Purpose of This Handbook 1-1

CHAPTER 2 - FORCE PROJECTION 2-1
Force Projection Principles 2-1
Intelligence Readiness 2-2
Indications and Warnings 2-5
Stages of Force Projection Operations 2-6

CHAPTER 3 - MILITARY DECISION-MAKING PROCESS (MDMP) 3-1

CHAPTER 4 - S2 OPERATIONS CHECKLISTS 4-1

APPENDIX A. UNIT INTELLIGENCE TRAINING CHECKLIST A-1
APPENDIX B. INTELLIGENCE PREPARATION OF THE BATTLEFIELD PRODUCTS B-1
APPENDIX C. RECONNAISSANCE AND SURVEILLANCE PLANNING C-1
APPENDIX D. PRIORITY INTELLIGENCE REQUIREMENTS, INFORMATION REQUIREMENTS, AND INDICATORS D-1
APPENDIX E. GRAPHIC REPORT FORMATS E-1
APPENDIX F. TARGETING F-1
APPENDIX G. IEW SYSTEMS G-0
APPENDIX H. MILITARY INTELLIGENCE UNITS AND CAPABILITIES H-1
APPENDIX I. INTELLIGENCE TRANSITION CHECKLIST I-1
APPENDIX J. INTELLIGENCE REFERENCE LIST J-1
APPENDIX K. WEATHER ELEMENTS AND SUPPORT K-1
GLOSSARY Glossary-1
REFERENCES References-1

DISTRIBUTION RESTRICTION: Approved for public release; distribution is unlimited.

LIST OF TABLES AND FIGURES

Page

Table 1-1. Collection resources 2-1
Table 4-1. Mission checklist 4-2
Table 4-2. N-Hour critical times 4-4
Table 4-3. N-Hour critical actions list. 4-5
Table 4-4. Mission planning sequence. 4-6
Table C-1. G2/S2 R&S responsibilities C-1
Table F-1. Bulk electric power supply F-38
Table K-1. Weather effects from cloud ceilings K-13
Table K-2. Weather effects from reduced visibility K-14
Table K-3. Weather effects from precipitation K-17
Table K-4. Weather and environmental data elements impacting Army systems and operations K-19
Table K-5. Windchill chart K-21
Table K-6. Daily water consumption requirements for three levels of activity K-23
Table K-7. Work time in hot weather operations K-24
Table K-8. WBGT index (light work) K-24
Table K-9. Conversion factors K-25

Figure 2-1. Principles of force projection IEW operations 2-2
Figure B-1. Modified combined obstacles overlay B-2
Figure B-2. Population status overlay B-2
Figure B-3. Key facilities and target overlay B-3
Figure B-4. Logistics sustainability overlay B-4
Figure B-5. Concealment and cover overlay B-5
Figure B-6. Lines of communication overlay B-6
Figure B-7. Doctrinal template - depicts enemy forces according to doctrinal deployment, unconstrained by terrain B-7
Figure B-8. Situation template - depicts deployed enemy forces adjusted for obstacles and terrain B-7
Figure B-9. Decision support template B-8
Figure B-10. Partial BOS synchronization matrix B-9
Figure B-11. Event template - considers COAs of reinforcing or counterattacking forces B-9
Figure B-12. Event template - depicts key events in each threat COA B-10
Figure B-13. Event matrix B-11
Figure B-14. Sample of an ADA-tailored IPB B-12
Figure C-1. R&S planning process C-2

Page

Figure C-2.	R&S planning considerations	C-6
Figure C-3.	Example of a brigade reconnaissance OPORD	C-8
Figure C-4.	R&S overlay with instructions on acetate	C-12
Figure C-5.	R&S tasking matrix	C-15
Figure C-6.	Example of a GSR OPORD	C-17
Figure C-7.	Sample IREMBASS employment OPORD	C-19
Figure C-8.	Sample patrol employment OPORD	C-20
Figure C-9.	Sample debrief format	C-21
Figure E-1.	Graphic INTSUM	E-3
Figure E-2.	Threat unit locations and mission activities (committed)	E-4
Figure E-3.	Threat unit locations and mission activities (uncommitted)	E-5
Figure E-4.	Threat mission capabilities assessment	E-6
Figure E-5.	Threat problem area symbology	E-7
Figure E-6.	Threat air activity symbology	E-8
Figure E-7.	Predicted threat activity timelines	E-9
Figure F-1.	Functions of intelligence support to targeting	F-2
Figure F-2.	Targeting methodology.	F-3
Figure F-3.	Targeting checklist	F-3
Figure F-4.	The targeting process	F-7
Figure F-5.	Example high-payoff target list	F-9
Figure F-6.	Example target selection standards matrix	F-10
Figure F-7.	Example attack guidance matrix	F-13
Figure F-8.	BOS detection capabilities	F-17
Figure F-9.	Intelligence disciplines	F-19
Figure F-10.	Deliver functions and responsibilities	F-22
Figure F-11.	BDA functions	F-27
Figure F-12.	CARVER techniques	F-31
Figure H-1.	MI battalion (heavy division)	H-1
Figure H-2.	MI Battalion (Light, Airborne, Air Assault Division)	H-2
Figure H-3.	Corps MI Brigade	H-3
Figure H-4.	Organization, MI Detachment, Spt Co, SFG	H-4
Figure H-5.	Organization, MI Detachment, Spt Co, SFB	H-4
Figure K-1.	Common weather elements	K-2
Figure K-2.	IPB weather overlay criteria	K-4
Figure K-3.	Example of a weather forecast chart	K-9
Figure K-4.	Example of a weather impacts display chart	K-10
Figure K-5.	Critical weather factors	K-11

PREFACE

This publication is a roles and missions manual for G2/S2 sections. As the companion handbook to FM 34-8, this manual is written for officers serving as the G2 or S2 in combat, CS, and CSS units. It provides guidance for officers and NCOs assigned to G2/S2 sections. G2s should find this handbook a useful MTP when executing intelligence training responsibilities.

The proponent of this publication is the United States Army Intelligence Center and Fort Huachuca, Fort Huachuca, AZ. Send comments and recommendations on DA Form 2028 (Recommended Changes to Publications and Blank Forms) directly to Commander, US Army Intelligence Center and Fort Huachuca, ATTN: ATZS-TDL-D, Fort Huachuca, AZ 85613-6000.

This manual does not implement any ISAs. However, it complies with the following STANAGs:

- STANAG 2022, Intelligence Reports, Edition 8.
- STANAG 2077, Order of Battle, Edition 5.
- STANAG 2149, Intelligence Requests, Edition 5.
- STANAG 2844, Counterintelligence Procedures, Edition 2.
- STANAG 2936, Intelligence Doctrine, Edition 2.
- STANAG 6010, Electronic Warfare in the Land Battle, Edition 1.

It also complies with QSTAG 593, Mutual Support Between EW Units; and QSTAG 1034, Intelligence Preparation of the Battlefield.

Unless specifically designated, all references to the intelligence officer at corps, division, brigade, or battalion will be stated as S2.

Acronyms and brevity codes used in this manual are identified only in the glossary.

Unless this publication states otherwise, masculine nouns and pronouns do not refer exclusively to men.

Chapter 1

G2/S2 ROLES AND MISSIONS

WHY YOU NEED THIS HANDBOOK

The G2/S2 must provide continuous intelligence and information for the commander to conduct operations and minimize risk.

Intelligence is the commander's decisionmaking tool. The commander, who drives intelligence, does so for planning before deployment, while enroute, and during operations and redeployment. The S2/NCO—

- Provides the commander timely and accurate intelligence, IPB, I&W, and vulnerability assessments for force protection, targeting, and BDA.
- Makes decisive predictions on when and where an action will take place.
- Prioritizes IR.
- Integrates with other staff elements on I&S issues.
- Provides the commander with a view of all facets of the battlefield.
- Ensures his staff is trained.

PURPOSE OF THIS HANDBOOK

This manual does not replace the doctrine and TTP contained in the other FM 34-series manuals; it does, however, focus on their application. It also summarizes information that helps the S2 manage and coordinate the CCIR. It provides the S2 the roles and missions required for executing the intelligence support function.

The G2/S2 is the “Top Down”/“Bottom Up” integrator of RISTA operations, which have always been performed at the brigade and battalion levels. Three factors help to redefine traditional R&S planning:

- Top Down reporting.
- Bottom Up reporting.
- Digitization.

Systems and technologies available to units make an integrated approach to managing “top down” and “bottom up” reporting feasible. The ACT serves as the nexus of RISTA operations, digitally linking the brigade S2 with the automated capabilities of the DS MI company, resulting in RISTA operations which blend intelligence, R&S, and TA. (See FM 101-5 for G2/S2 responsibilities and Table 1-1 for RISTA collection resources.)

Table 1-1. Collection resources

IEW	RISTA
SIGINT	Troops in contact
IMINT	Other troops in contact (RAS)
HUMINT	Scouts (aerial & ground)
CI	LRS, SOF
MASINT	Countermortar & CB radars
TECHINT	Gun cameras
	Hand emplaced sensors
	CA, PAO, PSYOP

Chapter 2

FORCE PROJECTION

FORCE PROJECTION PRINCIPLES

Future Army operations will rely more heavily on the force projection of US combat power. There is no single method to support force projection. This chapter identifies key principles and considerations for planning and executing IEW force projection.

Successful force projection of IEW support is based on understanding and applying the key principles shown in Figure 2-1.

Other key force projection components are intelligence readiness and a requirement to define responsibilities each echelon performs down to the lowest tactical level. This chapter discusses—

- Intelligence readiness.
- I&W.
- Stages of force projection operations (minus operations).

Considerations are in a logical order but may not be sequential nor applicable for all force projection missions. Corps and division G2s must provide primary planning support for force projection operations because of their expertise. The S2 at each level identifies—

- Personal knowledge deficiencies (e.g., communications architecture, imagery dissemination systems and methods, ability to identify the staff's shortcomings).

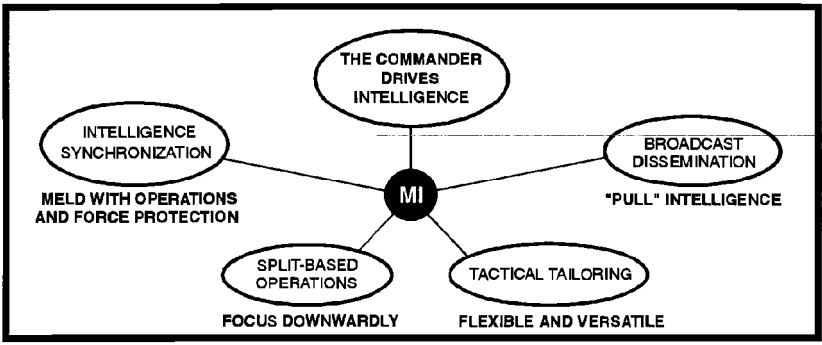


Figure 2-1. Principles of force projection IEW operations.

- Technical limitations (e.g., ASAS, SIDS capability).
- Intelligence gaps with adequate specifics.

INTELLIGENCE READINESS

In a JTF force projection operation, higher echelons will provide intelligence for situation and target development to lower echelons (top down) until the tactical ground force completes entry and secures the lodgment area. The JTF J2 may be reluctant to push everything down through tactical intelligence channels due to the volume of the intelligence information available. The S2 may receive support on a “smart push” basis, and needs to know his requirements to be able to do a “smart pull.”

The most significant change in the evolution of force projection operations is the enhanced information flow through hierarchical and non-hierarchical networks (computer, communications, and personal). The S2 should—

- Review available databases on assigned contingency AIs; conduct IPB on these AIs; and develop appropriate IPB products.
- Be aware of higher HQ SOPs and DIA manuals for specific CM guidance.
- Prepare, practice, and conduct information collection activities as part of in-garrison IO rehearsals.

- Preplan and practice an intelligence "surge" on likely contingency crises.
- Prepare and practice coordination from predeployment through redeployment with personnel from imagery, SIGINT, HUMINT, SWO, CA, PSYOP, and SF units, to include databases and connectivity.
- Ensure the following are a part of the daily operating environment:
  - — RC and other augmentation.
  - — Line numbers and SOPs including a linguist plan with proficiency scores (alert through early entry phases of deployment).
  - — Training (individual and collective).
- Form ad hoc intelligence links and networks early on to meet a developing contingency. Incorporate, request, and receive intelligence from unfamiliar sources (linguists, MI augmentation, other services); exploit NGOs and PVOs once a crisis emerges. Exchange communications protocols with theater and higher HQ and subordinate and lateral units.
- Forward all RIIs to the higher HQ IAW SOPs. The J2, G2, and S2 can focus intelligence downward based on the commander's needs.
- Understand the JTF J2's multiple echelon and broadcast dissemination capability to ensure NRT reporting to all deployed, in transit, or preparing to deploy forces.
- Maintain an intelligence database on the battlefield environment and threats for each contingency. The S2 must state and record the CCIR as PIR, subordinate SOR, and SIR, and include the following:
  - — For the battlefield environment, the commander's approval of the AI, to include separate ground, air, littoral waters, and political AIs.
  - — Maps, terrain, and weather products. Request from National Imagery and Mapping Agency hard copies (unclassified or at the lowest classification). Request authority to declassify these products locally.

— Digitized products (map sheets for ASAS, terrain data, and imagery).

— Physical environmental information. The TERRA BASE program allows S2s to template the effects of terrain on communications and direct fire. During mission analysis, TERRA BASE or other automated terrain products—WINCATS, TOPOSKINNER—provide the S2 a tool to help the commander visualize how terrain can affect friendly and enemy forces. These products can illuminate terrain effects for subordinate commanders in the OPORD brief. [Technique: Use the program at Home Station to develop and sustain proficiency.] The supporting engineer staff officer may also have terrain visualization products.

— Threat or potential threats. The intelligence community, primarily the NGIC, and open sources produce products useful for intelligence readiness. These products can be tailored to best support the commander. (See FM 34-3 for information on intelligence analysis.) INTELLINK will be an S2's primary access to any type of requested strategic intelligence. Examples of strategic level products include—

- Global security forecast.
- Battlefield development plans.
- Automated and hardcopy databases.
- Arms proliferation and military power studies related to the weapons acquisition strategies and the overall military power and potential of selected foreign military forces.
- TECHINT and User Bulletins.
- CIA World Fact Book and DIA country studies.
- Open source studies and articles.
- Other services.

INDICATIONS AND WARNINGS

Theater and national intelligence units monitor regional and global threats to

provide I&W intelligence to the NCA and military commanders. I&W intelligence flows to strategic, operational, and tactical commanders; it prevents surprise, reduces risk, and supports development and refinement of CONPLANs. The S2 must ensure the commander identifies PIR, IR, and targeting requirements for each assigned contingency area. The S2 should—

- Conduct CM and synchronization planning on I&W requirements. Review your unit's collection plan and preplanned SOR for each contingency area. If necessary, refine existing collection plans and SOR.
- Review and modify reporting procedures for I&W contingency areas. This may involve changing intelligence reporting (e.g., increasing reporting on one area and decreasing reporting on another) and message routing addresses and precedence (e.g., FLASH designation).
- Prioritize and forward SOR to higher headquarters.
- Disseminate intelligence and information to the commander, staff, and subordinate units.
- Coordinate for direct dissemination when possible.
- Recommend to the commander whether to maintain or increase unit readiness levels; plan and surge the intelligence effort for the impending operation; or move the unit from its current mission to contingency, branch, or subsequent operations.
- Adjust intelligence readiness steps according to pre-crisis I&W.

STAGES OF FORCE PROJECTION OPERATIONS

REMINDER: All phases of the intelligence cycle are being executed continuously during all stages of force projection.

MOBILIZATION:

Mobilization is a process in which the armed forces augment the AC capability in preparation for war or other national emergencies. It includes activating all or part of the RC assembling and organizing personnel, supplies, and materiel; and certifying the proficiency of individuals and units.

(See FM 100-17 for mobilization process.) In peacetime, AC and RC MI units plan, train, and prepare together to accomplish mobilization and deployment tasks. During the mobilization phase, the S2 should—

- Assist the mobilizing RC unit by preparing and conducting intelligence training and threat update briefings and by disseminating intelligence.
- Identify force requirements for the different types of operations and CONPLANs.
- Employ and adhere to existing procedures.
- If possible, use prior coordinated IMAs to fill gaps created by personnel shortages. These IMAs should already have a working knowledge of your SOPs and understand the mission.
- Monitor intelligence reporting on threat activity and I&W indicators.
- Conduct or coordinate CI and OPSEC training and operations.
- Manage IR and RII from your unit and subordinate units.
- Evaluate reporting.
- Update collection planning.

PREDEPLOYMENT ACTIVITY:

Predeployment activity provides the foundation for subsequent force projection operations.

- I&W will continue throughout force projection operations. The S2 must perform IPB early and continuously. (See FM 33-1, FM 34-130, FM 41-10.)
- Accelerated training will ensure all AC and RC MI units are able to conduct IEW operations. Integrate mobilization and deployment tasks into unit METL and training; emphasize and integrate critical aspects of force projection into battle tasks and planning.
- Focus broadbased knowledge to support CONPLAN refinement (IPB).

- Ensure tactical tailoring or split-based operation planning is based on an existing CONPLAN.

- Establish appropriate relationships; establish higher, lower, and lateral liaisons if they are different.

- Continuously conduct and update CM and IEW synchronization planning.

  — IO synchronization ensures IO are linked to the CCIR and respond in time to influence decisions and operations. IO encompasses more than just MI assets and requires MI support. (See FM 34-40 and FM 100-6.)

— IEW synchronization ensures IEW operations are linked to the CCIR and respond in time to influence decisions and operations. IEW is a subset of IO.

— The commander generates CCIR. CCIR focus on what is critical. They should change as the situation changes. CCIR affect PIR, IR, EEFI, and FFIR.

o Plan imagery coverage for target nomination, validation, and PSA.

o Require from collection assets, timelines for preplanned and dynamic collection requests.

o Plan synchronization through all five steps of the intelligence cycle.

o Ensure each PIR is related to a specific operational decision. (See FM 34-2 and FM 100-6.)

o Prepare an ISM and backward plan so collection production efforts are executed with the operation; deliver focused intelligence to support operational decisions.

o Coordinate with the S3 and signal officer for EW offensive and electronic deception operations, specifically for target nomination, no-fire target criteria, protected frequencies, and synchronized EW effort during all phases of the operation.

o Plan BDA requirements.

o Refine, manage, and update SOR. Monitor and maintain synchronization.

- Anticipate and initiate collection early against long lead-time requirements.

- Ensure CCIR process is continuous and the intelligence cycle and IEW operations remain tied to the commander's decisions and concept of operations.

- Identify collection gaps after you synthesize available information on the AO and coordinate the collection efforts of existing intelligence organizations. (Consider national, EAC, other US forces and services, and HN support.)

- Develop a collection strategy which factors PIR, IR, and METT-TC. Submit RII and other requests for support to adjacent, higher, and HN units. Develop a collection plan which supports all PIR and IR and maintains synchronization.

- Develop your intelligence team:

— *Commander's intelligence support*: The S2 and supporting MI commander form the maneuver commander's intelligence team. ASAS is the primary intelligence processing system supporting this team. A unit may need to augment its S2 staff, to include area experts, TECHINT LNOs, linguists, interrogators, intelligence analysts, and CI agents. Tailor the size and sophistication of the deploying unit's intelligence staff to the mission.

— *ACT*: The DS MI company provides an ACT to support the commander's intelligence team at brigade.

— *Additional attachments*: These could include PSYOP and CA.

— *DISE*: This is a small intelligence support team that provides communications, automated intelligence fusion, and broadcast downlinks in a small package capable of deploying with Army early entry forces.

- Decide whether you will form the DISE from the organic assets of the early entry force or from the corps ACE, supporting EAC MI brigade, or a combination thereof.

- Plan the configuration, which can range from "briefcases" (Mini-DISE) to HMMWVs (DISE vehicular), and are normally staffed by 5 to 12 soldiers, respectively. Build the supporting hardware systems around the Army's ASAS and integrate them with other Army, joint intelligence, and communication capabilities.

- Plan whether the DISE will expand to a full ACE as lodgment operations are completed or will disband once the mission is accomplished.

- Plan situations in which the DISE will go directly to higher headquarters for information without the home base's approval.

- Plan on requirements to support the DISE with 24-hour operations.

— *ISB*: This is the rear element of split-based operations that provides processed and analyzed intelligence to the DISE.

- Plan the automation, communications capacity, and personnel necessary to provide continuous intelligence requirements management, collection, processing, and reporting.

- Plan all procedures for the DISE to "pull" specific intelligence products and reports, obtain status of collection, and "push" the current intelligence picture from the lodgment back to the ARFOR and JTF commanders if not in theater.

— Plan all links to higher intelligence organizations, including the JIC and the elements designed to leverage theater intelligence; focus on support down to the corps and echelons below corps (e.g., the CMISE).

— Coordinate with and understand the capabilities of the JTF to include the NIST if formed.

— Plan to use RC augmentation. Some examples are a mix of CI agents, UAVs, interrogators, and linguists.

- Transportation availability (aircraft or naval vessel) for deployment.

- Sustainability.

- Portability once deployed.

- Disciplined operations. The commander's ability to collect may be affected by nonmilitary decisionmakers. The CINC can contribute to the deploying commander by ensuring at the outset that intelligence is decompartmented and releasable to allied units (if

applicable).

— Review applicable publications (ARs, DA Pamphlets, USSIDs).

— Review SOFAs, ROE, international laws, and other agreements. (Coordinate with SJA on these issues.)

— Review applicable NIMA guidance.

— Establish force deployment priorities based upon METT-T. Sequence initial required forces and capabilities, build-up priorities, and follow-on forces to ensure a sequenced plan, a tailored force, and established command and support relationships. Consider sensors, processors, preprocessors, CI, and HUMINT. Maintain unit integrity.

— Plan communications architecture (build redundancy when possible). Remember to—

  - Plan links to the JTF DISE, if formed, that complements the NIST. (See FM 34-25-3 and FM 34-37).

  - Ensure intelligence links provide the early entry commander vital access to multisource Army and joint intelligence collection assets, processing systems, and databases.

— Ensure collection is synchronized with production, and intelligence is still synchronized with operations (specify reporting procedures and timelines).

— Finalize the IEW OPLAN (terrain and communications deconfliction). Coordinate with the MI commander on his tactical decisionmaking process. Understand the MI commander's SOR that are his specified tasks, implied tasks, task organization, concept of operation (the organization, deployment, allocation, and employment of subordinate MI units), and coordination requirements with forward maneuver units.

— Establish the intelligence crossover point. Estimate the time and establish a measurable criteria to indicate when you have reached that point. Intelligence crossover occurs when enough tactical

collection assets are in theater to reduce the dependency upon strategic

or national assets. (See FM 34-1, Chapter 3.)

- Receive all augmentation and support elements quickly (ACT, DISE) and incorporate them within your unit, SOP, and training.
- Update databases to support the IPB process that will follow. Practice using INTELLINK.
- Support force protection. Intelligence operations—MDCI in particular—identify, locate, and target an enemy's ability to target and affect friendly forces, facilities, and operations. Intelligence support must—
  - — Conduct threat and risk assessment.
  - — Consider elements of fratricide avoidance:
    - Accurate target identification.
    - Collateral weapon effects.
    - Familiarity with supporting units.
    - ROE.
  - — Consider elements of force protection:
    - Information Warfare:
      - OPSEC.
      - Physical destruction.
      - PSYOP.
      - Deception.
      - EW.
    - COMSEC.
    - NBC.

- Personnel security.
- Neutrality maintenance.
- Personal awareness.
- Sniper threat.
- Counterreconnaissance.
- Arms and physical security.

— Using the MDCI process, assess and review friendly vulnerabilities and the threat's ability to exploit them.

- S2s should inform commanders and operators on CI and MDCI analysis.
- Train your MDCI analysts to conduct reverse IPB and think like the enemy S2, to include the enemy's perception of friendly centers of gravity and how he will attack or influence them.
- Incorporate your MDCI analysis into the G2/J2 situation and decision briefings and all planning (especially deception planning).
- Assign CI and MDCI sections appropriate missions and analytical responsibilities, such as rear area threat analysis, and continuously assess effectiveness.

— Identify potential countermeasures to deny the enemy access to friendly critical areas.

— Identify and recommend actions to counter enemy intelligence collection capabilities.

— Implement the following controls to support force projection:

- Establish access to national HUMINT and CI databases, automated links to joint service, coalition, and HN sources to help identify, assess, and develop countermeasures for threats. Develop FLASH precedence reporting procedures.

- Receive and disseminate CI information and specific CI tasks from ASAS and other means such as the CHATS.

- Support further CONPLAN and OPLAN development. MI units continually monitor and update their CONPLANs to reflect the evolving situation, especially during crises.

- Immediately before deployment, update deploying forces with the most recent intelligence on the AO and update your technical databases and situation graphics.

- Develop contingency tailored packages that allow the G2/S2 to place the right force support teams in a deployable posture with an adequate amount of training.

DEPLOYMENT:

Success in force projection operations hinges on the capability of airlift and sealift assets to move forces into the AO. Force protection is more critical during this stage.

- Monitor intelligence reporting on threat activity and I&W indicators. Continuously conduct and update IEW, CM, and synchronization planning.

- Plan enroute updates to eliminate information voids and allow your commander to adjust OPLANs prior to arrival in theater. Request supporting intelligence organizations use SATCOM, broadcast technology, and ADP systems to provide graphic and textual intelligence updates while enroute.

- Continue IPB.

- Provide timely, accurate, and specific infrastructure and weather information. IMETS can provide weather information.

- Use accurate situation development to help the commander understand and reduce risk on the battlefield.

- Use the DST, collection plan, R&S plan, ISM, and SOR to anticipate which decisions the commander and staff will make.

ENTRY OPERATIONS:

During initial entry operations, EAC organizations provide major intelligence support in a "smart push" mode. This support may include departmental, joint, and scalable Army intelligence elements capable of deploying forward. Entry units must continue to "smart pull" the intelligence they need for operations.

- Continue to conduct force protection planning.
- Monitor the buildup of the in-theater capability required to conduct sustained IEW operations and to reduce your total dependence on split-based, "top driven" intelligence from outside the AO. As organic IEW assets flow into the theater, assess their reliability for tactical intelligence. (National and theater organizations will still remain sources of strategic intelligence.) Determine intelligence crossover point.
- Monitor intelligence reporting on threat activity and I&W indicators.
  - — Routinely debrief troops.
  - — Use local nationals employed by or in frequent contact with your force to provide information (area experts must analyze it).
- Ensure liaison personnel and basic communications are in place prior to the scheduled arrival of parent commands.
  - — Deploy HUMINT forces into theater as early as possible.
  - — Contact HN or civil authority. (Contact CA units; see FM 41-10.)
  - — Contact other services.
  - — Contact lateral units.
  - — Coordinate with supporting CI unit for CI support to force protection.
- Emplace ACT, DISE, NIST, and other elements.
  - — Establish security.
  - — Establish communications.

- — Establish analytical capability.
- — Perform IPB.
- — Continue to conduct CM and intelligence synchronization planning. Recommend revised PIR and IR. Refine, manage, and update SOR. Evaluate reporting.
- — Consider space requirements, power, and logistical support for high use or unique items.

- Conduct situation development, target development, and support to targeting. During this stage as combat strength increases, your unit's organic tactical systems will conduct situation and target development (intelligence crossover point).

- Develop measurable criteria to evaluate the results of your collection plan. Reassesses—
  - — "Push" versus "pull" requirements.
  - — Communications architecture.
  - — Reporting procedures and timelines.
  - — Crossover point in intelligence.
  - — Intelligence support to OPLANs and OPORDs, branches, and sequels (to include planning follow-on forces).

WAR TERMINATION AND POSTCONFLICT OPERATIONS:

Upon cessation of hostilities or truce, deployed forces transition to a period of postconflict operations.

Commanders redirect PIR and IR to support units conducting restoration operations (e.g., engineer units conducting infrastructure reconstruction operations, medical and logistics units providing humanitarian relief). The nature of the PIR shifts from assessing threat forces to assessing political, economic, social, religious, and other conditions that affect force protection and the desired end-state; planning residual presence of US forces; and preparing for redeployment of forces.

- Continue to conduct force protection planning.
- Remain open to the possibility that hostilities could resume.
- Monitor intelligence reporting on threat activity and I&W indicators.
- Continue to conduct CM and intelligence synchronization planning. Update collection planning.
- Refine, manage, and update SOR.
- Evaluate reporting.
- Disseminate intelligence.
- Use pre-deployment tactical tailoring procedures to plan a phased redeployment of IEW assets and personnel ensuring continual coverage of the commander's requirements.

REDEPLOYMENT AND RECONSTITUTION:

As the combat power and resources decrease in the AO, force protection and I&W become the focus of the CCIR. This drives the selection of those MI units that must remain deployed and those which may redeploy.

- Monitor intelligence reporting on threat activity and I&W indicators.
- Continue to conduct force protection planning.
- Request intelligence BOS support (theater and national systems) and provide intelligence in support of redeployment and reconstitution (reverse intelligence crossover point).

DEMOBILIZATION:

Demobilization is the process by which MI individuals and units transfer from active to a premobilization or other approved posture. MI units resume intelligence readiness posture. RC MI units transition to peacetime status.

- Monitor intelligence reporting on threat activity and I&W indicators.
- Capture consolidated databases.

- Capture lessons learned via AARs (doctrine and TTP).
- Maintain intelligence readiness (e.g., training).
- Adjust MTOEs and evaluate the need for IMAs.

Chapter 3

MILITARY DECISION-MAKING PROCESS (MDMP)

MDMP in General

- FM 101-5 is the doctrinal source.
- The MDMP is a single, established, and proven analytical technique.
- The commander must follow the one-third/two-thirds planning rule.
- MDMP helps the commander and staff examine a battlefield situation and reach logical decisions.
- The commander can decide to use the complete or abbreviated version.
- Staffs should train on both the complete and abbreviated versions.
- Incomplete execution of the MDMP is a recurring deficiency at the CTCs.

Intelligence in the MDMP

- MDMP is based on continuous IPB, especially initial IPB during mission analysis.
- The commander drives intelligence; IPB is an integrated staff function driven by the commander.
- Train your section to conduct IPB so you can coordinate closely with other staff and BOS representatives.
- You must understand how all the BOS operate and how to integrate intelligence during planning, especially within the targeting process IAW FM 6-20-10.
- "Push" the staff to develop a robust and integrated R&S plan.

Staff Estimates

- FM 101-5 provides a generic staff estimate.
- The generic staff estimate is the base for the commander's operations, personnel, intelligence, logistics, CMO, communications, and special staff estimates.
- These staff estimates are designed to form, analyze, compare, and recommend friendly COAs.
- Staff estimates are continuous, must not be overly time consuming, and do not have to be a written product (time dependent).
- The wargame results and staff estimates help the staff compare COAs.

The Intelligence Estimate

- The purpose, scope, and content of the intelligence estimate changed with draft of FM 101-5.
- The old intelligence estimate was a text-based product derived from IPB that focused on ECOAs, capabilities, strengths, and vulnerabilities.
- This old intelligence estimate is functionally replaced by IPB products.
- A standard staff estimate prepared by the G2/S2 is the new intelligence estimate—it is radically different.
- The new intelligence estimate focuses on the G2/S2's ability to support friendly COAs and is used to compare and approve friendly COAs.

Step 1: Receipt of Mission ■ The mission comes from higher headquarters or is derived from an ongoing mission. ■ On receipt of a new mission, the G3/S3 issues a WARNO to the staff. ■ The staff immediately prepares for mission analysis (SOP preparation). ■ Immediately the commander and staff do a quick initial assessment with emphasis on an initial allocation of available time. ■ The commander issues his initial guidance, and the G3/S3 issues a WARNO to subordinate units.	**Intelligence in Step 1** ■ Collaborate with your higher G2/S2 before and during receipt of mission to facilitate the initial IPB. ■ As part of the initial assessment, look for gaps in your intelligence database and products. ■ Proactively request/prepare terrain products, weather, light, and climatology data; update the MCOO and doctrinal templates; maintain the enemy situation. ■ Focus on the initial time allocation (complete or full MDMP), R&S guidance, and any additional tasks or focus from the commander's initial guidance. ■ Establish/verify an IHL.
Step 2: Mission Analysis 1. Analyze the higher HQ order. (If confused by or you disagree with it, seek immediate clarification or resolution.) 2. Conduct initial IPB. 3. Determine specified, implied, and essential tasks. (It is important to understand specific requirements for each task.) 4. Determine the AI. 5. Review available assets. (The staff must identify additional resources needed to ensure the mission's success.) 6. Determine constraints (normally found in the scheme of maneuver, concept of the operation, and coordinating instructions). 7. Identify critical facts and assumptions. (List all appropriate assumptions from higher; state relevant conditions over which the commander has no control.) 8. Conduct risk assessment. 9. Determine initial CCIR. (Limit to 10 or less.)	**Intelligence in Step 2** ■ Intelligence and intelligence-related products: ❙ AI. ❙ Initial PIR (from the commander.) ❙ Initial OPSEC vulnerabilities and EEFI.***** ❙ MCOO and terrain as described by OCOKA and its effects. ❙ Assumptions (include enemy mission, objectives, threat BOS activities). ❙ Other elements of the battlefield. ❙ Situation templates (unrefined). ❙ Event templates and matrices (unrefined). ❙ Center/centers of gravity. ❙ HVTs. ❙ The IPB portion of the mission analysis brief and associated graphics (OB, weaknesses and peculiarities, activities and capabilities, and COAs). ❙ Collection plan (initial, G2 only).

10. Determine the initial reconnaissance plan. (The resulting R&S annex sets reconnaissance in motion.) 11. Plan use of available time. (The commander and staff refine initial plan for use of available time.) 12. Write the restated mission. Who, what, when, where, and why. 13. Conduct mission analysis briefing. (Given to commander and staff. The briefing is critical to ensure a thorough understanding of planning.) 14. Approve the restated mission. 15. Develop the initial commander's intent. A clear, concise statement of what the force must do regarding the enemy, terrain, and desired end-state. 16. Issue the commander's guidance. This provides additional guidance to focus staff planning. 17. Issue a WARNO. 18. Review facts and assumptions. When facts or assumptions change, the commander and staff must assess their impact.		The R&S plan (initial plan that starts R&S operations) and associated FRAGOs or WARNOs. | Intelligence estimate (initial). ■ These products are used to write Annex B to the OPORD or OPLAN and as the foundation for the DST* later in the MDMP. ■ Based on mission analysis, request information or intelligence based on intelligence gaps. ■ Develop as many ECOAs as time will allow. ■ Your higher HQ OPORD, OPLAN, and/or Annex B will task your unit to perform certain collection or R&S tasks. ■ Start the subsequent steps of CM & intelligence synchronization (FM 34-2) to support the initial collection plan (at a minimum SII, SIR, and SOR). ■ The R&S plan is a coordinated staff effort that must include FS, MEDEVAC, and CONPLANs (e.g., what the brigade does if 2 key scout sections are destroyed). ■ The MI Bn/DS MI Co participates in mission analysis and briefs the collection status and capabilities.
Step 3: COA Development 1. Analyze relative combat power. See FM 34-130 for estimating relative-force ratios. 2. Generate options. Goal is to develop COAs for every feasible ECOA; however, the commander usually limits that option with his guidance. 3. Array initial forces. Identify number of units needed and operational methods; develop a knowledge base to help make decisions. 4. Develop the scheme of maneuver. 5. Assign headquarters. This creates the task organization.	**Intelligence in Step 3** ■ Intelligence and intelligence-related products: | Situation templates (refined and prioritized). | Event templates and matrices (refined). | EWTL (initial).* ■ Ensure the G3/S3 uses the IPB facts, assumptions, and products developed during mission analysis and subsequently refined. ■ Work with the entire staff to ensure that friendly COAs take advantage of the environment and threat situation.*

6. Prepare COA statements and sketches. ■ The G3/S3 uses appropriate media to clearly portray how unit will accomplish the mission (e.g., scheme of maneuver).	■ Key on threat vulnerabilities. ■ Your input is critical in analyzing relative combat power. ■ Do not forget to support deception planning (when appropriate).
Step 4: COA Analysis (Wargme) 1. Gather the tools. 2. List all friendly forces. 3. List known assumptions. 4. List known critical events and DPs; include an HVTL list. 5. Determine evaluation criteria. 6. Select the wargame method. 7. Select a method to record and display results. 8. Wargame the battle and assess results. ■ The wargame is a critical and disciplined process used to visualize the flow of battle. ■ The commander selects the order of comparison of threat to friendly COAs. ■ The staff must evaluate the need for branches and sequels. ■ When technically possible, the staff should capture as much of the wargame on ATCCS as possible; otherwise, use a wargame worksheet or ISM. ■ These wargame results are key to developing DSTs and BOS synch matrix. ■ Use the action, reaction, counteraction method (consider at a minimum maneuver, FS, mobility, counter-mobility, survivability, and IEW). ■ The staff should track force ratios throughout the wargame.	**Intelligence in Step 4** ■ Intelligence and intelligence-related products: ❙ PIR with LTIOV (refined). ❙ HPTs. ❙ Confirmation of the enemy center/ centers of gravity. ❙ Situation templates (final). ❙ Some force protection issues (e.g., NBC vulnerabilities). ❙ EWTL (refined).***** ■ You wear both a "red" and "blue" hat in wargaming. ■ As the enemy commander you project enemy actions or reactions, develop DPs, and project enemy losses. ■ During the wargame you must address all relevant enemy BOS capabilities. ■ As the friendly G2/S2, you identify IR and NAIs; refine the situation template; and participate in the targeting conference. ■ Ensure the G3/S3 honestly portrays friendly capabilities during the wargame.***** ■ Work with entire staff to ensure friendly COAs take advantage of environment and threat situation. ■ Ensure HPTs, AGMs, and TSS support the operation.***** ■ The AGM is approved by the commander and addresses which targets will be attacked, how, when, and the desired effects. ■ TSS are criteria used in deciding whether to pass information as a target nomination.

	■ The MI Bn/DS MI Co commander and collection manager are important players at the wargame.
Step 5: COA Comparison ■ Used to identify COA that has highest probability of success. ■ Staff may use any technique; the decision matrix is the most common. ■ Staff gets its criteria from the commander (e.g., the principles of war or tenets of Army operations).	**Intelligence in Step 5** ■ Intelligence product: ❙ Intelligence estimate (final). ■ Ensure you play a key role during this step.
Step 6: COA Approval ■ If the commander modifies a proposed COA or gives the staff a new COA, staff must wargame that COA.	**Intelligence in Step 6** ■ Intelligence and intelligence-related products: ❙ PIR with LTIOV (approved). ❙ DST (an integrated staff product). ❙ BOS synch matrix.***** ❙ ISM. ❙ Event templates and matrices (final). ❙ The R&S plan (final).***** ❙ Collection plan (refined, G2 only). ■ Start the subsequent steps of CM and intelligence synchronization (FM 34-2) (i.e., development of new SII, SIR, and SOR). ■ If the commander designates you to perform BDA to support one of his decisions, you must thoroughly plan the BDA support and tie that plan into the collection plan.
Step 7: Orders Production ■ Based on the commander's decision and final guidance.	**Intelligence in Step 7** ■ Intelligence and intelligence-related products: ❙ OPORD or OPLAN Annexes B (Intelligence), L (R&S), P (C^2W)*****, Q (OPSEC)*****, S (Deception)*****, and T (EW).*****
***** The G2 participates in developing the products but is not the proponent.	

ACCELERATING THE MDMP:

The MDMP involves three techniques that can be applied in different situations: deliberate, abbreviated, and accelerated. Only the accelerated technique is discussed herein because it is the most difficult to implement. (See CALL Newsletter Update No. 95-12.)

The accelerated technique may be used when one or more of the following conditions apply:

- Commander has a staff available to assist him in developing the plan, but little time to use a more formal process.
- Commander does not have a staff, or the staff is not accessible.

When these conditions apply, the commander must rely primarily on TLP to develop his plan. The accelerated technique assists the commander in developing a tentative plan. Under extreme circumstances, this may be little more than a mental process; nonetheless, the commander can use it to assist him and key staff members (S2/S3/FSO/XO) as he develops his plan.

The accelerated technique follows the basic procedures in the deliberate and abbreviated processes, but the differences are more significant. The major differences between the abbreviated and accelerated techniques involve the commander's guidance and the COA development phase (Figure 3-1). The accelerated technique is characterized by active participation by the commander, and development of one COA that is suitable, feasible, and flexible.

In some situations, the products developed using the accelerated technique may be the same as those developed when using the deliberate or abbreviated technique. Because time is the key factor, the accelerated technique will normally result in the development of a FRAGO.

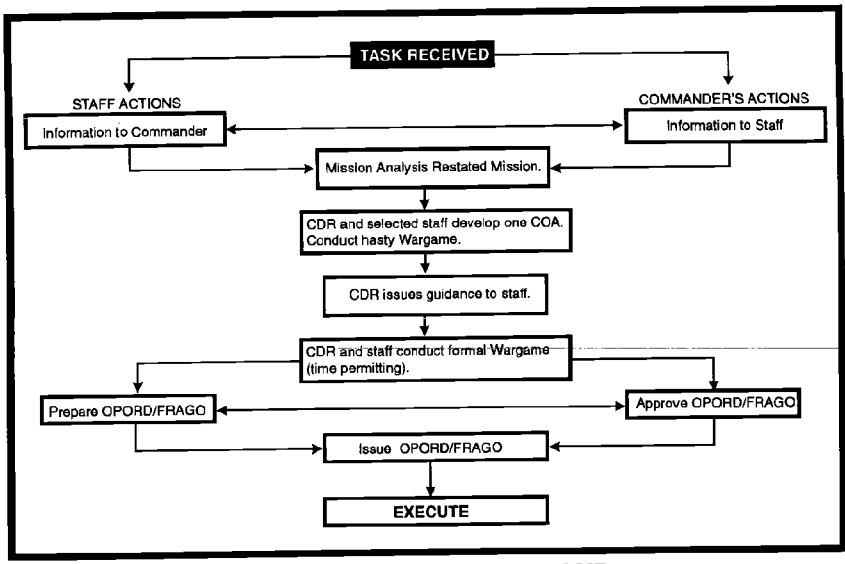


Figure 3-1. Accelerated MDMP.

MISSION ANALYSIS:

ISSUE: The commander and staff must be able to rapidly conduct the mission analysis to determine the restated mission.

DISCUSSION: When using the deliberate or abbreviated technique, the staff conducts a detailed mission analysis to develop the restated mission. As previously stated, resorting to a mental process in lieu of a detailed restated mission is acceptable; however, this should be the exception rather than the norm. The staff may be forced to brief their initial estimates orally, without the use of charts or viewgraphs. Conduct as formal a mission analysis as time allows. During the mission analysis, there are no major differences between the three techniques. There are no techniques that will significantly reduce the amount of time required to conduct the mission analysis. Anticipation, prior preparation, and experience by the staff are the keys to a timely mission analysis process.

TECHNIQUES:

- Commander must get personally involved by supervising and managing the mission analysis process.

- In extreme situations, the staff must be prepared to brief the commander without the use of visual aids.

COA DEVELOPMENT:

ISSUE: When time is severely limited, providing the commander's guidance after the mission analysis may not be the most appropriate time.

DISCUSSION: Instead, the commander may decide to immediately begin personally developing *one* COA with input from selected staff officers. There is probably not time to seek input from every staff officer, so the commander must determine relevant and critical staff officers (e.g., S2, F3, FSO, XO). This team may vary depending on the type of mission. For example:

- In the defense include staff engineer.

- During SASO include CA, PAO, SJA, PSYOP.

- In other situations, include subordinate commanders because of their experience.

This team must then quickly develop a flexible COA to accomplish the mission. The key to success, when using the accelerated technique, is to rapidly develop a base plan with appropriate branches that is flexible, feasible, suitable, and acceptable. *DO NOT WORRY ABOUT DEVELOPING THE PERFECT COA; THERE IS NOT TIME FOR IT*. This is the major distinction between the accelerated technique and the others.

Once the COA is developed, the commander might consider conducting a hasty wargame. In extreme situations, this may be the only opportunity to conduct the wargame process. Next, the commander should begin to quickly develop his guidance to the staff. The accelerated technique is

characterized by an active role of the commander, and very specific guidance to the staff.

TECHNIQUES:

- Focus on developing one COA with branch plans that is flexible, feasible, suitable, and acceptable.

- The commander plays the central role when developing this COA.

COMMANDER'S GUIDANCE:

Once the commander has developed the COA, he must issue guidance to his staff so it can refine and wargame the COA. The commander's guidance to the staff must be directive and specific. The staff's responsibility is to support the commander's plan, not to develop the perfect plan. Well-developed and clearly communicated commander's guidance can be a significant timesaver. The commander's guidance should serve to keep the staff focused by establishing parameters to work within. Commander's guidance must be constantly reviewed and analyzed. As the situation changes and information becomes available, the commander may have to alter his guidance to the staff.

COA ANALYSIS:

ISSUE. The commander and staff must rapidly conduct the COA analysis process.

DISCUSSION: Conducting the wargame process using the accelerated technique is the most difficult of the three processes because only one COA was developed. The purpose of the COA analysis is not to analyze and compare multiple COAs that result in a recommendation to the commander, but to synchronize and integrate the commander's directed COA. This wargame session should focus on refining the branches or contingencies to the base plan and follow the formal wargame process as much as time allows. Focus on the most critical events. You do not have time to wargame the entire operation. When wargaming using the accelerated technique, the commander's involvement is even more important. The staff should use the box technique, focusing on actions at the objective or the engagement area. If time permits, wargame other critical events as well. The staff must work to support the commander's plan. However, as the staff works to refine the plan, it cannot become so biased that it develops a plan that is infeasible and insupportable. If the staff determines that it cannot support the commander's plan, then a new COA must be developed.

TECHNIQUES:

- If time permits, conduct a hasty wargame session during the COA development step. Ensure you identify and develop branches to the base plan.
- Involve the commander. He must supervise the wargame session, actively participate, make decisions, and provide guidance as required.
- Use the box technique, focusing on the most critical event first.

DECISION:

When using the accelerated technique, a decision brief is not required because only one COA was developed. The only decision that may be required is if the developed COA becomes unsuitable, infeasible, or unacceptable. If this occurs, another COA must be developed.

ADVANTAGES:

- Requires less time.
- Facilitates adaptation to a rapidly changing situation.
- Allows commander to compensate for lack of a staff or an experienced staff.

DISADVANTAGES:

- Significantly limits staff initiative and flexibility.
- Very directive, explores only one friendly COA.
- May result in only an oral order or FRAGO.

CHAPTER 4

S2 OPERATIONS CHECKLISTS

Intelligence operations will usually begin with a notice tasking statement. CONPLANs, training, the N-Hour sequence, and the MDMP contribute to mission readiness. The S2 can use the following checklists to monitor intelligence readiness prior to receipt of a mission and subsequently to verify preparations and facilitate mission planning.

The timelines used could apply to any echelon.

- Mission Checklist (Table 4-1).
- N-Hour Critical Times (Table 4-2).
- N-Hour Critical Actions List (Table 4-3).
- Mission Planning Sequence (Table 4-4).
- Reconnaissance Planning (Table 4-5).

Table 4-1. Mission checklist .

Mission Day Minus	ACTION	REMARKS
A-28	Notify attachments to provide updated access rosters prior to A-Day.	
	Provide open access to national and strategic databases.	
	Initiate verification of clearances within battalion.	Include sensitive positions and RTOs.
	Coordinate security briefings for unit personnel.	Include all OPSEC program components and SAEDA program.
	Coordinate contingency AI briefings.	
	Verify access to intelligence databases through division or higher.	Disseminate hard copy products to subordinate units.
	Inspect unit areas and equipment for physical security deficiencies.	Coordinate for support and access. Check equipment compatibility.
	Review section files.	Designate deployable and nondeployable records.
	Obtain current TECHINT/User Bulletins and DIA Top Ten Equipment Acquisition list from 203d MI Bn (TECHINT).	Acquire information on disposition directives from JCS and theater commander.
A-21	Obtain higher HQ access roster.	Update as required throughout mission cycle.
	Coordinate security force requirements with tasked units and MP.	
	Identify linguists in unit or update current file.	Provide list, crosscheck with S1 data.
	Provide updated list of telephone numbers to be cut off at N+2 to the S1.	
A-14	Finalize security plans and instructions.	Check guard/MP patrols.
A-8	Coordinate security requirements for filler personnel.	Barrier material, lighting, container seals, security of vehicle holding area, motor pool, empty barracks.

Table 4-1. Mission checklist (continued).

Mission Day Minus	ACTION	REMARKS
A-8	Prepare DA Form 3964 for classified material transported with deploying elements.	
	Brief MI battalion LNO on duties.	
A-7	Finalize MI battalion personnel and equipment support list.	Ensure copy placed in SDO book.
	Update section alert notification roster.	
	Continually monitor intelligence WATCHCON levels.	
A-4	Check alert rosters in SDO book and completion of all unit OPSEC and SAEDA briefings.	
A-Day	Brief RDC on battalion security plan.	EEFI material, handle accordingly.
	Issue guard instructions.	
	Provide access rosters to rear detachment personnel, higher and supported HQ.	

Table 4-2. N-Hour critical times.

N-Hour	EVENT	REMARKS
N-Hour	Notify and assemble units.	
	Initiate telephone control.	
	Initiate area security plan.	
	List questions for N+2 brief.	
N+1:30	Prepare staff equipment to go to staging area.	
	Verify basic load, load plans.	Maps, batteries, etc.
N+1:45	Depart for N+2 brief location.	
	Distribute updated access roster.	
	Secure battalion conference room.	
N+2:00	Present N+2 briefing.	
	Coordinate with CI to initiate OPSEC plan; inspect battalion area for physical security violations.	
N+3:30	Present the intelligence estimate.	
N+3:45	Confirm transfer of company arms room keys to the rear detachment S2 before departing to staging area.	
	Verify security clearances of attachments through supporting S2.	
N+4:30	Sweep battalion area with CI personnel.	
N+5:00	Impose restrictions on incoming/ outgoing mail.	When given proper authority.
N+6:30	Issue OPORD at staging area.	
N+8:00	Ensure rear detachment is briefed on security.	
	Provide latest intelligence update to commander and staff. Have LNOs, DS MI CDR attend.	

NOTE: Modify times depending on mission requirements and SOPs.

Table 4-3. N-Hour critical actions list.

H-HOUR		ACTION	ACTION OFFICER(S)
	_____	Mission Receipt	
1	_____	WARNO----------	CDR, S2/S3
-	_____	Do IPB----------	S2 (w/asst from ENGR, Terrain, Weather, etc)
2	_____	Mission Analysis	
2	_____	Brief Mission to CDR----------	Coordinating Staff
-	_____	Initial CDR's Guidance	
2	_____	Do COAs----------	CDR, S2/S3
3	_____	Staff IPB & COAs----------	S2, S3
4	_____	Do Staff Estimates----------	Unit Staff
-	_____	COA Analysis (wargaming)----------	CDRs, Unit Staff
5	_____	Select Best COA----------	S3, Selected Staff
6	_____	Do DST----------	S2/S3, FSO, ADA, ENGR, SIG, CHEM
5	_____	Brief DST	
7	_____	Brief Selected COA----------	Selected Staff
-	_____	CDR's Decision	
7	_____	WARNO Scouts/Patrols Recon----------	S2/Asst S2/BICC officer/S3
8	_____	Mission Brief	
8	_____	OPORD Prep/Staff Coord----------	Unit Staff
8	_____	Turn in OPORD Annex	
9	_____	Proof OPORD	
10	_____	Issue Targeting Overlay----------	FSO
11	_____	Brief Scouts/Patrols Recon----------	S2/Asst S2/BICC officer/S3/ENGR/FSO/ADA
12	_____	Execution Matrix----------	S3
13	_____	BOS Synchronization Matrix----------	Unit Staff
14	_____	Maps/Charts Prep----------	Unit Staff
14	_____	CDR's Map Updated----------	S2/S3
15	_____	OPORD Rehearsal----------	XO, S3
16	_____	OPORD Briefing----------	XO
17	_____	Initial Backbrief	
17	_____	TF CDR Brief Higher HQ----------	CDR, S2, S3
17	_____	Co/Bn CDR Backbrief	
18	_____	Rehearsal----------	Unit Staff, CDR
19	_____	Final INTEL Update----------	S2
	_____	LD/LC	

NOTE: These items are not listed in a definite order; some may not occur at all.

Table 4-4. Mission planning sequence .

S2 ACTIONS UPON RECEIPT OF A MISSION:

1. Receive and analyze mission:
   - Receive CDR's guidance and assist in development of CDR's PIR.
   - Understand CDR's intent.

2. Define the battlefield environment:
   - Identify AO and AI.
   - Identify battlefield characteristics that will influence friendly and threat operations.
   - Identify intelligence gaps.
   - Develop preliminary IR.
   - Identify specified and implied intelligence tasks:
     - **Specified:** From OPORD Annex B, R&S Appendix, tasks to subordinate units, MI task organization for combat, coordinating instructions, and collection plan.
     - **Implied:** Mission dependent METT-T.
       M—**Mission** (CDR's intent, PIR, scheme of maneuver).
       E —**Enemy** (OB and IPB to develop collection IR).
       T—**Troops** (Organic and Higher Assets).
       T—**Terrain and Weather** (R&S asset LOS, LOCs, obstacles, weather effects on system's collection ability).
       T—**Time Available** (Plan, Move, Operate, Report).
   - Determine availability of organic/attached/supporting intelligence assets.

3. Request support/information from higher HQ if items/information are not available organically:
   - Maps/Imagery/sketches/blueprints of objectives, NAIs.
   - Collection plan, asset available times and asset tracks.
   - Weather - light data and climatic summary.
   - Enemy OB data.
   - Terrain products (LOC/vegetation/CCM/MCOO/elevation/LOS/hydrology).
   - Higher R&S plan.
   - Determine R&S assets you and higher HQ will control (intelligence architecture).
   - Determine availability, coordinate intelligence support from non-MI systems and organizations (AN/TPQ-36/37, OH-58D, FISTV, AN/TPS-25A, AN/TPS-58B, Engr, Co/teams, Cavalry, chemical units).
   - Obtain SOI; sign and countersign information through unit SIGO.
   - Advise higher of your recommended PIR and expected intelligence gaps.

4. Distribute maps, imagery, and sketches (maintain accountability).

5. Brief staff on abbreviated intelligence estimate to assist their mission planning.

6. Issue WARNO to R&S assets.

7. Describe the battlefield's effects:
   - Analyze terrain.
   - OCOKA factors.
   - Effect on friendly and enemy operations.
   - Analyze weather effects on terrain, troops, equipment, and friendly and enemy operations.

Table 4-4. Mission planning sequence (continued).

8. Assess other characteristics of the battlefield (mission dependent):
   - Politics.
   - Population.
   - Demographics.
   - Social ethnic/Religion.
   - Economic

9. Evaluate threat:
   - Evaluate enemy OB, current disposition and strength, committed and reinforcing units (maneuver, artillery, engineer, ADA, NBC, UW, air, intelligence assets, smoke, E-O sensors) and current significant activities.
   - Evaluate threat capabilities and tactics.
   - Develop/refine intelligence database and threat models.
   - Prepare doctrinal templates.
   - Prepare threat critical event lists.

10. Determine ECOAs:
   - Use doctrinal templates to develop event and situation templates (include all forces that can affect mission completion), AAs and MCs.
   - Identify enemy mission and intent.
   - Determine (in simple terms) how the enemy sees us acting in this operation.
   - Determine how the enemy is currently disposed and what must be accomplished to get from now to his desired end state, given that this ECOA must account for our actions determined in 3 above.
   - Determine enemy concept of the operation and subunit tasks. How will each of the following contribute to accomplishing the intent determined in 2 above:
     - Maneuver.
     - RISTA.
     - FS.
       - Artillery/mortars/rockets.
       - CAS.
       - Aviation.
       - NBC weapons.
       - EA.
     - Air defense - Recommend task organization for MI assets.
   - Identify most likely and most dangerous ECOAs.
   - Identify IR and NAIs for each friendly COA identified; TAIs with S3/FSO for each COA.
   - Develop HPTs for each friendly COA with S3/FSO.
   - Assist in developing HVTs for each ECOA.
   - Integrate EA into targeting.
   - Determine BDA criteria (damage required for each target, a means to determine damage).
   - Finalize and prioritize PIR (obtain CDR's approval).
   - Define indicators and SIR.
   - Send WARNO on threat to subordinate units to facilitate planning.

11. Develop ISM:
   - Tie to PIR/IR (include LTIOV).
   - Include timeline, required decisions, decision criteria, SIR, collection assets.
   - Plan for system cross-cue, back-up coverage.
   - Ensure it answers CDR's requirements for intelligence, targeting, and BDA in time to make decisions.

Table 4-4. Mission planning sequence (continued) .

- Participate in staff wargame of DST and targeting plan (as opposing CDR).
- Never hold MI assets in reserve.

12. Develop R&S plan and overlay to support DST (with support from S3/FSO/ENGR/ ADO) (see **Reconnaissance Planning** below):
- Determine indicators, SIR, NAIs, DPs, TAIs.
- Ensure NAI/TAI support synchronization or R&S plan with fire plan and scheme of maneuver.
- Identify intelligence gaps and request collection support from higher (RII).
- Develop communications plan/reporting schedule.
- Wargame R&S and collection plan.
- Update ISM, R&S, and/or collection plan.
- Receive, consolidate, and deconflict subordinate R&S plans and overlays.
- Consider "Reconnaissance Fundamentals" [Maximum reconnaissance force forward, orient on the location or movement of the reconnaissance objective, report all information rapidly and accurately, retain freedom to maneuver, gain and maintain enemy contact, develop the situation rapidly (FM 17-95).]
- Consider "R&S Principles" [(1) Tell the commanders what they need to know in time for them to act and (2) Do as much as possible ahead of time (FM 34-2-1)].

RECONNAISSANCE PLANNING

While the DMP for reconnaissance operations is conducted in the same manner as for any other combat operation, the following steps will assist the reconnaissance planner in ensuring that the unique features of reconnaissance operations are addressed.

Reconnaissance Mission Analysis

■ Identify Reconnaissance Objectives. Reconnaissance mission analysis must identify the objectives of the unit's reconnaissance effort. These objectives are obtained from—
- PIR.
- DPs.
- HPTs/HVTs.
- Confirming Events. (These are enemy actions and counteractions that confirm an ECOA and are determined by event analysis.)

The reconnaissance planner may determine that some of the above requirements may be accomplished by RFIs to higher HQ, but all of those that are not must become reconnaissance objectives.

■ Identify Reconnaissance AO. Reconnaissance planners identify the area in which reconnaissance forces will be operating, either specified by control measures such as LOAs or CFLs or implied by the location of reconnaissance objectives.

■ Restate Reconnaissance Missions. Once reconnaissance objectives have been determined, the mission for each element of the unit reconnaissance force must be determined from task analysis and stated as a subunit task. The task analysis process—determining specified, implied, and essential reconnaissance tasks and identifying limitations and constraints—is described in FM 101-5. Reconnaissance missions will be determined to be reconnaissance-in-force or zone, area, route, or force-oriented reconnaissance missions.

■ Identify Available Reconnaissance Force. Reconnaissance planners must identify the subunits that are available to execute the unit's reconnaissance effort and their current and projected status.

Table 4-4. Mission planning sequence (continued) .

■ Identify Available Equipment. Reconnaissance planners must identify the equipment available in an FMC status that will be used by elements of the reconnaissance force to accomplish reconnaissance tasks.

RCOA Development

■ Identify Required Reconnaissance Force. Reconnaissance planners must identify the force required to accomplish the unit's reconnaissance objectives. The number and type of elements involved will be based on the following:

- Number, type, location, and sequencing of reconnaissance objectives. Some objectives will require constant surveillance. Some will be time-phased and need only be observed for part of the battle. Some elements of the reconnaissance force will be able to accomplish several reconnaissance objectives.

- Type of reconnaissance mission. A route reconnaissance will require a different element than a reconnaissance-in-force.

- Strength, composition, and disposition of enemy security force. For each element of the reconnaissance force, the decision will have to be made whether it will have to infiltrate or penetrate the enemy security force. Infiltrations dictate stealthy elements and techniques while penetrations will require the correct reconnaissance force ratio.

■ Identify Required Equipment. Each reconnaissance objective will require specific reconnaissance equipment based on the following:

- Proximity of the reconnaissance element to the objective. What is the effective observation range?
- Environmental conditions. What will be the impact of severe weather? Night?
- Signature provided by the target. Does it emit a signal? Heat? Does it need to talk to anyone?

■ Determine the Reconnaissance Scheme. The RCOA must ensure that all reconnaissance objectives are addressed by elements of the reconnaissance force that can provide the read on the objective required by the commander. The reconnaissance force must therefore be in the right place, at the right time, and with the right observation, communications, and force protection equipment. The RCOA must deploy the reconnaissance force in depth to ensure that contact is not lost with moving reconnaissance targets. It must identify reconnaissance objectives that cannot be addressed so that RFIs may be prepared or risk accepted. In developing the RCOA, reconnaissance planners must answer the following questions:

- Are all PIR, HPT, DP, and confirming events addressed as reconnaissance objectives or RFI?
- What role will other BOS/combat operations play in the reconnaissance scheme?
  - FS (to include EA and SEAD for air insertions/extractions).
  - Air defense.
  - Mobility/counter-mobility.
  - CSS.
  - Deception.
  - OPSEC.
- How will this RCOA—
  - Maintain focus on the reconnaissance effort?
  - Gain and **maintain** contact with reconnaissance targets?
  - Provide early warning?
- How will we ensure that reconnaissance operations remain the bde/TF initial main effort?

Table 4-4. Mission planning sequence (continued) .

- What is the reconnaissance force's relationship with security force?
- How far forward will we conduct reconnaissance? Is there a force in front of us? What are the control measures?
- How will fire support be integrated into this RCOA?

■ Determine Task Organization, C^2 Relationships. Once the reconnaissance force and its associated equipment are determined, it must be task organized to accomplish the RCOA in the most efficient manner. The C^2 structure must address unity of effort by identifying the COR. **The COR must have the control structure and authority to direct the reconnaissance force.** Reconnaissance operations often take place over large distances and long periods of time where communications systems are subject to attack. The communications plan will require careful attention to the use of retransmitted teams and redundant systems.

■ Identify Control Measures. While reconnaissance operations require the same positive control measures as any other, some require special attention.
- LOA. This measure identifies the forward edge of the reconnaissance battlespace and is usually associated with a CFL or FSCL.
- BHL. Reconnaissance forces operate throughout the unit's AO, but must be able to coordinate the acceptance of reconnaissance targets entering their battlespace with the unit to their front.
- TF Forward Boundary. In brigade operations there will often be a need to identify a brigade zone forward of the subordinate maneuver TFs.

■ Determine CSS Requirements:
- Resupply: How often, by whom, where, how?
- CasEvac: By whom, how?
- Reconstitution: From where will reconstituted reconnaissance forces come? What are the priorities?

RCOA Analysis and Wargaming

■ Key Events to Wargame During Analysis of an RCOA:
- Infiltration or penetration of the enemy security force.
- Insertion/extraction methods.
- Backup communications plan.
- CasEvac operations.
- Change in reconnaissance objectives based on new information.
- Handover of reconnaissance target leaving reconnaissance unit's LOS or AO.

R&S Ten Keys To Success

1. Commander's intent and **CCIR** drive R&S.
2. Support **R&S** early with integrated staff products.
3. Be adept at abbreviated **IPB** for **Quick** or **Combat Decision Making Process.**
4. S2 focus on the event template to capture the moving enemy.
5. S2 then provides **situation template,** depicting enemy in the engagement area.
6. Use automation tools like **ASAS** to enhance products.
7. Deploy organic R&S assets early and request support from higher. Issue S3 **FRAGO** with S2 graphic overlay.
8. Provide continuous coverage throughout the depth of the battlefield.
9. Use all possible assets from national level to scouts.
10. Evaluate reporting and provide **immediate and continuous feedback** to the commander.

APPENDIX A

UNIT INTELLIGENCE TRAINING CHECKLIST

This checklist will help a newly assigned brigade or battalion S2 maintain technical and tactical intelligence proficiency. Its building-block approach is systematic. The phases are supported by tasks to be completed for certification during the time specified. Some tasks may not apply to a particular echelon of staff.

PHASE I - ORIENTATION PHASE

This phase covers basic orientation to the division and the unit's mission. **This phase should be completed within the first 30 days** . The goal is to quickly acquaint the S2 with an understanding of the battalion, brigade, and division roles within corps, possible missions, and deployment areas.

Initial/Date	Task
_____	Coordinate with and receive briefing from outgoing S2.
_____	Review unit's intelligence library of publications listed in Appendix J.
_____	Read unit METL and latest training brief to determine overall unit missions and status.
_____	Receive unit CDR in-brief.
_____	Talk with unit CDR; ask what are his desires for intelligence and intelligence products. Tailor intelligence to the needs of the CDR.
_____	Visit and receive briefing from ACofS G2, Deputy G2, G2 Operations Chief, G2 Plans Chief, G2 Training Chief.
_____	Meet with subordinate S2's and gain an understanding of—
_____	● Their commander's intelligence priorities.

- Personnel and equipment status.
- Training proficiencies and deficiencies.
- Areas where they need your echelon's help.

Visit MI battalion or DS MI Co commander for unit and equipment briefings, display, and demonstrations.

Study division, brigade, and battalion OPLANs.

Review and evaluate intelligence annex to unit SOPs. (Use FM 34-1, FM 101-5, your SOP, and intelligence annex to the division SOP.) Provide CDR an updated evaluation of the unit intelligence annexes. Develop an SOP if one is missing or outdated.

Receive an organizational and functional briefing from the next higher G2/S2.

Study the CDR's current PIR and IR as developed.

Meet and discuss intelligence missions, products, and training with the—

- Scout platoon leader.
- GSR platoon leader.
- Local division CI team.
- ACT.
- ACE Chief, IPS Chief, and CM Chief.
- EWO.
- Terrain detachment team.

Determine all organic or assigned division intelligence collection assets that may support collection efforts. (See Appendix G.)

Learn to use section's automation equipment and programs.

_____ Learn the connectivity, reporting, and requesting procedures.

_____ Meet with next higher echelon G2/S2 to discuss the CM process.

_____ Review unit's collection plan.

_____ Become knowledgeable of the unit's and division's FSOP, RSOP, and deployment procedures.

_____ Read unit and division history.

_____ Obtain SI access through the SSO and review SCI billets for unit.

_____ Review unit's arms room security SOP.

_____ Inventory all sensitive items in one company.

_____ Review key control program SOP.

_____ Review physical security and crime prevention SOP.

_____ Receive a crime prevention and physical security program briefing from the MP and Directorate of Security.

_____ Become familiar with the S2 section vehicles and generators, as necessary.

_____ Become familiar with the TOC SOP, setup, and multisystem, multiechelon connectivity.

_____ Visit G2 training for intelligence training products.

_____ Test an arms room’s J-SIIDS.

_____ Visit unit staff sections and attached sections from other units (FSO, ADA, NBC, SOCCE, and ENGR).

_____ Develop and implement a detailed internal security inspection program that covers intelligence areas within the unit.

_____ Develop working relationship with higher echelon G2/S2.

_____ Review mission and section METL and battle tasks. Have section members give their assessment of current training level.

PHASE II - FUNDAMENTAL PHASE

This is the most critical phase for the newly assigned S2. The knowledge, insight, and assessments of I&S will establish the foundation for future development. This phase focuses on the IPB process, intelligence production and dissemination, collection operations, and security. **This phase should be completed within 90 days** .

Initial/Date **Task**

_____ Present to unit personnel an officer professional development class on the threat.

_____ Update unit's collection plan as needed; submit revisions to the CDR and forward a copy to higher HQ G2/S2.

_____ Brief the CDR on division and corps IEW assets.

_____ Brief next lower units on division and corps IEW assets.

_____ Inspect unit map program. Identify basic map load and training requirements.

_____ Inspect and evaluate unit training for intelligence tasks, including awareness of AR 381-10.

_____ Determine country and area study requirements from open and classified sources based on contingency and assigned OPLANs.

_____ Begin country studies.

_____ Understand additional duty responsibilities as required:

_____ ● Security manager.
_____ ● Physical security officer.
_____ ● Personnel security officer.
_____ ● Crime prevention officer.
_____ ● Key custodian.
_____ ● Top secret document custodian.
_____ ● Information systems security officer.

_____ Receive briefing and training from unit SIGO on communications procedures and communications equipment PMCS.

_____ Become familiar with capabilities, limitations, and vulnerabilities of unit's equipment (tanks, Bradleys, other assigned, attached, DS systems, or OPCON BOS operating in the unit's battlespace; particularly the TA and information dissemination capabilities).

_____ Update, as needed, the unit's—

_____ ● Arms room SOP.
_____ ● Physical security SOP.
_____ ● Key control SOP.
_____ ● Crime prevention program.

_____ Conduct random unannounced security spot checks. Report the results and any recommendations to the CDR.

_____ Brief CDR on the unit's intelligence estimate.

_____ Brief CDR on the intelligence collection and reporting system from platoon through corps.

_____ Develop, update, and evaluate an S2 section METL and battle tasks.

_____ Be knowledgeable on CTC threat vehicles, E-O devices, doctrine, and tactics. Teach a class on this subject at least once in this phase.

_____ Visit nearest battle simulation center and become familiar with computer operations.

_____ Visit and observe training of primary weapon systems in the division.

_____ Understand current division policy on CONUS and OCONUS transportation of classified material.

_____ Work with commanders. Ask what intelligence they want during FTXs and OPORD briefings.

_____ Know how to read a TACFIRE direction system message. Let FSO know you want to receive these during FTXs and deployments.

_____ Work with FSO to develop and review unit targeting and BDA procedures.

_____ Know unit air LNO. Request BDA and in-flight reports that will bolster reporting.

_____ Obtain recent CTC and applicable CALL. Develop plan to correct any deficiencies.

_____ Obtain inspector general checklist and CIP checklists; conduct internal inspection on all S2 functional areas. Brief CDR on inspection results and solutions.

_____ Review language proficiency requirements; assist S3 in coordinating training. Retain list of unit's capabilities; include unpaid abilities.

_____ Conduct classified materials inventory; learn destruction and verification methods; review destruction and transfer SOPs.

_____ Constantly review clearance requirements, applications, and updates.

PHASE III - DEVELOPMENTAL PHASE

This phase will build and expand on the knowledge gained during Phase II. It will cover the same basic intelligence functions but in greater detail. **This phase should be completed within 180 days.**

Initial/Date	Task
_____	Fully understand the functions of the S2 at the unit's TOC and how S2 functions drive other TOC functions.
_____	Submit REDTRAIN requests through applicable higher S2 to G2 training, as required.
_____	Review threat OB holdings and files. Order update material as required.
_____	Determine available intelligence databases and actually "work the system" to obtain data in support of a CONPLAN. Brief CDR on the results.
_____	Identify gaps of information in battle books, OB holdings and files, and intelligence annexes. Submit RIIs to satisfy intelligence requirements.
_____	Identify S2 and intelligence weaknesses from the last EXEVAL and present a correction plan to the CDR.
_____	Evaluate intelligence training classes and provide written results to the CDR.
_____	Evaluate unit soldier's knowledge of intelligence training tasks and provide a written report to the CDR.
_____	Determine if all ADP systems are accredited. Brief CDR on steps needed to correct any problems.

_____ Demonstrate a thorough understanding of the intelligence reporting system during FTXs.

_____ Act as threat CDR during the wargaming process and TF rehearsals.

_____ Develop an internal S2 section intelligence cross-training program. Have section soldiers teach the classes.

_____ Determine unit's security posture during FTXs and recommend corrective actions to the CDR.

_____ Become familiar with and teach a class on doctrine, tactics, and current vehicles of a CONPLAN threat.

PHASE IV - ADVANCE PHASE

This phase will take the S2 who has mastered the intelligence fundamentals through **the first year,** during which the unit will have participated in the full annual training program.

Initial/Date **Task**

_____ Successfully complete an EXEVAL.

_____ Successfully deploy section and perform S2 operations during a CTC rotation.

_____ Successfully deploy section and perform S2 operations during a BCTP Warfighter Exercise.

_____ Qualify or familiarize yourself on all unit weapon systems.

_____ Update unit's intelligence annex as required.

_____ Research a classified intelligence topic that is relevant to the unit's mission and brief the CDR on the conclusion.

_____ Accurately predict threat actions during FTXs using IPB and all intelligence assets.

_____ Successfully integrate with higher echelon G2/S2.

APPENDIX B

INTELLIGENCE PREPARATION OF THE BATTLEFIELD PRODUCTS

This following examples of various overlays, templates, and matrices are constructed and used during the IPB process to enhance the battlespace visualization of the commander and staff. These samplings are not all-inclusive. Your products will be dictated by your mission statement, resources available to you, and the time allowed.

Figures B-1 through B-6 are terrain overlays. Figures B-7 through B-13 are templates and associated matrices. Figure B-14 is a sample of an ADA-tailored IPB.

The MCOO includes—

- **MCs** and **AAs** stated in terms of concealment and cover, size and deployment type of formation that can move along them (armored battalion in company wedge), speed the formation can reasonably achieve; dismounted, mounted, and aerial routes; trails and passes that will allow column movement if unopposed.

- **Obstacles** in terms of what they are an obstacle to.

- **Key terrain**.

- **Restricted terrain** in terms of what size force can deploy there and what mobility work could be done to "unrestrict" it.

- **Severely restricted** terrain in terms of what will allow a dismounted force to traverse it and at what speed.

- **IVLs**. Without a 1- or 5-meter resolution terrain product, IVLs will have to be determined by historical knowledge or ground reconnaissance.

- **Soils** and **weather analysis** that indicate trafficability and "dig-ability."

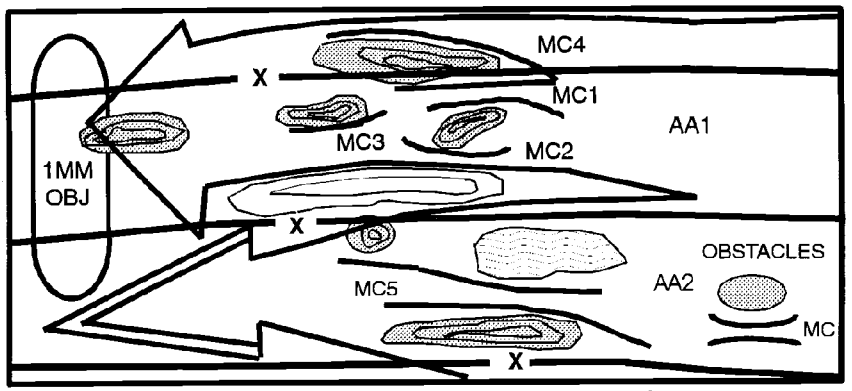


Figure B-1. Modified combined obstacles overlay.

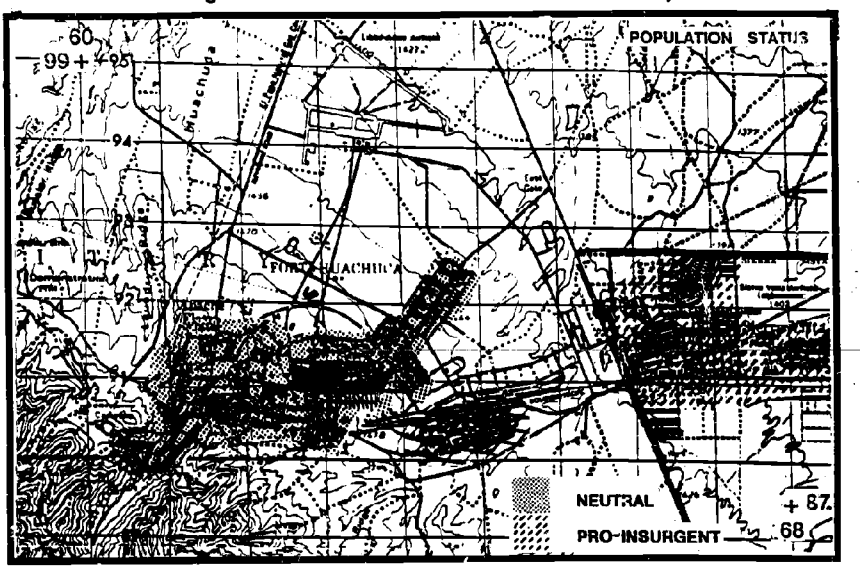


Figure B-2. Population status overlay.

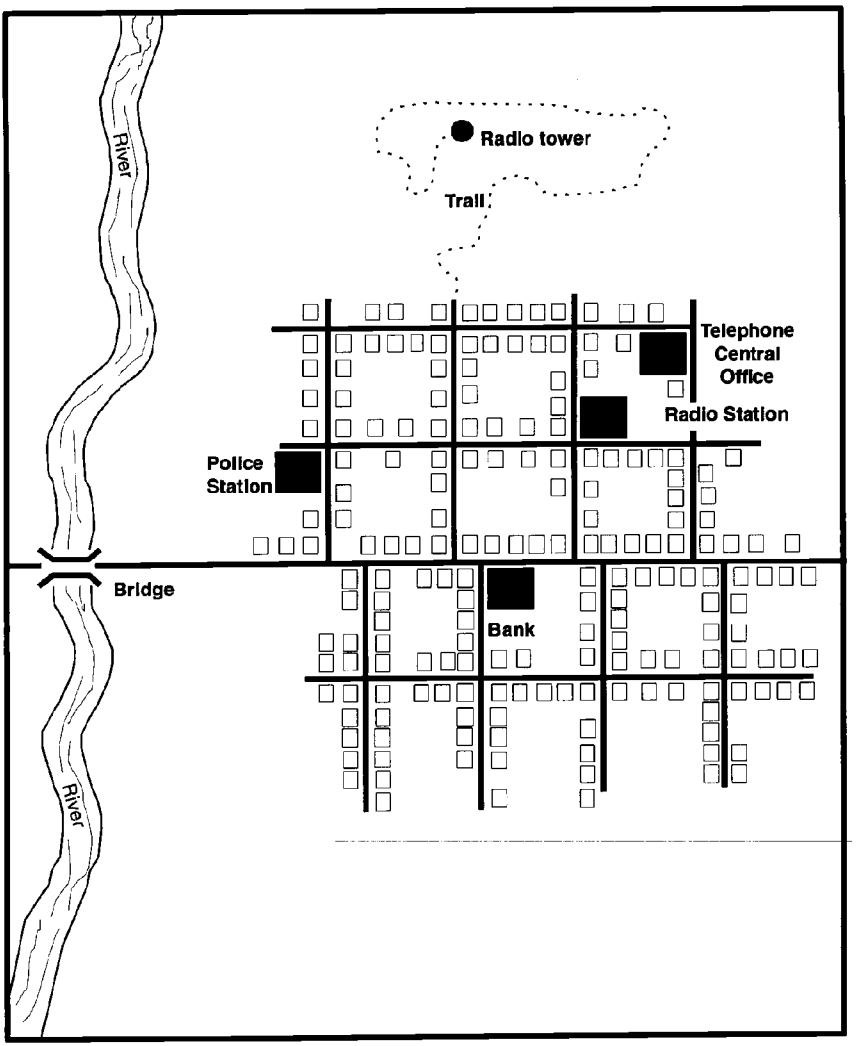


Figure B-3. Key facilities and target overlay.

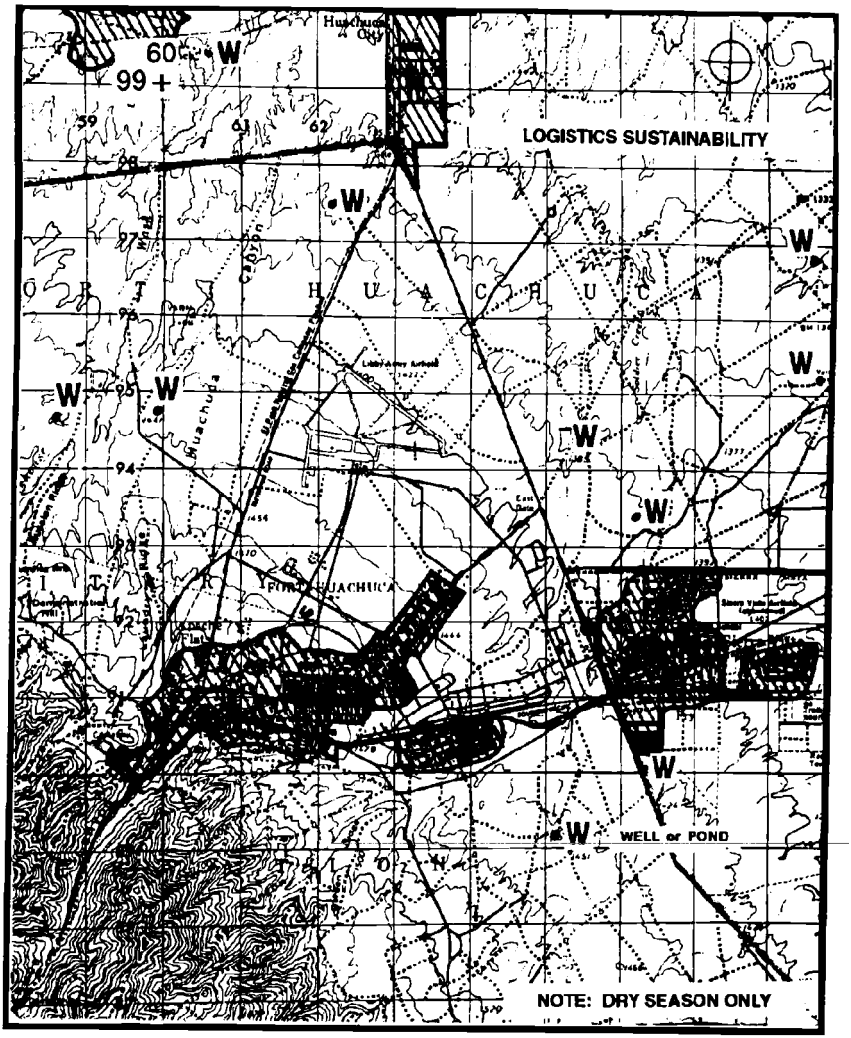


Figure B-4. Logistics sustainability overlay.

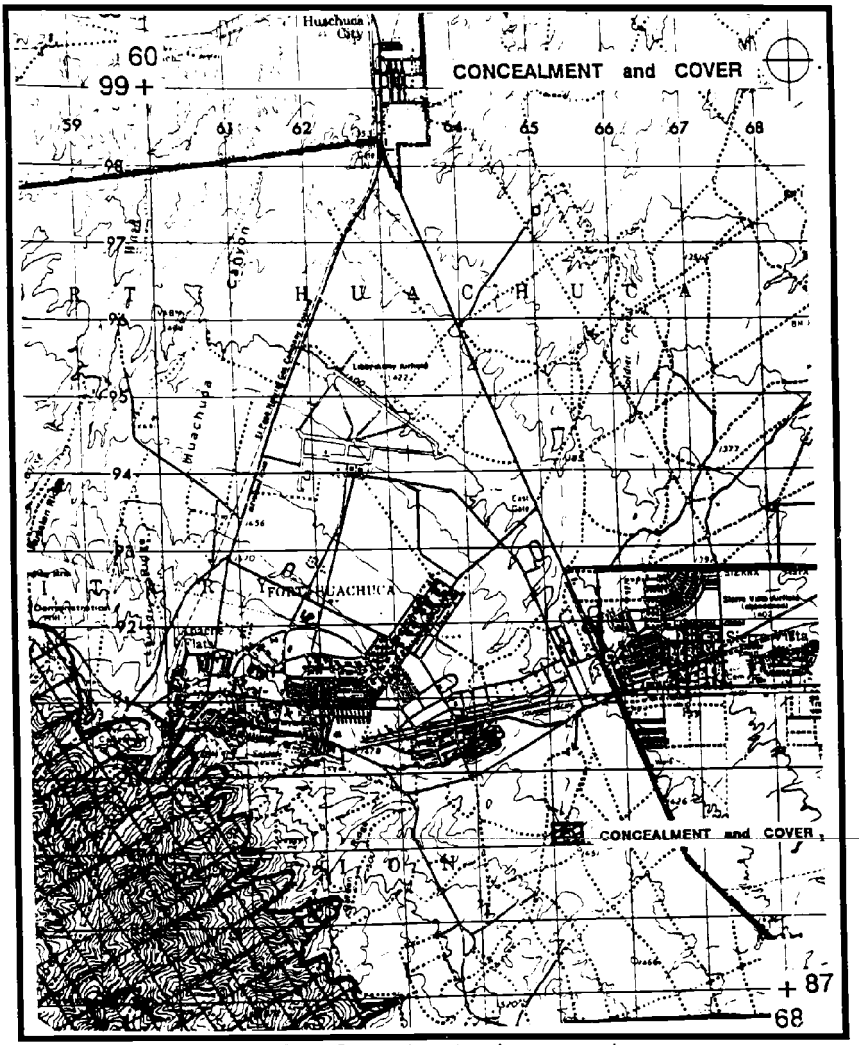


Figure B-5. Concealment and cover overlay.

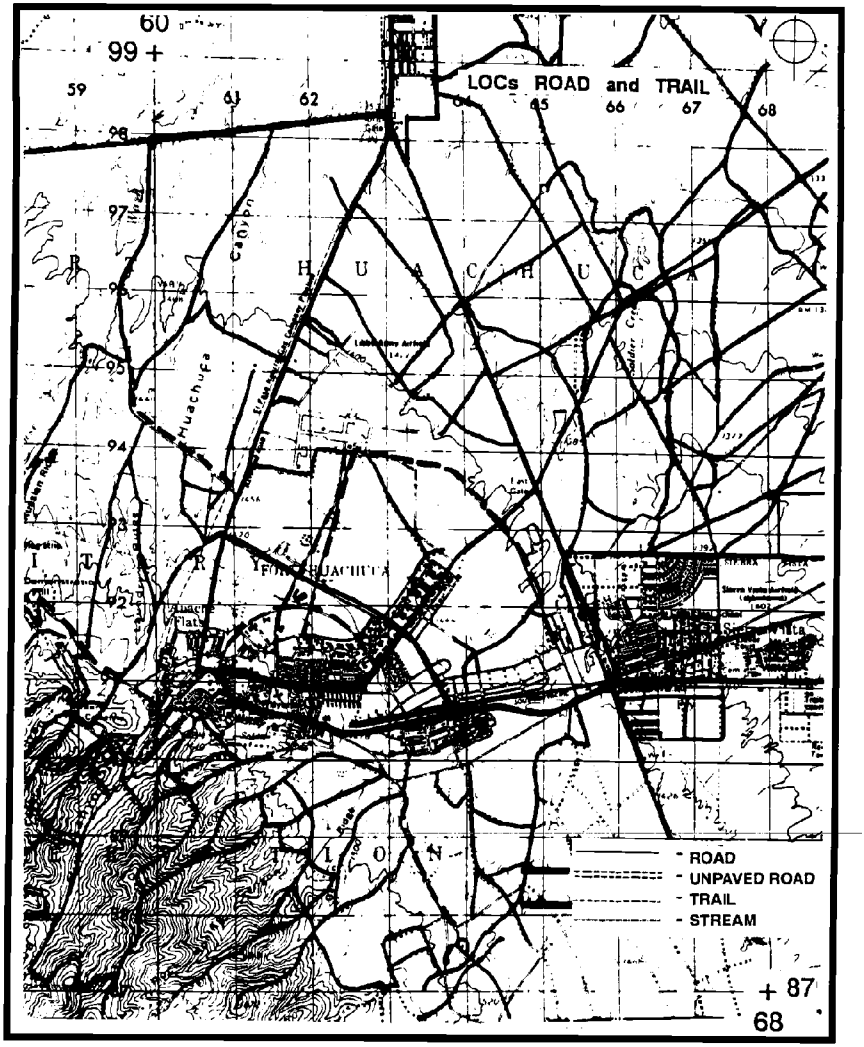


Figure B-6. Lines of communication overlay.

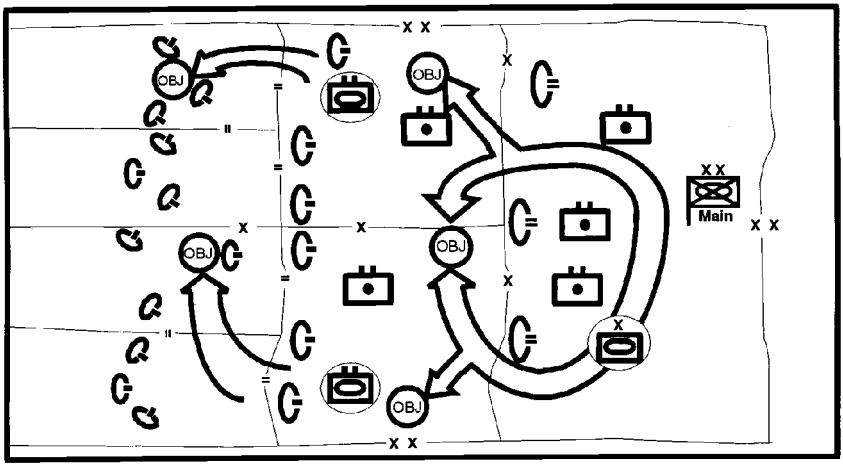


Figure B-7. Doctrinal template - depicts enemy forces according to doctrinal deployment, unconstrained by terrain.

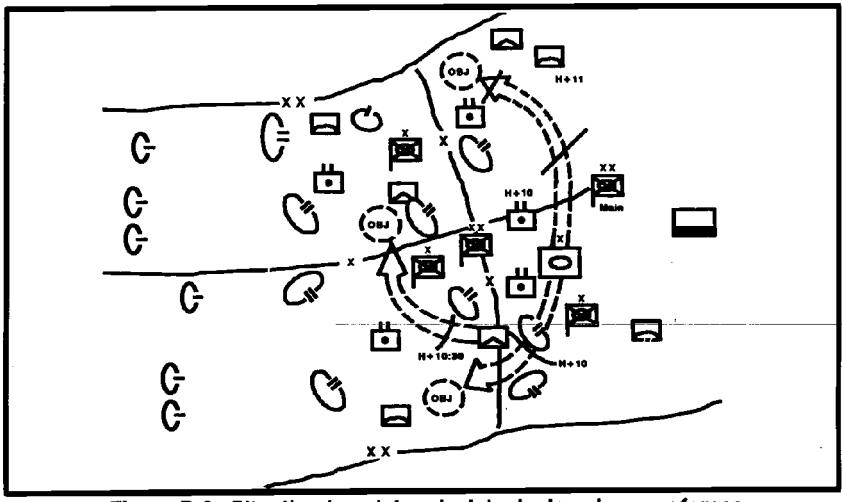


Figure B-8. Situation template - depicts deployed enemy forces adjusted for obstacles and terrain.

The situation template should include the following for mechanized armor-based offense and defense.

In the offense:	**In the defense:**
• Objectives & LOA. • AAs & MCs. • Recon routes, OP & IEW sites. • Firing lines & direct fire range fans. • Formations & deployment lines. • Artillery targets & range fans. • Artillery & ADA position areas. • ADA coverage. • Attack helicopter routes, BPs & range fans. • LZs. • CAS routes. • Situational obstacles. • Chemical agent targets. • Smoke targets	• BPs & direct fire range fans. • Reserve & hide positions. • CATK routes & firing lines. • Counter-SOPs & counterrecon forces. • Recon routes, OP & IEW sites. • Ambush sites. • Artillery targets & range fans. • Artillery & ADA position areas. • ADA coverage. • Attack helicopter routes, BPs & range fans. • Tactical & protective obstacles. • CAS routes. • Situational obstacles. • Chemical agent targets. • Smoke targets.

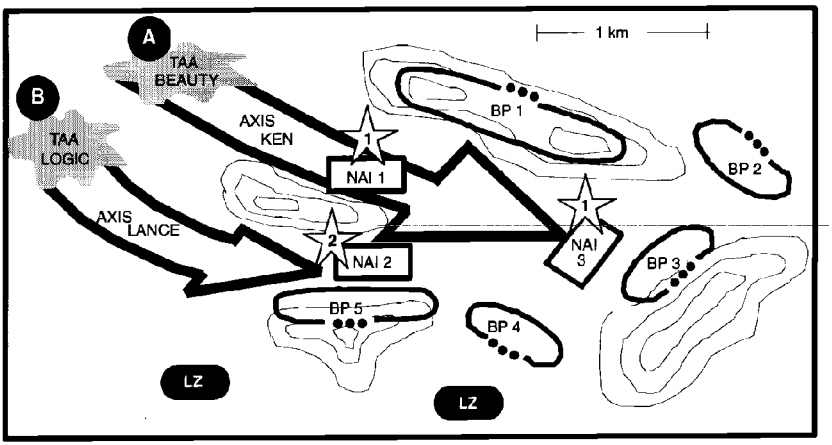


Figure B-9. Decision support template.

DP No.	1	2
Decision Criteria	Insurgent Camp is in NAI 1 or 3.	Insurgent Camp is in NAI 2.
Maneuver	A Co receives 3/B, occupy TAA BEAUTY, O/O movement to CATK along AXIS KEN.	A Co occupies TAA BEAUTY, O/O occupy BPs 1, 2, and 3.
FS	Priority: A, B, C.	Priority: C, B, A.
M-CM-S	1/A/13th Engr to A.	1/A/13th Engr to C.

Figure B-10. Partial BOS synchronization matrix.

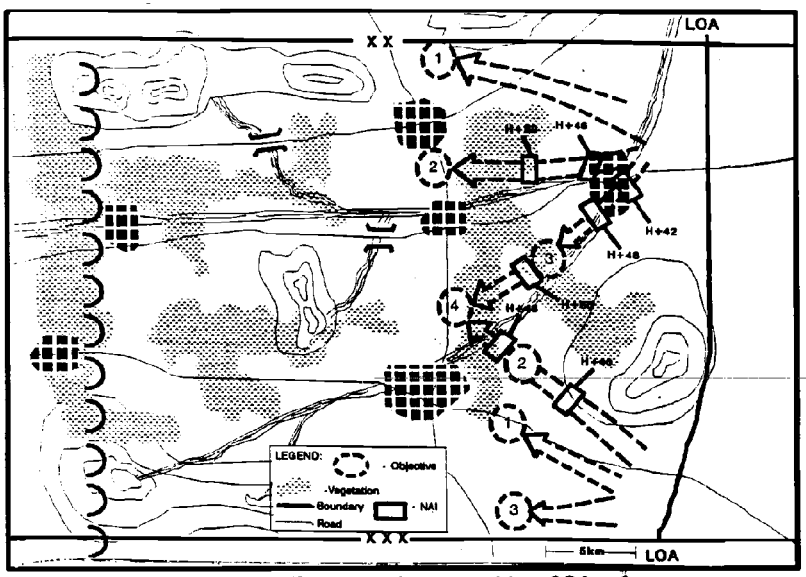


Figure B-11. Event template - considers COAs of reinforcing or counterattacking forces.

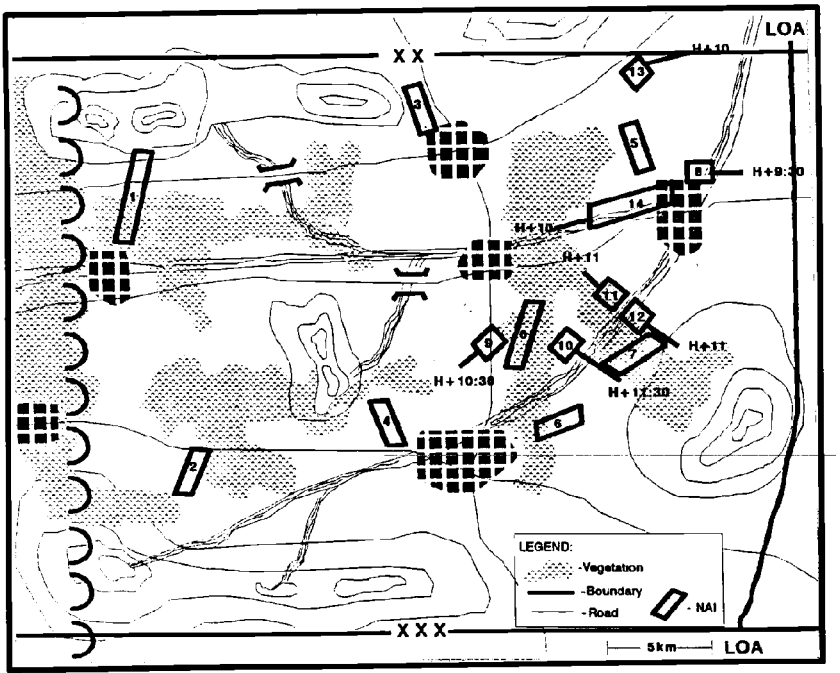


Figure B-12. Event template - depicts key events in each threat COA.

NAI	EST TIME	INDICATORS THAT WOULD HELP CONFIRM COA 1	COA 2	COA 3	OTHER
1	H-15		AASLT Forces		
2	H-15		AASLT Forces		
3	H-15	AASLT Forces		ASSLT Forces	
4	H-15		Infil of LT Inf		
5	H-4		LT Inf ATK NAI 5		
6	H-4	LT Inf ATK NAI 7	LT Inf ATK NAI 6		
7	H-4	LT Inf ATK NAI 8		LT Inf ATK NAI 7	
8	H-4	■Poised to ATK		LT Inf ATK NAI 8	
9	H-4	■Poised to ATK	■Poised to ATK		TD ATKs
10	H-4		■Poised to ATK	■Poised to ATK Abreast	TD ATKs
11	H-6			■Shifts N	
12	H-18				1 or 2 Bdes ATK N
13	H-18				1 or 2 Bdes ATK S
■ Indicates ECOAs.					

Figure B-13. Event matrix.

CONSIDERATIONS FOR AIR IPB

1. DEFINE THE BATTLEFIELD .

- AI for air IPB is significantly larger than ground IPB.
  - – Includes airfields which can range supported unit AO to include those within aerial refueling radius.
  - – AAAs which lead into supported unit's AO.
  - – Three types of air avenues:
    - * F/W Attack = Normally follows ground forces.
    - * F/W Transport = Bombers and R/W lift uses terrain to mask ingress and egress routes.
    - * R/W Attack = Normally follows ground forces.

2. DESCRIBE THE BATTLEFIELD'S EFFECTS . See the following example of weather effects on aviation operations.

TYPE AIR-CRAFT	MINIMUM VIS	WIND-SPEED & DIREC-TION[1]	PRECIPI-TATION	TEMPER-ATURE & HUMIDITY[2]	ILLUMI-NATION
Fixed Wing	2.5 nmi vis 2.5 nmi AGL ceiling in hilly terrain 1.0 nmi AGL in flat terrain	For airborne operations speed must be <13 knots	Severe weather within 3 miles of target will hinder acquisition. Freezing rain greatly limits lift capability	Temp >100 and humidity <80% will degrade payload capability	Little air-to-air or point CAS capability at night except newest F/W
Rotary Wing	1.0 nmi vis 300 ft AGL	For airmobile operations speed must be <13 knots	Same	Same	No CAS without illumina-tion except newest R/W

[1] Strong winds perpendicular to AAA increase difficulty in hitting target.
[2] Amount of degradation differs with type of aircraft.

Figure B-14. Sample of an ADA-tailored IPB.

- Terrain Analysis.
  - Determine impact of geographic factors on the ability of the aircraft to approach, acquire, and engage a target.
  - Predict how an aircraft would most likely approach target or area to deliver ordnance.
  - Locate positions that rotary wing could use for stand-off and/or pop-up attacks.
  - Determine locations of possible LZs, DZs, and the AAAs to these areas.
  - AAAs do not stop at FLOT or FEBA and they do not enter your AO solely from the FLOT or FEBA; watch your flanks and rear.
  - The closer an aircraft is to a target the greater an influence terrain will have on the aircraft and how it is employed.
  - The best method for formulating AAAs is based on fixed factors:
    * Locations of enemy airbase or staging area (known or suspected).
    * Position of friendly targets.
    * Most aircraft will fly a straight-in approach from the airbase to the vicinity of the target.

    Reason: Shorter overall mission time, less fuel needed, more payload or ordnance.
  - Exceptions which cause deviation from this rule:
    * Heavy concentrations of air defense.
    * Major terrain features that can mask the approach of aircraft at low altitudes.
    * Terrain that may force unnecessary exposure.
    * Terrain exceeding the operating ceiling of rotary-wing aircraft.
  - What happens in the vicinity of the target?
    * Most attacking aircraft will drop lower to use terrain masking and minimize early warning and exposure times to associated air defenses.
    * How will the enemy aircraft approach the target (Hi-Hi-Lo, Lo-Hi-Lo, or Lo-Lo-Hi, etc)?
    * To engage the target the pilot must be able to see it (visual, radar, sensor).
    * The pilot must approach his target so he can see it at far enough distance to allow lock-on and engagement by his weapon system.
    * The pilot will maximize his standoff range to increase survivability.
  - How to determine the direction of attack:
    * Know the enemy HPT; what friendly asset he must destroy.
    * Know the location of these assets.
    * Know the location of known or suspected enemy airbases and FARP.

Figure B-14. Sample of an ADA-tailored IPB (continued).

* Determine AAA which could be used by fixed- or rotary-wing aircraft making the attack.
* Determine locations from which stand-off and pop-up rotary-wing attacks are most likely.
* These locations will provide terrain masking for the aircraft to hide behind.
* The location must also provide observation and fields of fire into the target area when the aircraft pops-up.
* This type of location + a masked ingress and egress route = a stand-off or pop-up position.
* Within the vicinity of the target, consider the following:
  _ LOS acquisition of the target.
  – Weapon stand-off capability.
  – Pilot reaction time.
  – Aircraft survivability.
  – Standard tactics.

3. EVALUATE THE THREAT.

- Should address the following:
  – AOB—How many and what type aircraft. (Include different models such as Mi-24 E or F because they all have varying payloads, optics, and weapon systems.)
  – Capabilities of the aircraft in the enemy inventory.
  – Types of ordnance available to the enemy.
    * Guns.
    * Rockets.
    * Tactical ASMs, CBUs, PGM, AAM, NBC, and mines.
  – Capabilities:
    * Range.
    * Guidance (aerial, ground).
    * Release altitude.
  – Doctrine:
    * Raid sizes and composition.
    * Ingress and egress altitude and speed.
    * Delivery profiles.
    * Use of EP and SEAD.
  – C^2:
    * Most non-Western aircraft operate under strict ground control. They are vectored toward a target rather than being sent to an area to seek

Figure B-14. Sample of an ADA-tailored IPB (continued).

targets on their own. The vector is from ground emplaced beacons which normally operate in HF range.
- – Work to template high value C^2 targets:
  - * GCI nodes.
  - * FAC.
  - * RNP.
  - * Beacons.
- – Maintenance and Sortie Generation Capability:
  - * OR rates determine the percentage of aircraft able to fly. OR rate x number of aircraft = the maximum aircraft that can fly at any one time.
  - * The average sortie generation rate for most modern air forces is 2.5 to 3 for first 24-hour period. Second and succeeding day's planning factor is 5% of available number of aircraft.
  - * To get sortie generation rate: number of aircraft x sortie generation rate = number of sorties in a 24-hour period.
  - * To estimate number of sorties in your AO, consider ground situation, enemy main effort, enemy doctrine.

4. DETERMINE THREAT COURSES OF ACTION.

- Enemy air operations are conducted in support of their ground operations. The most important part of determining enemy air COAs is to understand the ground situation and enemy ground COAs.

- With the information and analysis you've done in the first three steps, determine how the enemy will employ his air assets.

- Consider enemy doctrine, AAAs, terrain in the target area, and current weather conditions.

- You must answer the following questions:
  - – When will the enemy commit his air assets?
  - – Where will the enemy commit his air assets (target area)?
  - – What air assets will the enemy commit (number of aircraft)?
  - – How will the aircraft attack in the target area (AAA or delivery profile)?

Figure B-14. Sample of an ADA-tailored IPB (continued).

APPENDIX C

RECONNAISSANCE AND SURVEILLANCE PLANNING

R&S planning is continuous. You must understand the commander's intent for each mission. After mission analysis, the commander should tell you the key information needed before and during the mission. This key information is the commander's PIR and IR. The PIR and IR provide the initial focus to R&S planning. Plan to conduct R&S throughout the depth of the battle in space and time. (See FM 34-2-1.)

G2/S2 R&S RESPONSIBILITIES (Table C-1)

Table C-1. G2/S2 R&S responsibilities.

REQUIREMENT	EFFECTS
Coordinate with higher, flank, forward units.	Better guidance from higher & integration with adjacent units; less redundancy & gaps in coverage.
Identify R&S requirements; rehearse R&S plan.	Success of unit mission.
Supervise & coordinate the command's aerial & ground reconnaissance (include LRRPs).	Better use of survl systems (GSR/REMBASS employment), LRRPs, and tasking UAVs or other aerial assets to answer CDR's PIR.
Brief GSR, REMBASS, and patrol team leaders (plt leaders of every BOS in AO to collect) (e.g., LLVI, LRSD, scouts).	Effectiveness of R&S assets which, in turn, affects success of R&S effort.
Prepare R&S WARNO and OPORD early-on.	Start the reconnaissance effort ASAP.
Update R&S OPORD as info is received.	Effectiveness of R&S effort and unit mission.
Provide R&S plan to higher, lower, and adjacent units.	R&S effectiveness and other unit actions; prevention of negative effects.

EXAMPLE: The primary R&S planning objective is to task subordinate units (all possible assets; e.g., MI, MP, FA, Signal, Engr, FSB) to cover NAIs important to brigade mission or directed by higher HQ. Subordinate units plan the use of available R&S assets to satisfy taskings from the brigade and their own requirements. They strive to complete their plans quickly (using the 1/3, 2/3 rule) so R&S assets have time to prepare and execute the plan. As soon as they are complete, the subordinate unit plans are consolidated at brigade to form the brigade R&S plan. You now have a draft plan that shows when and in what areas to begin R&S planning.

R&S PLANNING PROCESS (Figure C-1)

I. PLANNING PROCESS.

A. Initial Requirements:

1. Did higher HQ provide tasking requirements?
2. Was the commander's PIR and IR stated and included?
3. Did commander provide R&S intent?
4. Did S2 brief the staff on enemy collection capabilities?
5. Were other staff tasks performed?

B. SIR Developed (IPB Driven):

1. Did S2 identify air or ground AA?
2. Did situation and event templates reflect probable or prioritized ECOAs?
3. Was NAI developed in detail? (What is expected? When? Where?)
4. Were collectible indicators at NAIs developed?
5. Were SIR developed from NAIs and indicators?
6. Were reporting requirements developed for priority collection missions to allow the commander time to change plans?

C. Possible Collectors Analyzed:

1. Did S2 coordinate with staff, S2, and G2 to identify all available collection assets?
2. Did S2 analyze asset capabilities to develop collection requirements based on range to target, time available, target characteristics, terrain, weather, enemy (obscurant use), and communication?
3. Did S2 analyze collection redundancy (is it necessary)?

Figure C-1. R&S planning process.

4. Did staff identify support requirements (communication nets, retransmission, FS, NBC reconnaissance support, logistic support, special equipment support)?
5. Did S2 identify gaps in collection?
6. Did S2 back brief S3 or the commander on R&S concept?
7. Were WARNOs sent to appropriate assets?
8. What were timelines?
   a. When was mission received?
   b. What is NLT time for execution?
   c. When was templating done?
   d. When was tentative plan made? Back briefed?
   f. When was initial reporting needed?
   g. Who was in charge of R&D planning?
   h. Who was in charge of counterreconnaissance planning?
   i. What is LTIOV.

II. PREPARATION FOR R&S OPERATIONS.

A. Specific Collection Instructions:

1. What assets could be available? Used? **(See Figure C-4.)**
   a. Scouts.
   b. Patrols.
   c. Forward Observers.
   d. Armor.
   e. Aviation.
   f. Infantry.
   g. EW.
   h. REMBASS.
   i. Chemical.
   j. UAV.
   k. Medical.
   l. CI teams.
   m. GSR.
   n. OPs and LPs.
   o. Signal.
   p. Antitank.
   q. Engineer.
   r. Cavalry.
   s. MP.
   t. ADA.
   u. SOF.
   v. Support units.
   w. GRCS.
   x. Interrogation teams.

2. Did the S2 provide detailed instructions to tasked assets? Did the instructions include—
   a. Who is tasked?
   b. What to look for?
   c. Why to look?
   d. When to look?
   e. Where to look?
   f. What you could expect to see?
   g. How to get there?
   h. Who to coordinate with?

Figure C-1. R&S planning process (continued).

i. Passage of lines and recognition signals?
j. Reporting requirements?
k. Friendly assets in AO?
l. Resupply?
m. Obstacles?
n. MEDEVAC?
o. NBC hazards?

3. Was the collection location appropriate (concealment, collectable)?
4. Were there sufficient control measures included to control assets during mission?
5. Did the S2 request assistance from higher HQ for identified collection gaps?
6. Did the R&S plan cover all collection requirements?
7. Were assets overtasked?
8. Was redundancy appropriate for this mission?

B. Coordination:

1. What is format of plan (collection plan, overlay, matrix)?
2. Were direct or indirect fires or jamming coordinated between staff and S2?
3. Was a CI vulnerability assessment made?
4. Was additional equipment (special) planned for?
5. Were communication nets established to meet reporting needs?
6. Were commanders and staff briefed on plan before execution?
7. Did commander or S3 approve final plan?
8. Did assets know specific requirements (PIR and IR)?
9. Was plan disseminated to all involved or with a need to know (FRAGO, overlay)?
10. Was plan sent to higher HQ?

C. Asset Internal Coordination:

1. Was equipment checked?
2. Were internal procedures clarified?
3. Did coordination between assets occur?
4. Was mission rehearsed?
5. Was plan developed far enough in advance for assets to prepare or rehearse?
6. Was plan developed in time for higher HQ to review?

III. EXECUTION.

A. Continuity of R&S and counterreconnaissance operations:

Figure C-1. R&S planning process (continued).

1. Did unit plan provide for operations when scout or other R&S assets are inoperable?
2. Did unit SOP provide for operations during briefings, debriefings, or rehearsals?
3. Are unit and leaders cross-trained to facilitate substitutions or replacement of scouts?

B. Asset and Unit Response:

1. Did assets depart and set up on time?
2. Did assets use concealment, cover, and camouflage?
3. Were assets able to observe enemy undetected?
4. Was low-level deception used?
5. What were meteorological report requirements?
6. Were enemy locations pinpointed?
7. Was objective reconnoitered?
8. Were obstacles identified and marked?
9. Were routes marked?
10. Did assets submit route/obstacle overlay?
11. Was enemy reconnaissance located?
12. Were counterreconniassance missions performed?
13. Did assets help with C^2 during attack?
14. Did assets help direct or control fires?
15. Was terrain reconnoitered (trafficability reported)?

C. Reporting:

1. Were reports timely, accurate, and concise?
2. Were assets debriefed?

D. Results:

1. Did S2 plot asset reports (track results of plan)?
2. Did S2 identify inadequately tasked or unproductive assets and change tasking (with approval of commander and S3)?
3. Did reports or analysis answer PIR and IR?
4. Was R&S plan updated and recoordinated?
5. Were templates updated?

E. Dissemination:

1. Was commander briefed on answer to PIR?
2. Has commander updated PIR?
3. Did units get intelligence based on priority?
4. Did higher HQ get answers to taskings?
5. Did assets receive feedback on level of success?

Figure C-1. R&S planning process (continued).

OTHER R&S PLANNING CONSIDERATIONS (Figure C-2)

1. General.
   a. Combat information is knowledge of the enemy, weather, and terrain.
   b. R&S collection should answer the commander's PIR and IR.
   c. Every soldier is an important HUMINT collection asset.

2. Analysis of information collected on PIR and IR is an objective process.

3. Determine requirements:
   a. Set priorities. Develop SIR and SOR. Do not let the R&S elements decide what answers the commander's PIR.
   b. Terrain and weather.
   c. Tactical situation (deep, close, rear).
   d. Focus the R&S mission.

4. Develop R&S plan based on the principles of reconnaissance:
   a. Timely information.
   b. Aggressive reconnaissance.
   c. Continuous reconnaissance.
   d. Focus combat power.
   e. Relevant information (focused on PIR and CCIR).
   f. Reconnaissance OPSEC. Coordinate with G3/S3 to establish control measures which deconflict and help protect R&S assets on the battlefield.
   g. Accurate information.
   h. Complementary with operations.
   i. Consideration of threat counterreconnaissance threat.
   j. Destruction of threat reconnaissance elements when detected.
   k. Plan for CasEvac, resupply, and reconstitution for teams in the field.

5. Identify METT-T.

6. Develop communications plan and reporting schedule.

7. Issue WARNO to R&S asset leaders.

8. Coordinate R&S plan with—
   a. Commander and commanders of areas in which teams will operate.
   b. Adjacent and higher G2/S2.

Figure C-2. R&S planning considerations.

c. Unit S1/S3/S4.
d. FSO.
e. SIGO.
f. Engineer LNO.
g. ADA LNO.
h. Chemical Officer.
i. G3/S3 to tie R&S plan into the maneuver plan.

9. Brief R&S team leaders and all other R&S assets.

10. Advise higher and lower S2 of R&S plan.

11. Request support from higher headquarters.

12. Write R&S tasks into paragraph 3 of the OPORD.

13. Evaluate reports, review requirements, and identify intelligence gaps.

14. Analyze reports to deny or confirm your templates; then update templates.

15. Ensure combat information is passed immediately to those elements that can react to it.

16. Update the R&S plan based on known intelligence.

17. Plan for future operations.

18. Maximize use of all available assets.

Figure C-2. R&S planning considerations (continued).

You can now begin adding some detail to the R&S plan. Integrate any requirements from higher HQ. Translate the initial PIR and IR into indicators on which R&S assets can collect. Use the indicators to develop the SIR and SOR. The SIR and SOR ensure assets are collecting specific information that answers the PIR and IR.

Once you have a picture of the coverage required for the R&S effort, prioritize the SIR. Assign a high priority to those SIR that, when answered, will provide the greatest amount of intelligence in the shortest amount of time. After you prioritize the SIR, draft the R&S plan and distribute to the appropriate R&S assets. It is critical that you deploy R&S assets early-on and update them as additional information is received.

TOOLS TO TRACK DEPLOYED R&S ASSETS

Three methods are used to track deployed R&S assets:

- Reconnaissance base OPORD (Figure C-3).
- R&S overlay (Figure C-4).
- R&S tasking matrix (Figure C-5).

Select any method as long as the assets receive clear, specific instructions. Some S2s use all three methods by attaching the R&S overlay and R&S tasking matrix to the reconnaissance order prior to dissemination. When possible, using all three is best because each asset then has a graphic, a matrix, and a written set of instructions.

RECONNAISSANCE ORDER:

The reconnaissance order is the narrative instructions for deployed assets. Figure C-3 is an example of a brigade reconnaissance order.

RECONNAISSANCE ORDER

1. SITUATION.
   a. Enemy forces.
   b. Friendly forces.
   c. Attachments and detachments.
   d. Assumptions (OPLAN only).

2. MISSION. Expressed as task and purpose derived from planning process. Clearly stated reconnaissance objectives.

3. EXECUTION. Commander's intent, derived during planning process:

a. Concept of Operation. State how reconnaissance assets are operating in relation to the parent organization. This scheme must identify if the reconnaissance force is infiltrating or penetrating the enemy's security forces (or both) and how this will occur.

Figure C-3. Example of a brigade reconnaissance OPORD.

(1) Manuever.
(2) FS. (Refer to FS annex if required.)
(a) Scheme of fires that specifies what fires are available and how to get them.
(b) Engagement criteria.
(c) Scheduled fires in support of insertions and extractions.
(3) Mobility and survivability.
(4) Air defense.
(5) C^2W.

b. Tasks to maneuver units. [List all units from task organization into subparagraphs, and only unique items for those units; all other tasks go into d below.] For each of the elements in the reconnaissance force, state the following:
(1) How to get there.
(2) Where to look (NAI for static targets).
(3) What to look for.
(4) When to look for it.
(5) Plan to maintain contact with moving target.
(6) What equipment to bring.
(7) How (what communications systems, how often) to report.
(8) To whom to report:
(a) Brigade reconnaissance teams.
(b) Task forces.
(c) MI company (EW, UAV, other).
(d) ADA battery.
(e) Engineer battalion.
(f) FA battalion.
(g) Chemical company.
(h) MP platoon.
(i) Signal company.
(j) FSB.

c. Tasks to combat support units (if applicable).
(1) Fires (or refer to FS annex).
(a) Air support.
(b) Chemical support.
(c) FA support.
(2) Mobility and survivability. (Refer to mobility and survivability annex if required.)

Figure C-3. Example of a brigade reconnaissance OPORD (continued).

(3) Air defense. (Refer to air defense annex if required.)
(4) C^2W. (Refer to C^2W annex if required; address applicable subcomponents of C^2W: deception, EW, psychological warfare, UAVs.)

d. Coordinating instructions.
(1) Time or condition when OPORD or OPLAN becomes effective.
(2) EEFI.
(a) PIR.
(b) EEFI.
(c) FFIR.
(3) Risk reduction control measures.
(4) Environmental considerations.
(5) Any additional coordinating instructions.
(a) LD or defend NLT _____ .
(b) MOPP level.
(c) Rally points, alternate positions.
(d) Rehearsal time, type, location.
(e) Extraction plan.
(f) PZ and LZ.
(g) Fratricide avoidance measures.
(h) ROE and actions on contact.
(i) IHL.

4. SERVICE SUPPORT. State the concept of logistic support.
a. Support concept.
b. Material and services (resupply location or time and days of supply, emergency resupply, vehicle evacuation).
c. Medical evacuation (CasEvac plan).
d. Personnel (reconstitution plan).
e. Civil-military cooperation. NA.
f. Miscellaneous.

5. COMMAND AND SIGNAL.
a. Command (C^2 structure, report plan).
b. Signal (nets used, retransmission or relay plan).

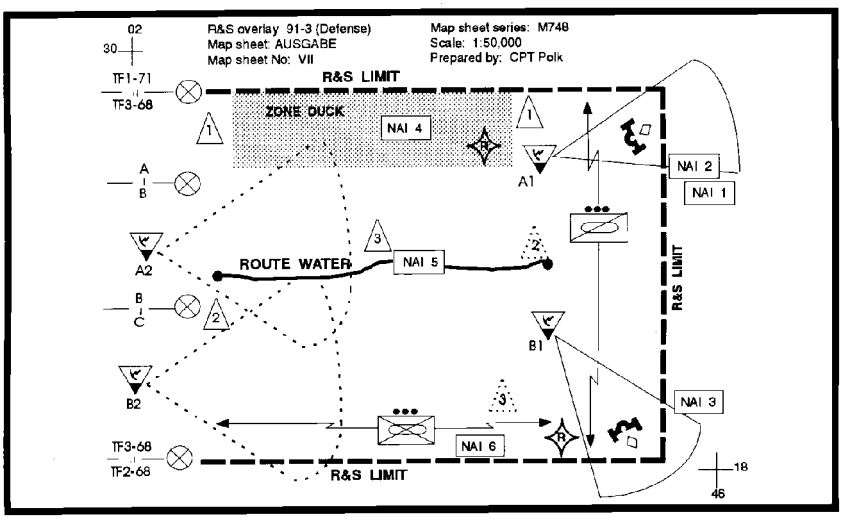
Figure C-3. Example of a brigade reconnaissance OPORD (continued) .

R&S OVERLAY:

The R&S overlay is the R&S plan in graphic format. Its purpose is to show exactly where and when R&S assets are operating. Use FM 101-5-1 for overlay graphics and symbols. Due to various R&S operational techniques and the unique nature of some SASO missions, you will need to construct some new graphics and explain them in your legend (Figure C-4).

The R&S overlay has two parts: (1) The graphic display of deployed or planned deployment of R&S assets, and (2) The marginal data consisting of the legend, administrative data, specific instructions to each asset, and the distribution list. The latter part consists of standard wording found on all overlays. (See top of Figure C-4.)

With digitized systems coming online, the location, heading, range to target, system health, and logistical data will be available NRT in digital, preformatted report format available to the S2/S3/S4 in the TOC, TAC, and ALOC.



INSTRUCTIONS:

SCOUTS: Establish forward screen NLT 1600 at coordinate_____. Target enemy recon (BRDM, BMP, tanks). Coordinate with B Co for route to screen position and GSR team.

REMBASS: Establish two strings vicinity____and____ NLT 1800. Target enemy dismount recon and MR troops infiltrating along forest trails. Coordinate passage with B Co, Scout platoon, and GSR team.

GSR: Establish position A1 vicinity____NLT 1700. Target enemy recon (BDRM, BMP, tanks, dismounted troops). Coordinate with A Co for passage, Scout platoon, and REMBASS team. Establish position A2 on order. Coordinate with B Co for position. Establish position B1 vicinity____ NLT 1700. Target enemy recon. Coordinate with B Co for passage, Scout platoon, and REMBASS team. Establish position B2 on order. Coordinate with C Co for position.

PATROLS: A Co conduct recon and security patrols in Zone Duck. Begin patrols NLT 1830 to 0600. Target enemy dismounted troops, BMP, and BRDMs. Coordinate with GSR team and Scout platoon. C Co establish screen along southern flank NLT 1800. Target enemy recon, BMP, BRDM, tanks. Coordinate with Scout platoon and GSR team.

OP/LP: Position as per battalion R&S SOP.

REPORTS: Report on battalion intelligence net using SALUTE format. Patrol leaders report on intelligence net after each patrol. Report combat information on intelligence or operations net. Assets report using schedule in R&S SOP. React to jamming as per battalion TAC SOP.

DISTRIBUTION: A, B, and C Companies, Scout platoon, GSR team, REMBASS team, S3, FSO, and brigade S2.

Figure C-4. R&S overlay with instructions on acetate.

The key portion of the administrative data contains the written instructions to each R&S asset. The instructions should focus on—

- The required operational timeframes. Give each asset a start and a finish time for each observation or action.

- The target. To answer the PIR, look for specific indicators. Each asset should be told exactly what to look for. Never give broad-based generic mission statements. Specific guidance will promote specific answers.

- Coordinating instructions. All assets at one time or another will move through or near another unit's AO. To keep units from shooting (directly or indirectly) friendly R&S assets, assets and units must coordinate with each other. FSO should restrict fires around R&S assets.

- Reporting requirements. All assets should know when, how often, and what format to use when reporting. Provide frequencies, alternate frequencies, and reactions during jamming, as well as the LTIOV for specific information to be reported.

Initially, the locations for assets are areas in which you recommend that they deploy. After the assets have deployed to the NAI, they report to the S2 or the S3 the actual coordinates from which they can best accomplish their mission. The S2 or the S3 then updates the R&S overlay graphics to show actual locations. Include the following control measures on your R&S overlay:

- Friendly boundaries, R&S limit of responsibility, NAIs, SPs, RPs, and checkpoints.

- Graphics depicting route, area, and zone reconnaissance.

- Primary, alternate, and supplementary positions.

- Sectors of scan for sensors.

R&S TASKING MATRIX:

Another less preferred method of disseminating R&S guidance is the matrix method (Figure C-5).

- **Priority.** The priority number of each mission, which should correspond with the PIR number.
- **NAI.** The NAI number and grid coordinate.
- **START/STOP.** The times for this mission.
- **SIR INSTRUCTIONS.** Explains to the assets exactly what they are looking for (target).
- **TASKINGS.** Lists the actual assets tasked to conduct each mission. An "X" placed under each asset identifies the tasking.
- **COORDINATION.** Tells the assets which units to coordinate with for this mission.
- **REPORTS.** Provides the assets with reporting requirements.

(Classification)

DTG: _____

MISSION: _____

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
PRIORITY	NAI	START / STOP	SI/INSTRUCTIONS	A	B	C	D			SCOUTS	MORTARS	GSR	REMBASS	OTHER	COORDINATION	REPORTS
1	1 2 3	1600 / 2400	When? Where? What type equipment does the recon element have? Do not Engage							X					With B Co for route to screen position. With GSR TM and REMBASS TM.	Per BN R&S SOP.

(Classification)

Figure C-5. R&S tasking matrix.

BRIEFING OPORDs

The following OPORDs are additions to the base reconnaissance OPORD (see Figure C-3). GSR, REMBASS, and patrol employment OPORDs would be issued to the teams by the respective platoon leaders.

GSR EMPLOYMENT:

- Give GSR teams adequate time to prepare and deploy.
- Deploy GSRs for best area coverage.
- Deploy GSRs, with a security force, so they scan an area and provide early warning.
- Plan logistical support.
- Limitations:
  - — Limited to LOS acquisition and gives off detectable signal.
  - — Visibility hindered by heavy precipitation, thick vegetation, and broken terrain.
  - — Limited range and ability to identify except by personnel and wheeled or tracked vehicles.

- Brief team leader using the OPORD format at Figure C-6.

1. SITUATION.

   a. Enemy. Intelligence estimate format.

   b. Friendly.
      (1) Current unit locations.
      (2) Scheme of maneuver.
      (3) Boundaries.
      (4) Objectives.

2. MISSION. Who, what, where, when, and why for this R&S mission. Surveillance of threat antiaircraft from location and time.

3. EXECUTION.

   a. Concept of operation.
      (1) Primary and alternate routes to sites (SPs, PPs, checkpoints, RPs).
      (2) Primary, alternate, and supplementary sites.
      (3) Sectors of scan.
      (4) Operating times.

   b. Coordinating instructions.
      (1) Battalion and brigade R&S plan: patrols, scout routes, times, sizes, LP and OP locations, ground and air cavalry screens, REMBASS, asset replacement plan, NAI redundancy coverage backup plan, etc.
      (2) Link-up plan with security forces.
      (3) Obtain target list from FSO (recommend additional targets).
      (4) Coordinate fire control measures with FSO and plan NFA for team locations.
      (5) Obtain obstacle plan from TF engineer and check routes for obstacles.
      (6) Coordinate with supported commander to tie the R&S site into unit defensive plan or scheme of maneuver.
      (7) Review engagement and disengagement criteria.
      (8) Review actions upon mission completion.

Figure C-6. Example of a GSR OPORD.

4. SERVICE SUPPORT. Coordinate with S4, battalion maintenance officer, SIGO for—

a. Class I (Food).
b. Class III (Fuel).
c. Class IV (Barrier materials) (during prepared defense).
d. Class V (Ammunition).
e. Class IX (Repair parts).
f. Organizational maintenance.

5. COMMAND AND SIGNAL.

a. Signal.
(1) Issue SOI extract.
(2) Review reporting requirements and communications connectivity.
(3) Identify multiple reporting paths and methods.
(4) Review communications check requirements.
(5) Execute COMMEX prior to employment.
(6) Review actions upon EA.

b. Command.
(1) Review chain of command.
(2) Review leaders' locations.

6. SAFETY.

Figure C-6. Example of a GSR OPORD (continued).

IREMBASS EMPLOYMENT:

Brief team leader using the reconnaissance OPORD format (see Figure C-3) with the changes shown in Figure C-7.

1. SITUATION.

2. MISSION. Who, what, where, when, and why for this R&S mission. Monitor NAIs, DPs, routes.

3. EXECUTION.

a. Concept of operation.
   (1) SIR required.
   (2) Team leader recommends sensor mix, emplacement sites, and relay sites.
   (3) Primary and alternate routes and transportation to emplacement sites, PPs, and checkpoints.
   (4) Emplacement method.

b. Coordinating instructions.
   (1) Battalion and brigade R&S plan: patrols, scout routes, times, sizes, LP and OP locations, ground and air cavalry screens, IREMBASS.
   (2) Link-up plan with security forces.
   (3) Obtain target list from FSO (recommend additional targets).
   (4) Coordinate fire control measures with FSO.
   (5) Obtain obstacle plan from TF engineer and check routes for obstacles.
   (6) Review engagement and disengagement criteria.
   (7) Actions upon mission completion.

Figure C-7. Sample IREMBASS employment OPORD.

PATROL EMPLOYMENT:

Brief patrol leader using reconnaissance OPORD format (see Figure C-3) with the changes shown in Figure C-8.

1. SITUATION.

2. MISSION.

3. EXECUTION.

   a. Concept of operation.
      (1) Maneuver.
      (2) Fire support.

   b. Subunit tasks.

   c. Coordinating instructions.
      (1) Actions at the objective.
      (2) Time of departure and return.
      (3) Movement techniques and order of movement.
      (4) Routes.
      (5) PPs.
      (6) RPs and actions at RPs.
      (7) Actions upon enemy contact.
      (8) Actions at danger areas.
      (9) Actions at halts.
      (10) Locations of friendly obstacles, mine fields.
      (11) Rehearsals and inspections.
      (12) Debriefings.
      (13) SIR.

Figure C-8. Sample patrol employment OPORD.

DEBRIEFING Debrief patrols using the sample debriefing format below.

1. Size and composition of team. Team leader, assistant team leader, radio operator, and observers.

2. Mission.

3. SIR.

4. Reporting requirements.

5. Time of departure, method of infiltration, and point of departure.

6. Enemy observed enroute.
   a. Ground activity.
   b. Air activity.
   c. Miscellaneous activity.

7. Routes.
   a. Dismounted.
   b. Vehicle.
   c. Air.

8. Terrain.
   a. Key terrain.
   b. Significant terrain.
   c. Decisive terrain.
   d. Terrain compartment.
   e. Terrain corridor.
   f. Map corrections.

9. Enemy forces and installations.

10. Miscellaneous information.
    a. Lack of animals or strange animal behavior. Did animal reaction to patrol's presence generate alarm? If so, when, where, type of animal, activity that caused the alarm, and nature of alarm.

Figure C-9. Sample debrief format.

b. Mutilated plants.
c. Strange, uncommon insects.
d. Abandoned military equipment, number and type.
(1) Out of fuel.
(2) Unserviceable; estimate reason.
(3) Destroyed or damaged; how.
(4) Operational equipment left intact.

e. Abandoned towns or villages.

11. Results of encounters with enemy forces and local populace.

12. Condition of team including disposition of dead and wounded.

13. All of team's maps or any other identifiable material returned with team. For missing items, describe item and approximate location lost.

14. Conclusions and recommendations.

15. Process CEE, CEM, photographs, and videos taken by teams.

16. Time of exfiltration, method of exfiltration, exfiltration point.

17. Routes of return.
a. Dismounted.
b. Flight.

18. Time of return.

19. Point of return.

20. Enemy observed on return route.

21. What pre-mission intelligence support was provided and not needed? What intelligence support was not provided but needed? What intelligence was provided but turned out to be misleading or erroneous?

Figure C-9. Sample debrief format (continued).

R&S TEN KEYS TO SUCCESS :

1. Know that the commander's intent or CCIR drives R&S.

2. Support R&S early with integrated staff products.

3. Be adept at abbreviated IPB for quick or combat decisionmaking process.

4. Focus on the event template to capture the moving enemy.

5. Provide situation template depicting enemy in the engagement area.

6. Use automation tools like ASAS to enhance products.

7. Deploy organic R&S assets early and request support from higher HQ. Issue S3 FRAGO with S2 graphic overlay.

8. Provide continuous coverage throughout the depth of the battlefield.

9. Use all possible assets from national levels to scouts.

10. Evaluate reporting and provide immediate and continuous feedback to the commander.

APPENDIX D

PRIORITY INTELLIGENCE REQUIREMENTS, INFORMATION REQUIREMENTS, AND INDICATORS

PIR are intelligence requirements associated with a decision that will affect the overall success of the command's mission. PIR may change in order or be replaced entirely.

IR are requirements for intelligence to fill a gap in the command's knowledge and understanding of the battlefield or threat forces. They target specific COAs.

Indicators are positive or negative evidence of threat activity or any AO characteristic which points toward threat vulnerabilities or adoption or rejection by the threat of a particular capability, or which may influence the commander's selection of a COA.

During wargaming, the S2 develops a set of PIR for each friendly COA. Each is linked to a specific enemy action that requires a friendly response (DPs).

PIR are those IR critical to accomplishing the mission. Wargaming will dictate which IR will become PIR as the mission runs its course.

The S2 should nominate PIR for approval ONLY FROM THE LIST OF ALREADY PLANNED AND COORDINATED IR.

EXAMPLE OF A POOR PIR:

"Will the enemy attack? If so, how, when, where, and in what strength?"

- The PIR contains five significantly different questions. Which one is the priority? Unless the S2 gives more guidance, the individual collector must determine which part of this PIR to work.

- The S2 probably knows more about the situation than "the enemy might attack somehow, sometime, somewhere, and in some strength." The PIR as stated might prompt some collection assets to collect known information.

- Even for issues that the S2 does not know, the enemy can only select from a limited range of COAs due, for example, to terrain, weather, policies. If the PIR consider IPB, the S2, through more specific tasking, will minimize the chance that collection assets will look for the enemy where they are not likely to be.

- When the staff wargames, it may find some aspects of this question to be irrelevant to the present situation. For example, the defense may be fully capable of defeating an enemy attack regardless of when they actually attack. Why waste collection assets on a question that does not need to be answered?

EXAMPLE OF A GOOD PIR:

There is no "set" of PIR we can present that will be useful for all tactical situations any more than there is a set of maneuver paragraphs that the S3 can plug into any OPORD. Below are examples of *types* of PIR the S2 presents to the commander for approval. Because intelligence needs change over time, most PIR will be important only during certain times.

Referring to PIR as "timephased" is redundant. They are dynamic just as the battle will be dynamic. Just as there are no standard situation templates or friendly COAs that will serve in all situations, there is no standard set of PIR. Good PIR, however, have some things in common:

- They ask only one question.
- They focus on a specific fact, event, or activity.
- They provide intelligence required to support a single decision.
- They are tied to key decisions that the commander has to make.
- They give an LTIOV.

Examples:

- "Will the enemy defend OBJ JAMES using a forward slope defense?"
- What size force is defending OBJ NACO?"
- Which bridges over the San Pedro River are intact?"

Not all PIR are appropriate as questions, particularly those associated with moving targets or formations. PIR are *requirements* and should be stated as such when appropriate. In addition, PIR for moving targets must include the requirement to continue to maintain contact with the target. Simply locating the target once will not prevent it from surprising the commander later.

Example: "Locate and track the enemy's battalion reserve."

APPENDIX E

GRAPHIC REPORT FORMATS

Intelligence personnel use a variety of formats to request, report, and disseminate information (see FM 34-3). Personnel working in a joint environment should use JCS Pub 6-04.11. The formats assimilate information into automated intelligence support systems, such as the ASAS.

This appendix concentrates on graphic report formats, specifically the graphic INTSUM and the graphic intelligence estimate. The INTSUM is the main focus, but a graphic intelligence estimate is also provided.

GRAPHIC INTELLIGENCE SUMMARY

The graphic INTSUM is used by units at all echelons to rapidly convey threat situation dynamics. The graphic INTSUM is a current depiction of significant threat dispositions, activities, strengths, and weaknesses and an assessment of the most probable ECOA. A current, complete graphic INTSUM will provide for efficient collection and enable the commander to exploit fleeting threat vulnerabilities.

The graphic INTSUM can be maintained on conventional maps of any scale as an overlay or created electronically and disseminated to computer and television screens. For example, army-level organizations may utilize a 1:250,000 map scale and focus on an army or front-level threat, whereas in SASO activities the deployed unit may utilize a map scale of 1:25,000 or smaller and focus on a platoon or company-size threat.

The graphic INTSUM (Figure E-1) may contain 12 components:

- Legend and margin information.
- Area orientation.
- Threat unit locations and mission activities.
- Threat mission capabilities assessment.
- Threat boundaries and front-line trace.
- Threat objectives.
- Threat air activity.
- Threat weaknesses and vulnerabilities.
- Threat strengths and capabilities.
- Threat intentions assessment.

- Friendly commander's intent and PIR.
- Predicted future threat activity.

LEGEND AND MARGIN INFORMATION:

Components include—

- Overall classification of the INTSUM, posted top and bottom, to include a "Classified By" line and declassification instructions.
- Title.
- Issuing headquarters.
- "As Of" DTG. Use either local or Zulu time; this is critical since predicted threat activity will be depicted based upon the "As Of" DTG plus a given number of hours.
- Map reference, to include scale, and at least two coordinate registration marks.
- A symbology key can be added for increased clarity and **must** be included if symbols used are not in FM 101-5-1.
- SASO symbology is not standardized, but there are several symbol methodologies that have been developed. (See MIPB Jan-Mar 94, p 35.)

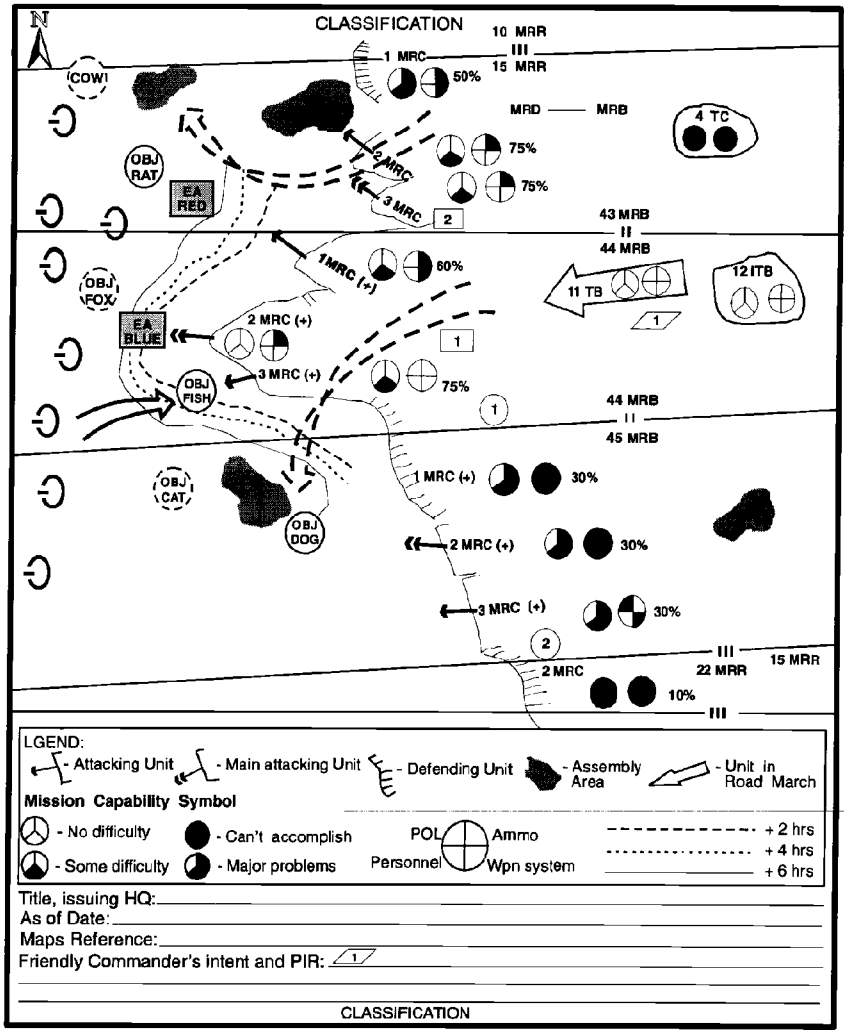


Figure E-1. Graphic INTSUM.

AREA ORIENTATION:

Selected geographic features will be highlighted on the overlay in order to orient the user to the area being displayed. The features selected will depend on the specific AO and type mission in which the friendly unit is involved.

Common features could include cities, rivers, and major relief features. Selected features for some SASO activities may be highlighted on a smaller scale. In an NEO highlighted features could include airports, LOCs, embassies, consulates, and American housing areas, and other features that will play prominently in the operation. Provide only the features necessary for orientation; do not clutter the INTSUM.

THREAT UNIT LOCATIONS AND MISSION ACTIVITIES :

Depict **committed** threat unit locations with a bracket followed by the unit identification. The size of the bracket will indicate the frontage occupied by the unit. The mission of the unit will be shown graphically (Figure E-2).

Depict **uncommitted** threat units with the symbology shown in Figure E-3.

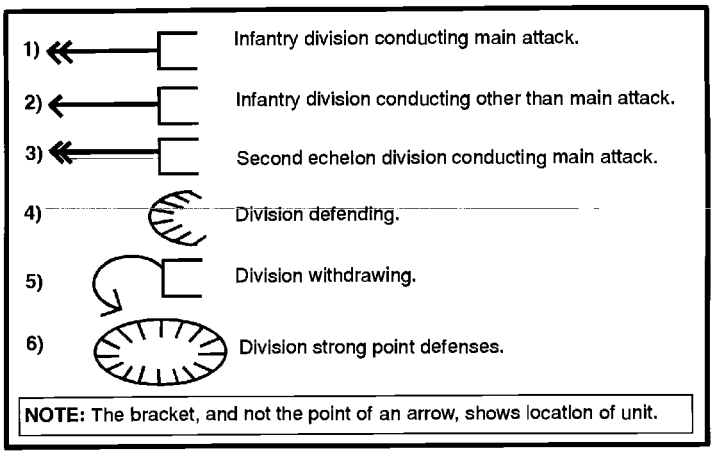


Figure E-2. Threat unit locations and mission activities (committed).

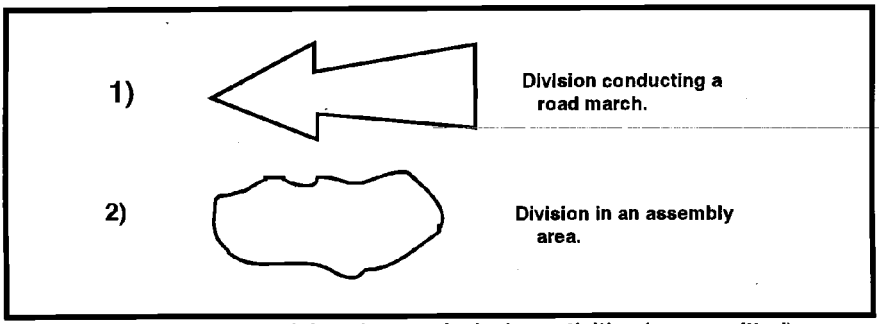


Figure E-3. Threat unit locations and mission activities (uncommitted).

THREAT MISSION CAPABILITIES ASSESSMENT :

Use combat effectiveness graphics to assess and display the capability of a threat unit to perform its mission. Consider all factors, tangible and intangible, in making the assessment; include unit strength, logistics status, maintenance and readiness status, morale, mission, weather, and terrain. Place selected symbols in the vicinity of the unit identification (Figure E-4).

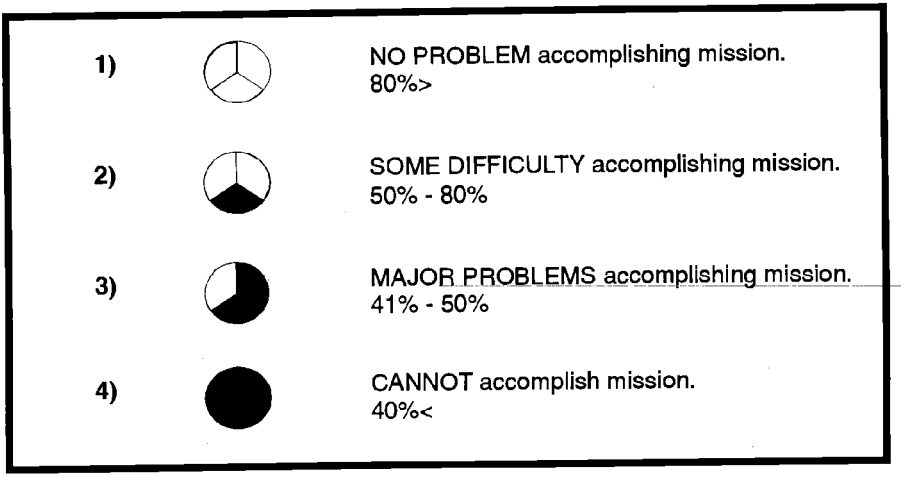


Figure E-4. Threat mission capabilities assessment.

A diminished threat mission capability is due usually to one or more specific problem areas such as damaged or destroyed weapons systems or a lack of ammunition, POL, or replacement personnel. If known, graphically depict these problem areas for each unit immediately next to the threat mission capabilities assessment symbol so the friendly commander can exploit what may be a very crucial, but fleeting, threat vulnerability.

Specific problem areas are indicated by blackening in the appropriate quadrant of the circle. The problem area categories are not static; other problem areas can be selected for display on this symbol as long as the selection is clearly explained in the key. Figure E-5 shows a sample problem area symbol and an example of the problem area symbol used in conjunction with the threat mission capabilities assessment symbol.

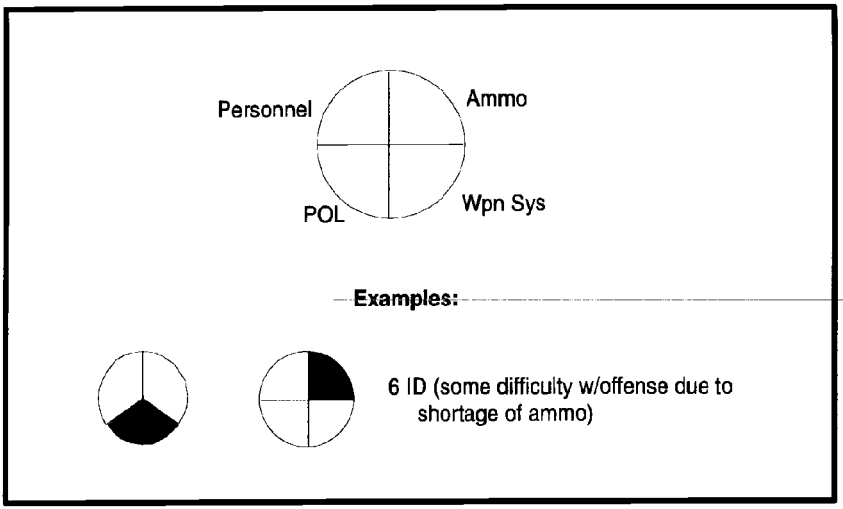


Figure E-5. Threat problem area symbology.

THREAT BOUNDARIES AND FRONT-LINE TRACE:

In conventional military operations, threat boundaries below the division level normally will not be included in the INTSUM. These lower level boundaries are often difficult to delineate and clutter the INTSUM. In some SASO activities, such as support to insurgency and COIN, smaller units will be the rule and must be constantly accounted for on the INTSUM.

The front-line trace will not be shown on the graphic INTSUM. The brackets depicting the frontages of the threat units in contact will suffice for an effective front-line trace. Addition of a front-line trace can be easily confused with the depictions of predicted threat activity.

THREAT OBJECTIVES:

If threat objectives can be discerned, they will be placed on the INTSUM.

THREAT AIR ACTIVITY :

Depict threat air activity on the INTSUM. Use an aircraft symbol with direction of travel and total number of sorties. Some units may opt to break down the sortie count by category, such as fighter (F), bomber (B), and reconnaissance (R). Example: A total sortie count of 12 could be depicted as (12). The same sortie count could also be depicted as (4F/6B/2R). The sortie breakdown should be used only if it will not clutter the INTSUM unnecessarily. Sortie breakdown symbols, such as F, B, and R must also be included (Figure E-6).

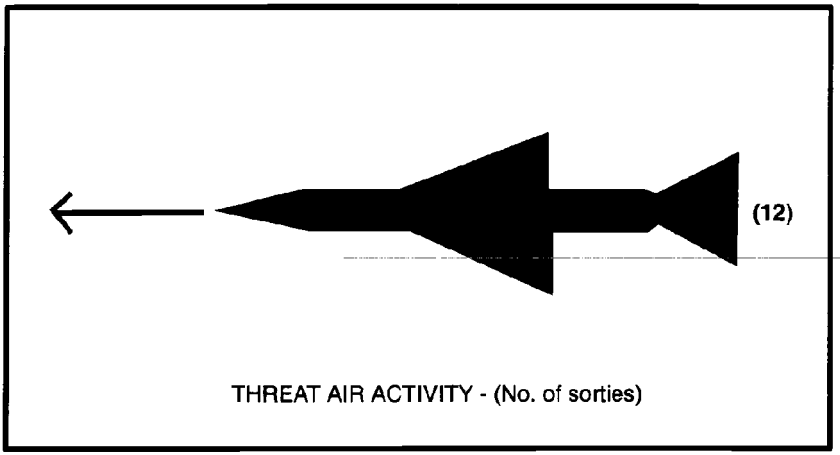


Figure E-6. Threat air activity symbology.

HREAT WEAKNESSES AND VULNERABILITIES:

Show specific weaknesses or vulnerabilities by using a numbered circle on the INTSUM (see Figure E-1). A supporting message could list threat weaknesses and vulnerabilities in narrative form.

THREAT STRENGTHS AND CAPABILITIES :

Show threat strengths and capabilities by using numbered squares (see Figure E-1).

THREAT INTENTIONS ASSESSMENT :

Write an assessment of threat intentions and most probable COA in a concise narrative format; graphically key it to the INTSUM when possible.

FRIENDLY COMMANDER'S INTENT AND PIR :

List the friendly commander's intent and PIR in narrative format on the INTSUM. Graphically key these statements to the overlay.

PREDICTED FUTURE THREAT ACTIVITY :

Draw predicted lines of threat advance or withdrawal and tie them to a timeline to convey as much information about future threat activity as possible (Figure E-7). Predicted lines of advance or withdrawal will be based on the "As Of" time found in the legend and margin information. Remember: Predicted lines are only an aid to planners; current threat situation must be continuously monitored to update the predictions.

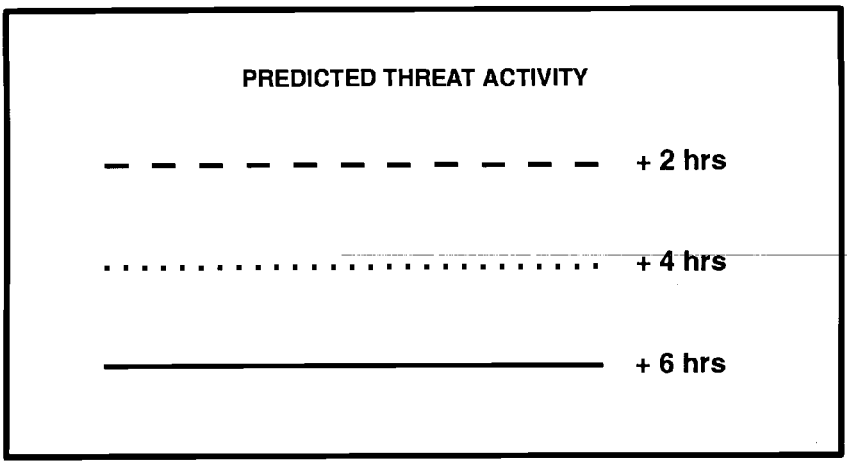


Figure E-7. Predicted threat activity timelines.

APPENDIX F

TARGETING

TARGETING PROCESS

Targeting is the process of selecting targets and matching the appropriate response to them, including operational requirements and capabilities. The purpose of targeting is to disrupt, delay, or limit threat interference with friendly COAs; it requires coordinated interaction between FS operations, intelligence, EW, and plans cells. Targeting is based on the enemy's assets that provide him an advantage (HPTs), friendly scheme of maneuver, and tactical plans. (See FM 6-20-10.)

Target development is one of the six IEW tasks. Mission analysis must precede generating any ECOAs. These ECOAs are the starting point for all other staff actions to wargame against, and to develop follow-on products. The products of the decide function are briefed to the commander. Upon his approval, his decisions are translated into the OPORD with annexes. (See FM 34-130.)

METHODOLOGY

Decisions create the guidelines for the acquisition and engagement of targets. TA and attack are made through a decision cycle. The methodology used to translate the commander's intent into a plan is **DECIDE, DETECT, DELIVER,** and **ASSESS.** Figure F-1 shows the functions of intelligence support to targeting, Figure F-2 shows the targeting methodology, and Figure F-3 is a targeting checklist.

RECEIVE GUIDANCE ON:	• Commander's intent. • HPTs. • Attack criteria. • Lead time between DPs and TAIs. • ROE. • Conditions to establish BDA requirements.
DEVELOP:	• MCOO. • Situation and event templates. • HVTs.
EXPLAIN:	• ECOA as part of wargaming. Based on friendly COA, refine event template; assist in developing HPT list, TSS matrix, and sensor or attack systems matrix.
PRODUCE:	• Collection plan, ISM, and AGM. • SOR.
BRIEF: (Ensure all analysts & collectors understand the CDR's intent.)	• ACE sections (ECOA, HPTL, TSS, and AGM).
COLLECT:	• Information for nomination, validation, and PSA.
DISSEMINATE:	• HPT related information and intelligence to FS immediately. • Pertinent information and BDA per SOP and TTP.
ENSURE:	• Information collection and intelligence production support all FRAGOs.

Figure F-1. Functions of intelligence support to targeting.

DECIDE	DETECT	DELIVER	ASSESS
• Target Development • TVA • HPT and HVT • TSS • Attack Options • Attack Guidance	• Target Detection Means • Detection Procedures • Target Tracking	• Attack • Planned Targets • Targets of Opportunity • Desired Effects • Attack Systems	• Tactical Level • Operational Level • Restrike • Feedback
Tracking your target is applicable during all of these steps.			

Figure F-2. Targeting methodology.

DECIDE:

_____ Do the commander's planning guidance and intent contain enough detail to enable the targeting team to determine—
- — HVTs to nominate as HPTs?
- — Desired effects on each HPT?
- — When to attack each HPT?
- — Any restrictions or constraints?
- — Which HPTs require BDA?

_____ What targeting assets (organic, attached, supporting) are available to detect and attach HPTs?

_____ What detect, deliver, and assess support is needed from higher HQ?

_____ When must requests to higher HQ be submitted to obtain the support when required?

_____ Have target tracking responsibilities been established?

_____ Are systems in place to handoff the detected targets to assets that are capable of tracking them?

_____ What detect, deliver, and assess support is required from subordinate units; when is it required?

Figure F-3. Targeting checklist.

_____ What detect, deliver, and assess support requests have been received from subordinate units; what has been done with them?

_____ Has the AGM been synchronized with the DST and the maneuver and FS plans?

_____ Are all commands using a common datum for locations? If not, are procedures in place to correct differences in data?

DETECT:

_____ Does the collection plan focus on PIR HPTs? (Which includes HPTs designated as PIR?)

_____ What accuracy, timeliness, and validity standards (TSS) are in effect for detection and delivery systems?

_____ Are all TA systems fully employed?

_____ Have backup TA systems been identified for HPTs?

_____ Have responsibilities been assigned to the appropriate unit and/or agency for detecting each HPT?

_____ Are HPTs being tracked?

_____ Have verification procedures using backup systems been established where necessary?

_____ Are TA and BDA requirements distributed properly among systems that can accomplish both?

DELIVER:

_____ Have communications links been established between detection systems, the decisionmaker, and delivery systems?

_____ Have responsibilities been assigned to the appropriate unit and/or agency for attacking each HPT?

_____ Has a backup attack system been identified for each critical HPT? (The primary system may not be available at the time the HPT is verified.)

_____ Have FSCMs or AGMs and clearance procedures been established to facilitate target engagement?

Figure F-3. Targeting checklist (continued).

_____ Have O/O FSCMs or AGMs been established to facilitate future and transition operations?

_____ Have potential fratricide situations been identified; have procedures been established to positively control each situation?

_____ Have responsibilities been assigned to the appropriate unit or agency for tracking specific HPTs and providing BDA on specified HPTs?

_____ What are the procedures to update the HPTL and synchronize the AGM and DST if it becomes necessary to change the scheme of maneuver and FS as the situation changes?

ASSESS:

_____ Are the collection assets linked to specific HPTs still available?

_____ Have the collection asset managers been notified of the attack of a target requiring assessment?

_____ Have assessment asset managers been updated as to the actual target location?

_____ Has all the coordination for the assessment mission, particularly airborne assets, been accomplished?

_____ What is the status of BDA collection?

_____ Has the information from the mission been delivered to the appropriate agency for evaluation?

_____ Has the targeting team reviewed the results of the attack to determine restrike requirements?

_____ Has the target intelligence gathered from the assessment been incorporated into the overall enemy situation development?

Figure F-3. Targeting checklist (continued).

STEP 1 - DECIDE:

DECIDE provides the overall focus and sets priorities for intelligence collection and attack planning (Figure F-4). Targeting priorities must be addressed for each phase or critical event of an operation. The decisions made are reflected in visual products as follows:

- HPTL is a prioritized list of HPTs whose loss to the enemy will contribute to the success of the friendly COA.

- Intelligence collection plan, or R&S plan, answers the commander's PIR, to include those HPTs designated as PIR. The plan, within the availability of additional collection assets, supports the acquisition of more HPTs. Determining the intelligence requirements is the first step in the CM process. (See FMs 34-2 and 34-2-1.)

- TSS matrix addresses accuracy or other specific criteria that must be met before targets can be attacked.

- AGM, approved by the commander, addresses which targets will be attacked, how, when, and the desired effects.

The formats for the HPTLs, TSS, and AGMs are examples only. Targeting personnel must understand all that is involved in building these targeting tools. However, experienced staffs may prefer to develop their own tailored formats.

IPB and Mission Analysis. IPB, including EPB, is a continuous process and starts in the preparation phase. It continues to provide updated as well as new products and supports the targeting process. The intelligence estimate provides key support to target development. MCOOs, doctrinal, situation, event, and DSTs help identify ECOAs, NAIs, TAIs, HVTs.

***TVA and Wargaming*.** The battlefield environment, its effects on combatants, and the threat are considered in IPB analysis to arrive at an intelligence estimate. TVA yields HVTs for a specific ECOA. Target spreadsheets identify the HVTs in relation to a type of operation, and target sheets (see FM 6-20-10, App A) give detailed targeting information for each HVT. This information is used during the IPB and the wargame processes. Both tools are developed by the G2 ASPS.

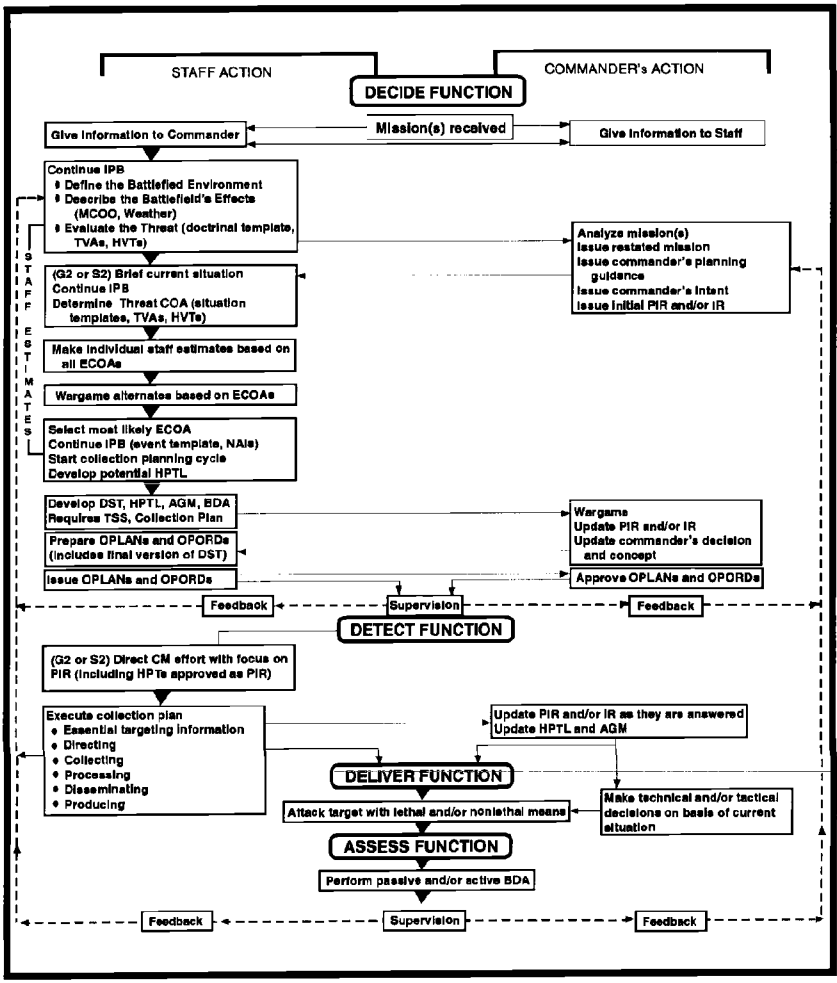


Figure F-4. The targeting process.

TVA, which is a detailed analysis of the enemy in selected COAs, uses the following enemy characteristics:

- Doctrine.
- Tactics.
- Equipment.
- Organizations.
- Expected behavior.

TVA methodology provides a relative ranking of target sets, or categories. It begins when target analysts in the G2/S2 assume the position of enemy commander. The target analyst, in coordination with other staff members, wargames the operation.

During wargaming, alternate friendly COAs are analyzed in terms of their impact on enemy operations and likely responses. The enemy battlefield functions that must be attacked to force the best enemy response are identified. The commander and staff analyze the criticality of friendly battlefield functions on a specific COA. The best places to attack HPTs are identified as TAIs. DPs or decision TPLs are used to ensure that the decision to engage or not to engage occurs at the proper time. Wargaming also identifies HVTs in priority that are critical to the success of the enemy mission. It also identifies the subset of HVTs which are HPTs that must be acquired and attacked for the friendly mission to succeed. HPTs selected are recorded on the DST.

Collection managers evaluate HVTs to determine asset detection capability. HPTs receive priority in the allocation of assets. The FSO determines friendly weapons systems capable of attacking HVTs with lethal fires, and the EWO nominates and coordinates to provide non-lethal fires.

Using the capabilities of the system to attack the targets, the G2/S2 analyzes and synthesizes the threat's response to each attack. Targets should be assigned priorities according to description, signature, degradation, and graphic representation. If targets have the same relative importance, a targeting team must prioritize the targets and seek advice from the FSE targeting analyst and the FAIO. After the targets are prioritized, they are placed on an HPTL (Figure F-5). After the HPTL is approved, the G2 will use it to develop the collection plan.

EVENT OR PHASE:		
PRIORITY	CATEGORY	TARGET

Figure F-5. Example high-payoff target list.

TSS. TSS are criteria applied to enemy activity (acquisitions and battlefield information) used in deciding whether the activity is a target. TSS break nominations into two categories: targets, which meet accuracy and timeliness requirements for attack; and suspected targets, which must be confirmed before any attack.

- HPT. This refers to the designated HPTs which the collection manager is tasked to acquire.
- TIMELINESS. Valid targets are reported to attack systems within the designated timeliness criteria.
- ACCURACY. Valid targets must be reported to the attack system meeting the required TLE criteria. The criteria is the least restrictive TLE considering the capabilities of available attack systems.

Considering these factors, different TSS may exist for a given enemy activity on the basis of different attack systems. For example, an enemy artillery battery may have a 150-meter TLE requirement for attack by cannon artillery and a 1 km requirement for attack helicopters. TSS are developed by the FSE in conjunction with MI personnel. Intelligence analysts use TSS to quickly determine targets from battlefield information and pass the targets to the FSE.

Attack system managers, such as FSEs, FCEs, or FDCs, use TSS to quickly identify targets for attack. Commands can develop *standard* TSS based on anticipated enemy OB and doctrine matched with the normally available attack systems.

The G2/S2 knows the accuracy of acquisition systems, associated TLE, and the expected dwell times of enemy targets. He can then specify whether

information he reports to the attack system manager is a target or a suspected target. Some situations may require the system to identify friendly and neutral from threat before approval to fire is given. HPTs that meet all the criteria should be tracked until they are attacked IAW the AGM. Location of targets that do not meet TSS should be confirmed before they are attacked. The TSS can be depicted in a TSS matrix (Figure F-6).

The matrix lists each system that forwards targets directly to the FSE, FCE, or FDC. The effects of weather and terrain on the collection assets and on enemy equipment are considered. TSS are keyed to the situation. However, the greatest emphasis is on the enemy situation considering deception and the reliability of the source or agency that is reporting.

HPT	TIMELINESS	ACCURACY
COPs	3 hr	150 m
RISTA	30 min	150 m
2S3	30 min	500 m
M-46	30 min	500 m
ADA	15 min	500 m
CPs	3 hr	500 m
Ammunition	6 hr	1 km
Maneuver	1 hr	150 m

Figure F-6. Example target selection standards matrix.

Attack Guidance. Knowing target vulnerabilities and the effect an attack will have on enemy operations allows a staff to propose the most efficient available attack option. Key guidance is whether the commander wishes to disrupt, delay, limit damage, or destroy the enemy. During wargaming, DPs linked to events, areas (NAIs and TAIs), or points on the battlefield are developed. These DPs cue the command decisions and staff actions where tactical decisions are needed.

On the basis of commander's guidance, the targeting team recommends how each target should be engaged in terms of the effects of fire and attack options to use. Effects of fire (see Joint Pub 1-02) can be to **harass, suppress, neutralize,**

or **destroy** the target. The subjective nature of what is meant by these terms means the commander must ensure the targeting team understands his use of them. Applying FS automation system default values further complicates this understanding.

- Harassing fire is designed to disturb the rest of the enemy troops, to curtail movement, and, by threat of losses, to lower morale. The decision to employ harassing fires needs careful consideration. Harassing fire has little real effect on the enemy, subjects gun crews to an additional workload, and increases the threat of counter-battery fires. ROE or the potential for adverse public opinion may prohibit its use. However, harassing fires may be a combat multiplier in some situations. Consider their use in SASO, delaying actions, and economy of force operations.

- Suppressive fire on or about a weapons system degrades its performance below the level needed to fulfill its mission objectives. Suppression lasts only as long as the fires continue. The duration of suppressive fires is either specified in the call for fire or established by SOP. Suppression is used to prevent effective fire on friendly forces. It is typically used to support a specified movement of forces. The FSCOORD needs to ask or calculate the *when* and *how long* questions.

- Neutralization fire is delivered to render the target ineffective or unusable temporarily. Neutralization fire results in enemy personnel or material becoming incapable of interfering with an operation or COA. Key questions the FSCOORD must ask are when and how long does the commander want the target to be neutralized. Most planned missions are neutralization fires.

- Destruction fire is delivered for the sole purpose of destroying material objects. It physically renders the target permanently combat-ineffective unless it is restored, reconstituted, or rebuilt. Setting automated FS default values for destruction of 30 percent does not guarantee achieving the commander's intent. The surviving 70 percent may still influence the operation. Destruction missions are expensive in terms of time and material. **Consider whether neutralization or suppression may be more efficient.**

The decision of what attack system to use is made at the same time as the decision on when to acquire and attack the target. Coordination is required when deciding to attack with two different means (such as EW and combat air operations). Coordination requirements are recorded during the wargame process.

The attack guidance must be approved by the commander and detail the following:

- A prioritized list of HPTs.
- When, how, and desired effects of attack.
- Any special instructions.
- HPTs that require BDA.

This information is developed during the wargame. Attack guidance—

- Applies to planned targets and targets of opportunity.
- May address specific or general target descriptions.
- Is provided to attack system managers via the AGM (Figure F-7).
- May change as the operation progresses.

The AGM must be updated during staff planning meetings and as the enemy situation changes. Consider separate AGMs for each phase of an operation.

PHASE/EVENT: Attack through the security zone				
HPTL	**WHEN**	**HOW**	**EFFECT**	**REMARKS**
COPs	P	GS ARTY	N	PLAN IN INITIAL PREP
RISTA and OPs	P	GS ARTY	N	PLAN IN INITIAL PREP
2S1 and 2S3	P	MLRS	N	PLAN IN INITIAL PREP
2S6, SA9 and SA13	P	GS ARTY	S	SEAD FOR AVN OPS
REGT CP	A	MLRS	N	
RESERVE BN	P	AVN BDE	D	INTENT TO ATTACK RESERVE BN IN EA HOT
LEGEND:	I = IMMEDIATE A = AS ACQUIRED P = PLANNED		S = SUPPRESS N = NEUTRALIZE D = DESTROY	
NOTES: [1]This is only an example of an AGM. Actual matrices are developed on the basis of the situation. [2]An "H" for harassing fires may be included in the EFFECT column during SASO.				

Figure F-7. Example attack guidance matrix.

HPTL. Lists the prioritized HPTs identified during wargaming. They have priority for engagement.

WHEN. Timing the attack of targets is critical to maximizing effects. During wargaming, the optimum time is identified and reflected in the WHEN column. A " **P"** indicates the target should not be engaged now but should be *planned* for future firing (e.g., a preparation, a SEAD program, or a countermobility program) or simply put on file. An **"A"** indicates such targets should be engaged in the sequence received in the headquarters, with respect to the priority noted in the HPTL. An **"I"** indicates the attack

must be *immediate* and is a special case. This designation should be limited to a small percentage of targets and only for the most critical types. Too many immediate targets are disruptive and lower the efficiency of attack systems. Immediate attacks take precedence over all others and are conducted even if attack systems must be diverted from attacks already underway. Examples of important targets include:

- Missile systems capable of NBC attacks.
- Division headquarters.
- NBC weapons storage and support facilities.

MRLS may be considered for immediate attack depending on their demonstrated effectiveness against friendly forces and their tactical employment. The G3/S3 and FSCOORD or FSO must establish procedures within the TOC that allow for immediate attack of targets.

HOW. Links the attack system to the HPT. It is best to identify a primary and backup attack system for attack of HPTs.

EFFECT. Refers to the target attack criteria. The targeting team should specify attack criteria according to the commander's guidance. Target attack criteria should be quantifiable (e.g., percentage of casualties or destroyed elements, time, ordnance, and allocation or application of assets). Also, it can be noted as the number of battery or battalion volleys.

REMARKS. Notes which targets should not be attacked in certain tactical situations (e.g., if the enemy is withdrawing). Examples of how to use this column:

- Accuracy or time constraints.
- Required coordination.
- Limitations on the amount or type of ammunition.
- Any need for BDA.

STEP 2 - DETECT:

DETECT is the next critical function in the targeting process. The G2/S2 is the main figure in directing the effort to detect identified HPTs. To identify who, what, when, and how for TA, the G2/S2 must work closely with the—

- ACE.
- FAIO.
- Targeting officer and FSO.

This process determines accurate, identifiable, and timely requirements for collection systems. The ACE must ensure collection system asset managers understand these requirements.

Information needs for target detection are expressed as PIR and IR. Their priority depends on the importance of the target to the friendly COA and tracking requirements. PIR and IR that support detection of HPTs are incorporated into the overall unit collection plan.

Targets are detected by the maximum use of all available assets. The G2/S2 must focus the intelligence acquisition efforts on the designated HPTs and PIR. Situation development information, through detection and tracking, will be accumulated as collection systems satisfy PIR and IR. The collection manager—

- Considers availability and capabilities of all collection assets within his echelon and those available to subordinate, higher, and adjacent units.
- Considers joint or combined force assets.
- Translates the PIR and IR into SIR and SOR.
- Arranges direct dissemination of targeting information from the collector to the targeting cell or targeting intelligence to the FSE if possible.

Detection Procedures. Use all TA assets effectively and efficiently. Avoid duplication of effort among intelligence available assets unless it is required to confirm target information. At corps and division, the ACE develops and manages the collection plan and ensures that no gaps in planned collection exist. This allows timely combat information to be collected to answer the commander's intelligence and TA requirements. To detect HPTs, give clear and concise

taskings to those TA systems capable of detecting a given target. This information lets analysts develop the enemy situation and identify targets (Figure F-8).

FS personnel provide the G2/S2 with the degree of located accuracy. The accuracy requirements are matched to the TLE of the collection systems. This allows the G2/S2 to develop more detailed TSS. NAIs and TAIs identified are matched with the most capable detection system available. If the target type and its associated signatures (e.g., electronic, visual, thermal) are known, the most capable collection asset can be directed against the target. The asset can be placed in the best position according to estimates of when and where the enemy target will be located.

Assets are positioned based on friendly estimates of where the enemy target is located. Information needed to detect targets are expressed in PIR and IR, which are incorporated into the collection plan. The collection manager translates the PIR and IR into SIR.

The collection manager considers the availability of all collection assets at all echelons. When a target is detected, the information is passed to the FAIO to determine if it is an HPT, its priority, and if it meets the TSS. To ensure that target information is passed quickly, the FAIO should be located in the ACE with communications to the FSE. Once an HPT is discovered, the FAIOs coordinate with their respective G2s/S2s and pass the targets directly to the FSE. If the commander approves the target, it is then passed to a firing unit. Mobile HPTs must be detected and tracked to maintain a current target location. Target tracking is inherent to detection.

BOS	TARGET ACQUISITION MEANS
INTELLIGENCE	SIGINT/EW, IMINT, HUMINT, TECHINT, MASINT systems.
MANEUVER	Patrols, scouts, units in contact, air/ground cavalry/air units.
FS	TAB, AN/TPQ-36/37 radars, FOs, AFSOs, COLTs.
AD	ADA scouts, ADA system's acquisition radars.
MOBILITY, COUNTER-MOBILITY, SURVIVABILITY	Engineer and NBC reconnaissance.
CSS	Truck drivers, base cluster recon/counterrecon patrols.
C^2	MIJI reports.
AIR FORCE	Joint STARS, AWACS.

Figure F-8. BOS detection capabilities.

As the assets collect information for target development, the information is forwarded to ACE intelligence analysts who use the information to perform situation and target development. Once a target specified for attack is identified, the analysts pass it to the FSE. The FSE executes the attack guidance against the target. Coordination between the intelligence staff and the FSE is essential to ensure that the targets are passed to an attack system that will engage the target.

The FAIOs can coordinate with the G2 and FSE to pass HPTs and other targets directly to the FCE at the division artillery TOC or, if approved by the maneuver commander, directly to a firing unit. The result is an efficient attack of targets which have been designated in advance for attack.

When the FAIO gets intelligence information which warrants attack, he notifies the FSE. This allows the FAIO to focus on intelligence analysis and the FSE to manage the control of fires. The targeting officer at the maneuver brigade and the S2 at the battalion perform FAIO functions.

Tracking priorities are based on the commander's concept of the operation and targeting priorities. Tracking is executed through the collection plan. Not all targets will be tracked. Because many critical targets move frequently or constantly, these HPTs require tracking.

Synchronization of Intelligence Collection. While conducting operations, the G2/S2 monitors execution of the collection plan. He uses an ISM to synchronize the intelligence system in order to give answers to PIR in time to affect the decisions they support. As HPTs are identified, he informs the appropriate FSE and cross-cues collection assets to support BDA as needed.

During delivery, NRT collectors and observers are cued to continue tracking targets during their engagement. Planned or cued BDA collection and reporting help determine if the engagement produced the desired effects. If not, continued tracking supports immediate reengagement.

To facilitate hand-off of target and tracking responsibilities, the G2/S2 coordinates with higher and subordinate units. Requirements for intelligence in a given area can then be directed to the unit responsible for that area. Operational graphics are useful when tracking particular threat units or HPTs. Passing responsibility for the target as it crosses the graphic ensures that it is not lost in crossing.

Synchronization continues during the CM process. The G2/S2 uses the products of the targeting process to develop SIR and SOR that synchronize the collection effort with command DPs. He plans and allocates time for collection, processing, and dissemination.

During execution the collection manager monitors the collection and reporting to ensure synchronization. He prompts asset managers to meet timelines, cross-cueing, and retasking as necessary to keep intelligence operations synchronized with command operations.

IEW Systems. The collection manager at each echelon gives appropriate IEW agencies missions through the collection plan and ISM. The intelligence analyst directly supports the collection manager. To properly synthesize information being received from forward units and collection systems intelligence analysts must understand their capabilities and limitations.

Figure F-9 explains the intelligence disciplines that provide targeting information through collection.

DISCIPLINE	FUNCTION
SIGINT/EW	• Friendly SIGINT/EW systems search for, intercept, and locate threat electronic signals emanating from radios, radars, and beacons. • Signatures are caused by electronics associated with the particular C^2 functions of the target. • Signatures identify signals based on characteristics of the signal or content of any messages intercepted. • The signals are then associated with an adversary's OB. • Electronic systems organic to tactical and operational (corps and theater) EW units can locate threat radio, radar, beacon, and C^2 system emissions using DF equipment. • DF efforts have inherent considerations that affect target accuracy such as DF system accuracy, terrain, and distance to target.
IMINT	• Imagery assets can be located in the AEB of the corps MI Bde, GRCS, and GS and DS companies of the Div MI Bn TUAV when fielded. • TUAV is organic to the DS Co of a heavy division. • TUAV is organic to the GS Co in a light infantry division. • FCE is assigned to the GS Co. • Predator UAV and Joint-STARS are USAF assets. They include airborne and ground-based IMINT sensors such as photo, TV, infrared, and MTI radar. • Targets have visual and infrared signatures that can be imaged. • Imagery analysts study results of IMINT missions to determine the presence, location, and assessed damage to threat targets. These films and devices can detect thermal signatures produced by equipment (engines, heaters, or any device producing or absorbing heat). These devices can also differentiate camouflaged equipment and structures. • Mounted sensors in UAVs provide TA capability which can locate threat elements unseen by ground observers and

Figure F-9. Intelligence disciplines.

	can successfully direct engagement of the targets. SLAR can detect the movement of vehicles beyond visual range of ground observers. • Imagery and intelligence analysts look for the threat's patterns of activity or intentions produced from IMINT systems. • Patterns of movement (numbers, direction, times) are analyzed and synthesized with other combat information to determine a threat commander's intentions. • Imagery can be requested from national and theater systems to support area studies and operations. • Imagery can also be used for training in garrison and at CTCs.
HUMINT	• HUMINT is produced by LRSUs, CI teams that are positioned throughout the depth of the battlefield, and interrogation teams that may be at maneuver battalions and higher. • Interrogation of threat prisoners can be focused on the detection of HVT and HPTs. • Interrogators should receive lists of intelligence interests and the commander's PIR. • Giving current HPTLs to the interrogators allows them to focus their efforts on locating these targets while gleaning additional information for situation development. • LRSUs are another HUMINT source. They may be tasked to determine the presence or absence of threat activity within the NAIs developed during the IPB process. • Keying these NAIs to HPTs allows the LRSUs to contribute significantly to the target detection process. • Information gained from LRSUs is real or NRT and can result in immediate engagement. • Due to extensive preparation and support requirements, LRSUs should be planned early and used IAW its doctrine (e.g., depth, target selection, insertion techniques). • CI teams detect subversion, espionage, and terrorist threats to friendly forces, and can also work with the local population to gather items of intelligence interest. • SOF may be tasked through SOCCE assigned at brigade, division, or Corps.

Figure F-9. Intelligence disciplines (continued).

TECHINT	• The TECHINT system is made up of two parts: S&TI and battlefield TECHINT. • S&TI supports strategic level of war intelligence. • Battlefield TECHINT supports operational and tactical levels of war intelligence. • TECHINT aids the commander by providing products that either identify or counter an adversary's monetary technological advantage. • TECHINT is an integral part of all-source intelligence because it involves everyone from individual soldiers to the policy makers. • Foreign material is photographed or captured and exploited for information, capabilities, limitations, and vulnerabilities. • The 203d MI Battalion operates the CMEC for the Army, or forms the Army's component of JCMEC or CCMEC. • Teams are sent from the battalion down to ECB units. • The G2, G3, TECHINT commander, and MI commander comprise the battlefield TECHINT team. • The commanders execute the staff's directives to collect materials for the TECHINT teams to exploit.
MASINT	• A MASINT sensor collects energy emitted by or reflected from an object or event for the purpose of identification and characterization. • Enemy weapon systems have physical characteristics and distinct performance identifiers when used. • Dynamic targets and events are primary candidates for MASINT exploitation by the MI force projection brigades. • These sources create energy emissions across the EM spectrum which carry information about its characteristics and performance via waves or particles. • This information is the signature collected by MASINT sensors; it can be used when developing threat assessments, OBs, IPB, and targeting materials. • MASINT data becomes invaluable during the rapid reprogramming of *smart* weapons and sensors or when changing tactics.

Figure F-9. Intelligence disciplines (continued).

STEP 3 - DELIVER:

DELIVER executes the target attack guidance and supports the commander's battle plan once the HPTs have been located and identified (Figure F-10).

ATTACK OF TARGETS MUST:	■ Satisfy attack guidance developed in *decide* function. ■ Require two categories of decisions—*tactical* and *technical*.
TACTICAL DECISIONS DETERMINE:	■ Desired effect, degree of damage, or both. ■ Attack system to be used. ■ Time of attack. This is determined IAW type of target: Planned target or target of opportunity. ; **PLANNED TARGET:** –Some targets will not appear as anticipated. –Target attack takes place only when the forecasted enemy activity occurs in projected time or place. Detection & tracking of activities associated with target becomes trigger for target attack.
TARGETING TEAM:	
G2 RESPONSIBILITIES:	■ Verifies enemy activity as the planned target to be attacked. ■ Validates target by conducting final check of reliability of source & accuracy (time & location) of target. Passes target to FSE. ■ Current operations officer checks legality of target in terms of the ROE.
FSE RESPONSIBILITIES:	■ Determines if attack systems planned are available & still best systems for attack. ■ Coordinates with higher/lower/adjacent units, other services, allies & HN (important where potential fratricide situations are identified).

Figure F-10. Deliver functions and responsibilities.

	■ Issues fire mission request to appropriate executing units. ■ Informs G2 of target attack. G2 alerts appropriate system responsible for BDA (when applicable). ; **TARGETS OF OPPORTUNITY:** –Are processed the same as planned HPTs. –Those not on HPTL are first evaluated to determine when or if they should be attacked. ■ Decision to attack follows attack guidance & is based on— •Activity of the target. •Dwell time. •Target payoff compared to other targets currently being processed for engagement. –If decision is made to attack immediately, target is processed further. –Availability & capabilities of attack system to engage targets are assessed. –If target exceeds availability or capabilities, send target to higher HQ for immediate attack. –If decision is to defer attack, continue tracking; determine DPs for attack, and modify collection taskings as appropriate.
TECHNICAL DECISIONS (DETERMINED BASED ON TACTICAL DECISIONS):	■ Precise delivery means. ■ Number and type of munitions. ■ Unit to conduct the attack. ■ Response time of the attacking unit. ■ Results in physical attack of targets by lethal and/or nonlethal means. ■ FS cell directs attack system to attack target once tactical decisions have been made. ■ FS cell provides attack system manager with—

Figure F-10. Deliver functions and responsibilities (continued) .

	•Selected time of attack. •Effects desired IAW previous discussion. •Any special restraints or requests for particular munitions types. ■ Attack system manager (FSCOORD, ALO, AVN BDE, LNO, NGLO) determines if his system can meet requirements. If cannot, he notifies FS cell. Some reasons for not being able to meet requirements include— •System not available at specified time. •Required munitions not available. •Target out of range. ■ FS cell must decide if selected system should attack under different criteria or if a different system should be used.
TARGETS OF OPPORTUNITY ARE ATTACKED BASED ON:	■ The target's activity. ■ Estimated assembly area activity.
DESIRED EFFECTS: **DISRUPT** **DELAY** **LIMIT**	■ Planned Targets: •Verify enemy activity as that planned to be attacked. •Reaffirm decision to attack. •Issue the fire mission request (through FS cell) to appropriate executing units. ■ Targets of Opportunity: •Targeting team must decide payoff and availability of attack systems and munitions.
ATTACK SYSTEM:	■ Planned Targets: •Decision made during *decide* function. •Determine system availability & capability. •Targeting team must determine best system available to attack target if system not available or capable.

Figure F-10. Deliver functions and responsibilities (continued).

	■ Targets of Opportunity: •Targeting team must determine attack system, subject to maneuver commander's approval. •Consider all available attack systems. •Attacking targets should optimize capabilities of— –Light and heavy ground forces. –Attack helicopters. –FA. –Mortars. –Naval gun fire. –Combat air operations (CAS and air interdiction). –Offensive EW. •Consider availability & capabilities of each resource using the following: –Desired effects on the target. –Payoff of the target. –Degree of risk to use asset against target. –Impact on friendly operations. •Target attack must be coordinated among two or more attack systems. •Engaging a target by lethal means, along with jamming or monitoring, may be of greater benefit than simply firing at the target.

Figure F-10. Deliver functions and responsibilities (continued).

STEP 4 - ASSESS:

Combat assessment is the determination of the effectiveness of force employment during military operations. It is composed of three elements:

- BDA, which is the timely and accurate estimate of damage resulting from the application of lethal or nonlethal military force against a target.
- MEA, which is an assessment of the military force in terms of weapon systems and munitions effectiveness.

- Reattack recommendation.

In combination, BDA and MEA inform the commander of effects against targets and target sets. Based on this, the threat's ability to make and sustain war and centers of gravity are continuously estimated. During the review of the effects of the campaign, restrike recommendations are proposed or executed. BDA pertains to the results of attacks on targets designated by the commander. Producing BDA is primarily an intelligence responsibility, but requires coordination with operational elements. BDA requirements must be translated into PIR. It accomplishes the following:

- At the tactical level, commanders use BDA to get a series of timely and accurate snapshots of their effect on the enemy. It provides commanders an estimate of the enemy's combat effectiveness, capabilities, and intentions. This helps commanders determine when or if their targeting effort is accomplishing their objectives.

- BDA helps to determine if restrike is necessary. Commanders use BDA to allocate or redirect attack systems to make the best use of available combat power.

The G3 through the targeting team conducts MEA concurrently and interactively with BDA as a function of combat assessment. MEA is used as the basis for recommending changes to increase effectiveness in—

- Methodology.
- Tactics.
- Weapon systems.
- Munitions.
- Weapon delivery parameters.

The G3 develops MEA by determining the effectiveness of tactics, weapons systems, and munitions. Munitions effect on targets can be calculated by obtaining rounds fired on specific targets by artillery assets. The targeting team may generate modified commander's guidance concerning—

- UBL.
- RSR.
- CSR.

The need for BDA for specific HPTs is determined during the **decide** function. Record BDA on the AGM and intelligence collection plan. The resources used for BDA are the same resources used for target development and TA. An asset used for BDA may not be available for target development and TA. The ACE receives, processes, and disseminates to the targeting team the results of attack, which are analyzed in terms of desired effects.

The targeting team must keep the following BDA principles in mind:

- BDA must measure things that are important to commanders, not make important the things that are easily measurable.
- BDA must be objective. When a G2/S2 receives a BDA product from another echelon, he should verify the conclusions (time permitting). G2s/S2s at all echelons must strive to identify and resolve discrepancies among the BDA analysts at different headquarters.
- The degree of reliability and credibility of the assessment relies largely upon collection resources. The quantity and quality of collection assets influence whether the assessment is highly reliable (concrete, quantifiable, and precise) or has low reliability (best guess). The best BDAs use more than one collection discipline to verify each conclusion.

Each BDA has three assessment components (Figure F-11). Each requires different sensors, analytical elements, and timelines. They are not necessarily subcomponents of each BDA report. (See FM 6-20-10, Appendix D.)

COMPONENTS	DESCRIPTION
PDA	• Qualitative physical damage from munitions blast, fragmentation, and fire. • Based on observed or interpreted damage.

FDA	• Effects of military force to degrade or destroy capability of target to perform mission. • Assessment based on all-source intelligence. • Includes an estimate of time to reconstitute or replace target. • Temporary assessment compared to a TSA used for specific missions.
TSA	• The overall impact of the full spectrum of military operations on an entire target system's capability. • Can be applied against an adversary's combat effectiveness. • May address significant subdivisions of a target. • A more permanent assessment.

Figure F-11. BDA functions.

BDA is more than determining the number of casualties or the amount of equipment destroyed. The targeting team can use other information, such as—

- Whether the targets are moving or hardening in response to the attack.
- Changes in deception efforts and techniques.
- Increased communication efforts as the result of jamming.
- Whether the damage achieved is affecting the enemy's combat effectiveness as expected.

BDA may also be passive by compiling information regarding a particular target or area (e.g., the cessation of fires from an area). If BDA is to be made, the targeting team must give intelligence acquisition systems adequate warning for sensors to be directed at the target at the proper time. BDA results may change plans and earlier decisions. The targeting team must periodically update the decisions made during the **decide** function concerning—

- IPB products
- HPTLs.
- TSS.
- AGMs.
- Intelligence collection plans.
- OPLANs.

Based on BDA and MEA, the G2/G3 consider the level to which operational

objectives have been achieved and make recommendations to the commander. Reattack and other recommendations should address operational objectives relative to the—

- Target.
- Target critical elements.
- Target systems.
- Enemy combat force strengths.

BDA key players are the commander, operations officer, FSO, AAO, ALO, and S2. The S2 integrates intelligence and operational data. In coordination with the G3, the G2/S2—

- Recommends HPTs.
- Develops and recommends IR to include those for targeting and BDA. Some requirements become PIR.
- Coordinates with the G3/S3, AAO, and FSO to develop a fully coordinated targeting and BDA plan.
- Develops a synchronized collection plan to answer the commander's IR and tracks and maintains BDA charts and files.
- Tasks or requests collection support from the appropriate unit or agency to collect information required to satisfy the commander's targeting objectives and BDA reporting requirements.
- Establishes procedures to ensure reports from FOs, scouts, troops in contact, pilots, and AVTRs are quickly made available for BDA analysis.
- Matches BDA reporting requirements against the commander's objectives to determine targeting effort drain; develops and maintains historical BDA databases, and disseminates hard and soft copy intelligence and BDA results.
- Uses the results of BDA and combat assessment to determine the need to develop further threat COAs.
  - — Determines priority for collection assets between the targeting effort and

the BDA supporting requirements.

— Determines and updates enemy capabilities based upon results of the targeting effort.

SASO CONSIDERATIONS

Target development and targeting are difficult in an SASO environment. Although the principles of the targeting process still apply in SASO, consider the following:

- ROE tend to be more restrictive than in conventional combat situations. Everyone involved in the targeting process must completely understand the ROE.
- Identification of HVTs, threat intentions, threat locations, and weapons systems is slow to develop and may not be able to be acted upon when fully developed.
- Because of the nature of the threat (usually a relatively small, unconventional enemy may constitute a significant threat to US forces) determination of HVTs (specifically, what constitutes an HVT) is extremely difficult. Thus, it is difficult to develop precise time, location, and rates of march for a threat force.
- "Targets," which blend into the population, are often less visible than conventional targets.
- When identified, targets present less of a window of opportunity in which to react, decreasing decision time.
- Because of considerations of the HN population, targeting must be precise. Selecting the right weapons system for the right target is paramount.
- Interaction and coordination with nontraditional elements and agencies may be required. This may include private organizations, NGOs, other federal agencies, civil agencies, allies or coalition forces, and HN forces.

CARVER TECHNIQUE

ARSOF uses CARVER factors to assess mission, validity, and requirements. They are also used in technical appreciation and target analysis.

The CARVER selection factors assist in selecting the best targets or components to attack. As the factors are considered, they are given a numerical value, which represents the desirability of attacking the target. The values are then placed in a decision matrix. After CARVER values for each target or component are assigned, the sum of the values indicates the highest value target or component to be attacked within the limits of the statement of requirements and commander's intent. Figure F-12 explains the CARVER techniques.

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE
Criticality	•Means target value. •Primary consideration in targeting. •Target is critical when its destruction or damage has major impact on military, political, or economic operations. •Consider targets within a system in relation to other elements of the target system. •Value of target will change as situation develops. •Target requires use of time-sensitive methods which respond to changing situation. **EXAMPLE:** When one has few locomotives, railroad bridges may be less critical as targets; however, safeguarding bridges may be critical to maneuvering conventional forces requiring use of such bridges.	•Time—How rapidly will impact of target attack affect operations? •Quality—What % of output, production, or service will be curtailed by target damage? •Surrogates—What will be effect on output, production, and service? •Relativity—How many targets? What are their positions? How is their relative value determined? What will be affected in the system or complex stream?	•Immediate halt; target cannot function without it. •Halt within 1 day, or 66%. •Halt within 1 week, or 33%. •Halt within 10 days, or 10%. •No significant affect. *Refers to time or %; curtailment in output, production, or service.	9 to 10 7 to 8 5 to 6 3 to 4 1 to 2

Figure F-12. CARVER techniques.

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE
Accessibility	•Target is accessible when operations element can reach the target with sufficient personnel and equipment to accomplish mission. •Entails identifying & studying critical paths the operational element must take to achieve objectives & measuring those things that aid or impede access. •You must be able to reach target AND remain there for extended periods. •Basic steps identifying accessibility: –Infiltration from staging base to target. –Movement from point of entry to target/objective. –Movement to target's critical element. –Exfiltration.	•Active & passive EWS. •Detection devices. •AD capabilities within target area. •Road & rail transportation systems. •Type terrain & its use. •Concealment & cover. •Population density. •Other natural or synthetic obstacles & barriers. •Current & climatic weather conditions. •Analysis along each critical path to target should measure time it would take for action element to bypass, neutralize, or penetrate barriers/ obstacles. •Measured by relative ease or difficulty of movement for operational element & likelihood of detection. Consider using standoff weapons in such evaluations.	•Easily accessible standoff weapons can be employed. •Inside a perimeter fence but outdoors. •Inside a building but on ground floor. •Inside a building but on second floor or in a basement; climbing or lowering is required. •Not accessible or inaccessible without extreme difficulty.	9 to 10 7 to 8 5 to 6 3 to 4 1 to 2

Figure F-12. CARVER techniques (continued).

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE
Recuperability	•Measured in time—How long will it take to replace, repair, or bypass destruction of or damage to the target? •Varies with sources and type of targeted components and availability of spare parts availability.	•Onhand equipment such as railroad cranes, dry docks, and cannibalization. •Restoration and substitution through redundancies. •Onhand spares. •Equivalent OB equipment sets that backup critical equipment or components; effects of economic embargoes and labor unrest.	Replacement, repair, or substitution requires— •1 month or more. •1 week to 1 month. •72 hours to 1 week. •24 to 72 hours. •Same day replacement, repair, or substitution.	9 to 10 7 to 8 5 to 6 3 to 4 1 to 2
Vulnerability	•Target is vulnerable if operational element has means & expertise to successfully attack the target. •Scale of critical component needs to be compared with capability of attacking element to destroy or damage it. •Attacking element may tend to— –Choose special components. –Do permanent damage.	•Depends on— –Nature and construction of the target. –Amount of damage required. –Assets available, (e.g., personnel, expertise, motivation, weapons, explosives, and equipment.)	•Vulnerable to long-range laser target designation, small arms fire, or charges of 5 lbs or less. •Vulnerable to light antiarmor weapons fire or charges of 5 to 10 lbs.	9 to 10 7 to 8

Figure F-12. CARVER techniques (continued).

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE
	–Maximize effects through use of onsite materials. –Cause the target to self-destruct.		•Vulnerable to medium antiarmor weapons fire, bulk charges of 10 to 30 lbs, or very careful placement of smaller charges.	5 to 6
			•Vulnerable to heavy antiarmor fire, bulk charges of 30 to 50 lbs, or requires special weapons.	3 to 4
			•Invulnerable to all but the most extreme target-ting measures.	1 to 2
Effect	•Measure of possible military, political, economic, psychological & sociological impacts at target & beyond. •Closely related to the measure of target criticality. •Type & magnitude of given effects desired will help planners select targets & target components.	•Primary effect of destruction of 2 adjacent long-range radar sites in EWS may be to open hole in system that is of sufficient size & duration to permit attacker to launch a successful air or missile nuclear strike against defender.	•Overwhelmingly positive effects; no significant negative effects.	9 to 10
			•Moderately positive effects; few significant negative effects.	7 to 8
			•No significant effects; neutral.	5 to 6
			•Moderately negative effects; few significant positive effects.	3 to 4

Figure F-12. CARVER techniques (continued).

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE
	•Addresses all significant effects, whether desired or not, that may result once selected target component is attacked. •Traditionally, this element addressed effect on local population; now there are broader considerations. •Frequently neutral at tactical level.	•Can include— –Triggering of counter-measures. –Support of negation of PSYOP themes. –Unemploy-ment. –Reprisals against civilian popu-lace. –Collateral damage to other targets. •Possible effects can be specula-tive & thus should be labeled. •Effects of same attack may be different at tactical, opera-tional & strategic levels. **EXAMPLE:** Destruction of a substation may not affect local power but cuts off power to adjacent region.	•Overwhelmingly negative effects; no significant positive effects.	1 to 2

Figure F-12. CARVER techniques (continued).

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE
Recognizability	•Target's recognizability is degree to which it can be recognized by an operational element or intel collection & recon assets under varying conditions. •Weather impacts visibility. •Rain, snow & ground fog may obscure observation. •Road segments with sparse vegetation & adjacent high ground provide excellent conditions for good observation. •Distance, light & season must also be considered.	•Site & complexity of target. •Existence of distinctive target signatures. •Presence of masking or camouflage. •Technical sophistication & training of attackers.	•Target is clearly recognizable under all conditions & from a distance; requires little or no training. •Target is easily recognizable at small-arms range & requires small amount of training. •Target is difficult to recognize at night or in bad weather, or might be confused with other targets or components; requires some training. •Target is difficult to recognize at night or in bad weather, even within small-arms range; it is easily confused with other targets or components; requires extensive training. •Target cannot be recognized under any conditions, except by experts.	9 to 10 7 to 8 5 to 6 3 to 4 1 to 2

	DESCRIPTION	FACTORS	CRITERIA & VALUES*	SCALE

Figure F-12. CARVER techniques (continued).

CARVER factors and their assigned values are used to construct a CARVER matrix. Table F-1 is a tool for rating the desirability of potential targets and allocating attack resources.

- List the potential targets in the left column.
- For strategic level analysis, list the enemy's systems or subsystems (electric power supply, rail system).
- For tactical level analysis, list the complexes or components of the subsystems or complexes selected for attack by your higher HQ.
- As each potential target is evaluated for each CARVER factor, enter the appropriate value into the matrix.
- Once all the potential targets have been evaluated, add the values for each potential target.
- The sums represent the relative desirability of each potential target; this constitutes a prioritized list of targets.
- Attack those targets with the highest totals first.
- If additional men or munitions are available, allocate these resources to the remaining potential targets in descending numerical order.
- This allocation scheme will maximize the use of limited resources.

The S2 can use the CARVER matrix to present operation planners with a variety of attack options. With the matrix, he can discuss the strengths and weaknesses of each COA against the target. Having arrived at conclusions through the rigorous evaluation process, the S2 can comfortably defend his choices.

Table F-1. Bulk electric power supply.

POTENTIAL TARGETS	C	A	R	V	E	R	TOTAL
Fuel Tanks	8	9	3	8	5	6	41
Fuel Pumps	8	6	2	10	5	3	34
Boilers	6	2	10	4	5	4	31
Turbines	8	6	10	7	5	9	45
Generators	4	6	10	7	5	9	41
Condenser	8	8	5	2	5	4	34
Feed Pumps	3	8	5	8	5	6	33
Water Pumps	3	8	5	8	5	4	33
Generator Step up Transformer	10	10	10	9	5	9	53

APPENDIX G

IEW SYSTEMS

QUICKFIX (AN/ALQ-151(V1)) Advanced QUICKFIX (AN/ALQ-151(V2))

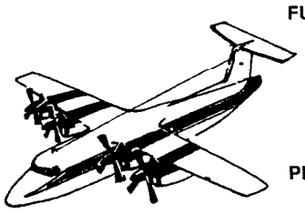
FUNCTION: VHF DF intercept, VHF EA, VHF DF (nets w/TRAILBLAZER for DF). Component of IEWCS AF/VHF/UHF ES

PRIME MOVER: EH-60A, EH-60L (BLACKHAWK)

UNIT AND QTY: HVY DIV: 3 Systems 3 Flt Plt, Avn Bde; LT DIV: 3 Systems, 3 Flt Plt, Avn Bde; AASLT DIV: 3 Systems, 3 Flt Plt, HHOC, MI Bn; ABN DIV: 3 Systems, 3 Flt Plt, Cbt Avn Sqdn; ACR: 3 Systems, 3 Flt Plt, Cbt Avn Sqdn

INTEL APPLICATION: COMINT

Airborne Reconnaissance Low (ARL)



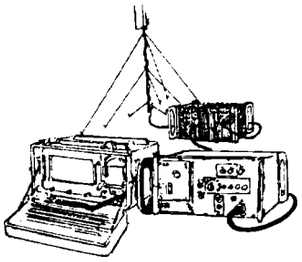
FUNCTION: Ground processing station, ACT 101 remote rcv sets, TACLINK video rcv sets, FLIR system, daylight imaging systems, infrared line scanner, radio intercept/DF systems; interoperates w/ASAS & CTT

PRIME MOVER: DHC-7 arrives ready for immediate employment

UNIT AND QTY: Select Brigades

INTEL APPLICATION: COMINT/IMINT

Commander's Tactical Terminal (CTT), AN/TSC-125



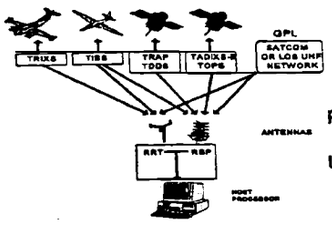
FUNCTION: Communications terminal; GUARDRAIL downlink on TRIXS network; RRS on board RC-12 & U2-R, RRTS; includes OT, RBP, RRT, LOS adaptive array antenna, SDS, embedded COMSEC

PRIME MOVER: NA

UNIT AND QTV: 1- MI at all echelons

INTEL APPLICATION: SIGINT

Joint Tactical Terminal: JTT/H3 (AN/USC-55)
JTT/H-R3 (AN/USR-6)



FUNCTION: Communications terminal, 2 LRUs, 1 RBP, 1 RRT, host processor & antenna array (both user provided); mobile & mountable in F/W & R/W, tracked & wheeled vehicles, shelters

PRIME MOVER: NA

UNIT AND QTY: Avn, ADA, FA, MI at all echelons; integrated into GSM/CGS, ASAS, ETRAC, THAADS, Patriot, JTAGS, TROJAN SPIRIT, AFATDDS, other multiservice systems

INTEL APPLICATION: SIGINT

Ground-Based Common Sensor (GBCS)

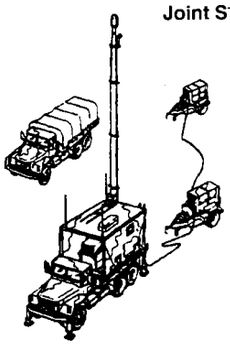
FUNCTION: ES (intercept& DF); EA (jamming); COMINT targeting location data; common subsystems with AQF & MEWSS

PRIME MOVER: EFVS (HVY DIV) or HVY HMMWV (LT DIV)

UNIT AND QTY: 6 GBCS-H per MI Bn (H); 4 GBCS-H per MI Co (ACR); 4 GBCS-L per MI Bn (ABN, AASLT, LT); 6 per MI Bn (H, LT, ABN, AASLT, DIV); 6 per MI Co; ACR

INTEL APPLICATION: COMINT/ELINT

Joint STARS Ground Station Module (GSM) (AN/TSQ-132)

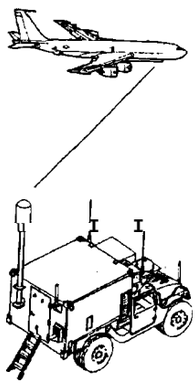


FUNCTION: MTI, FTI, SAR imagery; supports situation development, battle mgt, targeting, force protection, limited BDA/TDA, operations planning

PRIME MOVER: LT - 2xHMMWV; MED - 2X5-ton HMMWV

UNIT AND QTY: 6- Selected DIV; 6- Selected Corps; 1- ACR; 1- EAC

INTEL APPLICATION: IMINT/SIGINT/INTEL/ ARTY/AVN SUPPORT



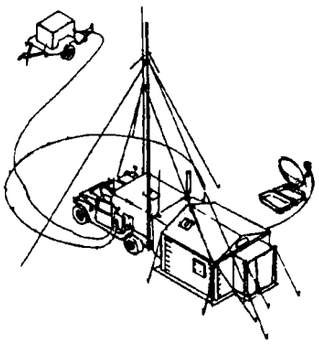
Joint STARS Common Ground Station (CGS)

FUNCTION: MTI, FTI, SAR imagery; supports situation development, battle mgt, targeting, force protection, limited BDA/TDA, operations planning; includes SATCOM & CTT communications

PRIME MOVER: LT - 2xHMMWV

UNIT AND QTY: 5 to 7- DIV; 5 to 7- Corps; 1- ACR; 1- SEP BDE; 1 to 5 EAC

INTEL APPLICATION: IMINT/SIGINT/INTEL/ ARTY/AVN SUPPORT



Integrated Meteorological System (IMETS)

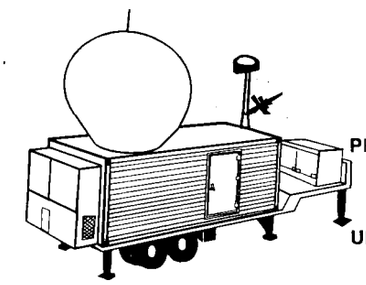
FUNCTION: Receives, processes & disseminates weather data.

PRIME MOVER: Heavy HMMWV mounted

UNIT AND QTY: DIV, Corps, EAC, SEP BDE, ACR, AVN BDE, other task organized contingencies

INTEL APPLICATION: Intelligence Support

Advanced Electronic Processing and Dissemination System (AEPDS)



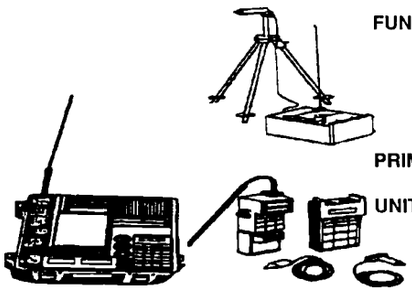
FUNCTION: Mobile, air & ground transportable comm system; receives, processes & exploits SIGINT data from multiple national, theater & organic ELINT/ COMINT systems. Combines functions of EPDS & ETUT into a single downsized system

PRIME MOVER: 30 ft van pulled by a 3-axle 10-ton tractor air deployable on C-130 or larger aircraft

UNIT AND QTV: 1- Corps (rear) 1- Select MI Bde (EAC)

INTEL APPLICATION: SIGINT

Improved Remotely Monitored Battlefield Sensor System (IREMBASS)



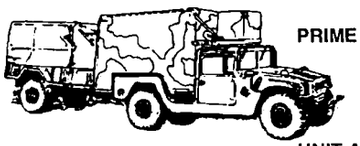
FUNCTION: Unattended ground sensor (seismic/ acoustic, magnetic, infrared, meteorological) that detects, classifies & determines direction of movement

PRIME MOVER: Manpacked and vehicle

UNIT AND QTY: LT DIV - 5 (GS Plt, I&S Co, MI Bn); ASSLT DIV - 5 (GS Plt, I&S Co, MI Bn); ABN DIV - 5 (GS Plt, MI Co (Fwd Spt), MI Bn)

INTEL APPLICATION: MASINT

Mobile Integrated Tactical Terminal (MITT)



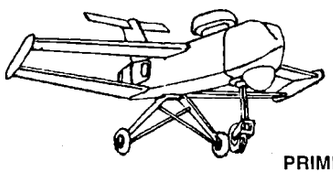
FUNCTION: Replaces THMT & FAST-I in force structure; compatible w/TROJAN, MSE, TIBS, DIN/DSSCS, STU III, TENCAP; TRAP/TADIXS-B, UHF SATCOM, S-BAND w/ROTERM/ CHARIOT

PRIME MOVER: Mobile, ground, air transportable (heavy duty HMMWV, cargo HMMWV, generator trailer, C-130, CH-47)

UNIT AND QTY: DIV and Corps ACE - 1

INTEL APPLICATION: SIGINT/IMINT

Tactical Unmanned Aerial Vehicle (TUAV) - OUTRIDER



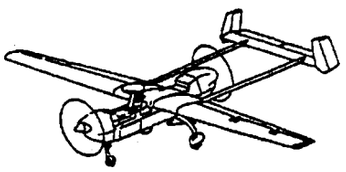
FUNCTION: Operates fwd of FLOT, in all conditions; provides NRT intel, recon, battlefield survl, color E-O camera, FLIR, plug-in optronic payload; future payloads: MTI, SAR, comm/ noncomm DF, intercept, jamming; MET

PRIME MOVER: C-130 or larger, roll-on/roll-off; ground equipment mounted on HMMWVs

UNIT AND QTY: 3 - HVY/AASLT DIV; 5 - LT DIV; 3 - ABN DIV; 3 - ACR; 5 - LT ACR; 1 - SEP BDE

INTEL APPLICATION: IMINT/SIGINT/PSYOP

Unmanned Aerial Vehicle-Short Range (UAV-SR) HUNTER



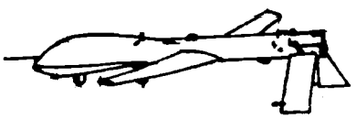
FUNCTION: Operates fwd of FLOT, in all conditions; provides NRT intel, recon, battlefield survl, color CCD, TA, BDA, recon, battlefield survl, E-O/FLIR, UAV data relay; future payloads: MTI, SAR, MET, ES, EA, mine detection, PSYOP, SIGINT, NBC recon

PRIME MOVER: NA

UNIT AND QTY: **Not fielded. For training use only**

INTEL APPLICATION: IMINT/SIGINT/PSYOP

Unmanned Aerial Vehicle (UAV)-Endurance PREDATOR



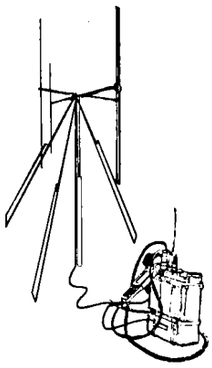
FUNCTION: Operates as stand-off system in all conditions, behind friendly lines; can penetrate into enemy territory; payloads: E-O/FLIR, MTI/SAR, SIGINT, MET, PSYOP, NBC recon, comm/data relay

PRIME MOVER: 2 C-141s or multiple C-130s

UNIT AND QTY: USAF Asset - Deployed in support of Joint Operations

INTEL APPLICATION: IMINT/SIGINT/PSYOP

Lightweight Man-Transportable Radio Direction Finding System (LMRDFS) AN/PRD-12



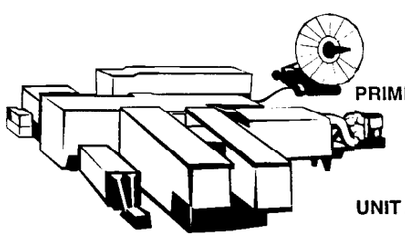
FUNCTION: Lightweight manportable comm intercept/DF system; on emitter location missions, works w/TEAMMATE; ideal in LT, ABN, AASLT, SOF opns; rapid relocation; optimizes collection in fwd AO; CNR for external comm

PRIME MOVER: Manpacked; 60 lbs, carried by 2 soldiers

UNIT AND QTY: 1 - LT ABN; 3 - HVY/AASLT DIV; 3 - ACR; 1 - SEP BDE; 7 - SOF BN; 10 - SOF SA

INTEL APPLICATION: COMINT

Modernized Imagery Exploitation System (MIES)



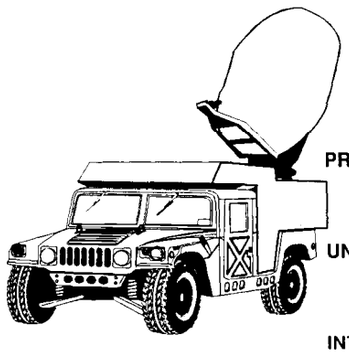
FUNCTION: NRT IMINT; provides exploitation/exploitation mgt, receipt, reporting, SID, archive of imagery & reports; replaces IPDS

PRIME MOVER: 40 ft hardcopy/softcopy exploitation van; 35 ft SATCOM van; 35 ft receive location van; air deployable, C-141, C-5

UNIT AND QTY: Selected MI Bde

INTEL APPLICATION: IMINT

TROJAN SPIRIT (AN/TSQ-190V)



FUNCTION: Satellite terminal; intel processing/dissem, secure voice, data, GPS, FAX, LAN wkstns, video, SID; receive, display, transmit digital imagery, weather/terrain prods among CONUS/OCONUS & deployed

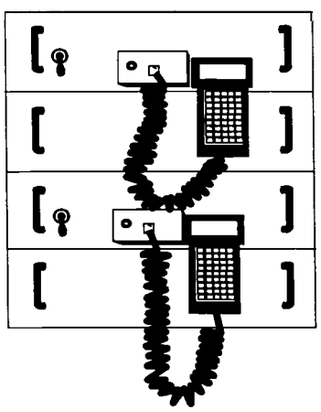
PRIME MOVER: Mounts on 2 heavy variant HMMWVs; tactical SATCOM trailer

UNIT AND QTY: Connectivity: Ft Belvoir TROJAN switching center for worldwide deployment

INTEL APPLICATION: IMINT/SIGINT/CI/ HUMINT/Intelligence Support

---

Synthetic UHF Computer-Controlled Equipment Subsystem (SUCCESS) UHF Radio



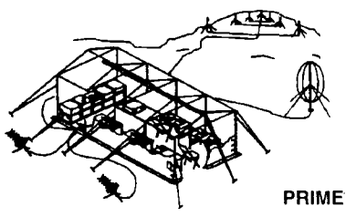
FUNCTION: Auto microprocessor UHF band radio; used w/TENCAP; simultaneous comm when stacked; 2 XMIT/6 RCV channels; SATCOM, point-to-point, TADIXS-B, direct data downlinks; comm w/abn, terrestrial & satellite systems; contains TRE processor

PRIME MOVER: Designed for ground/mobile sheltered environments

UNIT AND QTY: Demand assigned multiple access

INTEL APPLICATION: Intelligence Support

Enhanced TRACKWOLF (AN/TSQ-199)



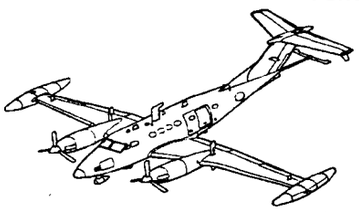
FUNCTION: Targets HF jammers/emitters; 3 netted or stand-alone stations; produces COMINT, TACREPs; spts EAC w/organic long-distance comm resources; open architecture; scaleable tier I-III; external comm via SINCGARS LPI VHF radio, DIN, DSSCS, TROJAN SPIRIT II, SSP-SIGINT, CROSSHAIR, UHF MIL SATCOM (DF Flashnet)

PRIME MOVER: NA

UNIT AND QTY: Special missions at EAC

INTEL APPLICATION: COMINT

Guardrail Common Sensor (GRCS)



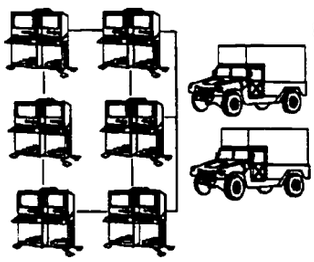
FUNCTION: Collects, identifies, classifies, locates radio signals; provides NRT reporting; gathers LOB & TDOA data; ARF relays platforms btwn IPF & cmds; incorp CHAALS; interfaces w/fixed locations & tactical users; future; expanded coll, LPI capability, embedded trng, 3-channel CTT, retrofit, and auto reporting

PRIME MOVER: Self-deployable; 4 - IPF vans; 3 - IDL trackers

UNIT AND QTY: 1 - Corps AEB

INTEL APPLICATION: ELINT/COMINT

All-Source Analysis System (ASAS)



FUNCTION: Provides auto intel, info & interface data handling for cdrs & ATCCS/ FLCS users; includes IEW sensors, preprocessors, ASAS & FLCS, ABCS HW/SW & info mgt; RWS operates outside ACE

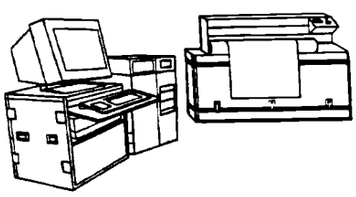
PRIME MOVER: CUCV/HMMWV 5-ton

UNIT AND QTY: 1 ACE set - EAC, Corps, DIV, Sep Bde, ACR; 1 ASAS-RWS at each Bn, Bde & required collateral locations EAC-DIV

INTEL APPLICATION: COMINT/ELINT/IMINT/ CI/HUMINT

Digital Topographic Support System Multi-Spectral Image Processor (DTSS/MSIP)

FUNCTION: Automates terrain TM; produces terrain anal prod; improves response time for IPB; collocated w/ASAS; msg traffic thru MSE; generates/updates multi-spectral imagery; contains 3-D visualization, scanning, map-sizing printer

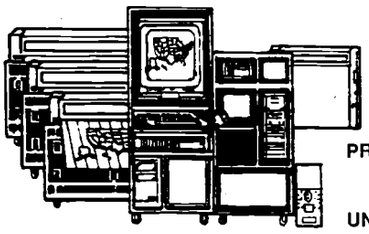


PRIME MOVER: NA

UNIT AND QTY: 1 DIV Terrain TM; 2 - EAC/Corps Terrain TM

INTEL APPLICATION: IMINT/Intelligence Support

Digital Topographic Support System Quick Response Multicolor Printer (DTSS/QRMP)



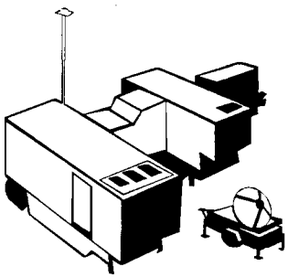
FUNCTION: Automates terrain TM; produces terrain anal prod; improves response time for IPB; collocated w/ASAS; msg traffic thru MSE; provides digital data/terrain anal from battlefield in hard/soft copy

PRIME MOVER: Tactically mobile; 2 LMS-788/gs shelters; 2 HMMWV-H

UNIT AND QTY: 1 DIV Terrain TM; 2 - EAC/Corp Terrain TM

INTEL APPLICATION: IMINT/Intelligence Support

Enhanced Tactical Radar Correlator (ETRAC)



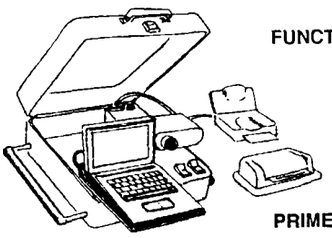
FUNCTION: Advanced mobile SAR processor; receives data from ASAR-2 via U2-R; converts radar to imagery; limited organic exploit for stand-alone opns; includes SUCCESS radio, TENCAP CSP; STU-III, DSVT

PRIME MOVER: Air deployable via C-130, C-141, C-5

UNIT AND QTY: XVIII ABN Corps and V Corps

INTEL APPLICATION: IMINT

CI/HUMINT Automation Tool Set (CHATS)



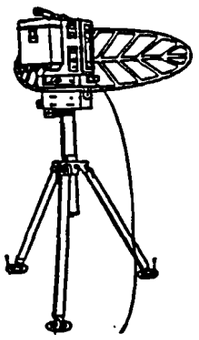
FUNCTION: Provides direct access into CI/HUMINT collateral LAN; uses INMARSAT, TROJAN SPIRIT, SINCGARS, MSE, DSN & phone lines; 2-way data comm; secure FAX; future: GPS, cellular comm, power mgt

PRIME MOVER: 2-manportable cases

UNIT AND QTY: 66th MI Group, Augsburg, GE

INTEL APPLICATION: CI/HUMINT

AN/PPS-5B



FUNCTION: Moving Target Indicators
Range:
6 km-Personnel
10 km-Vehicle

PRIME MOVER: Manpacked and vehicle

UNIT AND QUANTITY: HVY DIV: 12 systems
4/GSR Squad (3)
Survl Plt, I&S Co., MI Bn

AN/PPS-15A

FUNCTION: Moving Target Indicators
Range:
1.5 km-Personnel
3.0 km-Vehicle

PRIME MOVER: Manpacked and vehicle

UNIT AND QUANTITY: LT DIV: 12 systems
3/GSR Squad (4)
Survl Plt, I&S Co., MI Bn

ASSAULT DIV; 8 systems
3/GSR Squad (3)
Survl Plt, I&S Co., MI Bn

ABN DIV: 9 systems
3/I&S Plt (3)
MI Co., (Fwd Spt), MI Bn

APPENDIX H

MILITARY INTELLIGENCE UNITS AND CAPABILITIES

This appendix shows the structure of the MI Battalion (Heavy Division), the MI Battalion (Light Divisions, Airborne, Air Assault), and the Corps MI Brigade. The MI unit structures constitute approved MI force design.

DIVISION MI BATTALION

The MI Battalion (Heavy Division) (Figure H-1) provides dedicated IEW support to the heavy division. It responds to missions assigned by the commander and staff. (MI battalion IEW assets are shown in Appendix G.)

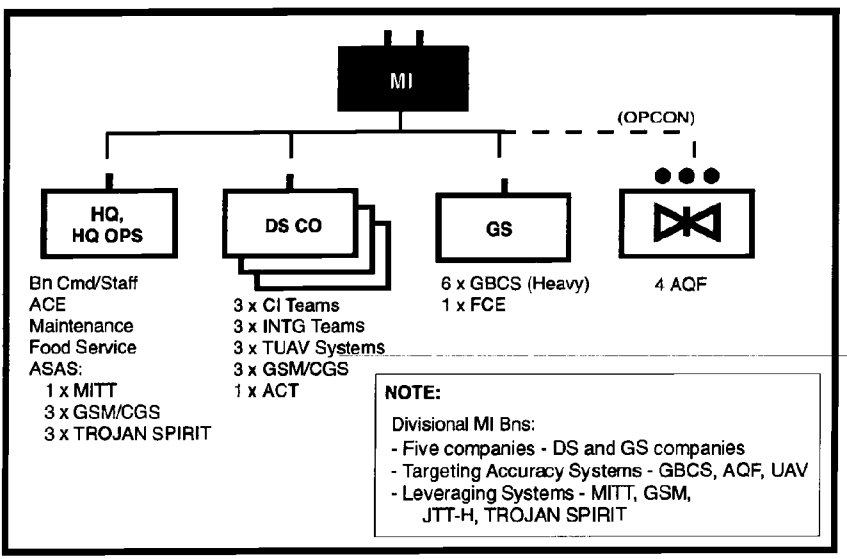


Figure H-1. MI Battalion (Heavy Division).

LIGHT, AIRBORNE, AND AIR ASSAULT DIVISION

The MI Battalion is organized as shown in Figure H-2.

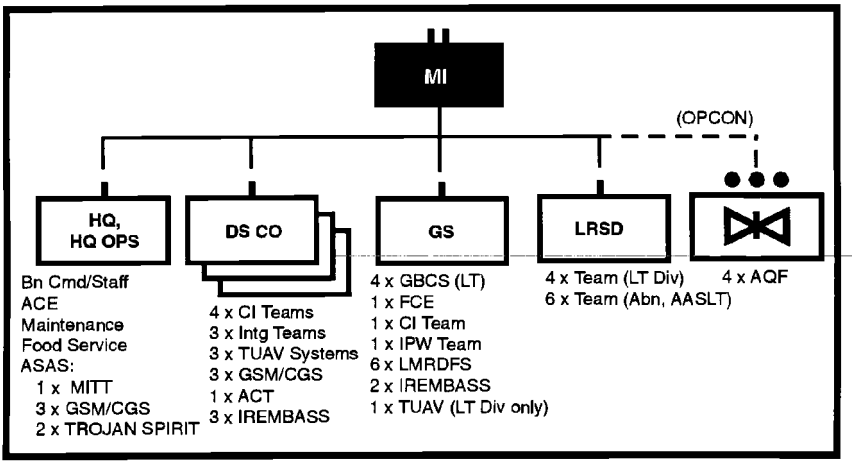


Figure H-2. MI Battalion (Light, Airborne, Air Assault Division).

CORPS MI BRIGADE:

The Corps MI Brigade (Figure H-3) provides dedicated IEW support to the Corps and its subordinate units.

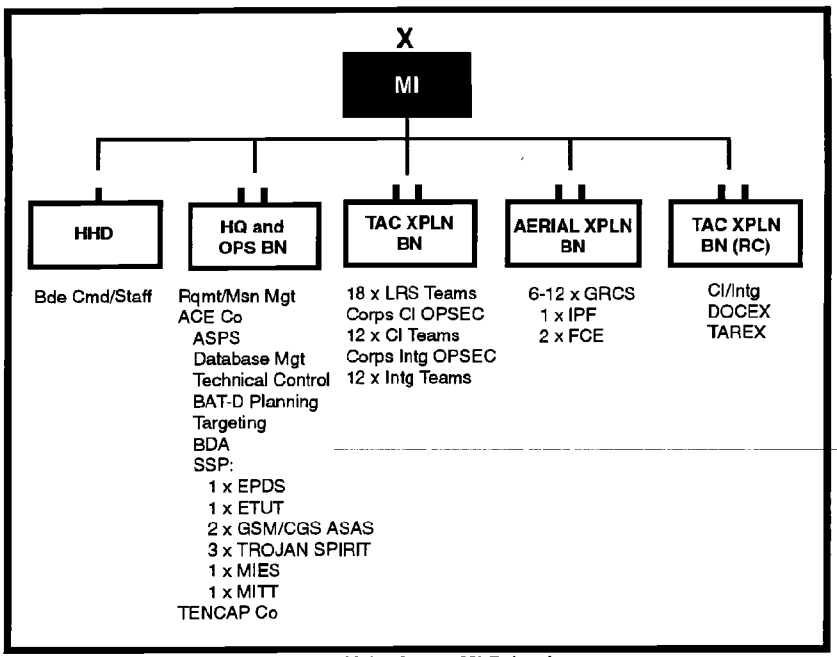


Figure H-3. Corps MI Brigade.

Figures H-4 and H-5 show the organizations of the MI Detachment, Support Company, Special Forces Group and the Special Forces Battalion, respectively.

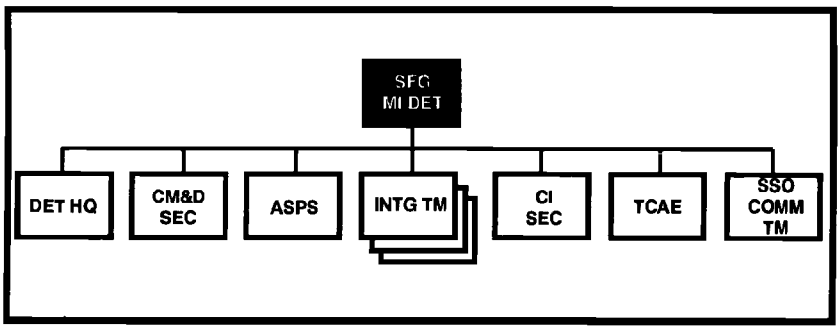


Figure H-4. Organization, MI Detachment, Spt Co, SFG.

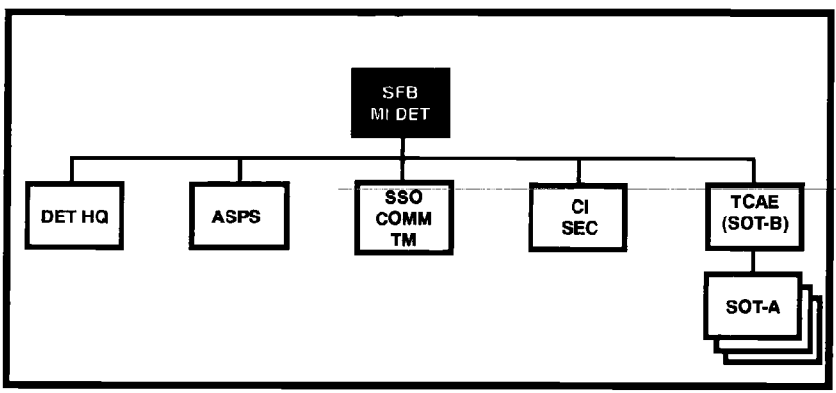


Figure H-5. Organization, MI Detachment, Spt Co, SFB.

APPENDIX I

INTELLIGENCE TRANSITION CHECKLIST

This checklist provides for transition of intelligence responsibility for an area between units. Status of all items listed must be thoroughly coordinated between the transitioning S2s to ensure an effective hand-off of responsibility.

INTELLIGENCE TRANSITION CHECKLIST

_____ CURRENT SITUATION.

_____ Threat disposition:

_____ Maneuver.
_____ Artillery.
_____ Counter-Air.
_____ Intelligence.
_____ Mobility-Countermobility-Survivability.
_____ Logistics.
_____ C^3.
_____ Deception.

_____ Threat strength:

_____ Percentage strength of units.
_____ BDA.

_____ Personnel.
_____ Equipment.
_____ Weapons.
_____ Logistics.

_____ Threat vulnerabilities.
_____ Threat capabilities.
_____ Probable COA.

_____ FRIENDLY INTELLIGENCE SITUATION.

_____ Collection plan.

_____ IMINT.
- _____ Required coverage.
- _____ Focus (CCIRs).

_____ SIGINT.
- _____ Required coverage.
- _____ Focus (EEFI/PIR).

_____ HUMINT.
- _____ NAIs.
- _____ Surveillance.
- _____ CI/IPW.
- _____ DOCEX.
- _____ Focus (RFI/PIR).

_____ Collection asset status.
- _____ Assets.
- _____ Asset schedule - previous 24 hours next 24 hours.

_____ POCs.
_____ Downlinks and COMINT.
_____ Reporting times (as of time to report and due times).
_____ COS/DEA/DOS.

_____ Lists of stay-behind elements.
- _____ Intelligence assets.
- _____ Communications architecture and frequencies.
- _____ CIA.
- _____ DIA national MIST.
- _____ JCMEC and FMIB.

_____ SIGINT.
- _____ Technical data (adds, changes, deletes).
- _____ MCSF.

_____ EPW.
- _____ Numbers, locations, Category A, SOFA.
- _____ Handover to JTF or ARFOR.
- _____ HN handover.

_____ HN Intelligence/security.
- _____ Support, assets, communications.
- _____ POCs and LNOs.

_____ KEY TERRAIN.

_____ MAP UPDATES AND CORRECTIONS.

_____ DETAINABLE, OF INTEREST, AND PROTECTABLE LISTS.

_____ INTELLIGENCE COLLECTION PLAN.

_____ COORDINATION FOR STAY-BEHIND PERSONNEL.

_____ COVER, SECURITY, OPSEC STATUS, AND PLAN.

_____ LIST OF STAY-BEHIND PRODUCTS:

_____ Intelligence map with current situation and sources.

_____ All-source intelligence support and sources.

_____ Imagery products and sources.

_____ Current weather forecast and on-hand weather, light data, and sources.

_____ Historical documents, locations, and sources.

_____ ENCLOSURES:

_____ List of threat, strengths, capabilities, COAs, weaknesses and vulnerabilities, and effects of friendly action.
_____ Threat situation overlays.
_____ Troop list of friendly collectors.
_____ Friendly collector location overlays.
_____ Intelligence communications net diagrams and POC list.
_____ Key terrain overlays.
_____ Map updates and corrections (may be overlay).
_____ Detainable, of interest, and protectable lists.
_____ Intelligence collection plan.

APPENDIX J

INTELLIGENCE REFERENCE LIST

NOTE: This list is not all inclusive. Include the series of field manuals for your particular unit; for example, FM 44-series for Air Defense. Make sure the publications clerk is aware of your requirements. Refer also to the References section in this manual.

AR 190-11	Physical Security of Arms, Ammunition and Explosive
AR 190-13	The Army Physical Security Program
AR 190-14	Carrying of Firearms and Use of Force for Law Enforcement and Security Duties
AR 190-51	Security of Unclassified Army Property
AR 525-13	The Army Combating Terrorism Program
AR 380-5	Department of the Army Information Security Program
AR 380-10	Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives
AR 380-19	Information Systems Security
AR 380-67	The Department of the Army Personnel Security Program
AR 381-1	Security Controls on Dissemination of Intelligence Information
AR 381-10	US Army Intelligence Activities
AR 381-12	Subversion and Espionage Directed Against the US Army (SAEDA)
AR 381-20	The Army Counterintelligence Program
(U) AR 381-172	Counterintelligence Force Protection Source Operations (CFSO) and Low Level Source Operations (LLSO), Secret.
AR 530-1	Operations Security (OPSEC)
FM 1-111	Aviation Brigades
FM 5-30	Engineer Intelligence
FM 5-36	Route Reconnaissance and Classification
FM 6-20	Fire Support in the AirLand Battle
FM 6-20-10	Tactics, Techniques, and Procedures for the Targeting Process
FM 6-121	Tactics, Techniques, and Procedures for Field Artillery Target Acquisition
FM 7-98	Operations in a Low-Intensity Conflict

FM 11-50	Combat Communications Within the Division (Heavy and Light)
FM 17-95	Cavalry Operations
FM 19-1	Military Police Support for the AirLand Battle
FM 19-30	Physical Security
FM 25-100	Training the Force
FM 25-101	Battle Focused Training
FM 33-1	Psychological Operations
FM 34-1	Intelligence and Electronic Warfare Operations
FM 34-2	Collection Management and Synchronization Planning
FM 34-2-1	Tactics, Techniques, and Procedures for Reconnaissance and Surveillance and Intelligence Support to Counterreconnaissance
FM 34-3	Intelligence Analysis
(U) FM 34-5	Human Intelligence and Related Counterintelligence Operations, Secret.
FM 34-7	Intelligence and Electronic Warfare Support to Low-Intensity Conflict Operations
FM 34-8	Combat Commander's Handbook on Intelligence
FM 34-10	Division Intelligence and Electronics Warfare Operations
FM 34-13	Military Intelligence (MI) Battalion, Combat Electronic Warfare Intelligence (CEWI) (Div), Leaders Handbook for Platoons and Teams
FM 34-25	Corps Intelligence and Electronic Warfare Operations
FM 34-25-1	Joint Surveillance Target Attack Radar System (JOINT STARS)
FM 34-25-3	All-Source Analysis System and the Analysis and Control Element
FM 34-36	Special Operation Forces Intelligence & EW Operations
FM 34-37	Echelons Above Corps (EAC) Intelligence & Electronic Warfare (IEW) Operations
(U) FM 34-40	Electronic Warfare Operations, Secret.
(U) FM 34-40-3	Tactical Signals Intelligence (SIGINT) Analysis Operations, Confidential.
FM 34-40-7	Communications Jamming Handbook
FM 34-40-9	Direction Finding Operations
(U) FM 34-40-12	Morse Code Intercept Operations, Confidential.
(U) FM 34-40-13	Electronic Intelligence (ELINT) Operations, Secret.
FM 34-52	Intelligence Interrogation
FM 34-54	Battlefield Technical Intelligence
FM 34-60	Counterintelligence
FM 34-80	Brigade and Battalion Intelligence and Electronic

	Warfare Operations
FM 34-81	Weather Support for Army Tactical Operations
FM 34-81-1	Battlefield Weather Effects
FM 34-82	Military Intelligence Unit Exercise Development Guide
FM 34-130	Intelligence Preparation of the Battlefield
FM 41-10	Civil Affairs Operations
FM 71-3	Armored and Mechanized Infantry Brigade
FM 71-100	Division Operations
FM 90-2	Battlefield Deception
(U) FM 90-2A	Electronic Deception, Secret.
FM 90-14	Rear Battle
FM 90-29	NEO
FM 100-5	Operations
FM 100-6	Information Operations
FM 100-19	Domestic Support Operations
FM 100-20	Military Operations in Low-Intensity Conflict
FM 100-23	Peace Operations
FM 100-25	Doctrine for Army Special Operations Forces
FM 101-5	Staff Organization and Operations
FM 101-5-1	Operational Terms and Graphics
TC 34-55	Imagery Intelligence
Joint Pub 1	Joint Warfare for the US Armed Forces
Joint Pub 1-01 series	Joint Publication System, Joint Doctrine and Joint Tactics, Techniques, and Procedures Development Program
Joint Pub 2-0 series	Joint Doctrine for Intelligence Support to Operations
Joint Pub 3-0 series	Doctrine for Joint Publications
Joint Pub 5-0 series	Doctrine for Planning Joint Operations
(U) Joint Pub 6-02	Joint Doctrine for Employment of Operational/ Tactical Command, Control, Communications, and Computer Systems, Secret.

NOTE: DOCTRINE WRITTEN PRIOR TO 1992 IS BEING REVISED. UPDATE YOUR REFERENCE LIST AS NEW DOCTRINE IS PUBLISHED.

APPENDIX K

WEATHER ELEMENTS AND SUPPORT

A working knowledge of weather elements is essential to provide your commander with a complete picture of potential adverse weather effects on the battlefield.

INTERACTION OF BATTLEFIELD ENVIRONMENT ELEMENTS

Weather conditions, terrain, BIC, illumination, and background signatures are some primary conditions found in a battlefield environment (Figure K-1).

A weather element is an atmospheric variable that is measured in a weather observation. A weather parameter is derived from one or more weather elements. Example: Density altitude is a weather parameter derived from the element's barometric pressure and temperature.

Weather conditions such as wind, precipitation, and clouds can impact or can be influenced by the other conditions of the battlefield. All of these conditions are interdependent, to a certain degree, and must be considered as a whole (Figure K-2).

WEATHER EFFECTS AND TERRAIN

Terrain features affect weather elements such as visibility, temperature, humidity, precipitation, winds, clouds. The most common example of terrain affecting weather is that on the windward side of high terrain, such as mountains, the rainfall rate will be greater than on the leeward (opposite) side.

Weather conditions have a definite effect on the terrain and can enhance or limit military operations such as trafficability, water crossing (fording), and the first-round accuracy of supporting FA fires. The responsibility for determining mobility and counter-mobility is given to the terrain team at division.

ATMOSPHERIC PRESSURE: Atmospheric pressure is the pressure exerted by the atmosphere at a given point and measured by a barometer in inches of mercury (Hg) or in millibars (Mb).

Pressure Altitude: This is indicated in an altimeter when 29.92 is set in the barometric scale window. High pressure altitude is critical to the lift capability of fixed wing aircraft.

Density Altitude: This is a place in the atmosphere corresponding to a particular value of air density. High pressure is critical to helicopter operations.

CLOUDS: The amount of sky covered by clouds is usually described in eighths: Overcast (8/8ths), broken (5 to 7/8ths), or scattered (1 to 4/8ths). Cloud conditions are described by the amount of cloud cover and the height of the base of the cloud AGL. A cloud ceiling is the height of the lowest broken or overcast layer, and is expressed in feet. A higher layer of several scattered layers of clouds is designated as a cloud ceiling when the sum of the coverage of the lower layers exceeds 4/8ths.

DEW POINT TEMPERATURE: Dew point is the temperature to which the air must be cooled for the air to become saturated and allow dew, and probably fog, to form.

HUMIDITY: This is the state of the atmosphere with respect to water vapor content. It is usually expressed as:

Relative Humidity: The ratio between the air's water content and the water content of saturated air.

Absolute Humidity: The measure of the total water content in the air. It is high in the tropical ocean areas and low in the arctic.

PRECIPITATION: Precipitation is any moisture falling from a cloud in frozen or liquid form. Rain, snow, hail, drizzle, sleet, and freezing rain are common types. The intensity of precipitation is described as light, moderate, and heavy.

Light Rain: Drops are easily seen, very little spray, and puddles form slowly, and accumulation is a trace to 0.10 in/h.

Figure K-1. Common weather elements.

Moderate Rain:	Drops are not easily seen, spray noticeable, puddles form rapidly, and accumulation rates are 0.11 to 0.30 in/h.
Heavy Rain:	Drops are not seen, rain comes in sheets with heavy spray, puddles form quickly, and the rate is more than 0.30 in/h.
Light Snow:	Visibility is equal to or greater than 5/8 miles, or 1,000 meters in falling snow; and a trace to 1 in/hr accumulates.
Moderate Snow:	Visibility is 5/16 to ½ statute miles, or 500 through 900 meters in falling snow with 1 to 3 in/hr accumulation.
Heavy Snow:	In heavy snow, visibility is cut to less than 1/4 statute miles, or 400 meters, with more than accumulation of 3 in/h.

TEMPERATURE: Temperature is the value of heat or cold recorded by a thermometer normally at 6 feet AGL at the observation site. Temperatures are normally given in both Fahrenheit and Celsius values. It is sometimes referred to as the ambient air temperature.

VISIBILITY: A measurement of the horizontal distance at the surface or aloft that the unaided human eye can discern a large object or terrain feature. Visibility is reported in meters or fractions of a mile, and is reported as a prevailing value of the visibility in all directions. Thus, a visibility report of 1,600 meters may not reveal that fog is diminishing visibility to 400 meters in the northwest if the observer has good visibility in other directions. However, such an event would typically be carried in the weather observation's remarks section.

WIND SPEED AND DIRECTION: These two measure the rate of movement of the air past a given point and the direction from which the wind is blowing. A gust is a rapid fluctuation in wind speed with a variation of 10 knots or more between peak and lull. Gust spread is the instantaneous difference between a peak and a lull and is important for helicopter operations.

Figure K-1. Common weather elements (continued).

WEATHER ELEMENTS	THRESHOLD VALUES	IMPACTED SYSTEMS
VISIBILITY	1.0 km 3.0 km	•DRAGON, Machine guns. •Main gun, TOW, CAS, thermal viewers.
CLOUDS	500 ft 1,000 ft 1,500 ft 5,000 ft	•NOE operations, airborne, helicopter TA. •CAS. •COPPERHEAD engagements. •Visual reconnaissance, ADA TA.
SURFACE WIND	6 kn 13 kn 18 kn 30 kn	•Chemical. •Airborne-round parachute. •Military free fall-ram air parachutes, artillery smoke loses its effectiveness, artillery fire accuracy. •Helicopter maneuver.
TEMPERATURE	>32^{C}C < 0^{C}C	•Helicopter lift capabilities. •NVG (PVS-5).
WINDCHILL	<10^{C}C	Personnel survival.
PRECIPITATION	Moderate Freezing	•Ground maneuver, chemical, laser systems, GSR. •Ground maneuver.

Figure K-2. IPB weather overlay criteria.

BATTLEFIELD-INDUCED CONTAMINANTS

During combat operations, visibility can become severely reduced by BIC. These contaminants are either induced directly by combatants or occur as by-products from battlefield operations.

Two significant sources of battlefield contaminants are dust produced by HE artillery or mortar rounds and deliberately employed smoke. HE rounds used in a pre-attack barrage not only may kill enemy forces but also may restrict the visibility of your own troops by dust caused by the HE if you do not consider the direction of the wind. Smoke produced by smoke generators, vehicle exhaust emission

systems, smoke pots, indirect fire, and smoke rounds also produce battlefield contaminants.

Wind speed and direction are critical to maintaining an effective smoke screen. Rain can remove BIC quickly. Weather inversions over valley areas can sustain airborne contaminants for long periods.

Other sources of BIC that will lower visibility in the AO are clouds of dust from vehicle traffic or smoke from fires. These types of contaminants not only blind you but also may help your adversary in detecting troop movements and pinpointing your location.

A unique BIC affecting visibility occurs in conditions when temperatures are in the range of -30EC or -22EF or colder. When a source of moisture or water vapor is released into the cold air by internal combustion engines, artillery fires, or launched self-propelled munitions, visibility can be reduced to zero when the moisture freezes instantly and changes into ice fog.

Ice fog may restrict visibility across a whole valley and can linger for hours. Ice fog crystals permit ground objects to be seen from above while severely restricting visibility on the ground—an advantage for aerial reconnaissance.

On airfields an ice fog created by fixed-wing aircraft may cover an entire runway. Visibility can be reduced so that other aircraft cannot take off or land if the wind is calm. The ice fog also draws attention to the airfield location.

Launching missiles such as the TOW in very cold air can create an ice fog. As the TOW moves to the target, the exhaust blast exits into the air where it condenses and creates the ice fog. If the wind is calm, this fog follows the trajectory of the missile and reduces launch point visibility to such an extent that the operator loses sight of the target. Also, the launch point can be identified by threat forces from the condensation trail of the missile.

ILLUMINATION

Natural light is critical in planning operations where NVD are used or in operations timed to use only available light. Natural light values vary as a function of the position of the sun, moon, stars, and clouds. Light data are available from your SWO for any time period and place. These data are particularly important for determining first and last light, moonrise, and moonset, and are most effective for planning use of NVD.

Variables such as altitude, cloud cover, terrain-produced shadows, visibility, and direction of vehicle or aircraft movement in relation to the sun or the moon can also affect light level availability.

Artificial light is intended to increase visibility but, under certain weather conditions, this does not always occur. Example: Low cloud ceilings will limit the area covered and effective time of flares. Rain, snow, or fog can reduce flare effectiveness. However, under the right conditions, cloud cover can enhance the effects of artificial light due to cloud base reflection. Snow- or sand-covered terrain also reflect both natural and artificial light.

BACKGROUND SIGNATURES

Temperature, wind, and precipitation have a major influence on your ability to pick out a target from the background in the infrared spectrum. They also affect seismic (sound and acoustic) signatures. Detection of objects in the infrared spectrum depends on a temperature contrast between the object and its surrounding environment. This difference is known as the background signature.

Snow, rain, and wind influence the background signature because they can change the surface temperature of objects. These elements lower object temperatures and thus reduce the differential between a target and its background.

A heavy layer of snow produces a washout during any part of the day since it causes both the object and the background to exhibit the same temperature.

Precipitation also degrades seismic sensors through the introduction of background noise (rain), while a snow-covered surface will dampen sound and the movement of troops.

SEVERE OR HAZARDOUS WEATHER

In addition to a continuous need for forecast updates, you need non-forecasted or unanticipated severe or hazardous weather warnings. WETMs normally issue severe weather warnings and advisories. Check for the values at which each weather element becomes known as severe. You will be concerned with conditions such as—

- Tornadoes.
- Thunderstorms producing winds in excess of 45 knots and hail greater than 3/4 of an inch.
- Hurricanes and typhoons.
- Precipitation (rain or snow) when X inches fall in Y hours.
- Surface winds in excess of X knots.
- Maximum and minimum temperatures; when a forecast value misses the actual temperature by X degrees.

You want to know that an earlier forecast for light snow was amended to a forecast of a 16-inch accumulation within the next 12 hours. We cannot over emphasize that you need to work with your next higher HQ S2/G2 and the SWO so that your needs are realistically stated and can be supported. All of your weather support needs should be reviewed every 6 months in garrison and as required in the field.

LIGHT DATA

Another weather-related element that your commander needs is light data. NVD and NVG have made many night operations feasible. Your SWO provides official times for sunrise and sunset, BMCT and EECT, BMNT and EENT, length of absolute darkness, moonrise, moonset, lunar phase in percent, and time periods for using NVD and NVG. Light data to support NVD is needed because there are times when there is not enough moon or starlight to use them.

Civil twilight is sufficient for conduct of combat operations while nautical twilight permits most ground movements without difficulty. Nautical twilight allows a general visibility of up to 400 meters (1,320 ft) and lets you distinguish silhouettes from the background.

The actual duration of light varies with latitude and time of year. For example, in the vicinity of 35 to 40 degrees north latitude, civil twilight generally occurs 30 to 45 minutes before sunrise and after sunset. In the tropics, twilight is shorter.

Once light requirements are determined, relay them to your next higher S2 and SWO. This information is important for your commander because he needs to know not only when he can begin friendly military operations (day or night) but also when threat operations could begin.

OTHER CONSIDERATIONS

Although HF radio wave propagation forecasts are not normally available to the SWO, he can make arrangements before he deploys to receive these forecasts. When available, they should be given to every signal and intelligence organization. The SIGO should know that when HF is not effective, it may be because of solar activity rather than enemy jamming.

The USAF Global Weather Central can routinely provide solar forecast products to the SWO even in the field. Other data, such as tidal information and sea state conditions, can be obtained from the SWO but are normally provided only to specific Army units upon request.

RECEIPT OF FORECASTS

Every tactical echelon should receive the weather forecast prepared and briefed to the commander at the next higher echelon. With no SWO at a maneuver brigade, you receive both the forecast briefed at division covering the division AO and the forecast made by the division SWO specifically for your brigade. Each forecast message received should be worked by you to discover the direct weather impacts on your unit.

A commander wants the weather forecast. He also needs the effects and impacts of the forecasted weather interpreted for his specific operations, systems, and personnel. Schedule your forecasts so they arrive in time for you to prepare your commander's briefing.

HOW G2 OR S2 RECEIVE WEATHER SUPPORT

It is your responsibility to provide weather and weather effects information to your commander and supported or subordinate units. Methods may vary among units and echelons. At higher echelons, the SWO has primary responsibility for providing weather support. There, the G2 simply contacts the SWO, states requirements, and receives the needed weather support.

If you have no SWO, you must pass the request up the chain of command to a level where one is assigned. Once your requirements have been validated, weather support products flow back over the same path. In addition to weather forecast products, the SWO can provide specialized weather effects products. You must provide the threshold values used in developing these products.

You alert your commander and staff about the adverse impact of the forecasted weather. You prepare two simple charts to use during your commander's stand-up briefing. You can post these charts in the CP for reference.

Update the charts when a new forecast is issued by the WETM. Methods used in briefing your commander during the morning and evening briefings may vary greatly among commands. The formats below are a guide and should be modified to suit your situation.

The first chart (Figure K-3) illustrates how the weather elements and parameters contained in the forecast might be displayed on the board. Blown up to poster size and covered with acetate, this chart can be updated easily.

WEATHER FORECAST
VALID FOR 121200Z to 131200Z

LOCATION: PUNGSAN

24-HOUR FORECAST:

SKIES:	CLEAR MORNING AND NIGHT, PARTLY CLOUDY IN THE AFTERNOON, BASES 3,000 FEET.
VISIBILITY:	UNLIMITED, OCCASIONALLY 1 TO 2 MILES IN BLOWING SNOW DURING AFTERNOON.
WINDS:	NORTH TO NORTHWEST, 10 TO 15 KNOTS, OCCASIONAL GUSTS TO 25 KNOTS IN AFTERNOON.
TEMPERATURES:	MAX: 10EF MIN: -20EF

72-HOUR OUTLOOK:

CLOUDY SKIES, SNOW FLURRIES DURING AFTERNOON HOURS LOWERING VISIBILITY TO 2 TO 4 MILES.

TEMPERATURES: MAX: 20EF MIN: -5EF

LIGHT DATA:

BMNT: 1247Z MOONRISE: 1924Z
BMCT: 2221Z MOONSET: 0819Z
SUNRISE: 2251Z
SUNSET: 0820Z NVG USE:
EECT: 0851Z

Figure K-3. Example of a weather forecast chart.

Figure K-4 shows color codes as one way to display potential weather impacts on operations, systems, and personnel in your unit. Another way would be to write the words "moderate" and "severe" in those blocks affected. Do not list all the equipment or systems, but have the list available to answer questions posed by the commander or staff. Stress those critical systems during the verbal portion of your briefing.

If the weather conditions change significantly during the period covered by the SWO's forecast, then an updated impact chart will have to be prepared. Because a brigade or battalion's AI is small, the SWO's forecast is likely to be uniform across the AI.

WEATHER IMPACT CHART
PERIOD 121200Z to 131200Z

IMPACTED ITEMS	CLOUDS	PRECIPI-TATION	WIND	VISIBILITY	TEMPER-ATURE
NBC DEFENSE	GREEN	GREEN	GREEN	GREEN	RED
NIGHT VISION DEVICES	GREEN	GREEN	GREEN	AMBER EXCEPT 07 /0 05Z	AMBER
CSS	GREEN	AMBER	AMBER	AMBER	AMBER
TOW/DRAGON	GREEN	GREEN	AMBER	GREEN	RED
M-1/M-2	GREEN	GREEN	GREEN	GREEN	AMBER
SMOKE/ CHEMICAL	GREEN	GREEN	AMBER	GREEN	GREEN
GROUND RADAR	GREEN	GREEN	AMBER	GREEN	GREEN
PERSONNEL	GREEN	GREEN	RED	GREEN	RED
THREAT	GREEN	GREEN	GREEN	AMBER	GREEN

GREEN No impact
AMBER Moderate impact (Normal effectiveness reduced 25 to 75%)
RED Severe impact (Normal effectiveness reduced to 0 to 25%)

Figure K-4. Example of a weather impacts display chart.

CRITICAL WEATHER FACTORS

Figure K-5 shows major critical weather factors that can enhance or degrade combat operations, systems, and personnel.

LOW VISIBILITY:	Low visibility (less than 3 km). • Can be beneficial to threat and friendly forces. • Conceals the center of gravity and maneuver of offensive forces. • Increases possibility of achieving surprise. • Disadvantages. –Hinders $C^{2.}$ –Reduces effectiveness of R&S and TA, especially during the defense.
SURFACE WINDS:	• Strong winds can reduce effectiveness of downwind forces by blowing dust, smoke, sand, rain, or snow on them. • Upwind force generally has better visibility and can advance faster and easier. • Strong winds limit airborne and aviation (primarily helicopters) operations. • Winds in excess of 35 knots can— –Cause personal injury. –Damage materiel and structures. –Create false radar returns. –Reduce visibility because of blowing sand, dust, and other battlefield debris.
PRECIPITATION:	• Affects trafficability, visibility, personnel effectiveness, and a wide variety of tracked and wheeled military equipment. • Heavy rains can make some unsurfaced, low-lying, and off-road areas impassable.

Figure K-5. Critical weather factors.

	• Both rain and snow can drastically reduce personnel effectiveness by limiting visibility, causing discomfort, increasing fatigue, and creating other physical and psychological problems.
CLOUD COVER:	• The type and amount of cloud cover and the altitude of cloud bases and tops influence aviation operations. • CAS employing fixed-wing aircraft would like a ceiling of at least 2,500 feet (762 m), but can be employed with ceilings as low as 500 feet. • Threat CAS rotary-wing aircraft and aerial resupply missions require a minimum ceiling of 300 feet (100 m). • Affects ground operations by reducing illumination and visibility or by enhancing effects of artificial light.
TEMPERATURE AND HUMIDITY:	• Have a direct impact on personnel and vehicle performance. • Excessively high temperatures cause heat-related injuries to personnel and vehicle engine wear that leads to equipment failure. • Very low temperatures increase cold weather injuries, cause damage to vehicle cooling systems and engines, decrease the effectiveness of vehicle lubrication, and create excessive logistics requirements.

Figure K-5. Critical weather factors (continued).

WEATHER EFFECTS ON THREAT SYSTEMS

MILITARY ASPECTS OF WEATHER:

US Forces must be prepared to fight in a variety of climatic conditions on short notice. Key to accomplishing our missions under any circumstances is

understanding how weather affects both friendly and threat forces and their operations, systems, and personnel.

Current weather conditions and weather forecasts for the AO and AI are analyzed to determine the effects on friendly and enemy operations. This is significant when threat forces have the capability to employ NBC weapon systems.

THREAT EQUIPMENT:

Some of the major arms merchants today are the former Soviet Union, Sweden, Brazil, Britain, Germany, France, Italy, and the United States. However, the major arms purchasers continue to be the underdeveloped or Third-World countries in the Middle East, Latin America, and Asia.

The types of threat equipment we may encounter on future battlefields will vary from artillery and mortars produced during World War II to the Austrian-produced GHN-45, a 155-mm towed gun with a range of 39,600 meters (using ERFB-BB technology). Almost all the Third-World countries have bought or made their own versions of Soviet-produced tanks, APCs, artillery, AAA, and assorted SAM and SSM systems. Tables K-1, K-2, and K-3 list the weather effects from cloud ceilings, reduced visibility, and precipitation, respectively.

Table K-1. Weather effects from cloud ceilings.

WEATHER VALUE (FEET)	SEVERE DEGRADATION		MODERATE DEGRADATION	
	SYSTEM/ EVENT	REMARKS	SYSTEM/ EVENT	REMARKS
LT 1,000			SA-9 SAM SA-14 SAM	
LT 2,500			ZU-23 ZSU-23-4 SA-13 (Contrast mode) SA-16 SA-19	

Table K-2. Weather effects from reduced visibility.

WEATHER VALUE (METERS)	SEVERE DEGRADATION		MODERATE DEGRADATION	
	SYSTEM/ EVENT	REMARKS	SYSTEM/ EVENT	REMARKS
LT 200			RPG-18 (RL) AKM/AKMS (7.62-mm) TKN-1T infrared periscope	ATW Rifle E-O device
LT 500	SA-14 GREMLIN SAM SA-13 SAM SA-16 SAM SA-19 (FSU) SAM		OU-3GK White infrared search light RPG-7 (GL) PT-76 (5.45-mm) AK-74	E-O device ATW AG/LT Rifle
LT 600			ERYX	
LT 750	SA-9 GASKIN SAM			
LT 800	AT-2 SWATTER AT-3 SAGGER AT-6 SPIRAL	ATGM ATGM ATGM	ASU-85 BMD (73-mm) BMP (73-mm) Sniper rifle, SVD RPK-74, squad AGS-17, GL RPG-16, GL	AG/LT LAV LAV Rifle MG

Table K-2. Weather effects from reduced visibility (continued).

WEATHER VALUE (FEET)	SEVERE DEGRADATION		MODERATE DEGRADATION	
	SYSTEM/ EVENT	REMARKS	SYSTEM/ EVENT	REMARKS
LT 1,000	All Types	ATGM	SPG-9 (73 mm recoilless rifle) SD-44 (85-mm) 14.5-mm KPU hvy MG 7.62-mm PKT MG DShK NSV/NSVT PK Series MT-LB 7.62-mm coaxial machine gun for all tanks	ATW ATW AA AA MG MG LAV MT
LT 1,500			7.62-mm 15.5-mm heavy BTR-50,-60,-70 (14.5-mm) KPVT ACRV M1974 DShK NSV/NSVT T-54, T-55, T-62 (main gun)	MG MG AA/LAV AA LAV MG MG MT
LT 2,000			T-12, MT-12 (100-mm) KPVT BRDM-2 (14.5-mm) T-80, T-72, T-64 (main gun) MATHOGO MILAN 2 RBS-56 SPIGOT	ATW MG LAV MT

Table K-2. Weather effects from reduced visibility (continued).

WEATHER VALUE (METERS)	SEVERE DEGRADATION		MODERATE DEGRADATION	
	SYSTEM/ EVENT	REMARKS	SYSTEM/ EVENT	REMARKS
LT 2,500			SA-7 GRAIL ZU-23 ZSU-23-4	FSU SAM AA AA
LT 3,000			RED ARROW 73 RED ARROW 8 SUSONGP'O AT-3 SAGGER	
LT 4,000			SA-9 GASKIN HOT 2 SWINGFIRE AT-2 SWATTER AT-5 SPANDREL AT-8 SONGSTER AT-10 STABBER SA-13 (contrast mode)	 FSU SAM FSU SAM
LT 4,500			MAPATS	
LT 5,000			NIMROD AT-6 SPIRAL AT-11 SNIPER SWIFT (SF)	ATGM
LT 6,000			120-mm, M-1943 S-60 (57-mm)	MO AA
LT 8,000			160-mm, M-160	MO

Table K-3. Weather effects from precipitation.

WEATHER CONDITION	SEVERE DEGRADATION		MODERATE DEGRADATION	
	SYSTEM/EVENT	REMARKS	SYSTEM/ EVENT	REMARKS
Light rain			LOW BLOW (fire control) STRAIGHT FLUSH (12gHz) (tracking) THIN SKIN (height finder)	SAM radar SAM radar SAM radar
Moderate rain			STRAIGHT FLUSH (acquisition)	SAM radar
Heavy rain			LOW BLOW (fire control) THIN SKIN (height finder)	SAM radar SAM radar
	NOTE: The list of AD radars on this page should be considered as a sample of the various other types of threat radars associated with EW operations and tactical and strategic SAM systems. Not listed are a large variety of threat combat equipment (wheeled and tracked) affected by moderate or heavy rain and snow.			

WEATHER AND ENVIRONMENTAL ELEMENTS AND PARAMETERS IMPACTING ARMY SYSTEMS AND OPERATIONS:

Table K-4 is compiled from a study conducted by the US Army Intelligence School as part of the IEWMAA. Each TRADOC branch was asked to survey the impact of weather and environmental elements on their operations, systems, and personnel and rate them as either **essential (E)** or **desired (D)**. Also included are other Army agencies' requirements.

- **E**—Some positive action had to be taken by the user based on severe current or forecasted weather conditions.

- **D**—Some impact, but the degree of impact is uncertain or not mission-threatening.

For each element or parameter listed, at least one responder identified it as essential for one or more of their operations, systems, or personnel.

Some data elements and parameters are known to have an impact, but exact critical thresholds have not been determined. Others cannot be measured or sensed with present technology. But identifying these data elements or parameters now allows for further research in how to collect the raw data (where applicable), determine the frequency of collection, establish data accuracy, and learn other supporting information.

As users and planners continue to learn more about weather and environmental impacts, the misconception that there is a hypothetical Army "all-weather" system or operation fades.

Table K-5 shows windchill factors.

Table K-4. Weather and environmental data elements impacting Army systems and operations.

WEATHER AND ENVIRONMENTAL DATA ELEMENTS IMPACTING ARMY SYSTEMS/OPERATIONS

A = AIR DEFENSE
B = ADJUTANT GENERAL
C = ARMOR
D = AVIATION
E = CHAPLAIN
F = DEFENSE AMMUNITION CENTER
G = ENGINEER
H = FIELD ARTILLERY
I = FINANCE
J = HEALTH SERVICES
K = INTELLIGENCE
L = INFANTRY
M = JUDGE ADVOCATE
N = MILITARY POLICE
O = CHEMICAL
P = ORDNANCE
Q = ORDNANCE M&M
R = PUBLIC AFFAIRS
S = QUARTERMASTER
T = SIGNAL
U = SPECIAL FORCES
V = SOLDIER SUPPORT
W = TRANSPORTATION
X = JOINT READINESS TRNG CENTER

REQUIREMENT DESIGNATORS: E = ESSENTIAL SUPPORT NEEDS D = DESIRABLE SUPPORT NEEDS

SPECIAL GROUP CATEGORIES: (GS) = GROUND STATE (SS) = SEA STATE (SW) = SEVERE WEATHER CRITERIA

DATA ELEMENT	CATEGORY	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1. ALTIMETER SETTING					E						E	E										E			
2. ATMOSPHERIC CONTAMINANTS				E	D	D	E	D		E	E								D			D			
3. ATMOSPHERIC DENSITY								E			E											E			
4. ATMOS. TRANSMISSION COEFFICIENT								E																	
5. BAROMETRIC PRESSURE		D		E	E				E		E	E										E			E
6. CLOUD COVER AMOUNT		D		E	E		E	E	E		E	E	E		D	E			D			D	E	E	E
7. CLOUD BASE HEIGHT		E			E		E	E	E		E	E	E	D		E						E		E	E
8. CLOUD TOP HEIGHT					E						E	E										D			
9. DAMAGING WINDS	[SW]	E	E	E	E	E	D	E	E	E	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E
10. DENSITY ALTITUOE					E						E	E										E			E
11. EXTINCTION COEFFICIENT									E			E										D			
12. EXTREME HEAT/COLO	[SW]	E	E	E	E	E	E	E	E	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E	E
13. FLOODING, RIVER STAGE	[GS]	E	E	E	E	E		E	D	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E	E
14. FREEZE/THAW DEPTH	[GS]	D		E	E			E	D		E	E	E		E	D	E	E		E	E	D			E
15. FREEZING PRECIPITATION	[SW]	E	E	E	E	E		E	E	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E	E
16. HEAVY RAIN/SNOW	[SW]	E	E	E	E	E	D	E	E	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E	E
17. HUMIDITY, ABSOLUTE		D			E			E			E	E				E						E			E
18. HUMIDITY, ABSOLUTE, PROFILE		D			E			E			E	E				E						E			E
19. HUMIDITY, RELATIVE							E	E	D		E	E				E			E			D	E	E	E
20. HUMIDITY, RELATIVE, PROFILE									E													D			
21. HURRICANES/TYPHOONS	[SW]	E	E	E	E	E		E	E	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E	E
22. ICE/SNOW DEPTH/COVER	[GS]	D		E	E			E	D		E	E	E		E	D	D	E		E	E	D			E
23. ICING, FLIGHT	[SW]				E						E	E	E									E			E
24. ILLUMINATION		E		E	E			E	E		E	E	E		E		D			D		E	E	E	E
25. IR TARGET/BACKGROUND CONTRAST				E	E				D		E	D										E			E
26. IR THERMAL CONTRAST X-OVER TIME				E	E				D		E	E										E			E
27. IONOSPHERIC DISTURBANCES					D						D	E									E	E			
28. LIGHT DATA		E		E	E		D	E	D		E	E	E		D	D				D	D	E		D	D
29. LIGHTNING/THUNOERSTORMS	[SW]				D		E	E	E		D	E								E		E			E
30. LITTORAL CURRENT	[SS]				D		D	E			D	D	E									E			
31. PRECIPITATION, ACCUMULATION			D	E	E	D	D	E	D	D	E	E	E		E	D	E		D	E	E	E	E	E	D

Table K-4. Weather and environmental data elements impacting Army systems and operations (continued).

DATA ELEMENT	CATEGORY	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
32. PRECIPITATION, RATE		E	D		E	D		E	E	D	E	E	E	D	E	E	D		D	E	E	E	E	E	E
33. PRECIPITATION, HAIL SIZE		E			E			E	D		E	E			E		E			E		D			
34. PRECIPITATION, TYPE		E	D	E	E	D		E	E	D	E	E	E	D	E	E	D		D	E	E	E	E	E	E
35. PRESSURE ALTITUDE				E							E	E	E								E			E	
36. REFRACTIVE INDEX		E		E	E				D		E	E			D										
37. RESTRICTION TO VISIBILITY				E				E	D		D	E			E	E				E	E	E			E
38. SEEABILITY (MILLIMETER WAVE, INFRARED, ULTRAVIOLET)		E		E	E			E	E		E	E	E		E	D					E		E	D
39. SEVERE WEATHER CONDITIONS	[SW]	E	E	E	E	E		E	E	E	E	E	E	E	E	E	D	E	E	E	E	E	E	E	E
40. SNOW STATE CONDITION	[GS]	D		E	E			E	E		E	E	E		E	D	D	E		E	E	D			E
41. SNOW DRIFT DEPTH	[GS]	D			D			E	D		D	E	E		E		E			D	E	E			E
42. SOIL/GROUND MOISTURE	[GS]	D		E	E		D	E	D		E	E	E		E	D	D	E		D	E	D			E
43. SOIL/GROUND TEMPERATURE	[GS]	D		E	E		D	E	D		E	E	E		E		E		D	D		E	E	E	E
44. SOLAR RADIATION							E				D	D										E			
45. STABILITY INDEX							E					E				E									E
46. STANDING WATER/POOLING	[GS]	D		E	E	D		E	D		E	E	E		E	D	D	E	D	E	E	D			E
47. STATIC ELECTRICITY POTENTIAL					E						E	E													
48. SURF HEIGHT	[SS]				D			E			D	D	E									E		E	
49. SWELL DIRECTION/HEIGHT	[SS]				D						D	D	E									E		E	
50. TEMPERATURE, AIR, SURFACE		E	E	E	E	E	E	E	E	E	E	E	E		E	E	D	E		D	E	E	E	E	E
51. TEMPERATURE, AIR, PROFILE					E		E		E		E	E										D			
52. TEMPERATURE, AIR, UPPER AIR					E				E		E	E										D			E
53. TEMPERATURE, DEWPOINT				E	E				D		E	E										E			E
54. TEMPERATURE, DEWPOINT, PROFILE					E				E		E	E										D			
55. TEMPERATURE, WINDCHILL FACTOR			D		D	D		E	D	D	E	E	E	D	E		E		D	E		E	E	E	
56. TEMPERATURE, INVERSION LEVEL(S)					E		E		E		E	E				E						D			E
57. TEMPERATURE, SEA SURFACE	[SS]				D			E			D	D	E									E		E	
58. TEMPERATURE, WATER, INLAND	[GS]				D			E			D	E	E									E		E	
59. TEMPERATURE, WBGT					D			E	D		E	E			E	E	E			E		E			E
60. TORNADO	[SW]	E	E	E	E	E		E	E	E	E	E		E	E	E	D	E	E	E	E	E	E	E	E	E
61. TURBULENCE, FLIGHT					E						E	E										E			
62. TURBULENCE, OPTICAL				E	E			E	E		E	D										E			
63. VISIBILITY, VISIBLE SPECTRUM, ALOFT					E				E														E		E
64. VISIBILITY, VISIBLE SPECTRUM, SFC		E			E			E	E		E	E	E		E	E	D			E		E	E		E
65. WAVE PERIODICITY	[SS]				D						D	D	E									E		E	
66. WAVE DIRECTION/HEIGHT	[SS]				D						D	D	E									E		E	
67. WIND, PROFILE					E				E		E	E										E			
68. WIND, PROFILE, TARGET, AGL - 3KM					E				E							E									
69. WIND, SHEAR					E						E	E										E			E
70. WIND, SURFACE, SPEED/DIRECTION		E		E	E		E	E	E		E	E	E		E	E	D	E	D	D	E	E	E	D	E
71. WIND, SURFACE, GUST SPEED				E			D	E	E		E	E	E		D						E	E			E
72. WIND, SURFACE, GUST SPREAD					E				E		E	E										E			E
73. WIND, UPPER AIR, SPEED/DIRECTION		E			E				E		E	E				E						E			E

Table K-5. Windchill chart.

WIND SPEED (KNOTS)	WIND SPEED (MPH)	LOCAL TEMPERATURE (EF)										
		32	23	14	5	-4	-13	-22	-31	-40	-49	-58
		EQUIVALENT TEMPERATURE (EF)										
	CALM	32	23	14	5	-4	-13	-22	-31	-40	-49	-58
4	5	29	20	10	1	-9	-18	-28	-37	-47	-56	-65
9	10	18	7	-4	-15	-26	-37	-48	-59	-70	-81	-91
13	15	13	-1	-13	-25	-37	-49	-61	-73	-85	-97	-109
17	20	7	-6	-19	-32	-44	-57	-70	-83	-96	-109	-121
21	25	3	-10	-24	-37	-50	-64	-77	-90	-104	-117	-127
26	30	1	-13	-27	-41	-54	-68	-82	-97	-109	-123	-137
30	35	-1	-15	-29	-43	-57	-71	-85	-99	-113	-127	-142
35	40	-3	-17	-31	-45	-59	-74	-87	-102	-116	-131	-145
39	45	-3	-17	-31	-45	-59	-74	-87	-102	-116	-131	-145
43	50	-4	-18	-33	-47	-62	-76	-91	-105	-120	-134	-148
		LITTLE DANGER FOR PROPERLY CLOTHED PERSONS		**CONSIDERABLE DANGER**			**VERY GREAT DANGER**					
DANGER FROM FREEZING OF EXPOSED FLESH												

HOT WEATHER ENVIRONMENT:

In hot weather, important factors are temperature and relative humidity. Primary concerns are physical exhaustion and dehydration. You must consider both because a common work task will take longer and additional water may have to be transported during hot weather. The following are specific concerns:

Water Adequacy. Water supplies and the enforcement of its intake before, during, and after physical activity is critical for survival.

Workload Correlation. Adapt workload or training activities to environmental heat stress conditions.

Rest Periods. Provide adequate break time for physically active personnel in a hot environment.

Chilled Drinking Water. Soldiers will often reject warm drinking water even when they are significantly dehydrated.

Physical Activity. Soldiers' introduction to physical exertion in a hot climate upon arriving from a temperate climate should be as gradual as circumstances allow. They will need 1 to 2 weeks' time to physiologically adjust to the new climate. Lighten physical activity during this period to ensure optimum performance.

Salt. Sodium intake must be maintained in hot weather. Two good meals a day normally provide enough salt for most soldiers.

Humidity. A low WBGT index (e.g., in the morning) may not be a totally safe indicator if the humidity is high. High humidity retards cooling by evaporation of sweat and decreases the urge to drink sufficient water.

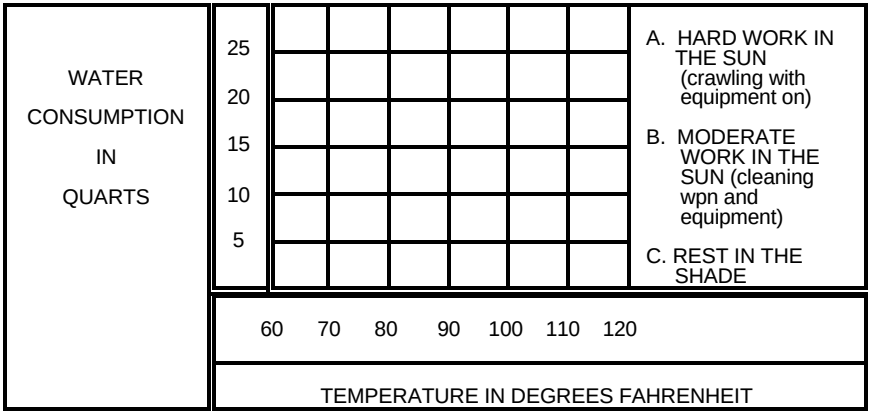
Water Spray. A water mist will cool a person. But it should never be substituted for adequate consumption of water before, during, and after strenuous activities in the heat.

The SWO can provide temperature measurement, forecast, and relative humidity forecasts from the following tables. If you need air temperature values measured at your particular location, use the thermometer included in the FALOP BWK.

HOT WEATHER WATER REQUIREMENTS:

Table K-6 shows the water needs for soldiers at 3 activity levels over an 8-hour work period. To determine soldiers' average water needs, you have to know the air temperature and decide the level of activity the troops will be doing. Example: If a soldier is doing 8 hours of hard work in the sun (curve C) when the average temperature for the day is 100EF, his water requirements for the day will be around 15 quarts. This amount of water can be converted into extra weight the soldier must carry. One quart is equal to 2 pounds, so the 15 quarts of water would weigh 30 pounds.

Table K-6. Daily water consumption requirement s for three levels of activity.



HOT WEATHER WORK TIME LIMITS:

Table K-7 shows the time limits during which work can be performed safely in hot weather. In computing the time limits, consider both air temperature and relative humidity. The values are based on a sitting soldier in BDUs doing light work. Do not consider these tables as absolute limits—especially since light, moderate, or heavy work are difficult to quantify. Table K-8 indicates work time in hot weather based on the WBGT index. Table K-9 shows conversion factors.

Table K-7. Work time in hot weather operations.

TEMPERATURE		RELATIVE HUMIDITY (%)					
(EC)	(EF)	10	30	50	70	90	100
60	140	1 HR	.25 HR				
54	130	2 HR	.5 HR	.25 HR	NO WORK RECOMMENDED		
49	120	4 HR	2 HR	.5 HR	.25 HR		
43	110	12 HR	4 HR	2 HR	.5 HR	.25 HR	
38	100	NO LIMIT	12 HR	4 HR	2 HR	1 HR	.5 HR
32	90	WITH PRECAUTIONS			12 HR	6 HR	4 HR

Table K-8. WBGT index (light work).

HEAT CONDITION/ CATEGORY *	WBGT(^{o}F)	WATER INTAKE QUARTS/HOUR	WORK/REST CYCLE (MINUTES)
1	78.0 to 81.9	AT LEAST ½	CONTINUOUS
2	82.0 to 84.9	AT LEAST 1.2	50/10
3	85.0 to 87.9	AT LEAST 1	45/15
4	88.0 to 89.9	AT LEAST 1-½	30/30
5 **	90.0 and ABOVE	MORE THAN 2	20/40

* MOPP gear or body armor adds at least 10 ^{o}F to the WBGT index.
** Suspend PT and strenuous activity. If operational (non-training) mission requires strenuous activity, enforce water intake to minimize expected heat injuries.

Table K-9. Conversion factors.

TO CONVERT:	TO:	USE:
	TEMPERATURE	
Degrees F	Degrees C	$^0C = 5/9\ ^0F - 32)$
Degrees C	Degrees F	$^0F = (9/5\ ^0C) + 32$
	DISTANCE	
Kilometers	Miles	0.62
Kilometers	Nautical Miles	0.54
Kilometers	Feet	3,280.80
Miles	Kilometers	1.61
Miles	Nautical Miles	0.87
Miles	Yards	1,760.00
Miles	Feet	5,280.00
Nautical Miles	Kilometers	1.85
Nautical Miles	Miles	1.15
Meters	Feet	3.28
Yards	Feet	3.00
	SPEED	
Kilometers/Hour	Miles/Hour	0.62
Kilometers/Hour	Knots (Nautical Miles/Hour)	0.54
Miles/Hour	Kilometers/Hour	1.61
Miles/Hour	Knots	0.87
Miles/Hour	Feet/Second	1.467
Knots	Kilometers/Hour	1.85
Knots	Miles/Hour	1.15
Meters/Second	Feet/Second	3.281
Meters/Second	Miles/Hour	2.237
	PRESSURE	
Inches of Mercury (Hg)	Millibar	33.86395
Millibar (Mb)	Inches of Mercury	0.295299
	LENGTH	
Feet Meters	0.3048	
Feet Centimeters	30.48	
Inches	Meters	0.0254
Inches	Centimeters	2.54
Meters	Yards	1.094
Yards	Meters	0.9144

GLOSSARY

Section I. Acronyms and Abbreviations

A

A	as acquired (effect used in AGM)
AA	avenue of approach
AAA	air avenue of approach
AAM	air-to-air missile
AAO	Army Aviation Officer
AAR	after-action report
AASLT	air assault
ABCS	Army Battle Command System
abn	airborne
AC	Active Component
ACE	analysis and control element
ACofS	Assistant Chief of Staff
ACR	armored cavalry regiment
ACT	analysis and control team
AD	air defense
ADA	air defense artillery
ADO	air defense officer
ADP	automated data processing
AEB	aerial exploitation battalion
AEPDS	Advanced Electronic Processing and Dissemination System
AF	audio frequency
AFATDS	Advanced Field Artillery Tactical Data System
AFSO	aerial fire support observer
AGL	above ground level
AG/LT	assault gun/light tank
AGM	attack guidance matrix
AI	area of interest
ALO	air liaison officer
ALOC	administrative and logistics center
AMSS	Automatic Meteorological Sensor System
AO	area of operations
AOB	air order of battle
APC	armored personnel carrier
AQF	Advanced QUICKFIX

AR	Army Regulation
ARF	airborne relay facilities
ARFOR	Army force
ARL	airborne reconnaissance low
ARSOF	Army Special Operations Forces
arty	artillery
ASAR	Advanced Synthetic Aperture Radar
ASAS	All-Source Analysis System
ASM	air space management
ASPS	all-source production section
asst	assistant
AT	antitank
ATCCS	Army Tactical Command and Control System
ATGM	antitank guided missile
ATK	attack
ATR	automated target recognition
ATW	antitank weapon
AUTL	Army Universal Task List
auto	automated
avn	aviation
AVTR	airborne video tape recorder
AWACS	Airborne Warning and Control System

B

B	bomber
BAT-D	battlefield deception
BCTP	battle command training program
BDA	battle damage assessment
BDE	brigade
BDU	battle dress uniform
BHL	battle handover line
BIC	battle-induced contaminants
BICC	battalion information control center
BMCT	beginning of morning civil twilight
BMNT	beginning of morning nautical twilight
BMO	battalion maintenance officer
bn	battalion
BOS	battlefield operating system
BP	battle position
BWK	belt weather kit

C

C^2	command and control
C^2I	C^2 and intelligence
C^2W	command and control warfare
C^3	command, control, and communications
C^3I	C^3 and intelligence
C^4I	C^3, computers, and intelligence
C^4I^2	C^4I and information
CA	Civil Affairs/combat assessment
CALL	Center for Army Lessons Learned
CARVER	criticality, accessibility, recuperability, vulnerability, effect, and recognizability
CAS	close air support
Cas Evac	casualty evacuation
CATK	counterattack
CB	counterbattery
cbt	combat
CBU	cluster bomb unit
CCIR	commander's critical information requirements
CCM	cross-country movement
CCMEC	Combined Captured Materiel Exploitation Center
CD	counter-drug
CDMP	combat decision-making
CDR	commander
CEE	captured enemy equipment
CEM	captured enemy materiel
CFE	Conventional Forces In Europe
CFL	coordinated fire line
CFSO	Counterintelligence Force Protection Source Operations
CGS	J-STARS common ground station
CHAALS	Communication High Accuracy Airborne Location System
CHARIOT	Portable S-Band Receive/Transmit Terminal
CHATS	CI/HUMINT Automation Tool Set
chem	chemical
CI	counterintelligence
CIA	Central Intelligence Agency
CINC	commander in chief
CIP	Command Inspection Program
CIR	critical intelligence requirements
CM	collection management
cmd	command

CMEC	Captured Materiel Exploitation Center
CMISE	Corps Military Intelligence Support Element
CMO	civil-military operations
CNR	combat net radio
co	company
COA	course of action
COIN	counterinsurgency
coll	collection
COLT	combat observation lasing team
COMINT	communications intelligence
comm	communications
COMMEX	communications exercise
COMSEC	communications security
CONPLAN	contingency plan
CONUS	continental United States
coord	coordination
COP	command observation post
COR	chief of reconnaissance
COS	critical occupational speciality
CP	command post
CS	combat support
CSBM	Confidence and Security Building Measures
CSP	communications system processor
CSS	combat service support
CSR	controlled supply rate
CTC	combat training center
CTT	commander's tactical terminal
CUCV	commercial utility cargo vehicle

D

D	destroy (effect used in AGM); desirable (weather designator)
DA	Department of the Army
DDMP	deliberate decision-making process
DEA	Drug Enforcement Administration
DF	direction finding
DIA	Defense Intelligence Agency
DIN	Defense Intelligence Network
DISE	Deployable Intelligence Support Element
dissem	dissemination
div	division

DMP	decision-making process
DOCEX	document exploitation
DOD	Department of Defense
DOS	Department of State
DP	decision point
DS	direct support
DSN	Defense Secure Network
DSSCS	Defense Special Security Communications System
DST	decision support template
DSVT	digital subscriber voice terminal
DTG	date-time group
DTSS/MSIP	Digital Topographical Support System/Multi-Spectral Image Processor
DTSS/QRMP	Digital Topographical Support System/QUICK-Response Multicolor Printer
DZ	drop zone

E

E	essential (weather designator)
EA	electronic attack; engagement area (used in AGM)
EAC	echelons above corps
ECB	echelons corps and below
ECOA	enemy course of action
EECT	end of evening civil twilight
EEFI	essential elements of friendly information
EENT	end of evening nautical twilight
EFVS	electronic fighting vehicle system
e.g.	for example
ELINT	electronic intelligence
EM	electromagnetic
ENGR	engineer
E-O	electro-optical
EP	electronic protection
EPB	electronic preparation of the battlefield
EPDS	Electronic Processing and Dissemination System
EPW	enemy prisoner of war
ERFB-BB	extended-range full-bore-based bleed
ES	electronic warfare support
est	estimated
etc	and so forth
ETRAC	Enhanced Tactical Radar Correlator

ETUT	Enhanced Tactical Users Terminal
EW	electronic warfare
EWO	electronic warfare officer
EWS	early warning system
EWTL	electronic warfare target list
EXEVAL	external evaluation

F

°F	degree Fahrenheit
F	fighter (sortie category)
FA	field artillery
FAC	forward air controller
FAIO	field artillery intelligence officer
FALOP	forward area limited observation program
FARP	forward arming and refueling point
FAST	Forward Area Support Terminal
FAST-I	Forward Area Support Terminal-Improved
FAX	facsimile
FBIS	Foreign Broadcast Information Service
FCE	fire control element
FDA	functional damage assessment
FDC	fire direction center
FDO	fire direction officer
FEBA	forward edge of the battle area
FFIR	friendly forces information requirements
FISTV	first support team vehicle
FLCS	Force Level Control System
FLIR	forward-looking infrared
FLOT	forward line of own troops
flt	flight
FM	field manual
FMC	fully mission capable
FMIB	Foreign Materiel Intelligence Battalion
FO	forward observer
FofF	field of fire
FRAGO	fragmentary order
FS	fire support
FSB	forward support battalion
FSC	fire support center
FSCL	fire support coordination line
FSCM	fire support coordinating measure

FSCOORD	fire support coordinator
FSE	fire support element
FSO	fire support officer
FSOP	field standing operating procedure
FSU	fire support unit
ft	feet
FTI	fixed target indicator
F/W	fixed wing
fwd	forward

G

G2	Assistant Chief of Staff, G2 (Intelligence)
GBCS-(H/L)	ground-based common-sensor (heavy/light)
GCI	ground control intercept
GE	Germany
GHz	gigahertz
GL	grenade launcher
GPS	global positioning system
GRCS	GUARDRAIL Common Sensor
GS	general support
GSM	J-STARS ground station module
GSR	ground surveillance radar

H

H	harrassing fires
HA	humanitarian assistance
HE	high explosive
HF	high frequency
Hg	mercury
HHD	headquarters and headquarters detachment
HHOC	headquarters, headquarters and operations company
HMMWV	high mobility multipurpose wheeled vehicle
HN	host nation
HPT	high-payoff target
HPTL	high payoff target list
HQ	headquarters
hr	hour
HUMINT	human intelligence
HVT	high-value target
hvy	heavy

H/W	hardware

I

I	immediate (effect used in AGM)
IAW	in accordance with
I&S	intelligence and security
I&W	indications and warnings
ID	identify
IDL	interoperable data link
IEW	intelligence and electronic warfare
IEWCS	Intelligence Electronic Warfare Common Sensor
IEWMAA	IEW mission area analysis
IFV	infantry fighting vehicle
IHL	intelligence handover line
IMA	individual mobilization augmentee
IMETS	Integrated Meteorological System
IMINT	imagery intelligence
incorp	incorporate
INF	Intermediate-range Nuclear Forces intelligence
infil	infiltration
info	information
in/h	inches per hour
INMARSAT	International Maritime Satellite
intel	intelligence
intg	interrogation
INTSUM	intelligence summary
IO	information operations
IPB	intelligence preparation of the battlefield
IPDS	Imagery Processing and Dissemination System
IPF	integrated processing facility
IPS	intelligence production section
IPW	interrogation, prisoners of war
IR	information requirements
I-REMBASS	Improved Remotely Monitored Battlefield Sensor System
ISA	International Standardization Agreement
ISB	intelligence support base
ISM	intelligence synchronization matrix
ISSO	information systems security officer
IVL	intervisibility lines

J

J2	Intelligence Directorate
JCMEC	Joint Captured Materiel Exploitation Center
JCS	Joint Chiefs of Staff
JIC	Joint Intelligence Center
J-SIIDS	Joint-Service Interior Intrusion Detector System
JSTARS	Joint Surveillance Target Attack Radar System
JTAGS	Joint Tactical Ground Station
JTF	joint task force
JTT/H	joint tactical terminal/hybrid
JTT/H-R3	joint tactical terminal/hybrid-receive only

K

km	kilometer

L

LAN	local area network
LAV	light armored vehicle
LC	line of contact
LD	line of departure
LEA	Law Enforcement Agency
LLSO	low-level source operations
LLVI	low-level voice intercept
LMRDFS	Lightweight Man-Transportable Radio Direction Finding System
LNO	liaison officer
LOA	limit of advance
LOB	line of bearing
LOC	line of communication
LOS	line of sight
LP	listening post
LPI	low probability of intercept
LRP	long-range patrol
LRRP	long-range reconnaissance patrol
LRS	long-range surveillance
LRSD	long-range surveillance detachment
LRSU	long-range surveillance unit
LRU	long-range unit
LT	light
LTIOV	latest time information is of value
LZ	landing zone

M

m	meter
MASINT	measurement and signals intelligence
Mb	millibar
MC	movement corridor
MC&G	mapping, charting, and geodesy
MCOO	modified combined obstacles overlay
MCSF	Mobile Cryptologic Support Facility
MDCI	multidiscipline counterintelligence
MDMP	military decision-making process
MEA	munitions effects assessment
med	medium
MEDEVAC	medical evacuation
MET	meteorological
METL	mission essential task list
METT-T	mission, enemy, terrain and weather, troops, and time available
METT-TC	mission, enemy, terrain and weather, troops, and time available civilians
MEWSS	Mobile Electronic Warfare Support System
MGS	magnetic grid system
mgt	management
MI	military intelligence
MIES	Modernized Imagery Exploitation System
MIJI	meaconing, intrusion, jamming, and interference
min	minute
MIPB	Military Intelligence Professional Bulletin
MIRS	Miniaturization Imagery Receive System
MIST	military intelligence support team
MITT	Mobile Integrated Tactical Terminal
MLRS	multiple launch rocket system
MOPP	mission-oriented protection posture
MP	military police
MR	moon rise
MS	moon set
MSE	mobile subscriber element
MT	medium tank
MTI	moving target indicator
MTOE	modified table of organization and equipment
MTP	mission training plan

N

N	north; neutralize (effect used in AGM)
NA	not applicable
NAI	named area of interest
NATO	North Atlantic Treaty Organization
NBC	nuclear, biological, and chemical
NCA	National Command Authority
NCO	noncommissioned officer
NEO	noncombatant evacuation operation
NFA	no fire area
NGIC	National Ground Intelligence Center
NGLO	naval gunfire liaison officer
NGO	non-governmental organization
NIMA	National Imagery Mapping Agency
NIST	National Intelligence Support Team
NLT	no later than
nmi	nautical miles
NOD	night observation device
NOE	nap of the earth
noncomm	noncommunications
NRT	near-real time
NVD	night vision devices
NVG	night vision goggles

O

OB	order of battle
OCOKA	obstacles & fields of fire, concealment & cover, key terrain, and avenues of approach
OCONUS	outside continental United States
O/O	on order
OOTW	operations other than war (see SASO)
OP	observation post
OPCON	operational control
OPLAN	operations plan
opns	operations
OPORD	operations order
OPSEC	operations security
OR	operational readiness
OT	operator terminal

P

P	planned
PAO	public affairs office

PDA	physical damage assessment
PEO	peace enforcement operations
photo	photography
PGM	precision-guided munitions
PIR	priority intelligence requirements
PKO	peacekeeping operations
plt	platoon
PMCS	preventive maintenance checks and services
POL	petroleum, oils, lubricants
PP	passage point
prep	preparation
PSA	post-strike assessment
PSYOP	psychological operations
PT	physical training
PVO	private volunteer organization
PZ	pickup zone

Q

QSTAG	Quadripartite Standardization Agreement
qty	quantity

R

R	reconnaissance (sortie category)
R&D	research and development
R&S	reconnaissance and surveillance
RAS	rear area security
RBP	red/black processor
RC	Reserve Components
RCOA	reconnaissance course of action
rcv	receive
RDC	rear detachment commander
recon	reconnaissance
REDTRAIN	readiness training
regt	regiment
REMBASS	Remotely Monitored Battlefield Sensor System
RFI	request for information
RII	request for intelligence information
RISTA	reconnaissance, intelligence, surveillance, and target acquisition
RL	rocket launcher
RNP	radio navigational points (USAF)
ROE	rules of engagement

ROTERM	receive only terminal
RP	release point
rqmts	requirements
RRS	radio relay system
RRT	radio receiver transmission
RRTS	radio relay test set
RSOP	readiness standing operating procedure
RSR	required supply rate
RTO	radiotelephone operator
R/W	rotary wing
RWS	remote workstation

S

S	South; suppress (effect used in AGM)
SA	small arms
S&TI	Scientific & Technical Intelligence
S1	Adjutant (US Army)
S2	Intelligence Officer (US Army)
S3	Operations and Training Officer (US Army)
S4	Supply Officer (US Army)
S5	Civil Affairs Officer (US Army)
SAEDA	Subversion and Espionage Directed Against the US Army
SALUTE	size, activity, location, unit, time, and equipment
SAM	surface-to-air missile
SAR	synthetic aperture radar
SASO	stability and support operations (formerly OOTW)
SATCOM	satellite communications
SCI	sensitive compartmented information
SDO	staff duty officer
SDS	security data system
SEAD	suppression of enemy air defenses
sep bde	separate brigade
SF	Special Forces
SI	special intelligence
SID	secondary imagery dissemination
SIDS	Secondary Imagery Dissemination System
SIGINT	signals intelligence
SIGINT/EW	signals intelligence/electronic warfare
SIGO	signal officer
SII	statement of intelligence interest

SINCGARS	Single-Channel Ground and Airborne Radio System
SIR	specific information requirements
SITMAP	situation map
SJA	Staff Judge Advocate
SLAR	side-looking airborne radar
SOCCE	Special Operations Command and Control Element
SOF	special operations forces
SOFA	Status of Forces Agreement
SOI	signals operating instructions
SOP	standing operating procedure
SOR	specific orders and requests
SOT-A	support operations team-Alpha
SOT-B	support operations team-Bravo
SP	start point
SPIRIT	Special Purpose Integrated Remote Intelligence Terminal
sqdn	squadron
SR	sunrise
SS	sunset
SSM	surface-to-surface missile
SSO	special security office
SSP	single-soure processing
ST	student text
STANAG	Standardization Agreement
STU III	Secure Telephone Unit-Third Generation
SUCCESS	Synthesized UHF Computer Controller Enhanced Subsystem
survl	surveillance
S/W	software
SWO	staff weather officer

T

TA	target acquisition
TAA	tactical assembly area
TAB	target acquisition battery
tac	tactical
TAC	tactical command post
TACFIRE	tactical fire direction system
TACLINK	tactical link
TACSAT	tactical satellite

TADIXS-B	Tactical Data Information Exchange System-Broadcast
TAI	target area of interest
TAREX	target exploitation
TB	tank brigade
TD	tank division
TDA	target development assessment
TDDS	TRAP Data Dissemination System
TDMP	tactical decision-making process
TDOA	time differential of arrival
TECHINT	technical intelligence
TENCAP	Tactical Exploitation of National Capabilities
TF	task force
tgt	target
THAADS	Theater High Altitude Area Defense System
THMT	tactical high mobility terminal
TIBS	Tactical Information Broadcast System
TLE	target location error
TLP	troop-leading procedures
TOC	tactical operations center
TOPS	Tactical Onboard Processing System (for TADIXS-B)
TOW	tube-launched, optically tracked, wire-guided
TPL	time phase line
TRAP	Tactical Related Applications
TRIXS	Tactical Reconnaissance Intelligence Exchange System
trng	training
TROJAN SPIRIT	Special Purpose Integrated Remote Intelligence Terminal
TRRIP	Theater Rapid Response Intelligence Package
TSA	target system assessment
TSOP	tactical standing operating procedure
TSS	target selection standards
TTP	tactics, techniques, and procedures
TUAV	tactical unmanned aerial vehicle
TVA	target value analysis

U

UAV	unmanned aerial vehicle
UBL	unit, basic load
UHF	ulltra high frequency
USAF	US Air Force
USMTF	United States Message Text Formats
USSID	United States Signal Intelligence Directive

UW	unconventional warfare
	V
VHF	very high frequency
vis	visibility
	W
w	with
WARNO	warning order
WATCHCON	watch condition
WBGT	wet-bulb-globe temperature
WETM	weather team
wkstn	workstation
wpn	weapon
	X
XO	executive officer
XPLN	exploitation
xmit	transmit

Section II. Terms.

Global security forecast. A forecast of where, when, and between whom conflicts can occur.

Battlefield development plans. A 5- to 20-year forecast of how selected threat forces will organize and operate on the battlefield.

Automated and hardcopy databases. Databases such as the Stylized Country Force Assessments and the Army Force Planning and Data Assumptions which provide detailed projections on OB, equipment, logistics, and readiness (ground, air, naval forces) of potential threats 2 to 25 years into the future.

TECHINT and User Bulletins. Provide a high resolution view of threat equipment and weapons systems and capabilities, and complement traditional OB information. They can be obtained from NGIC.

Open source studies and articles. State Department background papers, FBIS, public libraries, universities, and corporations with contracts in countries of interest). Databases of sources need to be researched and exercised in advance of mission execution.

Other services. The USMC, other nation's information, fact books, and fact sheets on tactics, terrain, and country studies.

REFERENCES

SOURCES USED

These are the sources quoted or paraphrased in this publication.

AR 381-10	*US Army Intelligence Activities.* 1 Jul 84.
FM 6-20-10	*Tactics, Techniques, and Procedures for the Targeting Process (MCRP 3-1.6.14).* 8 May 96
FM 17-95	*Cavalry Operations.* 24 Dec 96.
FM 33-1	*Psychological Operations (FMFM 3-53).* 18 Feb 93.
FM 34-1	*Intelligence and Electronic Warfare Operations.* 27 Sep 94.
FM 34-2	*Collection Management and Synchronization Planning.* 8 Mar 94.
FM 34-2-1	*Tactics, Techniques, and Procedures for Reconnaissance and Surveillance and Intelligence Support to Counterreconnaissance.* 19 Jun 91.
FM 34-3	*Intelligence Analysis.* 15 Mar 90.
FM 34-8	*Combat Commander's Handbook on Intelligence.* 28 Sep 92.
FM 34-25-3	*All-Source Analysis System and the Analysis and Control Element.* 3 Oct 95.
FM 34-37	*Echelons Above Corps (EAC) Intelligence & Electronic Warfare (IEW) Operations.* 15 Jan 91.
(U) FM 34-40	*Electronic Warfare Operations* , 9 Oct 87, Secret.
FM 34-130	*Intelligence Preparation of the Battlefield.* 8 Jul 94.
FM 41-10	*Civil Affairs Operations.* 11 Jan 93.
FM 100-6	*Information Operations.* 27 Aug 96.
FM 100-17	*Mobilization, Deployment, Redeployment, Demobilization.* 28 Oct 92.
FM 101-5	*Staff Organizations and Operations.* 25 May 84.
FM 101-5-1	*Operational Terms and Symbols.* 21 Oct 85.
Joint Pub 1-02	*Department of Defense Dictionary of Military and Associated Terms.* 23 Mar 94.
Joint Pub 6-04.11	*US Message Text Formatting Program Repository of USMTF Program Items for US Implementation Guidance.* 1 Oct 91.

DOCUMENTS NEEDED

These documents must be available to the intended users of this publication.

AR 190-11	*Physical Security of Arms, Ammunition and Explosives.* 30 Sep 93.
AR 190-13	*The Army Physical Security Program.* 30 Sep 93.

AR 190-14	*Carrying of Firearms and Use of Force for Law Enforcement and Security Duties.* 12 Mar 93.
AR 190-51	*Security of Unclassified Army Property (Sensitive and Nonsensitive).* 30 Sep 93.
AR 525-13	*The Army Combatting Terrorism Program.* 25 Feb 88.
AR 380-5	*Department of the Army Information Security Program.* 25 Feb 88.
AR 380-10	*Technology Transfer, Disclosure of Information and Contacts with Foreign Representatives.* 30 Dec 94.
AR 380-19	*Information Systems Security.* 1 Aug 90.
AR 380-67	*The Department of the Army Personnel Security Program.* 9 Sep 88.
AR 381-1	*Controls of Dissemination of Intelligence Information.* 12 Feb 90.
AR 381-12	*Subversion and Espionage Directed Against the US Army (SAEDA).* 15 Jan 93.
AR 381-20	*The Army Counterintelligence Program.* 15 Nov 93.
(U) AR 381-172	Counterintelligence Force Protection Source Operations *(CFSO) and Low Level Source Operations (LLSO),* Secret.
AR 530-1	*Operations Security (OPSEC).* 3 Mar 95.
FM 1-111	*Aviation Brigades.* 27 Aug 90.
FM 3-4	*NBC Protection (FMFM 11-9) (reprinted w/basic Incl C1).* 29 May 92.
FM 3-5	*NBC Contamination (FMFM 11-10).* 17 Nov 93.
FM 3-50	*Smoke Operations.* 4 Dec 90.
FM 5-30	*Engineer Intelligence (reprinted w/Basic Incl C1).* 22 Sep 67.
FM 5-34	*Enginer Field Data.* 14 Sep 87.
FM 5-36	*Route Reconnaissance and Classification.* 10 May 85.
FM 6-20	*Fire Support in the AirLand Battle.* 17 May 88.
FM 5-100	*Engineer Operations.* 27 Feb 96.
FM 5-101	*Mobility.* 23 Jan 85.
FM 5-102	*Countermobility.* 14 Mar 85.
FM 5-103	*Survivability.* 10 Jan 85..
FM 6-121	*Tactics, Techniques, and Procedures for Field Artillery Target Acquisition.* 25 Sep 90.
FM 7-7	*The Mechanized Infantry Platoon and Squad.* 15 Mar 85.
FM 7-7J	*Mechanized Infantry Platoon & Squad (BRADLEY).* 7 May 93.
FM 7-8	*Infantry Rifle Platoon and Squad.* 22 Apr 92.
FM 7-10	*The Infantry Rifle Company.* 14 Dec 90.
FM 7-20	*The Infantry Battalion.* 6 Apr 92.
FM 7-70	*Light Infantry Platoon & Squad.* 10 Sep 86
FM 7-71	*Light Infantry Company.* 28 Aug 87.
FM 7-92	*The Infantry Reconnaissance Platoon and Squad (Airborne, Air Assault, Light Infantry).* 23 Dec 92.
FM 7-93	*Long-Range Survival Unit Operations.* 3 Oct 95.

FM 10-14-2	*Guide for the Battalion S4 (reprinted w/Basic Incl C1).* 30 Dec 81.
FM 10-14-3	*Surveying Officer's Guide.* 30 Dec 81.
FM 11-30	*MSE Communications in the Corps/Division.* 27 Feb 91.
FM 11-32	*Combat Net Radio Operations.* 15 Oct 90.
FM 11-37	*MSE Primer for Smal-Unit Leaders.* 14 Nov 90.
FM 11-50	*Combat Communications Within the Division (Heavy and Light).* 4 Apr 91.
FM 17-15	*Tank Platoon.* 3 Apr 96.
FM 17-95	*Cavalry Operations.* 24 Dec 96.
FM 17-95-10	*The Armored Cavalry Regiment and Squad.* 22 Sep 93.
FM 17-97	*Cavalry Troop.* 3 Oct 95.
FM 17-98-1	*Scout Leader's Handbook.* 24 Sep 90.
FM 19-1	*Military Police Support for the AirLand Battle.* 23 May 88.
FM 19-30	Physical Security. 1 Mar 79.
FM 19-40	*Enemy Prisoners of War, Civilian Internees and Detained Persons.* 27 Feb 76.
FM 21-26	*Map Reading and Land Navigation.* 7 May 93.
FM 21-31	*Topographical Symbols (reprinted w/Basic Incl C1).* 19 Jun 61.
FM 25-100	*Training the Force.* 15 Nov 88.
FM 25-101	*Battle Focused Training.* 30 Sep 90.
(U) FM 34-5	*Human Intelligence and Related Counterintelligence Operations,* 29 Jul 94, Secret.
FM 34-7	*Intelligence and Electronic Warfare Support to Low-Intensity Conflict Operations.* 18 May 93.
FM 34-10	*Division Intelligence and Electronics Warfare Operations.* 25 Nov 86.
FM 34-13	*Military Intelligence (MI) Battalion, Combat Electronic Warfare Intelligence (CEWI) (Div), Leaders Handbook for Platoons and Teams.* 15 Apr 83.
FM 34-25	*Corps Intelligence and Electronic Warfare Operations.* 30 Sep 87.
FM 34-25-1	*Joint Surveillance Target Attack Radar System (JOINT STARS).* 3 Oct 95.
(U) FM 34-25-6	*Tactics, Techniques, and Procedures for the Electronic Processing & Dissemination System ,* 15 Jun 92, Secret.
(U) FM 34-25-7	Special Electronic Mission Aircraft (SEMA) Survivability 3 Oct 95, Secret.
FM 34-35	*Armored Cavalry Regiment (ACR) and Separate Brigade Intelligence and Electronic Warfare (IEW) Operations.* 12 Dec 90.
FM 34-36	*Special Operation Forces IEW Operations.* 30 Sep 91.
(U) FM 34-40-3	*Tactical Signals Intelligence (SIGINT) Analysis Operations,* 21 May 91, Confidential

FM 34-40-7	*Communications Jamming Handbook.* 23 Nov 92.
FM 34-40-9	*Direction Finding Operations.* 29 Aug 91.
(U) FM 34-40-12	*Morse Code Intercept Operations* , 26 Aug 91, Confidential.
(U) FM 34-40-13	*Electronic Intelligence (ELINT) Operations,* 10 Sep 91, Secret.
FM 34-52	*Intelligence Interrogation.* 28 Sep 92.
FM 34-54	*Battlefield Technical Intelligence.* 5 Apr 90.
FM 34-60	*Counterintelligence.* 3 Oct 95.
FM 34-80	*Brigade and Battalion Intelligence and Electronic Warfare Operations.* 15 Apr 86.
FM 34-81	*Weather Support for Army Tactical Operations (AFM 105-4).* 31 Aug 89
FM 34-81-1	*Battlefield Weather Effects.* 23 Dec 92.
FM 34-82	*Military Intelligence Unit Exercise Development Guide.* 26 Nov 85.
FM 71-3	*Armored and Mechanized Infantry Brigade.* 8 Jan 96.
FM 71-100	*Division Operations.* 28 Aug 96.
FM 90-2	*Battlefield Deception.* 3 Oct 88.
(U) FM 90-2A	*Electronic Deception,* 12 Jun 89, Secret.
FM 90-7	*Combined Arms Obstacle Integration.* 29 Sep 94.
FM 90-14	*Rear Battle.* 10 Jun 85.
FM 90-29	*Noncombatant Evacuation Operations.* 17 Oct 94.
FM 100-2-2	*The Soviet Army: Specialized Warfare and Rear Area Support.* 16 Jul 84.
FM 100-2-3	*The Soviet Army: Troops, Organization and Equipment.* 16 Jun 91.
FM 100-5	*Operations.* 14 Jun 93.
FM 100-13	*Battefield Coordination Detachment (BCD).* 5 Sep 96.
FM 100-19	*Domestic Support Operations. (FMFM 7-10).* 1 Jul 93.
FM 100-20	*Military Operations in Low-Intensity Conflict (AFP 3-20).* 5 Dec 90.
FM 100-23	*Peace Operations.* 30 Dec 94.
FM 100-25	*Doctrine for Army Special Operations Forces.* 12 Dec 91.
FM 101-10-1/1	*Staff Officer's Field Manual-Organizational, Technical, and Logistical Data (Volume 1).* 7 Oct 87.
FM 101-10-1/2	*Staff Officer's Field Manual-Organizational, Technical, and Logistical Planning Factors (Volume 2) (reprinted w/Basic Incl C1).* 7 Oct 87.
ST 101-5	*Command and Staff Decision Processes*
ST 101-9	*The Tactical Decisionmaking Process*
TC 12-17	*Adjutant's Call/The S1 Handbook.* 17 Mar 92.
TC 34-55	*Imagery Intelligence.* 3 Oct 88.
Joint Pub 1	*Joint Warfare for the U.S. Armed Forces.* 10 Jan 95.
Joint Pub 2-0	*Joint Doctrine for Intelligence Support to Operations.*

5 May 95.

Joint Pub 3-0	*Doctrine for Joint Operations*. 1 Feb 95.
Joint Pub 5-0	*Doctrine for Planning Joint Operations.* 13 Apr 95.
Joint Pub 6-02	*TAC C4 Systems.*
(U) Joint Pub 6-02	*Joint Doctrine for Employment of Operational/Tactical Comand, Control, Communications, and Computer System,* 1 Oct 96, Secret.
DA Form 2028	*Recommended Changes to Publications and Blank Forms.* 1 Feb 74.
DA Form 3964	*Classified Document Accountability Record.* Jul 79.

By Order of the Secretary of the Army:

DENNIS J. REIMER
General, United States Army
Chief of Staff

Official:

JOEL B. HUDSON
Administrative Assistant to the
Secretary of the Army
04459

DISTRIBUTION:

Active Army, Army National Guard, and U. S. Army Reserve: To be distributed in accordance with initial distribution number 115447, requirements for FM 34-8-2.

This Page Is Intentionally Left Blank

A Tradecraft Primer:
Structured Analytic Techniques
for Improving Intelligence Analysis

Prepared by the US Government

March 2009

This primer highlights structured analytic techniques—some widely used in the private sector and academia, some unique to the intelligence profession. It is not a comprehensive overview of how intelligence officers conduct analysis. Rather, the primer highlights how structured analytic techniques can help one challenge judgments, identify mental mindsets, stimulate creativity, and manage uncertainty. In short, incorporating regular use of techniques such as these can enable one to structure thinking for wrestling with difficult questions.

TABLE OF CONTENTS

Introduction 1

How To Use These Techniques 5

Diagnostic Techniques 7
- Key Assumptions Check 7
- Quality of Information Check 10
- Indicators or Signposts of Change 12
- Analysis of Competing Hypotheses (ACH) 14

Contrarian Techniques 17
- Devil's Advocacy 17
- Team A/Team B 19
- High-Impact/Low-Probability Analysis 22
- "What If?" Analysis 24

Imaginative Thinking Techniques 27
- Brainstorming 27
- Outside-In Thinking 30
- Red Team Analysis 31
- Alternative Futures Analysis 34

Strategies for Using Structured Analytic Techniques 38

Selective Bibliography 40

THE "MIND-SET" CHALLENGE

Using the analytic techniques contained in this primer will assist analysts in dealing with the perennial problems of intelligence: the complexity of international developments, incomplete and ambiguous information, and the inherent limitations of the human mind. Understanding the intentions and capabilities of adversaries and other foreign actors is challenging, especially when either or both are concealed. Moreover, transnational threats today pose even greater complexity, in that they involve multiple actors—including nonstate entities—that can adapt and transform themselves faster than those who seek to monitor and contain them. Finally, globalization has increased the diversity of outcomes when complex, interactive systems such as financial flows, regional economies or the international system as a whole are in flux.[2]

The first hurdle for analysts is identifying the relevant and diagnostic information from the increasing volume of ambiguous and contradictory data that is acquired through open source and clandestine means. Analysts must also pierce the shroud of secrecy—and sometimes deception—that state and nonstate actors use to mislead. A systematic approach that considers a range of alternative explanations and outcomes offers one way to ensure that analysts do not dismiss potentially relevant hypotheses and supporting information resulting in missed opportunities to warn.

Cognitive and perceptual biases in human perception and judgment are another important reason for analysts to consider alternatives. As Richards Heuer and others have argued, all individuals assimilate and evaluate information through the medium of "mental models" (sometimes also called "frames" or "mind-sets"). These are experience-based constructs of assumptions and expectations both about the world in general and more specific domains. These constructs strongly influence what information analysts will accept—that is, data that are in accordance with analysts' unconscious mental models are more likely to be perceived and remembered than information that is at odds with them.

Mental models are critical to allowing individuals to process what otherwise would be an incomprehensible volume of information. Yet, they can cause analysts to overlook, reject, or forget important incoming or missing information that is not in accord with their assumptions and expectations. Seasoned analysts may be more susceptible to these mind-set problems as a result of their expertise and past success in using time-tested mental models. The key risks of mind-sets are that: analysts perceive what they expect to perceive; once formed, they are resistant to change; new information is assimilated, sometimes erroneously, into existing mental models; and conflicting information is often dismissed or ignored.

> *"Intelligence analysts should be self-conscious about their reasoning processes. They should think about how they make judgments and reach conclusions, not just about the judgments and conclusions themselves."*
>
> —Richards Heuer, *The Psychology of Intelligence Analysis*[1]

[1] Richards J. Heuer, Jr., *The Psychology of Intelligence Analysis* (Washington: Center for the Study of Intelligence, 1999).

[2] These observations were drawn from a lengthier treatment of cognitive bias found in the Sherman Kent Center's Occasional Paper, *Making Sense of Transnational Threats*, Vol. 3, No. 1, October 2004.

Common Perceptual and Cognitive Biases

Perceptual Biases

Expectations. We tend to perceive what we expect to perceive. More (unambiguous) information is needed to recognize an unexpected phenomenon.

Resistance. Perceptions resist change even in the face of new evidence.

Ambiguities. Initial exposure to ambiguous or blurred stimuli interferes with accurate perception, even after more and better information becomes available.

Biases in Evaluating Evidence

Consistency. Conclusions drawn from a small body of consistent data engender more confidence than ones drawn from a larger body of less consistent data.

Missing Information. It is difficult to judge well the potential impact of missing evidence, even if the information gap is known.

Discredited Evidence. Even though evidence supporting a perception may be proved wrong, the perception may not quickly change.

Biases in Estimating Probabilities

Availability. Probability estimates are influenced by how easily one can imagine an event or recall similar instances.

Anchoring. Probability estimates are adjusted only incrementally in response to new information or further analysis.

Overconfidence. In translating feelings of certainty into a probability estimate, people are often overconfident, especially if they have considerable expertise.

Biases in Perceiving Causality

Rationality. Events are seen as part of an orderly, causal pattern. Randomness, accident and error tend to be rejected as explanations for observed events. For example, the extent to which other people or countries pursue a coherent, rational, goal-maximizing policy is overestimated.

Attribution. Behavior of others is attributed to some fixed nature of the person or country, while our own behavior is attributed to the situation in which we find ourselves.

Intelligence analysts must actively review the accuracy of their mind-sets by applying structured analytic techniques that will make those mental models more explicit and expose their key assumptions. The techniques found in this primer are designed to assist in this regard by:

- Instilling more structure into the intelligence analysis.
- Making analytic arguments more transparent by articulating them and challenging key assumptions.
- Stimulating more creative, "out-of-the-box" thinking and examining alternative outcomes, even those with low probability, to see if available data might support these outcomes.
- Identifying indicators of change (or signposts) that can reduce the chances of surprise.

Incorporating findings derived from these techniques into our intelligence products also serves the policymaker by:

- Highlighting potential changes that would alter key assessments or predictions.
- Identifying key assumptions, uncertainties, intelligence gaps and disagreements that might illuminate risks and costs associated with policy choices.
- Exploring alternative outcomes for which policy actions might be necessary.

Strategic Assumptions That Were Not Challenged

1941 World War II

Japan would avoid all-out war because it recognized US military superiority.

Given that US superiority would only increase, Japan might view a first strike as the only way to knock America out of the war.

1950s Korean War

China would not cross the Yalu River in support of the North Korean government.

Red China could make good on its threats to counter "US aggression" against the North.

1962 Cuban Missile Crisis

The Soviet Union would not introduce offensive nuclear weapons into Cuba.

The Kremlin could miscalculate and believe it could create a fait accompli that a young US President would not be prepared to reverse.

1973 Yom Kippur War

Arabs knew they could not win because they had failed to cooperate in the past and still lacked sufficient air defenses to counter Israeli airpower.

A surprise Arab attack, even if repelled, could wound Israel psychologically and prompt international calls for cease-fires and diplomatic negotiations.

1989 German Unification

East Germany could not unify with the West Germany against the wishes of the Soviet Union.

The Soviet Union—under Gorbachev—might not be prepared to intervene militarily in Eastern Europe as it had in the past.

1998 Indian Nuclear Test

Conducting a nuclear test risked international condemnation and US sanctions and would threaten a newly elected coalition government.

A successful and surprise nuclear test could boost Indian nationalist pride and solidify public support for a shaky coalition government.

2003 Iraq's WMD Programs

Saddam failed to cooperate with UN inspectors because he was continuing to develop weapons of mass destruction.

If Iraqi authorities had destroyed their WMD stocks and abandoned their programs, they might refuse to fully acknowledge this to the UN to maintain Iraq's regional status, deterrence, and internal regime stability.

HOW TO USE THESE TECHNIQUES

The analytic techniques in this primer are designed to help individual analysts, as well as teams, explore and challenge their analytical arguments and mind-sets. Some techniques are fairly simple to understand and employ—such as Brainstorming and Devil's Advocacy. Others are more complex and demand a greater degree of analytical sophistication, resource commitment, and time. All the techniques are included because they have helped other analysts avoid rigid ways of thinking or assisted them in exploring new outcomes or implications of an intelligence problem.

The techniques are grouped by their purpose: **diagnostic** techniques are primarily aimed at making analytic arguments, assumptions, or intelligence gaps more transparent; **contrarian** techniques explicitly challenge current thinking; and **imaginative thinking** techniques aim at developing new insights, different perspectives and/or develop alternative outcomes. In fact, many of the techniques will do some combination of these functions. However, analysts will want to select the tool that best accomplishes the specific task they set out for themselves. Although application of these techniques alone is no guarantee of analytic precision or accuracy of judgments, it does improve the sophistication and credibility of intelligence assessments as well as their usefulness to policymakers. As Richards Heuer notes in his own work on cognitive bias, "analysis can be improved."[3]

[3] Heuer, *Psychology of Intelligence Analysis*, p. 184.

KEY ASSUMPTIONS CHECK

List and review the key working assumptions on which fundamental judgments rest.

WHEN TO USE

A Key Assumptions Check is most useful at the beginning of an analytic project. An individual analyst or a team can spend an hour or two articulating and reviewing the key assumptions. Rechecking assumptions also can be valuable at any time prior to finalizing judgments, to insure that the assessment does not rest on flawed premises. Identifying hidden assumptions can be one of the most difficult challenges an analyst faces, as they are ideas held—often unconsciously—to be true and, therefore, are seldom examined and almost never challenged.

A key assumption is any hypothesis that analysts have accepted to be true and which forms the basis of the assessment. For example, military analysis may focus exclusively on analyzing key technical and military variables (sometimes called factors) of a military force and "assume" that these forces will be operated in a particular environment (desert, open plains, arctic conditions, etc.). Postulating other conditions or assumptions, however, could dramatically impact the assessment. Historically, US analysis of Soviet-Warsaw Pact operations against NATO had to "assume" a level of non-Soviet Warsaw Pact reliability (e.g., would these forces actually fight?). In this case, there was high uncertainty and depending on what level of reliability one assumed, the analyst could arrive at very different conclusions about a potential Soviet offensive operation. Or when economists assess the prospects for foreign economic reforms, they may consciously, or not, assume a degree of political stability in those countries or the region that may or may not exist in the future. Likewise, political analysts reviewing a developing country's domestic stability might unconsciously assume stable oil prices, when this key determinant of economic performance and underlying social peace might fluctuate. All of these examples highlight the fact that analysts often rely on stated and unstated assumptions to conduct their analysis. The goal is not to undermine or abandon key assumptions; rather, it is to make them explicit and identify what information or developments would demand rethinking them.

VALUE ADDED

Explicitly identifying working assumptions during an analytic project helps:

- Explain the logic of the analytic argument and expose faulty logic.
- Understand the key factors that shape an issue.
- Stimulate thinking about an issue.
- Uncover hidden relationships and links between key factors.
- Identify developments that would cause you to abandon an assumption.
- Prepare analysts for changed circumstances that could surprise them.

Key Assumptions Check: The 2002 DC Sniper Case

The outbreak of sniper shootings in the Washington, DC area in the fall of 2002 provides a good example of how this technique could have been applied. After the initial flurry of shootings, the operating assumption that quickly emerged was that the shootings were the work of a single, white male who had some military training and was driving a white van. If law enforcement officials had conducted a Key Assumptions Check, they could have broken this statement into its key components and assessed the validity of each statement as follows:

Key Assumption	Assessment
The sniper is a male.	Highly likely (but not certain) given past precedent with serial killers. We are taking little risk by not looking for a female.
The sniper is acting alone.	Highly likely (but not certain) given past precedents.
The sniper is white.	Likely, but not as certain, given past precedents. We would be taking some risk if we rule out nonwhites as suspects.
The sniper has military training/experience.	Possible, but not sufficient reason to exclude from consideration potential suspects who have not had any military training.
The sniper is driving a white van.	Possible because you have a credible eyewitness account but worthy of continuing scrutiny given the number of white vans in the area (more than 70,000 registered in the Maryland suburbs of Metropolitan Washington, DC) and that different kinds of vehicles are being described.

A Key Assumptions Check could have allowed law enforcement officials to:

- Avoid jumping to conclusions (the sniper is white, has military training, and is driving a white van) that did not hold up under closer scrutiny. By explicitly examining each assumption, officials could have avoided prematurely narrowing down the potential pool of suspects to a group that did not include the actual perpetrator. Similarly, they might have been more cautious about accepting that the sniper was driving a white van.
- Be receptive to new leads and citizen tips, such as eyewitness reports that the sniper fled the scene driving a specific model Chevrolet.
- More seriously consider evidence that subsequently became available, which contradicted a key assumption. If officials had stated explicitly that they were assuming the sniper was acting alone, they might have been sensitive to new information that contradicted that key assumption. Often this type of information gets “lost in the noise” if the analyst has not already thought about what key assumptions he or she is making.

THE METHOD

Checking for key assumptions requires analysts to consider how their analysis depends on the validity of certain premises, which they do not routinely question or believe to be in doubt. A four-step process will help analysts:

1. Review what the current analytic line on this issue appears to be; write it down for all to see.

2. Articulate all the premises, both stated and unstated in finished intelligence, which are accepted as true for this analytic line to be valid.

3. Challenge each assumption, asking why it "must" be true and whether it remains valid under all conditions.

4. Refine the list of key assumptions to contain only those that "must be true" to sustain your analytic line; consider under what conditions or in the face of what information these assumptions might not hold.

QUESTIONS TO ASK DURING THIS PROCESS INCLUDE:

- How much confidence exists that this assumption is correct?
- What explains the degree of confidence in the assumption?
- What circumstances or information might undermine this assumption?
- Is a key assumption more likely a key uncertainty or key factor?
- Could the assumption have been true in the past but less so now?
- If the assumption proves to be wrong, would it significantly alter the analytic line? How?
- Has this process identified new factors that need further analysis?

QUALITY OF INFORMATION CHECK

Evaluates completeness and soundness of available information sources.

WHEN TO USE

Weighing the validity of sources is a key feature of any critical thinking. Moreover, establishing how much confidence one puts in analytic judgments should ultimately rest on how accurate and reliable the information base is. Hence, checking the quality of information used in intelligence analysis is an ongoing, continuous process. Having multiple sources on an issue is not a substitute for having good information that has been thoroughly examined. Analysts should perform periodic checks of the information base for their analytic judgments. Otherwise, important analytic judgments can become anchored to weak information, and any "caveats" attached to those judgments in the past can be forgotten or ignored over time.

If a major analytic assessment is planned, analysts should individually or collectively review the quality of their information and refresh their understanding of the strengths and weaknesses of past reporting on which an analytic line rests. Without understanding the context and conditions under which critical information has been provided, it will be difficult for analysts to assess the information's validity and establish a confidence level in an intelligence assessment.

VALUE ADDED

A thorough review of information sources provides analysts—as well as policymakers—with an accurate assessment of "what we know" and "what we do not know." It is also an opportunity to confirm that sources have been cited accurately. In the case of HUMINT, this will require extensive review of the sources' background information and access as well as his or her motivation for providing the information. Similarly, reviewing technical sourcing can sometimes reveal inadvertent errors in processing, translation, or interpretation that otherwise might have gone unnoticed.

In addition, a quality of information check can be valuable to both collectors and policymakers:

- It can help to detect possible deception and denial strategies by an adversary.
- It can identify key intelligence gaps and new requirements for collectors.
- It can assist policymakers in understanding how much confidence analysts are placing on analytic judgments.

THE METHOD

An analyst or a team might begin a quality of information check by developing a database in which information is stored according to source type and date, with additional notations indicating strengths or weaknesses in those sources.[4] Ideally, analysts would have a retrieval and search capability on the database, so that periodic reviews are less labor intensive and result in a more complete review of all sources used in past analysis. For the information review to be fully effective, analysts will need as much background information on sources as is feasible. Knowing the circumstances in which reporting was obtained is often critical to understanding its validity. With the data in hand, analysts can then:

- Review systematically all sources for accuracy.
- Identify information sources that appear most critical or compelling.
- Check for sufficient and strong corroboration of critical reporting.
- Reexamine previously dismissed information in light of new facts or circumstances that cast it in a different light.
- Ensure that any recalled reporting is identified and properly flagged for other analysts; analysis based on recalled reporting should also be reviewed to determine if the reporting was essential to the judgments made.
- Consider whether ambiguous information has been interpreted and caveated properly.
- Indicate a level of confidence that analysts can place in sources, which are likely to figure in future analytic assessments.

[4] Analysis of Competing Hypotheses (ACH), discussed later in the primer, is a useful technique for exploring the possibility that deception could explain the absence of evidence.

Quality of Information Problem on Iraq

". . . Analysts community wide are unable to make fully informed judgments on the information they received, relying instead on nonspecific source lines to reach their assessments. Moreover, relevant operational data is nearly always withheld from analysts, putting them at a further analytical disadvantage . . ."

—*Senate Select Committee on Intelligence, Report on the US Intelligence Community's Prewar Intelligence Assessments on Iraq*

"Analytic errors included over-reliance on a single, ambiguous source, [and, in addition to collection shortfalls] failure of analysts to understand fully the limitations of technical collection . . ."

"The Intelligence Community relied too heavily on ambiguous imagery indicators . . ."

—*Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction.*

INDICATORS OR SIGNPOSTS OF CHANGE

Periodically review a list of observable events or trends to track events, monitor targets, spot emerging trends, and warn of unanticipated change.

WHEN TO USE

An analyst or team can create an indicators or signposts list of observable events that one would expect to see if a postulated situation is developing; e.g., economic reform, military modernization, political instability, or democratization. Constructing the list might require only a few hours or as much as several days to identify the critical variables associated with the targeted issue. The technique can be used whenever an analyst needs to track an event over time to monitor and evaluate changes. However, it can also be a very powerful aid in supporting other structured methods explained later in this primer. In those instances, analysts would be watching for mounting evidence to support a particular hypothesis, low-probability event, or scenario.

When there are sharply divided views on an issue, an indicators or signposts list can also "depersonalize" the argument by shifting analytic attention to a more objective set of criteria. Using an indicators list can clarify substantive disagreements, once all sides agree on the set of objective criteria used to measure the topic under study.

VALUE ADDED

By providing an objective baseline for tracking events or targets, indicators instill rigor into the analytic process and enhance the credibility of analytic judgments. An indicators list included in a finished product also allows the policymaker to track developments and builds a more concrete case for the analytic judgments. By laying out a list of critical variables, analysts also will be generating hypotheses regarding why they expect to see the presence of such factors. In so doing, analysts make the analytic line much more transparent and available for scrutiny by others.

THE METHOD

Whether used alone, or in combination with other structured analysis, the process is the same:

- Identify a set of competing hypotheses or scenarios.
- Create separate lists of potential activities, statements, or events expected for each hypothesis or scenario.
- Regularly review and update the indicators lists to see which are changing.
- Identify the most likely or most correct hypotheses or scenarios, based on the number of changed indicators that are observed.

Developing two lists of indicators for each hypothesis or scenario may prove useful to distinguish between indicators that a development is or is not emerging. This is particularly useful in a "What If?" Analysis, when it is important to make a case that a certain event is unlikely to happen.

Tracking the Potential for Political Instability in a Foreign Country

Topics	Indicators	1999				2000		
		I	*II*	*III*	*IV*	*I*	*II*	*III*
Government Capacity	Quality of leadership/organizational capabilities	●	●	●	■	●	●	●
	Responsiveness to popular demands	●	●	●	●	●	●	●
	Ability to deliver basic goods and services							
	Internal Security Capabilities							
	Effectiveness of civil/criminal justice systems							
Legitimacy of Regime	Breadth and depth of political participation	●	●	●	●	●	●	●
	Perceived level of corruption	●	●	●	●	●	●	●
	Human rights violations	●	●	●	●	●	●	●
	Weakness of civil society							
	Pervasiveness of transnational criminal organizations							
	External support for government							
Opposition Activity	Ethnic/religious discontent	●	●	●	●	●	●	●
	Military discontent with civilian government	●	●	●	●	●	●	●
	Popular demonstrations/strikes/riots							
	Insurgent/separatist/terrorist group activity							
	External support for opposition							
	Threat of conflict with or in neighboring state							
Economic Factors	Weakness of domestic economy/unemployment/ inflation							
	Degree of income disparity							
	Capital flight							
	Decreased access to foreign funds							
	Reduced trade openness							
Environmental Issues	Extent of environmental degradation							
	Food/energy shortages							
	Ability to respond to natural disasters							

Presence of Trigger Mechanisms (▶ if present)							
Contested elections				▶			
Unpopular changes in food/energy prices			▶				
Sudden imposition of unpopular policies							
Coup plotting				▶			
Government mismanagement of natural disaster or national emergency							
Death of key figure							

■ Serious concern
● Substantial concern
● Moderate concern
● Low concern
● Negligible concern

Tracking the Potential for Political Instability in an Indicators Matrix. Analysts tracked the potential for regime change in 2000 and identified a list of indicators, to which they posed the question, "is this occurring or not? Analysts also went further and developed a list of "trigger mechanisms" that might bring about a political shift.

ANALYSIS OF COMPETING HYPOTHESES (ACH)

Identification of alternative explanations (hypotheses) and evaluation of all evidence that will disconfirm rather than confirm hypotheses.

WHEN TO USE

Analysis of Competing Hypotheses (ACH) has proved to be a highly effective technique when there is a large amount of data to absorb and evaluate. While a single analyst can use ACH, it is most effective with a small team that can challenge each other's evaluation of the evidence. Developing a matrix of hypotheses and loading already collected information into the matrix can be accomplished in a day or less. If the data must be reassembled, the initial phases of the ACH process may require additional time. Sometimes a facilitator or someone familiar with the technique can lead new analysts through this process for the first time.

ACH is particularly appropriate for controversial issues when analysts want to develop a clear record that shows what theories they have considered and how they arrived at their judgments. Developing the ACH matrix allows other analysts (or even policymakers) to review their analysis and identify areas of agreement and disagreement. Evidence can also be examined more systematically, and analysts have found that this makes the technique ideal for considering the possibility of deception and denial.

VALUE ADDED

ACH helps analysts overcome three common mistakes that can lead to inaccurate forecasts:

- Analysts often are susceptible to being unduly influenced by a first impression, based on incomplete data, an existing analytic line, or a single explanation that seems to fit well enough.
- Analysts seldom generate a full set of explanations or hypotheses at the outset of a project.
- Analysts often rely on evidence to support their preferred hypothesis, but which also is consistent with other explanations.

In essence, ACH helps analysts to avoid picking the first solution that seems satisfactory instead of going through all the possibilities to arrive at the very best solution.

THE METHOD

ACH demands that analysts explicitly identify all the reasonable alternative hypotheses, then array the evidence against each hypothesis—rather than evaluating the plausibility of each hypothesis one at a time. To create a level playing field, the process must:

- Ensure that all the information and argumentation is evaluated and given equal treatment or weight when considering each hypothesis.
- Prevent the analyst from premature closure on a particular explanation or hypothesis.
- Protect the analyst against innate tendencies to ignore or discount information that does not fit comfortably with the preferred explanation at the time.

To accomplish this, the process should follow these steps:

- Brainstorm among analysts with different perspectives to identify all possible hypotheses.
- List all significant evidence and arguments relevant to all the hypotheses.

- Prepare a matrix with hypotheses across the top and each piece of evidence on the side. Determine whether each piece of evidence is consistent, inconsistent, or not applicable to each hypothesis.[5]
- Refine the matrix and reconsider the hypotheses—in some cases, analysts will need to add new hypotheses and re-examine the information available.
- Focus on disproving hypotheses rather than proving one. Talley the pieces of evidence that are inconsistent and consistent with each hypothesis to see which explanations are the weakest and strongest.

[5] The "diagnostic value" of the evidence will emerge as analysts determine whether a piece of evidence is found to be consistent with only one hypothesis, or could support more than one or indeed all hypotheses. In the latter case, the evidence can be judged as unimportant to determining which hypothesis is more likely correct.

- Analyze how sensitive the ACH results are to a few critical items of evidence; should those pieces prove to be wrong, misleading, or subject to deception, how would it impact an explanation's validity?
- Ask what evidence is not being seen but would be expected for a given hypothesis to be true. Is denial and deception a possibility?
- Report all the conclusions, including the weaker hypotheses that should still be monitored as new information becomes available.
- Establish the relative likelihood for the hypotheses and report all the conclusions, including the weaker hypotheses that should still be monitored as new information becomes available.
- Identify and monitor indicators that would be both consistent and inconsistent with the full set of hypotheses. In the latter case, explore what could account for inconsistent data.

Terrorism in Tokyo From Aum Shinrikyo

		Weight	H: 1	H: 4	H: 2	H: 3
			Kooky Cult	Terrorist Group	Political Movement	Criminal Group
	Inconsistency Score ⇨		-1.0	-1.0	-2.0	-3.0
E3	Attacks on Journalists	MEDIUM	I	N	I	I
E2	Religious Affiliation	MEDIUM	C	I	I	I
E4	Established Party	MEDIUM	N	N	C	I
E1	Blind Leader Mastsumoto	MEDIUM	C	C	C	C

ACH Matrix of Terrorism in Tokyo. In March 1995, a largely unknown group attacked the Tokyo subways by using a highly lethal nerve agent known as sarin. ACH provides a mechanism to carefully examine all the evidence and possible explanations for understanding what type of group could have been responsible. In simplified form, the above matrix arrays each piece of evidence on the vertical axis and then evaluates each in terms of the item's consistency with four possible explanations for the terrorist attack in Tokyo (horizontal axis). Analysts rate a piece of evidence as consistent (C); inconsistent (I); or neutral (N). This process allows analysts to see that some evidence will be consistent with more than one hypothesis and be less valuable in disproving hypotheses.

DEVIL'S ADVOCACY

Challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation.

WHEN TO USE

Devil's Advocacy is most effective when used to challenge an analytic consensus or a key assumption regarding a critically important intelligence question. On those issues that one cannot afford to get wrong, Devil's Advocacy can provide further confidence that the current analytic line will hold up to close scrutiny. An individual analyst can often assume the role of the Devil's Advocate if he or she has some doubts about a widely held view, or a manager might designate a courageous analyst to challenge the prevailing wisdom in order to reaffirm the group's confidence in those judgments. In some cases, the analyst or a team can review a key assumption of a critical judgment in the course of their work, or more likely, a separate analytic product can be generated that arrays all the arguments and data that support a contrary hypothesis. While this can involve some analytic time and effort, when a group of analysts have worked on an issue for a long period of time, it is probably wise to assume that a strong mind-set exists that deserves the closer scrutiny provided by Devil's Advocacy.

VALUE ADDED

Analysts have an obligation to policymakers to understand where their own analytic judgments might be weak and open to future challenge. Hence, the Devil's Advocacy process can highlight weaknesses in a current analytic judgment or alternatively help to reaffirm one's confidence in the prevailing judgments by:

- Explicitly challenging key assumptions to see if they will not hold up under some circumstances.
- Identifying any faulty logic or information that would undermine the key analytic judgments.
- Presenting alternative hypotheses that would explain the current body of information available to analysts.

Its primary value is to serve as a check on a dominant mind-set that can develop over time among even the best analysts who have followed an issue and formed strong consensus that there is only one way of looking at their issue. This mind-set phenomenon makes it more likely that contradictory evidence is dismissed or not given proper weight or consideration. An exercise aimed at highlighting such evidence and proposing another way of thinking about an issue can expose hidden assumptions and compel analysts to review their information with greater skepticism about their findings. The analyst could come away from the exercise more certain that: 1) the current analytic line was sound; 2) the argument is still the strongest, but that there are areas where further analysis is needed; or 3) some serious flaws in logic or supporting evidence suggest that the analytic line needs to be changed or at least caveated more heavily.

THE METHOD

To challenge the prevailing analytic line, the Devil's Advocate must:

- Outline the mainline judgment and key assumptions and characterize the evidence supporting that current analytic view.
- Select one or more assumptions—stated or not—that appear the most susceptible to challenge.
- Review the information used to determine whether any is of questionable validity, whether deception is possibly indicated, or whether major gaps exist.

- Highlight the evidence that could support an alternative hypothesis or contradicts the current thinking.

- Present to the group the findings that demonstrate there are flawed assumptions, poor quality evidence, or possible deception at work.

- Consider drafting a separate contrarian paper that lays out the arguments for a different analytic conclusion if the review uncovers major analytic flaws.

- Be sure that any products generated clearly lay out the conventional wisdom and are identified as an explicitly "Devil's Advocate" project; otherwise, the reader can become confused as to the current official view on the issue.

TEAM A/TEAM B

Use of separate analytic teams that contrast two (or more) strongly held views or competing hypotheses.

WHEN TO USE

A Team A/Team B approach is different from Devil's Advocacy, where the purpose is to challenge a single dominant mind-set. Instead, Team A/Team B recognizes that there may be competing and possibly equally strong mind-sets held on an issue that need to be clarified. Sometimes analysts confuse the two techniques by drafting a Team B exercise that is really a Devil's Advocacy exercise.

If there are at least two competing views within an analytic office or perhaps competing opinions within the policymaking community on a key issue, then Team A/Team B analysis can be the appropriate technique to use. Developing a full-blown Team A/Team B exercise requires a significant commitment of analytic time and resources, so it is worthwhile considering if the analytic issue merits this kind of attention.

A longstanding policy issue, a critical decision that has far-reaching implications, or a dispute within the analytic community that has obstructed effective cross-agency cooperation would be grounds for using Team A/Team B. If those circumstances exist, then analysts will need to review all of the data to develop alternative papers that can capture the essential differences between the two viewpoints.

VALUE ADDED

Managers have found that when there are office tensions among competing factions of analysts, a Team A/Team B approach can help opposing experts see the merit in the other group's perspective. The process of conducting such an exercise can reduce the friction and even narrow the differences. At a minimum, it allows those holding opposing views to feel that their views have been given equal attention.

For the policymaker, this technique helps to surface and explain important analytic differences within the expert community. Often senior officials can learn more by weighing well-argued conflicting views than from reading an assessment that masks substantive differences or drives analysis to the lowest common denominator. By making the key assumptions and information used for each argument more transparent, a policymaker can judge the merits of each case, pose questions back to the analysts, and reach an independent judgment on which argument is the strongest. Moreover, highlighting alternative views puts collectors on notice that they need to be searching for new information that can confirm or disconfirm a range of hypotheses.

If opposing positions are well established, it can be useful to place analysts on teams that will advocate positions they normally do not support; forcing analysts to argue "the other side" can often make them more aware of their own mind-set.

A Team A/Team B View: China's Military

A: *China's Hollow Military* by Bates Gill and Michael O'Hanlon	B: *China's Military: A Second Opinion* by James Lilley and Carl Ford
". . . We believe that the recent clamor over China's strategic ambitions is greatly overblown. Most of the Chinese aims that run counter to US interests are in fact not global or ideological but territorial in nature and confined primarily to the islands and waterways to China's south and southeast . . . An enormous gap separates China's military capabilities from its aspirations. The PRC's armed forces are not very good and not getting better very fast. Whatever China's concerns and intentions, its capacity to act upon them in ways inimical to US interests is severely limited, and will remain so for many years . . . The PRC's power projection capabilities, too, are constrained by huge weaknesses–especially in areas such as aerial refueling, electronic warfare, command and control and amphibious and air assault assets. China owns considerably less top-level equipment than medium powers like Japan and Britain; it owns even less than smaller powers such as Italy, South Korea or The Netherlands . . . The resources it devotes to acquiring modern weaponry are akin to those of countries spending $10-20 billion a year on defense . . ."	". . . We think they got it half right. China is no military superpower and will not acquire that status for some years to come. But measured in terms of its capacity to challenge key US allies in East Asia, China's capabilities have grown exponentially . . . By emphasizing direct comparisons between the defense capabilities of the United States and the PRC, the authors create an artificial and misleading construct . . . What the regime gives every indication of striving for is sufficient military clout to achieve its aims in Asia. In the short term, it wishes to intimidate Taiwan sufficiently to bring about unification on Beijing's terms . . . . . . Investments of the sort Beijing is making can mean only one thing: China is determined to improve the PLA's fighting capability. While most nations are reducing defense expenditures in the post–Cold War era, China is one of the few doing the opposite . . . Across the board, the PLA is engaged in a major spending effort to upgrade weapons and equipment and improve its operational capability. According to the Pentagon, these efforts have already enhanced China's ability to project military power . . ."

—Excerpted from journal articles found in The National Interest, Fall and Winter 2000/2001.

THE METHOD

Analysis Phase. A Team A/Team B exercise can be conducted on an important issue to:

- Identify the two (or more) competing hypotheses or points of view.
- Form teams or designate individuals to develop the best case that can be made for each hypothesis.
- Review all pertinent information that supports their respective positions.
- Identify missing information that would buttress their hypotheses.
- Structure each argument with an explicit presentation of key assumptions, key pieces of evidence, and careful articulation of the logic behind the argument.

Debate Phase. An oral presentation of the alternative arguments and rebuttals in parallel fashion can then be organized for the benefit of other analysts:

- Set aside time for an oral presentation of the alternative team findings; this can an informal brainstorming session or a more formal "debate."
- Have an independent "jury of peers" listen to the oral presentation and be prepared to question the teams regarding their assumptions, evidence, or logic.
- Allow each team to present their case, challenge the other team's arguments, and rebut the opponent's critique of its case.
- Let the jury consider the strength of each presentation and recommend possible next steps for further research and collection efforts.

HIGH-IMPACT/LOW-PROBABILITY ANALYSIS

Highlights a seemingly unlikely event that would have major policy consequences if it happened.

WHEN TO USE

High-Impact/Low-Probability Analysis is a contrarian technique that sensitizes analysts to the potential impact of seemingly low probability events that would have major repercussions on US interests. Using this technique is advisable when analysts and policymakers are convinced that an event is unlikely but have not given much thought to the consequences of its occurrence. In essence, this can be a warning that the intelligence and policy communities must be alert to an unexpected but not impossible event. For example, the fall of the Shah, the collapse of the Soviet Union, and the reunification of Germany were all considered low probability events at one time; however, analysts might have benefited from considering the consequences of such events and how they might plausibly have come about.

VALUE ADDED

Mapping out the course of an unlikely, yet plausible, event can uncover hidden relationships between key factors and assumptions; it also can alert analysts to oversights in the mainstream analytic line. In addition, an examination of the "unthinkable" allows analysts to develop signposts that may provide early warning of a shift in the situation. By periodically reviewing these indicators an analyst is more likely to counter any prevailing mind-set that such a development is highly unlikely.

THE METHOD

If there is a strongly held view that an event is unlikely, then postulating precisely the opposite should not be difficult.

- Define the high-impact outcome clearly. This process is what will justify examining what most analysts believe to be a very unlikely development.
- Devise one or more plausible explanations for or "pathways" to the low probability outcome. This should be as precise as possible, as it can help identify possible indicators for later monitoring.
- Insert possible triggers or changes in momentum if appropriate. These can be natural disasters, sudden health problems of key leaders, or new economic or political shocks that might have occurred historically or in other parts of the world.
- Brainstorm with analysts having a broad set of experiences to aid the development of plausible but unpredictable triggers of sudden change.
- Identify for each pathway a set of indicators or "observables" that would help you anticipate that events were beginning to play out this way.
- Identify factors that would deflect a bad outcome or encourage a positive outcome.

High Impact of a Low-Probability Event: Pearl Harbor

". . . So far as relations directly between the United States and Japan are concerned, there is less reason today than there was a week ago for the United States to be apprehensive lest Japan make "war" on this country.

Were it a matter of placing bets, the undersigned would give odds of five to one that the United States and Japan will not be at "war" on or before December 15; would wager three to one that the United States and Japan will not be at 'war' on or before the 15th of January (i.e, seven weeks from now); would wager even money that the United States and Japan will not be at "war" on or before March 1 (a date more than 90 days from now) . . ."

—State Department Special Assessment, 27 November 1941

High-Impact/Low-Probability Analysis on 9/11

The 9/11 Commission report includes examination of speculative analysis that was provided to senior policymakers highlighting what were thought to be highly unlikely scenarios that would have a very high impact. One of those items was the 6 August 2001 President's Daily Brief, which stated:

Al-Qai'da members—including some who are US citizens—have resided in or traveled to the US for years, and the group apparently maintains a support structure that could aid attacks. Two al-Qai'da members found guilty in the conspiracy to bomb our embassies in East Africa were US citizens, and a senior EIJ [Egyptian Islamic Jihad] member lived in California in the mid-1990s.

- A clandestine source said in 1998 that a Bin Ladin cell in New York was recruiting Muslim-American youth for attacks.

We have not been able to corroborate some of the more sensational threat reporting, such as that from a service in 1998 saying that Bin Ladin wanted to hijack a US aircraft to gain the release of "Blind Shaykh" 'Umar Abd al-Rahman and other US-held extremists.

—9/11 Commission Report, declassified and approved for release 10 April 2004.

"WHAT IF?" ANALYSIS

Assumes that an event has occurred with potential (negative or positive) impact and explains how it might come about.

WHEN TO USE

"What If?" analysis is another contrarian technique for challenging a strong mind-set that an event will not happen or that a confidently made forecast may not be entirely justified. It is similar to a High-Impact/Low-Probability analysis, but it does not dwell on the consequences of the event as much as it accepts the significance and moves directly to explaining how it might come about.

VALUE ADDED

By shifting the focus from whether an event could occur to how it may happen, analysts allow themselves to suspend judgment about the likelihood of the event and focus more on what developments—even unlikely ones—might enable such an outcome. An individual analyst or a team might employ this technique and repeat the exercise whenever a critical analytic judgment is made.

Using this technique is particularly important when a judgment rests on limited information or unproven assumptions. Moreover, it can free analysts from arguing about the probability of an event to considering its consequences and developing some indicators or signposts for its possible emergence. It will help analysts address the impact of an event, the factors that could cause—or alter—it, and likely signposts that an event is imminent.

A "What If?" analysis can complement a difficult judgment reached and provide the policymaker a thoughtful caution to accepting the conventional wisdom without considering the costs and risks of being wrong. This can help decision-makers consider ways to hedge their bets, even if they accept the analytic judgment that an event remains unlikely.

THE METHOD

Like other contrarian methods, "What If?" analysis must begin by stating clearly the conventional analytic line and then stepping back to consider what alternative outcomes are too important to dismiss, even if unlikely. Brainstorming over a few days or weeks can develop one or more plausible scenarios by which the unlikely event occurs:

- Assume the event has happened.
- Select some triggering events that permitted the scenario to unfold to help make the "what if" more plausible; for example, analysts might postulate the death of a leader, a natural disaster, or some economic event that would start a chain of other events.
- Develop a chain of argumentation based as much on logic as evidence to explain how this outcome could have come about.
- "Think backwards" from the event in concrete ways–that is, specifying what must actually occur at each stage of the scenario is often very useful.
- Identify one or more plausible pathways or scenarios to the unlikely event; very often more than one will appear possible.
- Generate a list of indicators or "observables" for each scenario that would help to detect the beginnings of the event.
- Consider the scope of the positive and negative consequences of each scenario and their relative impacts.
- Monitor the indicators developed on a periodic basis.

"What If?" Analysis: An Unlikely Outcome in Yugoslavia, 1990.

The possibility of muddling through is very low. In the unlikely event that it happens, this is what it would look like.

Memories of the internecine civil war during World War II and fear of another destructive conflict would lead the two most numerous South Slav people—Serbs and Croats—to reach some political accommodation. A compromise that preserves Yugoslavia would include:

- Basic principles:
  - -No change in existing Republic borders.
  - -No change in Yugoslavia's existing international status.
  - -Mutually recognized sovereignty of each republic

- Confederal institutions:
  - -A single foreign ministry, to which diplomatic representatives would be accredited.
  - -A central military organization with a joint General Staff responsible for planning.
  - -A central bank, determining macroeconomic policy, a common currency,

- Powers reserved to republics.
  - -Veto over actions of the Confederal Authority.
  - -Control of internal security, including guarantee of minority rights.
  - -Operational control over some or all military units stationed on the republic's territory.
  - -Raising taxes and allocating funds to discharge mutually agreed confederal responsibilities.

Only the Serbs can open the door to a confederal Yugoslavia, and Serbia's leader, Slobodan Milosevic, holds the key. Some observers felt there are pressures on him to try. If he does not, he would give his opponents the leverage to remove him. The potential penalties of failure to compromise would be too great, in this view, for the peoples and leaders of Yugoslavia to forgo every effort to find a compromise.

—*Excerpts from the declassified* NIE: Prospects for Yugoslavia*, October 1990.*

BRAINSTORMING

An unconstrained group process designed to generate new ideas and concepts.

WHEN TO USE

Brainstorming is a widely used technique for stimulating new thinking and it can be applied to virtually all of the other structured analysis techniques as an aid to thinking. Typically, analytic will brainstorm when they begin a project to help generate a range of hypotheses about their issue.

Brainstorming, almost by definition, involves a group of analysts meeting to discuss a common challenge; a modest investment of time at the beginning or critical points of a project can take advantage of their different perspectives to help structure a problem. This group process allows others to build on an initial idea suggested by a member of the brainstorming session.

An individual analyst also can brainstorm to produce a wider range of ideas than a group might generate, without regard for other analysts' egos, opinions, or objections. However, an individual will not have the benefit of others' perspectives to help develop the ideas as fully. Moreover, an individual may have difficulty breaking free of his or her cognitive biases without the benefit of a diverse group.

VALUE ADDED

This technique can maximize creativity in the thinking process, force analysts to step outside their normal analytic mind-sets, and suspend their typical "good judgment" about the practicality of ideas or approaches. More generally, brainstorming allows analysts to see a wider range of factors that might bear on the topic than they would otherwise consider. Analysts typically censor out ideas that seem farfetched, poorly sourced, or seemingly irrelevant to the question at hand. Brainstorming gives permission to think more radically or "outside the box." In particular, it can spark new ideas, ensure a comprehensive look at a problem or issues, raise unknowns, and prevent premature consensus around a single hypothesis.

THE METHOD

Paradoxically, brainstorming should be a very structured process to be most productive. An unconstrained, informal discussion might produce some interesting ideas, but usually a more systematic process is the most effective way to break down mind-sets and produce new insights. In particular, the process involves a divergent thinking phase to generate and collect new ideas and insights, followed by a convergent phase in which ideas are grouped and organized around key concepts. Some of the simple rules to be followed include:

- Never censor an analyst's ideas no matter how unconventional they might sound.
- Rather find out what prompted the thought, as it might contain the seeds of an important connection between the topic and an unstated assumption.
- Give yourself enough time to do brainstorming correctly. It usually takes one hour to set the "rules" of the game, get the group comfortable, and exhaust the conventional wisdom on the topic. Only then will the truly creative ideas begin to emerge.
- Involve at least one "outsider" in the process—that is, someone who does not share the same educational background, culture, technical knowledge or mind-set as the core group but has some familiarity with the topic.

A two-phase, twelve-step, structured process is often used to get the most out of the brainstorming sessions:

Brainstorming and Divergent Thinking: Perspectives of an Experienced Practitioner

". . . First, leave rank at the door and focus on "a democracy of ideas." Thoughts from experts, senior officers, and supervisors are of course, valuable and welcome, but such experts are not permitted to cut off debate by citing their seniority. In fact, it pays to invite junior officers as well as senior ones who are not involved directly in working the issue under discussion. Some of the most creative ideas at brainstorming sessions frequently come from relatively junior people who can look at a problem with fresh perspective, or from senior ones who are not experts on the issue.

Second, make sure there is no official analytic line. One of the most significant blocks to new thinking is the presence of a long held analytic line that analysts—and even more so managers—are reluctant to change. Rather than trying to fit ideas into the framework of "what we've said before," analysts need to feel free to go wherever bits of the evidence and informed supposition take them. They must feel free to throw out seemingly strange but plausible ideas that might be based on historical precedent and instinct rather than on concrete information. Facilitators can stimulate this process by deliberately posing an alternative outcome to a problem that differs starkly from the accepted analysis or by proposing a contrary way to think about an issue.

Third, don't permit killer phrases like "that would not work" or "that could not happen" to be voiced out loud. Effective brainstorming starts with ideas and possibilities, not with practicalities and self-imposed obstacles to fresh perspectives. Force the group to get as wide a range of ideas out for discussion as possible. At some point, a set of ideas might be winnowed down and subject to tests of workability, but that comes later—not during brainstorming.

Fourth, keep the brainstorming session to no more than 90 minutes. There is no hard and fast rule, but somewhere between 60 and 90 minutes, the idea stream starts to dry up, people repeat themselves, and jokes replace creative ideas.

Fifth, record ideas in a visible way. Lots of people take notes at brainstorming sessions for their own use, and that is good. We have found it valuable to have someone jot down the ideas presented on large paste-a-note sheets that we put on the walls. This allows participants in brainstorming sessions to react to ideas generated earlier. Moreover, analysts are encouraged to participate in such exercises if they see their own ideas put down in writing. Having a notional record of brainstorming also helps the analyst who ends up writing a report based on the discussion. Ideas that may not be used in one report are invariably put to use later, so it is good to have a record of them . . ."

Divergent Thinking Phase:

- Distribute “Post-It” notes and pens or markers to all participants. Typically, 10-12 people works best.
- Pose the problem in terms of a “focal question.” Display it in one sentence on a large easel or whiteboard.
- Ask the group to write down responses to the question, using key words that will fit on the small “Post-It” note.
- Stick all the notes on a wall for all to see—treat all ideas the same.
- When a pause follows the initial flow of ideas, the group is reaching the end of their conventional thinking and the new divergent ideas are then likely to emerge.
- End the “collection stage” of the brainstorming after two or three pauses.

Convergent Thinking Phase:

- Ask the participants as a group to rearrange the notes on the wall according to their commonalities or similar concepts. No talking is permitted. Some notes may be moved several times as notes begin to cluster. Copying some notes is permitted to allow ideas to be included in more than one group.
- Select a word or phrase that characterizes each grouping or cluster once all the notes have been arranged.
- Identify any notes that do not easily fit with others and consider them either useless noise or the beginning of an idea that deserves further attention.
- Assess what the group has accomplished in terms of new ideas or concepts identified or new areas that need more work or further brainstorming.
- Instruct each participant to select one or two areas that deserve the most attention. Tabulate the votes.
- Set the brainstorming group’s priorities based on the voting and decide on the next steps for analysis.

OUTSIDE-IN THINKING

Used to identify the full range of basic forces, factors, and trends that would indirectly shape an issue.

WHEN TO USE

Analysts find this technique most useful at the conceptualization of an analytic project, when the goal is to identify all the critical, external factors that could influence how a particular situation will develop. It would work well for a group of analysts responsible for a range of functional and/or regional issues. When assembling a large database that must identify a number of information categories or database fields, this technique can aid in visualizing the entire set of categories that might be needed in a research effort. Often analysts realize only too late that some additional information categories will be needed and then must go back and review all previous files and recode the data. With a modest amount of effort, "Outside-in Thinking" can reduce the risk of missing important variables early in the analytic process.

VALUE ADDED

Most analysts spend their time concentrating on familiar factors within their field or analytic issue. That is, they think from the "inside"—namely, what they control—out to the broader world. Conversely, "thinking from the outside-in" begins by considering the external changes that might, over time, profoundly affect the analysts' own field or issue. This technique encourages analysts to get away from their immediate analytic tasks (the so-called "inbox") and think about their issues in a wider conceptual and contextual framework. By recasting the problem in much broader and fundamental terms, analysts are more likely to uncover additional factors, an important dynamic, or a relevant alternative hypothesis.

THE METHOD

The process begins by developing a generic description of the problem or the phenomenon under study. Then, analysts should:

- List all the key forces (social, technological, economic, environmental, and political) that could have an impact on the topic, but over which one can exert little influence (e.g., globalization, social stress, the Internet, or the global economy).
- Focus next on key factors over which an actor or policymaker can exert some influence. In the business world this might be the market size, customers, the competition, suppliers or partners; in the government domain it might include the policy actions or the behavior of allies or adversaries.
- Assess how each of these forces could affect the analytic problem.
- Determine whether these forces actually do have an impact on the particular issue based on the available evidence.

RED TEAM ANALYSIS

Models the behavior of an individual or group by trying to replicate how an adversary would think about an issue.

WHEN TO USE

Frequently, analysts face the challenge of forecasting how a foreign leader or decisionmaking group may behave when it is clear that there is a risk of falling into a "mirror-image" problem. That is, analysts can sometimes impute to a foreign actor the same motives, values, or understanding of an issue that they hold. Traditional analysis sometimes assumes that foreign leaders or groups will behave "rationally" and act as the analysts would if faced with the same threats or opportunities. History has shown that foreign leaders often respond differently to events because of different cultural, organizational, or personal experiences.

Red Team analysis tries to consciously place analysts in the same cultural, organizational, and personal setting ("putting them in their shoes") in which the target individual or group operates. Whereas analysts normally work from the position of the "blue" (friendly forces), a "red" team of analysts attempts to work in the environment of the hostile forces.

VALUE ADDED

Like Devil's Advocacy and Team A/Team B techniques, Red Team analysis is aimed at freeing the analyst from the prison of a well-developed mind-set; in this case, the analyst's own sense of rationality, cultural norms, and personal values. Whereas analysts usually operate as "observers" of a foreign adversary, the Red Team technique transforms the analyst into an "actor" operating within the adversary's culture and political milieu. This form of "role playing" is useful when trying to replicate the mind-set of authoritarian leaders, terrorist cells, or other non-Western groups that operate under very different codes of behavior or motivations. Often this technique can introduce new or different stimuli that might not have been factored into traditional analysis—such as the target's familial ties or the international political, economic, and military pressures felt by the individual. For example, Red Team participants might ask themselves: "What would my peers, family, or tribe expect me to do? Alternatively, a Red Team analyst might pose the question to his colleagues: "How do we perceive the external threats and opportunities?" Finally, the Red Team technique can factor into its analysis the way in which personal power and status might influence a target's behavior.

THE METHOD

On issues that lend themselves to Red Team analysis, a manager needs to build a team of experts with in-depth knowledge of the operating environment, the target's personality, and the style of thinking used. The team should be populated not just with those who understand the language, but also with people who might have experienced the culture, share the ethnic background, or have worked in a similar operational environment. Once established and separated from traditional analysis, the team members should:

- Put themselves in the adversary's circumstances and react to foreign stimuli as the target would.
- Develop a set of "first-person" questions that the adversary would ask, such as: "How would I perceive incoming information; what would be my personal concerns; or to whom would I look for an opinion?"
- Draft a set of policy papers in which the leader or group makes specific decisions, proposes recommendations, or lays out courses of actions. The more these papers reflect the cultural and personal norms of the target, the more they can offer a different perspective on the analytic problem.

A Red Team Perspective
Iran's Military Strategy Vis-a-vis the United States

". . . The United States and Israel may be contemplating military operations against Iran, as per recent media reports . . . A week-long combined air and ground maneuver has just concluded in five of the southern and western provinces of Iran, mesmerizing foreign observers, who have described as 'spectacular' the massive display of high-tech, mobile operations, including rapid-deployment forces relying on squadrons of helicopters, air lifts, missiles, as well as hundreds of tanks and tens of thousands of well-coordinated personnel using live munitions.

Learning from both the 2003 Iraq war and Iran's own previous experiences of the 1980-88 war with Iraq and the 1987-88 confrontation with US forces in the Persian Gulf, Iranians have focused on the merits of a fluid and complex defensive strategy that seeks to take advantage of certain weaknesses in the US military superpower while maximizing the precious few areas where they may have the upper hand, e.g.; numerical superiority in ground forces, guerrilla tactics, terrain, etc.

Any US attack on Iran will likely be met first and foremost by missile counter-attacks engulfing the southern Persian Gulf states playing host to US forces, as well as any other country—e.g., Azerbaijan, Iraq, or Turkey allowing their territory or airspace to be used against Iran. The rationale for this strategy is precisely to pre-warn Iran's neighbors of the dire consequences, with potential debilitating impacts on their economies for a long time, should they become accomplices of foreign invaders of Iran.

Another key element of Iran's strategy is to "increase the arch of crisis" in places such as Afghanistan and Iraq, where it has considerable influence, to undermine the United States' foothold in the region, hoping to create a counter-domino effect wherein instead of gaining inside Iran, the US would actually lose territory partly as a result of thinning its forces and military 'overreach.'

Iran's counter-psychological warfare, on the other hand, seeks to take advantage of the 'death-fearing' American soldiers who typically lack a strong motivation to fight wars not necessarily in defense of the homeland. A war with Iran would definitely require establishing the draft in the US, without which it could not possibly protect its flanks in Afghanistan and Iraq.

There is a sense of national-security siege in Iran these days, in light of a tightening "security belt" by the US benefiting from military bases in Iraq, Turkey, Azerbaijan, Uzbekistan, Tajikistan, Kyrgyzstan, as well as Kuwait, Saudi Arabia, Qatar, Bahrain, Oman, and the island-turned garrison of Diego Garcia. From Iran's vantage point, the US, having won the Cold War, has turned into a 'leviathan unhinged' capable of manipulating and subverting the rule of international law and the United Nations with impunity, thus requiring a sophisticated Iranian strategy of deterrence, that, in the words of certain Iranian media pundits, would even include the use of nuclear weapons . . ."

—Excerpts from Kaveh L. Afrasiabi (Tehran University), "How Iran Will Fight Back," cited in Asia Times Online Ltd., 2004.

Red Team analysis is not easy to conduct. It requires significant time to develop a team of qualified experts who can think like the adversary. The team has to distance itself from the normal analysis and work as though living in the target's world. Without a sophisticated understanding of the culture, operational environment, and personal histories of the foreign group, analysts will not be able to behave or think like the enemy. Analysts can never truly escape their own experiences and mind-sets, but this technique can at least prevent them from falling into "mirror-imaging" unconsciously.

The most novel feature of Red Team analysis is its presentation.

- The analysis is often in a "first person" format—that is, drafted as memos to or from a leader or group.
- Red Team analysis avoids the use of caveats or qualifications and assumes that the recipient understands that the paper is aimed more at provoking thought or challenging the conventional understanding of how an adversary thinks.
- Such papers are rarely coordinated among other experts and do not purport to represent the consensus view on an issue.

Red Team papers do not plot out all possible courses of action but seek to give a prediction based on the target's special personal, organizational, or cultural experiences.

ALTERNATIVE FUTURES ANALYSIS

Systematically explores multiple ways a situation can develop when there is high complexity and uncertainty.

WHEN TO USE

Alternative futures analysis (often referred to as "scenarios") is most useful when a situation is viewed as too complex or the outcomes as too uncertain to trust a single outcome assessment. First, analysts must recognize that there is high uncertainty surrounding the topic in question. Second, they, and often their customers, recognize that they need to consider a wide range of factors that might bear on the question. And third, they are prepared to explore a range of outcomes and are not wedded to any preconceived result. Depending on how elaborate the futures project, the effort can amount to considerable investment in time, analytic resources, and money. A team of analysts can spend several hours or days organizing, brainstorming, and developing multiple futures; alternatively, a larger-scale effort can require preparing a multi-day workshop that brings together participants (including outside experts). Such an undertaking often demands the special skills of trained scenario-development facilitators and conferencing facilities.

This technique is a sharp contrast to contrarian techniques, which try to challenge the analysts' high confidence and relative certitude about an event or trend. Instead, multiple futures development is a divergent thinking technique that tries to use the complexity and uncertainty of a situation to describe multiple outcomes or futures that the analyst and policymaker should consider, rather than to predict one outcome.

VALUE ADDED

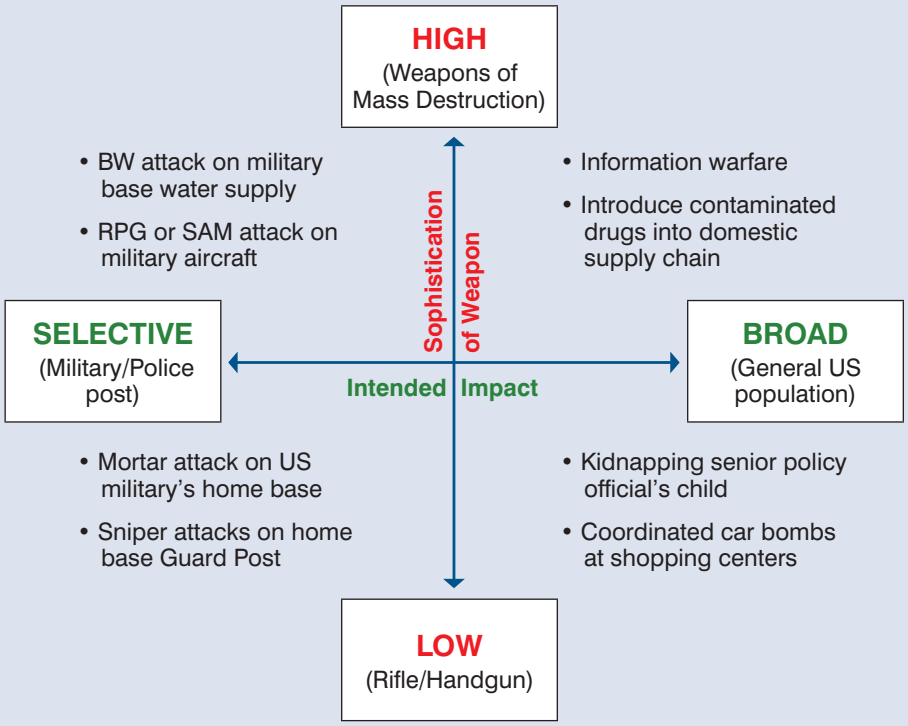
Alternative futures analysis is extremely useful in highly ambiguous situations, when analysts confront not only a lot of "known unknowns" but also "unknown unknowns." What this means is that analysts recognize that there are factors, forces, and dynamics among key actors that are difficult to identify without the use of some structured technique that can model how they would interact or behave. As the outcomes are not known prior to the futures exercise, analysts must be prepared for the unexpected and willing to engage in a more free-wheeling exchange of views than typically occurs in order to "imagine the future." Given the time and resources involved, scenario analysis is best reserved for situations that could potentially pose grave threats or otherwise have significant consequences.

From past experience, analysts have found that involving policymakers in the alternative futures exercise is the most effective way to communicate the results of this exploration of alternative outcomes and sensitize them to key uncertainties. Most participants find the process of developing such scenarios as useful as any finished product that attempts to capture the results of the exercise. Analysts and policymakers can benefit from this technique in several ways:

- It provides an effective means of weighing multiple unknown or unknowable factors and presenting a set of plausible outcomes.
- It can help to bound a problem by identifying plausible combinations of uncertain factors.
- It provides a broader analytic framework for calculating the costs, risks, and opportunities presented to policymakers by different outcomes.

> *"The future is plural."*
>
> —Peter Schwartz, author of *The Art of the Long View* and a widely acclaimed scenario developer.

Hypothetical Threats to the Homeland: Using Spectrums to Define Potential Targets



A Futures Exercise. The graphic captures four potential futures to understand how foreign insurgents might carry out an attack on the United States. A brainstorming exercise helped analysts identify two key uncertainties (the sophistication of weapons used by the insurgents and the intended impact of the attack) and arrayed these factors on a graph as the "x" and "y" axes. The four resulting quadrants in the 2 x 2 matrix allowed analysts to visualize potential targets from the various combinations (low to high sophistication of weapons and selective to broad intended impact of an attack). For example, if a group possessed highly sophisticated weapons and intended a broad attack on the United States, potential targets could include computer networks and domestic drug supplies. Having filled in a quadrant, analysts can then turn to devising likely indicators or signposts of such a future.

- It aids analysts and policymakers in anticipating what otherwise would be surprising developments by forcing them to challenge assumptions and consider possible "wild cards" or discontinuous events.

- It generates indicators to monitor for signs that a particular future is becoming more or less likely, so that policies can be reassessed.

THE METHOD

Although there are a variety of ways to develop alternative futures, the most common approach used in both the public and private sectors involves the following steps:

- Develop the "focal issue" by systematically interviewing experts and officials who are examining the general topic.

- Convene a group of experts (both internal and external) to brainstorm about the forces and factors that could affect the focal issue.

- Select by consensus the two most critical and uncertain forces and convert these into axes or continua with the most relevant endpoints assigned.

- Establish the most relevant endpoints for each factor; e.g., if economic growth were the most critical, uncertain force, the endpoints could be "fast" and "slow" or "transformative" and "stabilizing" depending on the type of issue addressed.

- Form a futures matrix by crossing the two chosen axes. The four resulting quadrants provide the basis for characterizing alternative future worlds.

- Generate colorful stories that describe these futures and how they could plausibly come about. Signposts or indicators can then be developed.

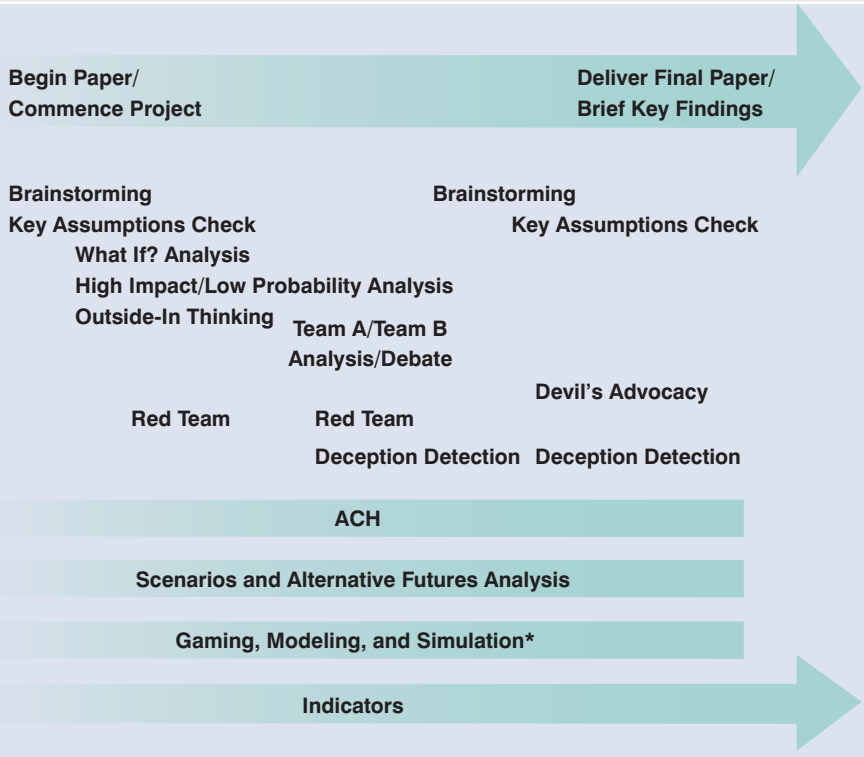
Participants, especially policymakers, can then consider how current decisions or strategies would fare in each of the four worlds and identify alternative policies that might work better either across all the futures or in specific ones. By anticipating alternative outcomes, policymakers have a better chance of either devising strategies flexible enough to accommodate multiple outcomes or of being prepared and agile in the face of change.

These structured analytic techniques can be used in a variety of ways when analysts begin a new assessment. Some can be used equally effectively at multiple points in the process and can promote an analyst's ability to keep an open mind, to consider multiple—including highly unlikely—hypotheses, to challenge conventional wisdom, and to assess the impact of important information gaps or deception on analytic judgments and confidence levels. The Timeline for Using Analytic Techniques provides some thoughts on when to use one or more of them during the course of an analyst's research and writing.

Starting Out

At the beginning of an analytic project, analysts are always wise to consider brainstorming and assumptions checks to insure that important factors are not being missed or taken for granted. Similarly, outside-in-thinking can sometimes put an analytic project into a broader international context, in which factors outside the lead analyst's area of responsibility might impact on his or her analytic judgments. For instance, economic assumptions about the price of oil might be key to a regional political analyst's understanding the prospects for political stability in an oil-exporting

A Timeline for Using Analytic Techniques Throughout an Analytic Project



*Gaming, Modeling, and Simulation are among the more sophisticated techniques taught in a more advanced analytic methods course and usually require substantial commitments of analyst time and corporate resources.

country or a underdeveloped country entirely dependent on expensive energy imports. A High Impact/Low Probability assessment can also sensitize analysts early on to the significance of dramatic events that might affect their analytic lines.

Some techniques like Indicators and Signposts or Analysis of Competing Hypotheses (ACH) can be useful throughout a project and revisited periodically as new information is absorbed and analyzed. ACH, in particular, is a good tool to use throughout a project to prevent premature closure and to highlight evidence that is most "discriminating" in making an analytic argument. Alternative Futures analysis is similarly useful at the beginning of a project, but can amount to the structure for the entire project.

Hypothesis Testing

As an analytic project takes shape, and hypotheses are being formed about the key intelligence question, it can be appropriate to use one or another contrarian technique to challenge the conventional analytic line that is being developed. If the assessment contains strong judgments about an adversary's behavior, then challenging this view with a "Red Team" effort might be a good corrective to too much of a rational actor approach. Also, a review of intelligence gaps at this juncture can also help give the analysts a better degree of confidence in the information base and judgments reached in the assessment.

A Final Check

As the assessment is being finalized, it can still be useful to review key assumptions as a sanity check on the underlying logic of the analysis. A brainstorming session also may be helpful to insure that no plausible hypothesis has been dismissed or left unaddressed. If a firm consensus has formed around an analytic line and has not been seriously questioned in some time, then a Devil's Advocacy exercise could be useful. Analysts might also use a final review to decide if they have identified a list of key indicators for future developments. This can be an important guide to include in the assessment as a way to track future developments and monitor whether the analytic judgments reached are being realized or in need of revision.

Graham Allison, *Essence of Decision*: *Explaining the Cuban Missile Crisis*: Examines the Kennedy Administration's decisionmaking style from alternative perspectives of the "rational actor," "organizational actor," and "bureaucratic politics" models.

Max Bazerman and Michael D. Watkins, *Predictable Surprises: The Disasters You Should Have Seen Coming and How To Prevent Them*. Examines the cognitive, organizational and political causes of some predictable surprises and outlines steps to overcome them.

Richard Betts, *Surprise Attack: Lessons for Defense Planning*. Explains why surprise attacks historically have succeeded and argues that the US needs strategies for avoiding surprise or at least reducing their consequences. Uses examples from World War II, Korea, and the Middle East.

Josh Epstein and Rob Axtell, *Sugarscape: Creating Artificial Societies from the Ground Up*. Develops a very simple agent-based model of a silicon-based society and then does simulations of various social, economic and political phenomena, including conflict.

Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference*. Examines how social trends, ideas, and products emerge from nowhere and take hold.

Cynthia M. Grabo, *Anticipating Surprises: Analysis for Strategic Warning.* Examines distinctive ingredients of the analytical method of intelligence and suggests ways of improving warning assessments.

Richards J. Heuer, Jr., *The Psychology of Intelligence Analysis*. Examines the impediments to good analysis and provides techniques for overcoming mind-sets and cognitive biases.

Barry Hughes, *International Futures*. Develops scenarios for international relations using a simulation tool contained in a CD ROM in the back jacket.

Robert Jervis, *Perception and Misperception in International Politics*. Examines how policymakers learn from history, perceive complexity, and form and change their beliefs.

Gary Klein, *Intuition At Work*. Shows how developing one's intuition can improve your analytic skills and that it is a "learnable" technique.

Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decisionmakers*. Uses case study methods to identify the perils of historical analogies and recommends identifying what is "known, unclear and presumed."

Peter Schwartz, *The Art of the Long View: Planning for the Future in an Uncertain World*. Explains the "scenaric" approach pioneered at Royal Dutch Shell and argues for making strategic decisions that will be sound for "all plausible futures."

James Surowiecki, *The Wisdom of Crowds*. Argues that diversity and independence of even non-expert individuals in groups, properly organized, can reach more accurate forecasts than individual experts.

M. Mitchell Waldrop, *Complexity: The Emerging Science at the Edge of Disorder and Chaos*. Introduces the literature of complex systems and suggests why forecasting anything complicated is so difficult.

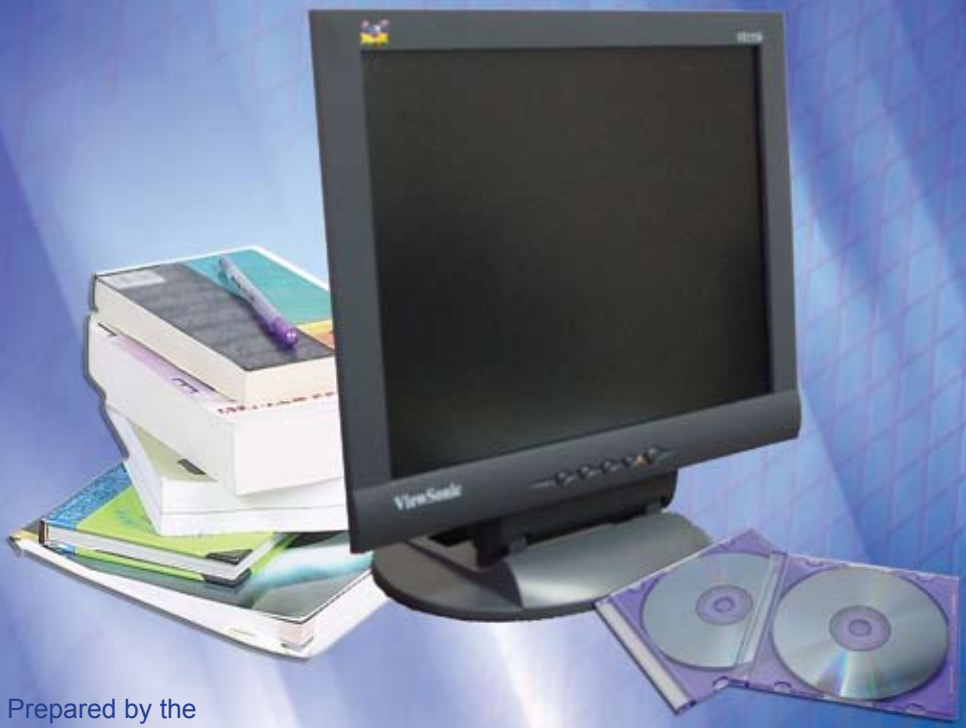
This Page Is Intentionally Left Blank

Global Justice Information Sharing Initiative

United States Department of Justice

Analyst Toolbox

A Toolbox for the Intelligence Analyst



Prepared by the
U.S. Department of Justice's Global Justice Information Sharing Initiative Intelligence Working Group

About Global

The U.S. Department of Justice's Global Justice Information Sharing Initiative (Global) serves as a Federal Advisory Committee to the U.S. Attorney General on critical justice information sharing initiatives. Global promotes standards-based electronic information exchange to provide justice and public safety communities with timely, accurate, complete, and accessible information in a secure and trusted environment. Global is administered by the U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance.

This project was supported by Grant No. 2007-NC-BX-K001 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, the SMART Office, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice.

Introduction and Background

There is a wide range of software available on the market to support intelligence analysis. In order to meet the challenges facing law enforcement today, it is important that intelligence professionals be equipped with the right tools to effectively and efficiently perform their duties and produce meaningful and useful intelligence products. The tools examined in this document represent the basic toolbox that the intelligence analyst will need to provide the vital intelligence service that is expected in today's law enforcement environment.

The *National Criminal Intelligence Sharing Plan* (NCISP)[1]—endorsed by the U.S. Department of Justice (DOJ), the U.S. Department of Homeland Security (DHS), and many different law enforcement organizations—contains 28 recommendations for local, state, tribal, and federal law enforcement agencies to implement in order to improve the quality of criminal intelligence in the United States. Two of the recommendations of the NCISP address the need to properly equip those persons involved in intelligence analysis:

- Recommendation 12: The International Association of Law Enforcement Intelligence Analysts (IALEIA) should develop, on behalf of the CICC (Criminal Intelligence Coordinating Council), minimum standards for intelligence analysis to ensure intelligence products are accurate, timely, factual, and relevant and recommend implementing policy and/or action(s). Law enforcement agencies should adopt these standards as soon as developed and approved by the CICC.
- Recommendation 28: The CICC, in conjunction with the Office of Justice Programs (OJP) and the connected sensitive but unclassified systems, shall develop an acquisition mechanism or centralized site that will enable law enforcement agencies to access shared data visualization and analytic tools. The CICC shall identify analytical products that are recommended for use by law enforcement agencies

1 Available at www.it.ojp.gov/documents/NCISP_Plan.pdf.

in order to maximize resources when performing intelligence functions, as well as a resource list of current users of the products.

Pursuant to Recommendation 12, IALEIA developed the *Law Enforcement Analytic Standards* booklet.[2] This booklet provides minimum standards for intelligence analysis to ensure that intelligence products are accurate, timely, factual, and relevant. These standards were approved by DOJ's Global Justice Information Sharing Initiative (Global) Advisory Committee in September 2004. Standard 16 of the *Law Enforcement Analytic Standards* states that "Analyses shall utilize the best and most current computerized visualization and analytic tools available to the analyst."

In order to provide law enforcement decision makers with as much information as possible concerning the tools available to the analysis process, the Global Intelligence Working Group (GIWG) tasked the Connectivity/Systems Committee to develop a list of tools to fulfill the needs expressed in NCISP Recommendation 28. To begin the process, a survey was conducted among randomly selected law enforcement analytic practitioners to determine a baseline of needed tools to adequately perform the analyst function.[3]

Another step in the process of developing tools to aid in the analysis process was the coordination with the Office of National Drug Control Policy to modify its secure Technology Toolbox for police Web-based collaboration programs to accommodate discussion forums for analytical software. This provides a secure mechanism for law enforcement analysts to discuss "how to" issues concerning these tools. Additionally, administrators can compare various intelligence products to gauge the effectiveness of the tools and determine whether they meet the needs of the agency. The Technology Toolbox can be reached via RISSNET™.

The *Analyst Toolbox* list represents the results of extensive Web-based, open source research and the collection of systems currently utilized by local, state, tribal, and federal law enforcement agencies.

2 Available at www.it.ojp.gov/documents/law_enforcement_analytic_standards.pdf.
3 The results of the survey are attached as Appendix A.

Analyst Toolbox

Word Processing

Purpose: To produce text documents, including bulletins, fact sheets, investigative summaries, and analytical reports. Analytic products should include a written report of some length and format that can be produced utilizing word processing software. In some instances, the only product of an analysis will be a written report.

Uses: Word processing software includes various formatting tools, such as footnoting, header and footer annotations, mailing labels, and correspondence formatting. This software also enables objects (photographs, graphics, tables, etc.) to be embedded in documents. Word processing software may also include editing and change tracking features for documents being modified by more than one individual.

Spreadsheet

Purpose: To organize numerical data in a column-and-row format for summarization and comparison of data and data charting.

Uses: Spreadsheets are capable of performing calculations and basic statistical computations, searches, defined filtering, and sorting of data. They are ideal for financial data storage and collation. Data can be entered by an operator or imported from files of similar structure. Additional capabilities of this tool should include the ability to generate graphs and tables to visualize data. Drawing toolbars may be used to create rudimentary link charts and flowcharts.

Relational Database

Purpose: To organize data in relation to other data in a format of records and fields arranged into several tables in order to determine commonalities and relationships among data. The relational database tool can also be used for record keeping.

Uses: Relational database software allows the option of records/fields within a database to be related to other fields (e.g., incident name, time, date, gist, and reported by). Records can be associated with other records by any of the fields (a query for records for a particular date will bring up all records associated with that date; e.g., a query for records reported by Officer Jones will retrieve all incidents reported by Jones). Likewise, tables can be related to each other through queries that connect similar fields and reduce data entry and repetition. A relational database also serves as an information management tool. User interface can be via simple forms through which data can be entered and fed directly into the database.

Mapping/Geographic Information System (GIS)

Purpose: To display geographic data using points or shapes corresponding to specific locations or areas on a map to aid in crime mapping and strategic intelligence charting.

Uses: Mapping/GIS software can aid in mapping and in the analysis of data points or areas related to crime or other patterns (dates, times, hot spots of activity, buffer zones). This software can also be used to look at patterns of movement relating to crime to delineate "hunting zones" and reduce the number of leads in predatory crimes.

Public Information Database Resources

Purpose: To provide access to compiled public data sources with one comprehensive search.

Uses: Public information records usually include personal information (address, phone number, date of birth) and asset information (real estate, vehicle, businesses). These types of databases are not considered the primary data source but are a compilation of information from other sources; therefore, the information should be verified at the primary source of the information. Law enforcement agencies may have direct access to these databases, or agencies may access this type of information through the Regional Information Sharing Systems® (RISS), Financial Crimes Enforcement Network (FinCEN), National White Collar Crime Center (NW3C), or High Intensity Drug Trafficking Areas (HIDTA).

Presentation Software

Purpose: To produce professional-looking slide show presentations, with the capability to incorporate text, photographs, graphics, and animation.

Uses: Presentation software provides not only slides but also handouts and presentation outlines that may aid in oral intelligence briefings. This tool can be used to provide a visual summary of pertinent information relating to the investigation or topic being discussed.

Graphics Software

Purpose: To illustrate concepts or conclusions using graphic arts.

Uses: Graphics software allows for cutting and pasting of information into other applications for projects beyond the graphics capability of word processing and spreadsheet software, thereby providing a complete and detailed representation of the applicable data.

PDF File Creation Software

Purpose: To allow the creation of PDF format files. PDF files can be viewed and printed on any operating system (Mac OS X®, Microsoft® Windows®, UNIX®), thereby facilitating the sharing of information.

Uses: PDF files look exactly like original documents and preserve source file information—including text, drawings, 3D, full-color graphics, and photos—regardless of the application used to create them. PDF files can also support full-text searches to locate words and phrases. This software can also be utilized to create electronic documents from paper originals.

Statistical Analysis Software

Purpose: To analyze large amounts of data to identify trends.

Uses: This software enables the user to create descriptive statistics, which in turn allows for the summarization and analysis of qualitative and quantitative data, using calculations such as frequency, percent change, mean, median, mode, and measures of variance (SD and SE). Inferential statistics are used for random sampling of populations (as in a survey) and allow the user to inferentially apply the results to the population from which the sample was drawn.

Publishing Software

Purpose: To produce professional-looking publications, such as newsletters or bulletins.

Uses: Publishing software enables the user to create publications to be distributed on a broad scale. Intelligence that is to be disseminated should be converted into a format similar to PDF to ensure that the quality of the document is not altered.

Communications/Telephone (Toll) Record Software

Purpose: To organize structured information collected from telephone billing systems (including cellular phones), pen registers, and dialed number recorders for analysis.

Uses: Communications/telephone records software aids in the analysis of communication and telephone information, including source or destination of a call; the times of calls; and the dates, frequency, sequence, patterns, and duration of calls to/from one or many telephones. With advancements in communications technologies—such as e-mail, instant messaging (IM), paging, Voice over Internet Protocol (VoIP), and direct connect technologies—software packages should be capable of dealing with nontraditional communications data elements, such as Internet Protocol (IP) addresses, e-mail addresses, direct connect private identification numbers, and IM account numbers and/or screen names.

Timeline/Flowcharting

Purpose: To display chronological events in an easy-to-understand format.

Uses: Timeline/flowcharting can support tactical or strategic planning, as well as investigations. Timeline software tools can visually show the order of events for an identified or suspected crime. Flowcharting can visually demonstrate the flow of goods within a criminal enterprise. Timeline/flowcharting can also serve administrative purposes, such as visual project tracking.

Link Analysis

Purpose: To link associated information from a structured data source and display the links between entities in a graphic display. Also useful for documenting data sources and can help find the links in a large, complex data set. This type of software can also include a timeline or flowcharting capability.

Uses: Link analysis software can visually show relationships, including association analysis and hierarchical relationships (e.g., organized crime hierarchies).

Data Mining/Text Mining

Purpose: To automate the process of determining patterns and relationships in extremely large volumes of information (either statistical or in text) too large for an individual to manage.

Uses: Data mining/text mining tools can assist in complex case management where there may be multiple targets, victims, and pieces of information related to the case. These types of tools aid in efficiently analyzing large amounts of data.

Data Visualization

Purpose: To automatically display information in formats such as graphs and pie charts. This capability can sometimes be part of a larger software application, such as spreadsheet software.

Uses: Data visualization software displays the relationships and findings in an easy-to-read format, such as link charts, flowcharts, or telephone toll-analysis charts.

Investigative Case Management

Purpose: To track investigations and leads and activities conducted in support of investigations in order to preserve a record for investigative and prosecutorial purposes, as well as to manage work flow of investigators and analysts.

Uses: Investigative case management tools provide a central repository for all information relating to a case. Users may query the system to determine whether subjects have previously been identified and current case status. This tool can also provide information and reports regarding strategic planning for law enforcement executives.

Conclusion

Each organization will have to determine the specific vendor to provide the tools listed in this report. It is important when examining these products that interoperability be considered. In order to connect the dots, law enforcement analysts must have a basic set of tools that provide the services they need and can easily communicate with each other.

Appendix A

Results of Analyst Survey to Determine Tools Needed by Analysts

November 2005

I. Hardware

A. Computer with sufficient processing speed and hard drive capability to run high-end programs and adequate data storage/memory servers
   1. CD and DVD Burner capability
   2. Backup equipment
   3. Video capture capability
   4. Laptops if fieldwork is required

B. Printers
   1. Laser for high-speed black and white with capability of printing up to 11" x 17" charts and documents
   2. Color printer with capability of printing up to 11" x 17" charts and documents
   3. Graphics plotter capable of printing large charts

C. Document scanner with auto feed and optical character recognition (OCR) software

D. Digital camera(s) (5-megapixel) for surveillance, target photos, and postseizure analysis

E. Digital video camera(s)

F. Facsimile machine

G. Color copier

H. Statistical calculator

I. Projection equipment

J. Television with cable or satellite access

II. Installed Software

A. Word processing program

B. Spreadsheet program

C. Relational database

D. Presentation software to include photo manipulation/enhancement

E. Internet browser

F. Flowcharting software

G. Link analysis software
H. Database reporting/visualization software
I. Mapping software
J. Photo enhancement software
K. E-mail program to include interoffice with ability to calendar/task
L. Desktop search engine for local and network drives
M. Telephone analysis software
N. Portable Document Format (PDF) creation software
O. Security software
    1. Virus blockers
    2. Internet restriction
    3. Firewall
    4. Smart Pass or other encryption software
P. Publication software
Q. Statistical analysis software
R. Data mining/text mining software

III. Access to Systems and Databases

A. Agency records management system
B. Agency intelligence system
C. Direct unfiltered Internet connection
D. State crime information system
E. National crime information system
F. State driver's license database
G. Commercial databases containing personally identifying information
H. Regional Information Sharing Systems (RISS)
I. Law Enforcement Online (LEO)
J. Homeland Security Information Network (HSIN)
K. Telephone database
L. Jail management databases
M. Financial Crimes Enforcement Network (FinCEN)
N. Immigration databases
O. State wage and hour database
P. State sex offender registries
Q. Crime-specific listservs
R. Really Simple Syndication (RSS) readers
S. Intelligence center databases (state, HIDTA, EPIC, NDIC, etc.)
T. State corrections/probation databases
U. Juvenile justice databases
V. Wireless Internet access
W. Cellular telephone and PDA

For more information on the U.S. Department of Justice's Global Initiative and its products, including those referenced in this document, call (850) 385-0600 or visit

www.it.ojp.gov

Issued: November 2006
Reprinted: November 2007

This Page Is Intentionally Left Blank

Joint Military Intelligence College

January 2000

INTELLIGENCE ANALYSIS IN THEATER JOINT INTELLIGENCE CENTERS: AN EXPERIMENT IN APPLYING STRUCTURED METHODS

Occasional Paper Number Seven

The Joint Military Intelligence College supports and encourages research on intelligence issues that distills lessons and improves support to policy-level and operational consumers

This series of Occasional Papers presents the work of faculty, students and others whose research on intelligence issues is supported or otherwise encouraged by the Joint Military Intelligence College through its Office of Applied Research. Occasional papers are distributed to Department of Defense schools and to the Intelligence Community, and additional copies of unclassified papers are available through the National Technical Information Service <*www.ntis.gov*>; copies of selected papers are also available through the U.S. Government Printing Office <*www.gpo.gov*>.

Proposed manuscripts for these papers are submitted for consideration to the Applied Research Editorial Board. Papers undergo review by senior officials in Defense, Intelligence and occasionally civilian academic or business communities.

Occasional Paper Number Seven

INTELLIGENCE ANALYSIS IN THEATER JOINT INTELLIGENCE CENTERS: AN EXPERIMENT IN APPLYING STRUCTURED METHODS

By MSgt Robert D. Folker, Jr. (USAF)

JOINT MILITARY INTELLIGENCE COLLEGE
WASHINGTON, DC
January 2000

The views expressed in this paper are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government

This paper has been approved for unrestricted public release by the Office of the Secretary of Defense (Public Affairs)

CONTENTS

Preface v

Foreword vii

Preamble 1

The Research Problem 2

The Art or Science Debate 6

The Experiment. 15

Considerations and Limitations 27

The Findings 29

Implications and Recommendations. 32

Final Impression 35

Bibliography 37

About the Author 43

INTELLIGENCE ANALYSIS IN THEATER JOINT INTELLIGENCE CENTERS: AN EXPERIMENT IN APPLYING STRUCTURED METHODS

Preface

In clear, articulate, unmistakable language, Master Sergeant Folker's learned thesis sets forth the key opposing arguments in the long-standing controversy over the role of structuring in intelligence analysis. The controversy is largely one-sided, because proponents of intuitive analysis see no purpose in debating the issue, as they are completely satisfied with the status quo. It is only the structuring enthusiasts who see a need for drastic change in the way analysis is conducted. Because, as Folker points out, supporters of the status quo include not only most analysts but most commanders as well, the structuring enthusiasts have never made progress in reforming the other side. And they won't make any progress until the superiority of structured analysis over intuitive analysis is proved, which Folker has taken a first giant step in doing.

And it is precisely on this point that Folker challenges the Intelligence Community—indeed the entire U.S. government and the private sector as well—to design and conduct reliable tests to demonstrate which analytic approach is superior: structured or intuitive. Given the wide range of available structuring techniques, each one should be tested in competition with intuition.

There are many myths prevalent in the analytic community, public and private, concerning structured analysis: It is time-consuming and overly complicated; it eliminates the indispensable role of intuition; it involves numbers and arcane formulae that render analysis mechanical and devoid of creative solutions; and so on. Tests like Folker's will surely dispose of these myths and demonstrate the immense value and power of structuring.

His thesis, moreover, should encourage students to undertake research experiments that challenge long-held beliefs and test new theories of military interest. JMIC students are especially well placed to conduct thoughtful, creative research because they bring to this scholarly environment a rich mixture of background and viewpoints, and because they remain vitally involved in the business of wringing meaning from a great variety of intelligence information.

Morgan D. Jones
Former intelligence analyst, supervisor and trainer, Central Intelligence Agency

INTELLIGENCE ANALYSIS IN THEATER JOINT INTELLIGENCE CENTERS: AN EXPERIMENT IN APPLYING STRUCTURED METHODS

Foreword

A growing number of JMIC students have begun to incorporate replicable research design into their theses. This distillation of Master Sergeant Folker's thesis shows how fruitful this approach can be. By taking advantage of on-site research funds available from the College, he managed, in brief visits to four Unified Command Joint Intelligence Centers, to carry out a controlled experiment to measure the impact of analyst familiarity with and use of one structured analytic technique — hypothesis testing. His findings, if corroborated by follow-on studies, could have a substantial impact on Intelligence Community analytical practices, and even some influence on how senior policy officials react to analytical products. Managers of analytical personnel might also note that structured methods would appear, from this study of non-specialized joint intelligence center analysts, to be useful to specialized analysts who may be required to move beyond their areas of deep expertise to cover new or unfamiliar assignments.

Of equal importance with his findings is MSgt Folker's documentation of applied field research procedures. His subsequent recommendations for follow-on research illustrate the close relationship between doing research and contributing to the corporate learning environment. The Editor welcomes other students to contribute the story of their unique discoveries about the intelligence profession to this series of Occasional Papers.

This paper benefited from reviews by a panel of JMIC faculty, the Director of Research of the Defense Intelligence Agency's Directorate of Intelligence, and by Morgan D. Jones, founder of Analytic Prowess, L.L.C. of Montclair, Virginia.

Russell G. Swenson, Editor and Director, Office of Applied Research,
AFswerg@dia.osis.gov.

INTELLIGENCE ANALYSIS IN THEATER JOINT INTELLIGENCE CENTERS: AN EXPERIMENT IN APPLYING STRUCTURED METHODS

Exploiting structured methodologies compels the intelligence analyst to analyze the intelligence problem at hand and distinguishes analytical endeavors from office administration.

—The author

PREAMBLE

A debate exists between those who prefer to think of intelligence analysis as an art form and those who would highlight the value of a structured, scientific approach to the assessment of intelligence problems. Analytical approaches to intelligence problems can be divided into two overlapping categories—qualitative and quantitative. Qualitative analysis attempts to answer questions or solve problems that are not easily broken down into quantifiable variables. Qualitative analysis is therefore most often used in political, military, and warning intelligence. Quantitative analysis, which uses variables that are more easily measured, generally attempts to solve scientific or technical intelligence problems. Of the two, qualitative intelligence analysis, if performed carefully, arguably provides the information most useful to national policymakers.[1]

A small number of analysts occasionally apply structured methods to qualitative intelligence analysis, but the traditional approach to solve qualitative intelligence problems is non-structured.[2] Surprisingly, no research known to this author has adequately examined whether exploiting structured methodologies will improve qualitative intelligence analysis.

Intelligence analysts who do use non-structured methods for qualitative analysis argue that structured methods too narrowly define a problem and ignore factors that cannot be measured. They assert that their intuitive approach produces superior results. For their part, analysts who employ structured methods for qualitative analysis intuitively believe that structured methods ensure sounder, more comprehensive, and accurate findings.[3] However, no empirical evidence is available to support either belief.

---

[1] Richard K. Betts, "Intelligence for Policymaking," *Washington Quarterly 3*, no. 3 (Summer 1980): 119.

[2] James D. Hammond, *So You Want to Be an Intelligence Analyst?* Research Paper (Washington, DC: Defense Intelligence College, October 1983), 10.

[3] Capt. William S. Brei (USAF), *Getting Intelligence Right: The Power of Logical Procedure*, Occasional Paper Number Two (Washington, DC: JMIC, 1996), 1-2.

The author conducted a controlled experiment among a small sample of non-specialized analysts at four Unified Command joint intelligence centers to test the effect of applying a structured method to the qualitative analysis of an intelligence problem. Only tentative conclusions can be drawn from the findings in this limited experiment, but the results, if corroborated, have some profound implications for Intelligence Community analysts and their managers.

In brief, the author found that analysts who apply a structured method—hypothesis testing, in this case—to an intelligence problem, outperform those who rely on "analysis-as-art," or the intuitive approach. The modest character of this experiment, and of this finding, clearly calls for follow-on research, but this study at least shows that intelligence value may be added to information by investing some pointed time and effort in analysis, rather than expecting such value to arise as a by-product of "normal" office activity.

THE RESEARCH PROBLEM

Because the Intelligence Community has used technology to increase its ability to collect information, intelligence analysts face an ever-increasing stream of intelligence data.[4] But the Community has not made similar improvements in its analytical capability, and intelligence analysts are not exploiting all of the analytical methodologies available to them.[5] Perhaps in part because intelligence analysts lack familiarity with the proper analytical tools, they are being overwhelmed by the amount of information they are expected to analyze, contributing to "analysis paralysis."[6] Congress is well aware of this phenomenon, and has raised the issue publicly.[7]

A Research Question

A variety of structured methodologies is available to help the intelligence analyst solve qualitative problems,[8] but most analysts display an inability or unwillingness to exploit them.[9] Most people instinctively prefer intuitive, non-structured approaches over structured methodologies. Moreover, identifying all relevant qualitative variables in any

---

[4] Stephen J. Andriole, "Indications, Warning, & Bureaucracies," *Military Intelligence Professional Bulletin* 10, no. 3 (July-September 1984): 8.

[5] David M. Keithly, "Leading Intelligence in the 21st Century: Past as Prologue?" *Defense Intelligence Journal* 7, no. 1 (Spring 1998): 80.

[6] Alvin Toffler and Heidi Toffler, *War and Anti-War: Survival at the Dawn of the 21st Century* (New York: Little, Brown and Company, 1993), 158.

[7] Vernon Loeb and Walter Pincus, "New Spy Satellites at Risk Because Funding Is Uncertain, Pentagon Told," *Washington Post*, 12 November 1999, A7.

[8] Robert M. Clark, *Intelligence Analysis: Estimation and Prediction* (Baltimore: American Literary Press, Inc., 1996), 11.

[9] Stephen J. Andriole, senior intelligence researcher and former director of the Cybernetics Technology Office of the Advanced Research Projects Agency, email interview by author, 15 December 1998.

problem is difficult, and quantifying them is daunting. The bottom line: Most analysts prefer a subjective approach.[10] Can intelligence analysts, specifically those conducting analysis in the "softer" sciences such as political intelligence, improve the quality of their analysis by better exploiting structured methodologies? Comparing the analytical results of structured methods with the analytical results derived from traditional non-structured practices used by intelligence analysts should provide valuable insights into improving qualitative intelligence analysis. The need for such an experiment has been clearly identified by a number of specialists.[11]

Improvement in qualitative intelligence analysis has been a goal of long standing in the Intelligence Community, but most attempts to improve the process have ignored analysis and focused on restructuring intelligence organization and providing additional training in non-analytical subjects. The U.S. Commission on the Roles and Capabilities of the United States Intelligence Community determined that too few resources are dedicated to all-source analysis, and even fewer resources are obligated to developing and maintaining analytical expertise.[12] Currently, only six percent of the intelligence budget authorized by the U.S. Congress is spent on analysis.[13] The House of Representative's Permanent Select Committee on Intelligence concluded that "[a]nalytical pitfalls have been recognized in post mortems and other studies of past warning situations, and limited organizational and training efforts have been undertaken in response."[14]

A Record of Analytic Failures

Although organizational restructuring may be of some benefit to the Intelligence Community, the root cause of many critical intelligence failures has been analytical failure. "Failure to predict the North Korean invasion in 1950 was a failure of analysis at higher echelons. ... No analyses accompanied this raw data."[15] The Intelligence

---

[10] Morgan D. Jones, *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving* (New York: Random House, Inc., 1998), 8.

[11] Andriole, "Indications, Warning, & Bureaucracies," 12; Stanley A. Feder, "FACTIONS and Policon: New Ways to Analyze Politics," in *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal 1955-1992*, ed. H. Bradford Westerfield (New Haven: Yale University Press, 1995), 274-275; and Thomas H. Murray, former analyst and trainer for the Central Intelligence Agency and Senior Vice President of Sequoia Associates, Inc., interview by author, 18 January 1999.

[12] U.S. Commission on the Roles and Capabilities of the United States Intelligence Community, "Chapter 8: Improving Intelligence Analysis," in *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (Washington, DC: GPO, 1 March 1996) URL: *http://www.access.gpo.gov/su_docs/dpos/epubs/int/int012.html.*

[13] Philip Seib, "Intelligence Gathering Remains a Vital Function," 1 March 1999, *Dallas Morning News*, URL: <*http://www.dia.ic.gov/admin/EARLYBIRD/990302/s199990302gathering.htm*>, accessed 2 March 1999.

[14] Andriole, "Indications, Warning, & Bureaucracies," 8.

[15] James P. Finley, "Nobody Likes to be Surprised: Intelligence Failures," *Military Intelligence Bulletin* 20, no. 1 (January-March 1994): 18-19.

Community also failed to predict the Tet Offensive in Vietnam until just hours before the attack. "The analysis failure occurred in where, when, and why."[16] Joseph Nye cites the "analytical disarray in 1978 that prevented the drafting of any estimate about the fall of the Shah, and the 1989 prediction that Saddam Hussein would not make trouble for the next three years."[17] Members of the Senate Select Committee on Intelligence recently voiced their concern about the Intelligence Community's inability to warn of the Indian nuclear tests, calling it the "greatest failure for more than a decade."[18] Others point out that by improving intelligence analysis the Intelligence Community can better support and protect U.S. embassies from terrorist threats.[19]

Some intelligence analysts believe that the ratio of intelligence successes to failures is actually quite good. Arthur S. Hulnick, a notable veteran in the intelligence profession, is one such believer. He stated in a conference paper delivered at the 1987 Annual Meeting of the American Political Science Association that

> the products of the [Intelligence Community] reflect continued growth in the expertise of the analysts, a broader and deeper range of subject materials, and an increasingly sophisticated data base from which to work. Coupled with advances in presentational methodologies, the intelligence product is more useful, timely and relevant than ever before.[20]

Despite his optimism for intelligence analysis, Hulnick agrees that the "analytic process itself is worthy of research."[21]

Because of the Intelligence Community's failures to foresee a number of strategically important foreign developments, intelligence consumers have tended to disregard any analysis of intelligence information. "Whether analysis is good or not, many policymakers will care less about it than they do about collection. They may even resent it, seeing it as naïve speculation by junior bureaucrats that wastes their time."[22] Roger Hilsman, former Assistant Secretary of State for Intelligence Research and Assistant Secretary of State for Far Eastern Affairs, argues that the benefits of funding a large team of field agents is not worth the cost or risk. Covert action tempts presidents into risking the hard work of analysts and diplomats on an "easy fix," damages America's reputation, and is antithetical to a democracy. He concludes that the Intelligence Community should

---

[16] Finley, "Nobody Likes to be Surprised: Intelligence Failures," 20.
[17] Joseph S. Nye Jr., "Peering into the Future," *Foreign Affairs* 73, no. 4 (July/August 1994): 84.
[18] "Don't Blame the CIA," *Economist*, 23 May 1998, 26.
[19] John Kifner, "Raids by U.S. Agents and Tirana Police Reportedly Thwart Attack on Embassy," *New York Times*, 21 August 1998, A13.
[20] Arthur S. Hulnick, "Managing Intelligence Analysis: Strategies for Playing the End Game," *International Journal of Intelligence and Counterintelligence* 2, no. 3 (Fall 1988): 341.
[21] Hulnick, 329.
[22] Richard K. Betts, "Intelligence Warning: Old Problems, New Agendas," *Parameters* 28, no. 1 (Spring 1998): 33.

focus its efforts on improving its analytical support.[23] If the Intelligence Community is to overcome this credibility problem, it must improve its ability to produce accurate, timely, and useful intelligence.

Furthermore, the military's use of precision, information-intensive weapons creates pressure on the intelligence analyst to deliver useful intelligence at faster rates. In the era of modern warfare, fast and precise weapons demand fast and precise intelligence. The intelligence analyst who is unable to conduct analysis quickly can become an information-bottleneck in this environment. It may be arguable that the use of structured analytical techniques helps to speed up the analytical process. This assertion has not been tested, and is beyond the scope of the present research.

Terms of Reference

Quantitative intelligence analysis separates the relevant variables of a problem for credible numerical measurement. Qualitative intelligence analysis breaks down topics and ideas that are difficult to quantify into smaller components for better understanding.[24] Structured methodologies are various techniques used singly or in combination to separate and logically organize the constituent elements of a problem to enhance analysis and decisionmaking.[25] Some structured methodologies, such as organized brainstorming techniques, complement the analyst's intuition and facilitate creativity.

Non-structured methodology is intuitive. Intuition is a feeling or instinct that does not use demonstrative reasoning processes and cannot be adequately explained by the analyst with the available evidence. For the purposes of this study the term "improve," when referring to qualitative intelligence analysis, means to increase, either singularly or in any combination, without decreasing, either singularly or in any combination, the accuracy, specificity, or timeliness of the result.

This study assumes that exploiting structured methodologies for qualitative intelligence analysis does not invariably subordinate one's intuition, education, or experience. The analyst must still make a conscious choice as to whether he will accept a conclusion based on exploiting a structured method or reject it in favor of his intuitive judgment. Moreover, intuition plays an inescapable role in analysis. However, although intuition can usually be relied upon to provide effective solutions to simple problems, it cannot cope with the highly complex problems that routinely face intelligence analysts.

Many factors affect the quality of intelligence analysis. This study is limited to arguing how structured methodologies may influence the results of qualitative intelligence analysis. Due to time and cost considerations, it was necessary to restrict the scope of the

---

[23] Roger Hilsman, "Does the CIA Still Have a Role?" *Foreign Affairs* 74, no. 5 (September/October 1995): 104-116.

[24] Clark, 30.

[25] Jones, xi-xvi.

experiments to intelligence analysts at four of the nine Joint Intelligence Centers (JICs) of the Unified Commands. Specifically, experiments were conducted with intelligence analysts from the U.S. Special Operations Command (SOCOM), the U.S. Central Command (CENTCOM), the U.S. Southern Command (SOUTHCOM), and the U.S. Joint Forces Command (JFCOM), formerly Atlantic Command (ACOM). Because of these limitations, the evidence presented here should be considered only provisional, not conclusive.

THE ART OR SCIENCE DEBATE

A long-standing debate exists within the Intelligence Community about whether more should be invested in structured methodologies to improve qualitative intelligence analysis. At the heart of this controversy is the question of whether intelligence analysis should be accepted as an art (depending largely on subjective, intuitive judgment) or a science (depending largely on structured, systematic analytic methods). Resolving this question is necessary to provide direction and determine an efficient and effective approach to improve analysis. If qualitative intelligence analysis is an art, then efforts to improve it should focus on measuring the accuracy of one's intuition, selecting those analysts with the best track record, and educating them to become experts in a given field. If, on the other hand, qualitative intelligence analysis is a science, then analysts should be trained to select the appropriate method for a given problem from a variety of scientific methodologies and exploit it to guide them through the analytical process.

Qualitative Analysis as an Art

Proponents of this argument contend that qualitative intelligence analysis deals with an infinite number of variables that are impossible to operationalize because they cannot be adequately quantified or fully collected. A foreign nation that attempts to conceal or disguise information on many of the same variables that an analyst seeks will further complicate the analytical function. Because in many cases the variables are so complex, countless, and incomplete, attempting to analyze them using scientific methods is pseudo-science.[26] Therefore, any attempt to make predictions based on quantifying these variables is futile.[27]

Other arguments attack the rational-actor assumption made by most scientific approaches to qualitative intelligence analysis. "Science can be of little help when dealing with the often irrational and unpredictable human mind."[28] But these critics acknowledge that the traditional approach to qualitative analysis, being an art, is vulnerable to failure — "humans are still fallible in matters of analysis and response."[29]

---

[26] Richard K. Betts, "Surprise, Scholasticism, and Strategy: A Review of Ariel Levite's *Intelligence and Strategic Surprises* (New York: Columbia University Press, 1987)," *International Studies Quarterly* 33, no. 3 (September 1989): 338.

[27] John L. Peterson, "Forecasting: It's Not Possible," *Defense Intelligence Journal* 3, no. 2 (Fall 1994): 37-38.

[28] Finley, "Nobody Likes to be Surprised," 40.

Those who advocate that qualitative intelligence analysis is an art maintain that the most successful analysts take an inductive approach, "in which powers of pattern recognition are enhanced and intuition is elevated."[30] They insist that this approach will lead to more creative and original analysis. They argue that qualitative intelligence analysis is an art because it is an intuitive process based on instinct, education, and experience.[31] Gary Klein, a cognitive psychologist and pioneer in pattern recognition, makes some convincing arguments to support this claim. He challenges the practicality of using scientific methods for qualitative intelligence analysis outside the classroom.

"It is time to admit that the theories and ideals of decisionmaking we have held over the past 25 years are inadequate and misleading, having produced unused decision aids, ineffective decision training programs and inappropriate doctrine."[32] He continues:

> The culprit is an ideal of analytical decisionmaking which asserts that we must always generate options systematically, identify criteria for evaluating these options, assign weights to the evaluation criteria, rate each option on each criterion and tabulate the scores to find the best option.... The technical term is multiattribute utility analysis.[33]

He concludes that:

> [t]hese strategies sound good, but in practice they are often disappointing. They do not work under time pressure because they take too long. Even when there is enough time, they require much work and lack flexibility for handling rapidly changing field conditions.[34]

It is important to note that the majority of Klein's research has been conducted with leaders in the armed forces and emergency service providers such as firemen, but not specifically members of the Intelligence Community. There has always been a clash of cultures between operators (commanders and other decisionmakers whose focus is on accomplishing the mission at hand) and intelligence analysts. As intelligence analysts have attempted to bridge the gap between the two cultures, they have tended to adopt the same intuitive decisionmaking strategies commonly used by operators.[35]

---

[29] James P. Finley, "Intelligence Failure Matrix," *Military Intelligence Professional Bulletin* 20, no. 1 (January-March 1994): 14.

[30] Tom Czerwinski, ed. *Coping with the Bounds: Speculations in Nonlinearity in Military Affairs* (Washington: National Defense University, 1998), 139.

[31] Czerwinski, 139.

[32] Czerwinski, 140.

[33] Czerwinski, 140.

[34] Czerwinski, 141.

[35] The relationship between operators and intelligence analysts has also been the subject of much controversy. For a good summary see Jack Davis' article "The Kent-Kendall Debate of 1949," *Studies in Intelligence* 35, no. 2 (Summer 1991): 37-49.

Science May Offer Only Minimal Analytic Improvements. One argument against the value of structured analysis is that intelligence failures may less accurately be attributed to problems with analysis than to "the decisionmakers who consume the products of intelligence services."[36] Given that intelligence consumers can and do perform their own analysis of intelligence information, they may care less about others' analysis than about collection issues, for example.[37] Nonetheless, if analysts were to make it possible for policymakers to focus "on the methodologies of competing intelligence producers, they would be more sensitive to the biases and leaps of faith in the analyses passed to them,"[38] even if the improvement in quality of analysis were minimal. Opponents of scientific methodologies further claim that, because qualitative intelligence analysis is largely an intuitive exercise, analysts should be encouraged to specialize and be educated into becoming experts in their field. These opponents question the validity of scientific methods and object to others who would use such methods to challenge their expert opinion. To improve analysis, they argue, the analyst must improve his intuitive ability by gaining "area knowledge" through frequent contact with the subject of his study. In the face of these challenges, however, and prior to further debating to what degree the quality of analysis may be improved by using structured methods, the basic research question remains unanswered: Will the use of structured methods improve qualitative intelligence analysis?

A Rebuttal. At first glance it seems that opponents of the scientific approach are criticizing the results of scientific methods. Yet they offer no empirical data to show which approach produces more accurate results, the scientific or the intuitive. The critics do denounce the amount of time it takes to scientifically analyze a problem. However, one should recognize that there are many scientific methodologies available to aid decisionmaking, and selecting and using one need only be as complicated and time-consuming as the analyst wishes.[39]

Unquestionably, the complexity of some scientific methodologies prevents them from being regularly exploited by most intelligence analysts. A graduate of the Joint Military Intelligence College (JMIC) made the following observation in his Masters thesis:

> A major issue common to all the methods is customer acceptance. Due to the highly mathematical nature of [Bayesian Decision Analysis], many users will feel uneasy trusting the resulting assessments. This will only be overcome through proper training of the analysts using [Bayesian Analysis] and repeated exposure to Bayes on the part of decisionmakers.[40]

---

[36] Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31, no. 1 (October 1978): 61.

[37] Betts, "Intelligence Warning: Old Problems, New Agendas," 26-35.

[38] Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," 83.

[39] Lieutenant Colonel W. Frank Ball, USMC (Ret.), and Morgan D. Jones, "Improving Marine Commanders' Intuitive Decisionmaking Skills," *Marine Corps Gazette* (January 1996): 63-64.

[40] Captain David Lawrence Graves, USAF, *Bayesian Analysis Methods for Threat Prediction*, MSSI Thesis (Washington: Defense Intelligence College, July 1993), second page of Abstract.

Nevertheless, this lack of confidence should not be allowed to stand as a sweeping indictment of other, more simple and appropriate methodologies.

It is apparent that what these critics are saying is that no one in the heat of producing actionable intelligence uses the scientific approach, so why bother? This brings up two important questions:

(1) Which analysts, if any, are exploiting scientific methodologies when conducting qualitative intelligence analysis?

(2) Which approach (the intuitive or the scientific) produces the more accurate, timely, and useful result?

Other critics concede that utilizing scientific approaches to solve qualitative intelligence problems may improve the product of analysis, but they argue that the benefits are only minor. They insist that allocating resources to other areas such as reorganizing the intelligence bureaucracy, increasing manpower, and improving communication will better improve the intelligence product. One cannot deny that a host of factors affects the quality of intelligence analysis, but improvements to the process do not have to be pursued through a linear approach, nor should effort be wasted trying to determine which approach will yield the most significant improvement. If there is sufficient evidence that a reform promises improvement, it should be pursued.

Qualitative Intelligence Analysis as a Science

A few analysts see qualitative intelligence analysis as a science. Since 1973 the Central Intelligence Agency (CIA) has experimented with quantitative methods in an attempt to apply innovations in the behavioral sciences to political intelligence analysis.[41] At that time neither the Departments of State nor Defense had attempted to integrate quantitative methodologies into their political intelligence production.[42] Much of the effort to incorporate quantitative methodologies into the realm of qualitative intelligence analysis was rejected by analysts because the scientific methods were thought to be too narrowly focused and not relevant to the questions the intelligence analysts were addressing. Most analysts tended "to be skeptical of any form of simplification inherent in the application of probabilistic models."[43]

In spite of the skepticism, advocates of using a more scientific approach in qualitative intelligence analysis assert that science is a necessary tool to use when conducting qualitative analysis. They argue that, although it is impossible to consider every variable when conducting analysis, one can identify key variables and weigh their importance. And although much may be unknown, identifying what is known and analyzing it

---

[41] Richards J. Heuer, Jr., "Adapting Academic Methods and Models to Government Needs," in *Quantitative Approaches to Political Intelligence:* The CIA Experience, ed. Richards J. Heuer, Jr. (Boulder: Westview Press, Inc., 1978), 1.

[42] Heuer, 2.

[43] Heuer, 6.

scientifically is an effective approach. As one Intelligence Community advocate of a more scientific approach to intelligence analysis notes, the identification and use of big-picture, strategic insights can yield intelligence of more value than merely continuing to try to fathom, through the "art of intelligence," transient ideographic actors or their actions: "[Y]ou can disregard [military or political leaders'] madness and genius more readily than societal, economic, or political trends (which are scientifically identifiable) in analysis."[44]

Proponents of qualitative analysis as a science argue that scientific methods help analysts determine the relevancy of information and form conclusions, a process that analysts do not perform well on their own. Hall makes the point that:

> in the absence of concrete guidance or structure[,] analysts generally don't do well in forming conclusions and in discerning relevancy.... They sometimes have difficulty in figuring out relationships among seemingly unconnected pieces of information and in forming fragments of information into a coherent whole.[45]

If qualitative intelligence analysis is art, there is also a concern that the artist will fall in love with his art and be reluctant to change it even in the face of new evidence. The more scientific and objective approach encourages the analyst to be an honest broker and not an advocate.

Science in Other Types of Qualitative Analysis. Scientific methods have been used effectively to assist qualitative analysis in areas outside intelligence. An article in *The Economist* discusses the use of mathematical formulas to solve "normal" business problems that most managers argued could not be solved through quantitative approaches.[46] These managers argued that in their decisionmaking process they practice an intuitive art rather than a rational science. However, science and the use of quantitative methodologies in this case proved to be a more systematic and profitable approach than instinctive trial-and-error. Although many of the managers remained skeptical that such methods would continue to work, these methods do provide another approach to decisionmaking that should not be ruled out without evidence from comparative testing.

Although still not a standard practice in the private sector, some companies are increasingly exploiting quantitative methods and technology to help them make better decisions, increase profits, and compete in the information revolution.[47] If applying quantitative methodologies to qualitative analysis facilitates management of technological

---

[44] Captain David T. Resch, USA, "Predictive Analysis: The Gap Between Academia and Practitioners," *Military Intelligence Professional Bulletin* 21, no. 2 (April-June 1995): 27.

[45] Lieutenant Colonel Wayne M. Hall, USA, "Intelligence Analysis in the 21st Century," *Military Intelligence Professional Bulletin* 18, no. 1 (January-March 1992): 9.

[46] "Art Hammer: The Numbers Man," *Economist*, 8 August 1998, 56.

[47] Rod Newing, "Consumer Information is the Fuel of a New Industrial Revolution," *Financial Times*, 3 February 1999, B7.

information, it stands to reason that the Intelligence Community can selectively use this same approach to improve qualitative intelligence analysis.

Inside and Outside of the Classroom. Many proponents of exploiting scientific methodologies to aid intelligence analysis assume that these methods are regularly used in real-world analysis. Hulnick presents the typical view:

> Advances in analytic methodology seem to have grown remarkably in the past decade. While a discussion of explicit methods goes beyond the scope of this article — and the knowledge of the author — a wide variety of ways of attacking a problem exists. Managers of intelligence must assume that analysts try different techniques, sometimes by giving the problem to separate groups for analysis by different disciplines, sometimes by seeking an outside expert to provide competing analysis.[48]

The former chief of the Analytic Support Group in the CIA's Directorate of Intelligence agrees with Hulnick. "An analyst must have a repertoire of analytic techniques to apply in problem solving. There now exists a rich set of analytic techniques such as pattern analysis, trend prediction, literature assessment, and statistical analysis."[49] The president of Evidence-Based Research, Inc., also expressed the opinion that most intelligence analysts use some type of systematic approach when conducting qualitative intelligence analysis.[50]

This assumption that intelligence analysts use these various scientific approaches is based not on empirical evidence, but on the belief that experience alone does not make an expert, and that an expert must have a tool for structuring knowledge to efficiently solve a problem. Yet the numerous interviews conducted in support of this study, among intelligence analysts from all different agencies and backgrounds, positively invalidate this assumption. Of the 40 intelligence analysts interviewed in direct support of this study, only one maintained that he regularly used a structured methodology (link analysis) and could adequately explain the method and provide current examples of his work.[51] Although the other analysts who attempted to explain their analytical methodology described how they were tasked and how they collected information and prepared it for dissemination, they consistently and strikingly made no mention of analysis. The interviews serve only to confirm Klein's more detailed study: "After studying over 150 experienced decisionmakers and 450 decisions, we concluded that [the intuitive] approach to decisionmaking is typical."[52]

---

[48] Hulnick, 331-332.

[49] Clark, 11.

[50] Richard E. Hayes, president of Evidence-Based Research, Inc., interview by author, 9 February 1999.

[51] Tim DiPace, U.S. Atlantic Command Anti-Terrorism/Force Protection Officer, interview by author, 19 March 1999.

[52] Czerwinski, 144.

> In further support of the author's findings, JMIC graduate Stewart Eales notes: Evaluating the analytical effort in the PURPLE SUNSET wargame is difficult because there was so little to measure. Despite assertions by some that 'the analyst is at the center of the intelligence process,' the... students virtually ignored analysis. ... As a result, there was little time or effort dedicated to thoughtful analysis and dissemination.[53]

This observation was confirmed during the interviews with the JIC analysts. A repeated complaint was the analyst's lack of time to devote to thoughtful intelligence analysis. In a separate interview at CIA, it was revealed that in spite of most intelligence analysts having a broad definition of what analysis involves, they spend little time or effort conducting analysis.[54]

As noted earlier, Betts asserts that many policymakers see little or no value in intelligence analysis because it is based on the views of less experienced personnel.[55] This may be the case because so many intelligence analysts are reluctant to exploit scientific methodologies, and most intelligence analysts are junior to the decisionmakers they support. Decisionmakers typically form conclusions based on intuition developed through years of experience. Therefore, the intelligence analyst who provides an assessment based on inexperience and his own (lesser developed) intuition should not expect to be taken seriously. To be credible the analyst must use objective scientific methodologies to support his conclusions.

While the research for this study sought to collect definitive evidence of frequent and widespread use of scientific methodologies within the Intelligence Community, only rare anecdotal information could be obtained showing that such methodologies are actually used by intelligence analysts in real-world situations, despite the ready availability of these methods. The National Warning Staff, for example, uses only one quantitative analytical methodology, a modified-Bayesian technique.[56]

A lack of expertise in exploiting scientific methodologies appears to be at the root of the Intelligence Community's failure to use them. One cannot expect intelligence analysts to exploit these methodologies unless they are trained how to select the appropriate analytical method and apply it to a real-world analytical problem. Analysts at the CIA have made use of computer programs, such as FACTIONS and Policon, based on a quantitative methodology, to assist in political analysis and warning. In one application, while both intuitive-based and scientific-based political intelligence forecasts were accurate about 90 percent of the time, intelligence analysts using Policon provided more specific and less ambiguous intelligence.[57] Although this example provides limited

---

[53] Stewart C. Eales, *Playing with Intelligence: Officer Application of Intelligence in the PURPLE SUNSET Wargame*, MSSI Thesis (Washington, DC: JMIC, August 1997), 121-122.

[54] An analytic methodologist in CIA's Directorate of Intelligence, interview by author, 29 April 1999.

[55] Betts, "Intelligence Warning: Old Problems, New Agendas," 33.

[56] Warning analyst at the National Warning Staff, interview by author, 05 November 1998.

[57] Feder, 274-275.

documentation, it raises the question, why do not other members of the Intelligence Community share, compare, and exploit these methodologies?

Qualitative Intelligence Analysis as Both Art and Science

The fallacy in the art or science debate may be the "either/or" proposition. If qualitative intelligence analysis is not exclusively an art nor a science, then it may best be considered a combination of both intuitive and scientific methods:

> In our world is an infinite set of problems which have no logically consistent answer; there are some problems which any framework alone cannot solve. ... Yet strategists must not live by inspiration alone. Inspiration unsupported by rigorous analysis becomes adventurism [sic]. Thus intuitive gifts must be paired with an effective theoretical framework.[58]

Availability of Structured Methodologies

In order to expand the applicability of quantitative methodologies to qualitative problem solving, relatively uncomplicated methods have been developed to help intelligence analysts structure their analysis. These structured methods, which can be applied to a broad range of problems and do not focus exclusively on mathematical solutions, provide a scientific and demonstrable approach to analysis that can enhance the intelligence analyst's objectivity. Structured methodologies do not try to replace the subjective insight of the intelligence analyst. Instead the intent is to use a logical framework to illustrate and capitalize on intuition, experience, and subjective judgment.

Some publications do identify which methods are best suited to solve particular types of analytical problems,[59] but not all intelligence analysts receive training in these methodologies. Morgan Jones, a former analyst for the CIA, has recently added *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving.* This book presents 14 structured methods to aid analysis and decisionmaking. Although it is written for both business and personal use, the structured methods he discusses are among those taught to the fraction of Intelligence Community analysts who enroll at the Joint Military Intelligence College or other intelligence schools.

Numerous other books and software are dedicated to teaching an analyst how to apply one specific structured methodology. The Rand Corporation, for example, offers a book providing a specific methodology for predicting ethnic conflict. The authors propose a model divided into three stages meant to help an analyst identify the fundamental

---

[58] Steven R. Mann, "Chaos Theory and Strategic Thought," *Parameters* 22, no. 3 (Autumn 1992): 67.

[59] For example, David A. Schum, *Evidence and Inference for the Intelligence Analyst,* Volumes I and II (Lanham, MD: University Press of America, 1987); Defense Intelligence Agency (DIA), *Methodology Catalog: an Aid to Intelligence Analysts and Forecasters* (Washington, DC: DIA, 1983) and Jerome K. Clauser and Sandra Weir, *Intelligence Research Methodology* (State College, PA: HRB-Singer, Inc., 1975).

potential for strife, the movement of possible strife into probable strife, and whether probable strife will turn into real conflict.[60] Many technology companies produce software to assist the user in problem solving by guiding him through a structured methodology and product demonstrations via the Internet.[61]

Exploitation of Structured Methodologies

A structured methodology provides a demonstrable means to reach a conclusion. Even if it can be proven that, in a given circumstance, both intuitive and scientific approaches provide the same degree of accuracy, structured methods have significant and unique value in that they can be easily taught to other analysts as a way to structure and balance their analysis. It is difficult, if not impossible, to teach an intelligence analyst how to conduct accurate intuitive analysis. Intuition comes with experience. What is clear is that, even though a mixture of science and intuition is probably needed to produce superior qualitative intelligence analysis, structured methodologies are severely neglected. Even in the rare cases where a specific methodology is regularly used, there is too much reliance on only one method and not a mix of various methods. No one method is appropriate to every problem. What is needed is a set of analytical tools that can be applied individually or in combination as appropriate.

Why Are Structured Methodologies Not Used?

Structured thinking is radically at variance with the way in which the human mind is in the habit of working.[62] Most people are used to solving problems intuitively by trial and error. Breaking this habit and establishing a new habit of thinking is an extremely difficult task and probably the primary reason why attempts to reform intelligence analysis have failed in the past, and why intelligence budgets for analytical methodology have remained extremely small when compared to other intelligence functions.[63]

Under the accelerating pressures of time, intelligence analysts feel that structured analytical approaches are too cumbersome.[64] They also sense that with the increased use of structured methods comes increased accountability. An excessively burdened intelligence analyst is less confident in his own ability and will not unnecessarily expose himself to criticism. Reliance on intuition and the resistance to incorporate scientific approaches complicate the task of getting analysts to exploit structured methodologies to assist qualitative intelligence analysis.

---

[60] Ashley J. Tellis, Thomas S. Szayna, and James A. Winnefeld, *Anticipating Ethnic Conflict* (Santa Monica: The Rand Corporation 1997), 9.

[61] Marek J. Druzdzel, "Decision Analysis Software," 5 September 1998, *Decisions Systems Laboratory*, URL: <*http://www.lis.pitt.edu/~dsl/da-software.html*>, accessed 17 February 1999.

[62] Jones, *The Thinker's Toolkit*, 8.

[63] Andriole, "Indications, Warning, & Bureaucracies," 10-11.

[64] Eales, 121-124.

Intelligence analysts are also not exploiting structured methodologies when they conduct qualitative intelligence analysis because they are not convinced that this will improve their analysis. If empirical evidence shows that such an improvement will take place, then analysts may consider it worth the investment of time, effort, and risk required on their part to regularly exploit structured methodologies. However, if such empirical evidence shows that exploiting structured methodologies will not significantly improve qualitative intelligence analysis, then analysts can devote their time and effort to enhancing their intuitive skills.

The results from the series of experiments conducted for this study may provide some empirical data needed by intelligence analysts to make a decision on whether they should begin exploiting structured methodologies.

THE EXPERIMENT

The Control Group Versus the Experimental Group

Arguments both for and against the use of structured methodologies to improve qualitative intelligence analysis may have merit. Therefore, empirical evidence is needed to determine if exploiting structured methodologies will improve qualitative intelligence analysis. A direct comparison of analytical results derived from using a structured method with results derived solely from an intuitive approach is necessary for a relevant experiment. The author designed an experiment to make such a comparison.

The purpose of the experiment was to compare the analytical conclusions drawn by individual analysts in two different groups: a control group and an experimental group. Individual analysts in the control group would use the traditional intuitive approach to analyze two different qualitative intelligence problems. Analysts in the experimental group would exploit a specific structured methodology to aid them in their analysis of these same two problems. Analysts' answers would be scored as either correct or incorrect and compared statistically to determine whether the experimental group did significantly better than the control group.

Competing Hypotheses and Level of Significance

The experiment would test the truth of both the null hypothesis (H_0) and the alternative, or research, hypothesis (H_1). The level of significance was set at .05 before the experiment was conducted.[65]

---

[65] A one-tailed test of statistical significance is appropriate to determine whether to reject the null and research hypotheses, given their directional nature. Two-tailed tests are appropriate to determine if factors such as rank, experience, education or branch of service may have affected the results of the experiment, as no assumption was made as to how these factors may influence qualitative intelligence analysis. The author is grateful to Francis J. Hughes, JMIC Faculty, for invaluable assistance in identifying statistical methods appropriate to this study.

H_0: Exploiting structured methodologies *will not* improve qualitative intelligence analysis.
H_1: Exploiting structured methodologies *will* improve qualitative intelligence analysis.

Determining Sample Size and Choosing a Statistical Test

Due to the real-world commitments of the intelligence analysts at each JIC, it was impossible to predetermine how many analysts would be sampled during the experiment. Not knowing the sample size or expected frequencies of each cell beforehand made it impossible to select an appropriate statistical test to analyze the information until all of it was collected. On the day of the experiment each JIC Commander decided which intelligence analysts would be available to participate. The decision of who would participate was made based upon that day's schedule as driven by operational requirements. The decision was not made based upon an attempt to alter the results of the experiment.

The available analysts from each JIC were randomly assigned to either the control or experimental group. Both the control group and the experimental group had 13 analysts each. The total number of analysts sampled (N) during the experiment was 26. Due to the small sample size and associated low cell frequencies, Fisher's Exact Probability Test was used to determine statistical significance for the hypotheses and for the influence of the controlled factors (rank, experience, education and branch of service).[66]

Collection Procedures

Analysts in both control and experimental groups completed a one-page questionnaire to provide the demographic information needed to crosscheck the validity of the results gathered from the experiment. Each analyst was asked to identify any training or familiarity they had with using various structured analytical methodologies and how frequently, if ever, they used structured methodologies during real-world analysis. Then the analysts in the control group were dismissed and asked to return at a later time. The analysts in the experimental group were given an hour of training on a specific structured methodology—hypothesis testing. The training was standardized at each JIC and taught from the same lesson plan and workbook.[67] The analysts in the experimental group were asked not to discuss their training with the analysts in the control group until after the experiment.

When the analysts assigned to the control group returned, the two groups were segregated. Each analyst in each group was then given a map, both intelligence scenarios,

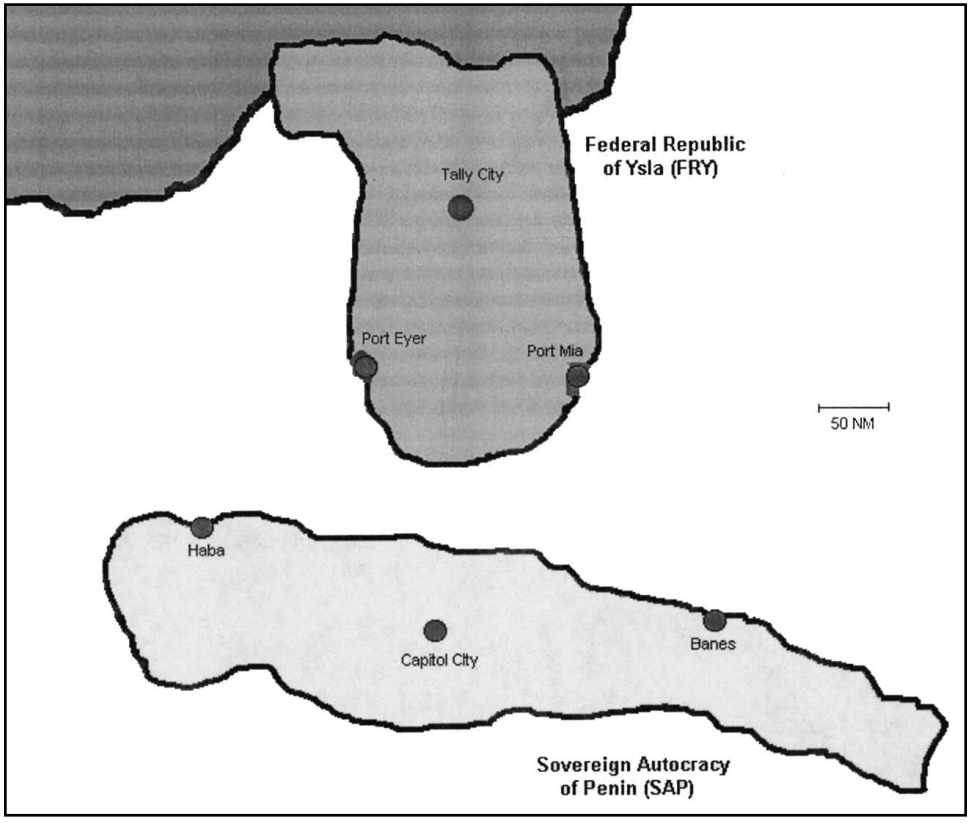
---

[66] Marija J. Norusis, *SPSS 8.0 Guide to Data Analysis* (Upper Saddle River, NJ: Prentice-Hall, 1998), 315. Fisher's Test produces a probability for a one-tailed test. Several theories address how one can use Fisher's Test to produce a probability for a two-tailed test. The most common method is to simply double the one-tailed test result, and not to exceed a probability of 1. Doubling the probability for one-tailed results is the method the author used. Other methods use more complicated mathematical formulas, but yield similar probabilities.

[67] Morgan D. Jones authored the Hypothesis Testing Lesson Plan and workbook, which were used by permission. For further information on his hypothesis testing methods, see Chapter 11 of Jones' *The Thinker's Toolkit.*

and an answer sheet for each scenario. (See information on following pages). Each person was asked to analyze the first scenario, then to complete the answer sheet as individuals within one hour. Once this task was completed, they were asked to analyze the second scenario and complete its answer sheet as individuals within 30 minutes. At the end of the allotted time they were asked to turn in their completed answer sheets and any other notes they had made. Both groups were given the same amount of time to analyze the scenarios and to complete the answer sheets, so neither group had an advantage of time over the other. All notes made by the analysts were collected to determine what approach analysts in the control group used and to ensure that analysts in the experimental group properly applied the hypothesis testing method. All analysts were interviewed after completing the experiment to gain further insights into how they approached analyzing intelligence problems presented both in the experiment and in their official duties.

Only the first question on the answer sheet for each intelligence problem was scored. It was scored as either correct or incorrect. For the first intelligence scenario the correct answer was to expect an attack at Port Mia. For the second scenario the correct answer was that the intentions of the adversary government were peaceful.



Map for Intelligence Scenarios 1 and 2.

INTELLIGENCE SCENARIO 1

You provide strategic intelligence to the military and political leaders of your country, the Federal Republic of Ysla (FRY). The Sovereign Autocracy of Penin (SAP) and FRY are at war. SAP is conducting air reconnaissance, special operations, and air bombing attacks against FRY to prepare the way for a military attack. You have determined that due to the unique geography of your country and the limited amphibious capabilities of the SAP military, only two places in FRY are vulnerable to an amphibious attack by the SAP military. SAP naval forces can conduct operations out to 250 nautical miles. To best defend FRY you need to determine how and where the SAP military invasion will occur. Using the above assumptions and the scenario map, conduct an analysis of the following intelligence information (it is listed chronologically). Keep in mind that the FRY National Leadership is concerned the SAP military will launch a diversionary attack against Port Mia while the main attack is against Port Eyer. They want your analysis to include information on whether the SAP military is planning to use deception, diversion, or neither in conjunction with their attack.

Based on order of battle from multiple sources you know the majority of SAP naval/ amphibious forces are docked in port at Banes. Multiple sources indicate that SAP has relocated most of its ground forces to Haba and reassigned them to the recently modernized Third SAP Corps. COMINT reporting indicates that a new SAP Marine General was assigned as Commander of the Third SAP Corps. On January 28th open sources report that General Sage, the SAP Supreme Military Commander, left SAP to encourage the nearby countries to remain neutral during the conflict; his travel schedule and return date are unknown. The SAP Government publicly announced a ban on all visits to the SAP coast. 007, one of FRY's top HUMINT agents working in Capitol City, reported the SAP main attack will occur near Port Eyer and may be preceded by diversionary attacks elsewhere in FRY. 086, another FRY spy, working near Banes reported that SAP would land a small force at Port Mia before the main attack at Port Eyer. Multiple sources indicate the SAP military has conducted amphibious exercises with submerged obstacles. COMINT reporting indicated major moves of SAP marine military forces to the northwest part of SAP. COMINT reports also indicated a major movement of forces from Capitol City to the northeast. SAP bombing raids against Port Eyer number twice that against Port Mia. The SAP bombing of Ports Eyer and Mia has restricted the flow of traffic in and out of both areas. The majority of SAP air reconnaissance and special operations have been against Port Eyer. On February 19th, FRY air reconnaissance showed no changes in ships at Haba. On February 25th, FRY air reconnaissance showed no change in shipping traffic in Banes. On March 8th, FRY air reconnaissance of both Haba and Banes showed increased shipping around Banes only. On March 30th, FRY air reconnaissance showed 20 new landing craft docked at Haba; air reconnaissance at Banes on the same day was inconclusive due to weather.

QUESTIONS FOR INTELLIGENCE SCENARIO 1

1. Where and how will the SAP's military attack FRY?

2. Support your conclusion. (Please attach any other notes you made.)

3. What other possible courses of action did you consider?

4. What analytical method did you use? How did you analyze this scenario?

5. Was this scenario similar to another current or historical event?

6. What is your assessment of the validity of this experiment?

7. Please provide your name and rank. Your answers and identity will be kept anonymous!

INTELLIGENCE SCENARIO 2

Due in part to your exceptional analysis, the Federal Republic of Ysla (FRY) successfully defended itself from a major invasion by the Sovereign Autocracy of Penin (SAP). On May 8th of last year, the war ended in a stalemate after the U.S. intervened, and both FRY and SAP governments signed an armistice. U.S. troops established a presence in FRY to deter SAP from attacking again. The SAP Government is concerned that the FRY military may launch an attack on SAP. The SAP Government wants the U.S. to withdraw its forces from FRY before SAP signs any peace treaty. Tensions between the FRY and SAP remained high throughout the year. However, at the beginning of the New Year, the leader of SAP, President Castrol, appeared to be making peaceful overtures to the FRY Government. Your superiors have asked you to analyze the evidence below and determine whether the SAP Government has new and peaceful intentions.

On January 15th, the SAP News Agency, the official news agency of the SAP Government, described an interview that President Castrol had with the editorial committee of a Caribbean newspaper, *The Island Times* on January 10th. President Castrol proposed: "a peace agreement...may be concluded between SAP and FRY and the military forces of both countries may be cut drastically under the condition where the U.S. imperialist troops are withdrawn from FRY."

In a subsequent meeting with U.S. Senator Harley (Democrat) in mid-January, President Castrol made it clear that a peace agreement between SAP and FRY could be concluded before U.S. forces were withdrawn.

U.S. intercepts since mid-February of secure, high-level, SAP military command communications have revealed no indications of unusual military activities or preparations for hostilities.

Over the next seven months the SAP News Agency was consistent in reporting the new peace proposals, only occasionally reverting to a "hard line" stance and then attributing this stance to unnamed spokesmen.

Last year, shortly after the armistice was signed, Red Cross delegates from both FRY and SAP began meeting on a regular basis to share information to help locate and identify soldiers from both sides who were missing in action during the war. Initially, the SAP News Agency coverage of the Red Cross meetings was very negative. After January of this year, however, the tone of the coverage changed. The reporting became essentially factual and objective.

In February of this year, the SAP Government began a national blood donation campaign claiming shortages, although the reason for shortages was not disclosed nor had there been any major disaster causing shortages to occur. Later the same month, President Castrol gave another "unofficial" interview to a journalist from the *Washington Times.* In the interview President Castrol again iterated that a peace treaty could be signed between SAP and FRY before U.S. troops withdraw from FRY.

INTELLIGENCE SCENARIO 2

On March 15th, SAP announced the execution of five SAP nationals who were members of a FRY spy ring during the war.

The commander-in-chief of SAP armed forces retired on March 29th and was replaced by the deputy commander-in-chief.

The number and tone of SAP propaganda broadcasts changed noticeably in the spring. The number of anti-FRY radio broadcasts declined from about 25 per day to about 16 broadcasts per day. Also, the usual abusive and slanderous words used in the broadcasts were toned down considerably.

In April, the two governments signed an agreement allowing each other's military attaches unrestricted movement without pre-travel approval.

Monitoring of SAP News Agency wire service releases containing anti-FRY statements declined from a high of 27 percent in January to 10 percent in April.

Over the past six months SAP military training has maintained its normal cycle.

Training flights of SAP fighter aircraft and bombers have been significantly curtailed over the past four months. In that same period the FRY Government has not detected any attempt by the SAP Government to infiltrate agents or armed guerrillas

The unusually large number of SAP reservists called to active duty during the war will be discharged this month.

SAP ground-force medical units conducted a large-scale, out-of-training-cycle exercise yesterday.

U.S. photoreconnaissance reveals that dozens of landing craft used in the SAP military operations against FRY during the war have not been repaired.

QUESTIONS FOR INTELLIGENCE SCENARIO 2

1. What are the intentions of the SAP Government?

2. Support your conclusion. (Please attach any other notes you made.)

3. List all the possibilities you considered.

4. What analytical method did you use? How did you analyze this scenario?

5. Was this scenario similar to another current/historical event?

6. What is your assessment of the validity of this experiment?

7. Please provide your name and rank. Your answers and identity will be kept anonymous!

HYPOTHESIS TESTING ILLUSTRATION: INTELLIGENCE SCENARIO 1

Possible Hypotheses are:

H1: Main attack at Port Eyer, no major deception or diversion.

H2: Main attack at Port Eyer, with deception pointing to Port Mia.

H3: Main attack at Port Eyer, with diversionary attack at Port Mia.

H4: Main attack at Port Mia, no major deception or diversion.

H5: Main attack at Port Mia, with deception pointing to Port Eyer.

H6: Main attack at Port Mia, with diversionary attack at Port Eyer.

EVIDENCE	H_1	H_2	H_3	H_4	H_5	H_6
1. Multiple Sources (MS), majority of SAP Naval forces at Banes.	I	C	C	C	I	I
2. MS, majority of ground forces assigned to modernized Third Corps at Haba	C	I	C	I	C	C
3. COMINT, new Marine general commanding Third SAP Corps	C	I	I	I	C	C
~~4. 28 Jan, General Sage visits neutral countries; return date unknown~~	~~?~~	~~?~~	~~?~~	~~?~~	~~?~~	~~?~~
~~5. SAP bans visits to coasts~~	~~C~~	~~C~~	~~C~~	~~C~~	~~C~~	~~C~~
6. 007, main attack at Port Eyer with possible diversion	I	I	C	I	C	I
7. 086, small force attacks Port Mia then main attack at Port Eyer	I	I	C	I	C	I
~~8. SAP conducts amphibious exercises with submerged obstacles~~	~~C~~	~~C~~	~~C~~	~~C~~	~~C~~	~~C~~
9. COMINT, Marines move to northwest SAP	C	I	I	I	C	C
10. COMINT, major movement of forces from Capitol City to northeast SAP	I	C	C	C	I	I
11. SAP bombs Port Eyer 2X as much as Port Mia	C	I	C	I	C	C
~~12. SAP bombing restricts traffic in/out of both ports~~	~~C~~	~~C~~	~~C~~	~~C~~	~~C~~	~~C~~
13. Majority of SAP air recon and SOF directed against Port Eyer	C	I	C	I	C	C
14. 19 Feb and 25 Feb, no change in ships at Haba or shipping at Banes	I	C	I	C	C	C
15. 8 Mar, increase in shipping at Banes	I	C	I	C	C	C
16. 30 Mar, 20 new landing craft at Haba; Recon at Banes is inconclusive due to weather	C	I	C	?	?	?

Hypothesis Testing Matrix Example for Intelligence Scenario 1.

Note: Letters characterize the attributed relationship between evidence and hypothesis: consistent=C; inconsistent=I; ambiguous=?; evidence that is either consistent or ambiguous for all hypotheses is "lined out" to show that it was considered, then disregarded, in favor of more telling "directional" evidence.

HYPOTHESIS TESTING ILLUSTRATION: INTELLIGENCE SCENARIO 2

Possible Hypotheses are:

H_1: Peace
H_2: Business-as-Usual
H_3: Deception.

EVIDENCE	H_1	H_2	H_3
1. Jan-Apr, SAP News Agency Anti-FRY statements decline to 10%	C	I	C
2. Jan-Apr, SAP fighter/bomber training sorties decline	C	I	C
3. Jan-Apr, FRY detects no SAP infiltration attempts	C	I	I
~~4. Jan-Jun, SAP military training cycle is normal~~	~~C~~	~~C~~	~~C~~
5. Jan 15, Castrol proposes peace with FRY	C	I	C
6. Mid-Jan, Castrol says peace before U.S. troops leave	C	I	C
7. Feb, SAP News Agency begins positive reporting of ICRC	C	I	C
8. Early Feb, SAP Government blood drive	I	C	C
~~9. Mid-Feb, no unusual SAP C2 activity~~	~~C~~	~~C~~	~~C~~
10. Late-Feb, Castrol says peace treaty before U.S. leaves	C	I	C
11. Feb-Aug, SAP News Agency consistently reports peace proposal	C	I	C
12. Mar 15, SAP executes members of FRY spy-ring	I	C	I
~~13. Mar 29, SAP CINC retires and replaced by his Deputy~~	~~C~~	~~C~~	~~C~~
14. April, FRY and SAP sign agreement allowing unrestricted travel	C	I	I
15. April, SAP discharges reservists called up during the war	C	I	I
16. April, SAP conducts a large, out-of-cycle medical exercise	I	C	C
17. April, SAP landing craft remain unrepaired	C	I	I
18. Spring, SAP propaganda broadcasts decrease in number and tone	C	I	I

Hypothesis Testing Matrix Example for Intelligence Scenario 2[68]

[68] Although assigning a C, I, or ? to an individual line of evidence is a subjective judgment, by visually displaying the evidence and hypotheses in a matrix the analyst can better judge each piece of evidence then aggregate all the evidence to determine which hypothesis is most likely true. Subjective judgments and intuition still play an inescapable role in analysis. Individual analysts will seldom assign C, I, or ? in the same way, but by visually displaying it, other analysts can question their logic, readily identify which pieces of evidence they disagree on, and more quickly form a consensus.

Experimental Results Arrayed in Contingency Tables

Tables 1 and 2 summarize the responses given by analysts in the control and the experimental groups to each intelligence scenario. Tables 3-10 show how the analysts answered each intelligence scenario based on rank, years of experience, level of education, and branch of service.

A. Comparison of Responses between Control and Experimental Groups:

	Control Group	Experimental Group
# of Incorrect Answers	11	10
# of Correct Answers	2	3

Table 1. Response by Group to Intelligence Scenario 1

	Control Group	Experimental Group
# of Incorrect Answers	4	0
# of Correct Answers	9	13

Table 2. Response by Group to Intelligence Scenario 2

B. Comparison of Responses between Civilian/Officer and Enlisted:

	Civilian/Officer	Enlisted
# of Incorrect Answers	9	12
# of Correct Answers	3	2

Table 3. Response by Rank to Intelligence Scenario 1

	Civilian/Officer	Enlisted
# of Incorrect Answers	1	3
# of Correct Answers	11	11

Table 4. Response by Rank to Intelligence Scenario 2

C. Comparison of Responses Based on Years of Experience:

	Less than 10 years	10 years or more
# of Incorrect Answers	12	9
# of Correct Answers	2	3

Table 5. Response by Years of Experience to Intelligence Scenario 1

C. Comparison of Responses Based on Years of Experience: (Cont'd)

	Less than 10 years	10 years or more
# of Incorrect Answers	2	2
# of Correct Answers	12	10

Table 6. Response by Years of Experience to Intelligence Scenario 2

D. Comparison of Responses Based on Level of Education:

	<Bachelor Degree	Bachelor Degree or Higher
# of Incorrect Answers	12	9
# of Correct Answers	2	3

Table 7. Response by Level of Education to Intelligence Scenario 1

	<Bachelor Degree	Bachelor Degree or Higher
# of Incorrect Answers	2	2
# of Correct Answers	12	10

Table 8. Response by Level of Education to Intelligence Scenario 2

E. Comparison of Responses between Military Services:

	Navy/Marine	Army/Air Force
# of Incorrect Answers	9	12
# of Correct Answers	1	4

Table 9. Response by Branch of Service to Intelligence Scenario 1

	Navy/Marine	Army/Air Force
# of Incorrect Answers	0	4
# of Correct Answers	10	12

Table 10. Response by Branch of Service to Intelligence Scenario 2

Analytical Strategy

Fisher's Exact Probability Test was used to statistically analyze the data and determine whether the null hypothesis could be rejected. This formula was also used in a two-tailed test to measure any variances in responses based on the different demographic groups. In these cases Fisher's Test would measure the probability that the differences in the answers were caused by some other factor than the use of a structured methodology to assist in qualitative intelligence analysis. The original tables displaying demographic data for the control and experimental groups contained several columns, not just two. However, Fisher's Test can be used to measure data only in a two-by-two matrix, so it was necessary to modify the original tables by combining some columns to arrange the data in an appropriate two-by-two matrix.

CONSIDERATIONS AND LIMITATIONS

Although this experiment did collect and analyze data on several different factors that might affect the answers an analyst would provide, it could not identify and analyze all factors. To encourage individual participation an agreement was made that the results of individual analysts would not be released. To encourage the JICs to provide as many analysts as possible it was agreed that the specific results of each JIC would be made available only to that particular JIC. This experiment was designed to compare the answers given by the control and experimental groups; it would not compare JIC against JIC. Therefore, the way in which analysts were made available, driven as it was by real-world events, did not alter the validity of the experiment.

Designing the Experiment

Certainly, one can find some fault in both intelligence scenarios used during the experiment. Nevertheless, both scenarios were submitted to a rigorous pre-testing and revision process to ensure both scenarios were valid and reliable measures of an intelligence analyst's qualitative analytical capability during the time allotted for the experiment and appropriate for the structured methodology taught to the experimental group.

Several obstacles hinder the design of an intelligence scenario to measure the accuracy of an analyst's conclusions. A hypothetical scenario begs the question of whether one can authoritatively claim that a correct answer exists. Since the event never occurred, the burden is on the creator of the scenario to ensure only one conclusion can be drawn. In contrast, using an actual historical event as the basis for an intelligence scenario runs the risk that the analyst will recognize the scenario for what it is and base his conclusions on the known outcome rather than on the evidence presented. The intelligence scenarios used in the experiment were based on actual historical events.

The first scenario was developed in coordination with Tom Murray, former CIA analyst and trainer and currently Senior Vice President of Sequoia Associates, Incorporated. The scenario was based on known strategic intelligence possessed by

German intelligence prior to the invasion of Normandy during World War II. It was necessary to alter some of the evidence such as the names of individuals, units, and geographic locations in the scenario to disguise the fact that this scenario was based on the invasion at Normandy, but the basic evidence remained unchanged. In this scenario the analysts were asked to determine where the actual invasion would occur.

The second intelligence scenario was based upon a case study presented in *Intelligence Research and Methodology*, by Jerome Clauser and Sandra Weir. The case study examined a series of incidents in which it appeared the North Korean Government was making a sincere effort to improve peace on the peninsula in the 1970's.[69] This scenario was modified with the assistance of Morgan D. Jones. The subjects were asked to determine whether the adversary in the scenario was sincerely pursuing peace, using peace as a deception, or conducting business as usual.

Various students at the JMIC tested both intelligence scenarios before they were used in the experiment at the JICs. The students were asked to analyze both scenarios and complete an answer sheet. The answer sheet asked them to draw some conclusions and also asked whether they recognized the scenarios as any actual historical event. The scenarios were then modified and given to another group of students to test. In the final round of testing only three out of 20 students recognized that the first scenario was related to the Normandy invasion; however, only one of the three who recognized the historical link provided the correct answer. None of the students could identify the actual event used as a basis for the second scenario. During the actual experiment at the JICs, five of the 26 subjects identified the Normandy invasion as the basis for the first intelligence scenario. Four of these five were in the control group and the other was in the experimental group. Of the five only one in the experimental group and another in the control group provided the correct answer to the first scenario. No one at the JICs identified the actual historical event used as a basis for the second scenario. These checks on the historical identifiability of the scenarios address the potential concern of "analysis as art" proponents that deep familiarity with a particular region or problem would affect the outcome of this or a similar experiment. It would appear that this concern, though well-founded, can be overcome by careful selection of scenarios. Scenario construction or borrowing is not a simple matter, as a real-world "outcome" must be captured to ensure a "correct" answer is known.

The questions on the answer sheets were open-ended rather than multiple choice. Although using a multiple choice test simplifies the scoring process, it does not accurately portray how analysts provide answers outside the classroom. A multiple choice test defines the range of options available; in qualitative intelligence analysis, defining and narrowing the range of options is a part of the answer in itself. Asking open-ended questions provided insights into how many possible hypotheses each analyst considered and how specific a response each analyst felt confident in providing.

---

[69] Clauser and Weir, 358-369.

Time Spent Analyzing the Scenarios

Rather than allow the analysts to work at their own pace, a specific period of time was allotted to work each problem; however, the analysts were allowed to turn in their answer sheets anytime before the allotted time expired. Although it would be interesting to compare the number of correct answers with the amount of time spent on the problem, it would be of little help in determining whether exploiting structured methodologies will improve qualitative intelligence analysis. Based on observations made during the experiment, it seems that the amount of time spent on analyzing a problem had little to do with the analyst correctly answering a problem or using a structured method. Both control and experimental groups had analysts who completed both problems quickly and had analysts who used the entire amount of time allotted.

Most analysts work under a deadline. Allotting a fixed amount of time to solve each problem put pressure on the analyst (simulating real-world constraints) and ensured the answer sheets were returned in time to be included in this study. It also held the variable of time constant so the results of the experiment were less likely to be tainted by the time factor. Many of the analysts remarked that they enjoyed the opportunity to concentrate on a specific problem without being interrupted.

THE FINDINGS

This exploratory research provides empirical evidence suggesting that exploitation of a structured methodology (hypothesis testing in this example) will improve qualitative intelligence analysis. Even though this evidence is for a narrowly defined instance (the second intelligence scenario) and not conclusive, such evidence did not exist before this experiment was conducted. Factors such as rank, experience, education, and branch of service did not appear to affect the results.

Description of the Findings

As Tables 1 and 2 show, the overall qualitative intelligence analysis of those in the experimental group was better than that of those in the control group for both scenarios. Despite this, the improvement measured in the first scenario did not meet the threshold of statistical significance (see results for Table 1 in Table 11). Nor did the probabilities computed for Tables 3-10 meet the established threshold of statistical significance (see results for Tables 3-10 in Table 11), confirming that the differences in responses are probably not due to these factors. However, the improved qualitative analysis of the experimental group over that of the control group in the second scenario was statistically significant (see results for Table 2 in Table 11).

Table No.	Description	Scenario No.	Fisher's Probability
1	Control and Experiment	1	.5
2	Control and Experiment	2	.048
3	Rank	1	.844
4	Rank	2	.718
5	Experience	1	.844
6	Experience	2	1.0
7	Education	1	.844
8	Education	2	1.0
9	Branch of Service	1	.686
10	Branch of Service	2	.244

Table 11. Probabilities that Results are Due to Chance

Expectations

The results were surprising. The author expected a significant improvement in qualitative intelligence analysis in the first scenario, whose inherent complexity, it seemed, would give the analysts who used the hypothesis testing method an advantage over those who did not employ a structured method. But this advantage did not materialize. Most of the analysts using hypothesis testing seemed to have had difficulty identifying all of the possible hypotheses and determining the consistency of each piece of evidence with each hypothesis.

Because the second scenario was simple and straightforward, the author thought that there would be little or no advantage to be gained by structuring the problem and sorting the evidence. In the event, however, the structured approach proved more effective.

In hindsight it was asking too much to expect the analysts to proficiently apply the hypothesis testing method to complex problems like the first intelligence scenario after just one hour of training. This may explain, in part, why the experimental group did not perform significantly better than the control group on the first scenario. Because the first scenario, with six hypotheses to consider, is more complicated than the second scenario, with only three hypotheses, one may be tempted to conclude that the hypothesis testing method is useful for structuring only simple problems. Nevertheless, based on the information gathered during this experiment, the author would guess that the hypothesis testing method can be useful in structuring more intricate problems, provided that the analyst has been adequately trained to proficiently apply the method.

What Does All This Mean?

Quite simply, the experimental group performed significantly better on the second intelligence scenario than did the control group. The improvement appears to be due to members of the experimental group using a particular structured methodology while the members of the control group did not use any structured methodology to aid their analysis. The improvement does not appear to be a consequence of rank, experience, education, or branch of service. The improvement measured in qualitative intelligence analysis during the first intelligence scenario is not significant.

Why Improvement in the Second Scenario But Not the First?

The first scenario may have affected the control group's analysis of the second scenario. In the first scenario it was obvious that some form of deception was being used; the problem was determining which attack was real and which was the deception. The second scenario was more clear and direct; however, some analysts may have been biased and assumed deception was being used in the second scenario because of their recent exposure to the use of deception in the first scenario. It appears that those analysts who used the hypothesis testing method were better able to remain objective and analyze the evidence in the second scenario without being influenced by the first scenario. It seems the analysts who based their analysis solely on their intuition were less objective in their analysis.

Another Approach to Analyzing the Data

During the experiment each analyst was asked one question from both intelligence scenarios. Their answers were marked as either correct or incorrect. Thus, an analyst who answered both questions correctly scored 100 percent. If an analyst answered one question correctly and the other incorrectly, he scored 50 percent. If he answered both questions incorrectly, he scored 0 percent. The scores from analysts who used a structured methodology ranged from 50-100 percent. The analysts who did not use a structured methodology ranged in scores from 0-50 percent. While three analysts in the experimental group answered both questions correctly, no one in the control group answered both questions correctly. By this measure, exploiting a structured methodology improved qualitative intelligence analysis.

To Reject H_0 or Not?

Considering all the arguments, the information collected, and the analysis and interpretation of that information, the null hypothesis—that exploiting structured methodologies *will not* improve qualitative intelligence analysis—can be rejected. Of course there are several qualifiers that affect the veracity of the alternate hypothesis— that exploiting structured methodologies *will* improve qualitative intelligence analysis. The single most critical qualifier is that analysts must be adequately trained to ensure they are able to proficiently apply the appropriate structured methodology.

Unquestionably one can create a problem where the answer is so obvious that a structured methodology will be of no benefit. Likewise, one can design a scenario so complicated and ambiguous that the correct answer will never be revealed. Nevertheless, as this experiment demonstrated, there are instances where qualitative intelligence analysis can be improved by exploiting structured methodologies. Only by applying different structured methodologies to different types of intelligence problems will one find out where and when structured methods are most effective.

This experiment examined only one structured methodology—hypothesis testing. Other experiments that examine different methods, different problems, and utilize different analysts from different agencies could be pursued by other investigators. In the meantime, analysts within the Intelligence Community should be encouraged to exploit various structured methodologies.

IMPLICATIONS AND RECOMMENDATIONS

A Conclusion

This study has produced an answer to the question: "Will exploiting structured methodologies improve qualitative intelligence analysis?" The approach taken to answer the question was straightforward. Competing hypotheses were developed based on the research question, arguments supporting both hypotheses were explored, an impartial experiment was designed to provide empirical evidence, and a statistical test was used to determine the significance of the evidence produced. For both scenarios the analysts who used structured methods outperformed the analysts who did not. The improvement measured in the second intelligence scenario was statistically significant; therefore, the null hypothesis—that exploiting structured methodologies *will not* improve qualitative intelligence analysis—was rejected.

The author has determined that exploiting structured methodologies will improve qualitative intelligence analysis. There are, however, several qualifiers. The improvement is not necessarily automatic or significant for every case. Intelligence analysts must be adequately trained to select an appropriate structured methodology or combination of methodologies germane to the problem and apply the method(s) proficiently. A more precise conclusion drawn from the experiment as presented in this study is: "Exploiting structured methodologies *can* improve qualitative intelligence analysis." Further research is needed to definitively answer the original research question.

Other Insights

Based on the numerous interviews the author conducted with intelligence analysts from many different intelligence units and agencies, it is apparent that more basic research is needed in this area of intelligence analysis. Nearly every analyst had a different definition of intelligence analysis. Most analysts believe that analysis occurs automatically as they gather information and prepare that information for dissemination. It is not a function for which they specifically allocate time.

Analysis involves critical thinking. Structured methodologies do not perform the analysis for the analyst; the analyst still must do his own thinking. But by structuring a problem the analyst is better able to identify relevant factors and assumptions, formulate and consider different outcomes, weigh different pieces of evidence, and make decisions based on the available information. While exploiting a structured methodology cannot guarantee a correct answer, using a structured methodology ensures that analysis is performed and not overlooked.

From the discussions with the test subjects after the experiment it became obvious to the author that analysts in the control group were not as clear in their thinking as the analysts in the experimental group. After reading the scenarios members of the control group formed a conclusion, then went back to the scenario to find evidence that supported their conclusion and ignored contradictory evidence. When asked to justify their answers, analysts in the control group often cited some "key" information that gave them a flash of insight. Members of the control group seemed to be looking for the one piece of information—the "Holy Grail"— that would make sense of everything else. This approach flies in the face of the fact that, more often than not, qualitative intelligence analysis must be accomplished with incomplete information.

Members of the experimental group examined all evidence provided in the scenario prior to making their decision. They felt confident that they were making the best decision they could with the amount of information available. They acknowledged that their decision may not be the right one and added that if more evidence became available they would reevaluate their conclusion taking into account this new information.

Even though most analysts had not received training in or used structured methods previously, analysts who received training in hypothesis testing expressed the opinion that exploiting such a method would aid and improve their analysis.

Recommendations

The author recommends that various structured methodologies be taught to all intelligence analysts of every service and agency during both initial and subsequent training. Intelligence analysts should be encouraged to use structured methodologies when drafting analytical narratives. Analysts should be expected to utilize structured methodologies to visually present their analysis during intelligence briefings. Also, intelligence units conducting real-world qualitative intelligence analysis should be encouraged to experiment with different structured methodologies and compete with other similar units in regular analytical exercises. The results from exploiting various structured methodologies from both real-world situations and during exercises should be published and shared with other intelligence units, services, and agencies.

Further Research

The results of this experiment need to be confirmed. The author recommends that a series of similar experiments be conducted, either separately or in any combination, to test other factors that may affect the outcome of qualitative intelligence analysis.

Reverse Order of Scenarios. Future researchers may wish to conduct the same experiment as the original except reverse the order in which the intelligence scenarios are given to the analysts. Alternatively the researcher may develop his own scenarios but present them to different test subjects in a different order and track the results to see if the order in which the scenarios were presented affected the results of their analysis.

Intensive Training. Expand the amount of time spent training the experimental group from one hour to three or more hours and include more complex problems. Use the same scenarios as in the original experiment to test this author's theory that more training would have allowed the analysts to proficiently apply the hypothesis testing method to more complicated problems such as the first intelligence scenario.

Sophisticated Scenario. Future researchers may wish to conduct a similar experiment using a more sophisticated scenario to determine whether design flaws in the original scenarios affected the results of the original experiment.

Before and After. Instead of dividing analysts into control and experimental groups, have them analyze a scenario intuitively then train the same analysts in an appropriate structured methodology and have them analyze the same problem using the structured technique. Compare their first response with their second response and measure the improvement. A researcher utilizing this approach must develop a test to measure if the improvement arises from analysts' exploiting a structured method or simply from seeing the same or similar problem again.

Different Method. Conduct an experiment using a structured methodology other than hypothesis testing. The researcher must develop a new intelligence scenario appropriate to the structured methodology being tested.

Team Approach. Instead of measuring the responses of individuals, divide the analysts into teams and ask them to develop a consensus and answer the questions as a team. Have some teams use a structured methodology and have other teams use the traditional intuitive approach.

Measure Time. Instead of holding time as a constant, ask the analysts to solve the problems as quickly as possible and record how long it takes each analyst to solve the problem. Consider both accuracy and timeliness when measuring improvement in qualitative intelligence analysis.

Multiple Choice. Instead of asking open-ended questions, provide the analysts with a multiple choice answer sheet. This will simplify the scoring process and measure improvement while ensuring that every analyst considers the same possible outcomes.

Two-Tailed Test. Develop a hypothesis and design an experiment to measure if exploiting structured methodologies will cause a change in qualitative intelligence analysis in either direction. Also, other demographic information (such as gender, age, and personality type) should be collected and analyzed to see if these factors affect the results.

FINAL IMPRESSION

The author's motivation to conduct research into qualitative intelligence analysis comes from his own experience with the difficulties common to conducting and training others in analysis. Somewhat surprisingly, the present research has revealed how remarkably little analysts within the Intelligence Community appear to know about analytic methods, and less surprisingly, how great is the gap between their current and future analytic potential. It is clear to this researcher that a moderate investment in analytic training would substantially improve intelligence analysis.

BIBLIOGRAPHY

An analytic methodologist in Central Intelligence Agency's Directorate of Intelligence. Interview by author, 29 April 1999.

Andriole, Stephen J., Ph.D. *Handbook of Decision Support Systems*. Blue Ridge Summit, PA: Professional and Reference Books, 1989.

_____. *Handbook of Problem Solving: An Analytical Methodology.* New York: Petrocelli Books, Inc., 1983.

_____. "Indications, Warning, & Bureaucracies." *Military Intelligence Professional Bulletin* 10, no. 3 (July-September 1984): 6-12.

_____. *Methods for Intelligence Analysis, Production, and Presentation*. Unpublished research paper funded by DIA. Contract no. MDA908-83-C-1899. December 1983.

_____. Senior Intelligence Researcher and former Director of the Cybernetics Technology Office of the Advanced Research Projects Agency. Email interview by author, 15 December 1998.

"Art Hammer: The Numbers Man." *Economist*, 8 August 1998, 56.

Ball, W. Frank, Lieutenant Colonel, USMC (Retired), and Morgan D. Jones. "Improving Marine Commanders' Intuitive Decisionmaking Skills." *Marine Corps Gazette* (January 1996): 63-64.

Betts, Richard K., Ph.D. "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable." *World Politics* 31, no. 1 (October 1978): 61-89.

_____. "Intelligence for Policymaking." *Washington Quarterly* 3, no. 3 (Summer 1980): 118-129.

_____. "Intelligence Warning: Old Problems, New Agendas." *Parameters* 28, no. 1 (Spring 1998): 26-35.

_____. "Policy-makers and Intelligence Analysts: Love, Hate, or Indifference?" *Intelligence and National Security* 3, no. 1 (January 1988): 184-189.

_____. "Strategic Intelligence Estimates: Let's Make Them Useful." *Parameters* 10, no.4 (Winter 1980): 20-27.

_____. "Surprise, Scholasticism, and Strategy: A Review of Ariel Levite's *Intelligence and Strategic Surprises* (New York: Columbia University Press, 1987)," *International Studies Quarterly* 33, no. 3 (September 1989): 329-343.

Brei, Captain William S. (USAF). *Getting Intelligence Right: The Power of Logical Procedure*. Occasional Paper Number Two. Washington, DC: Joint Military Intelligence College, 1996.

Brown, Thomas A., and Emir H. Shuford. *Quantifying Uncertainty Into Numerical Probabilities for The Reporting of Intelligence*. R-1185-ARPA. Santa Monica: The Rand Corporation, July 1973.

Clark, Robert M. *Intelligence Analysis: Estimation and Prediction*. Baltimore: American Literary Press, Inc., 1996.

Clauser, Jerome K., and Sandra Weir. *Intelligence Research Methodology.* State College, PA: HRB-Singer, Inc., 1975.

Coping with the Bounds: Speculations on Nonlinearity in Military Affairs. Ed. Tom Czerwinski. Washington, DC: National Defense University, 1998.

Critical Technologies for National Defense. Ed. J.S. Przemieniecki. Washington, DC: American Institute of Aeronautics and Astronautics, 1991.

Davis, Jack. "The Kent-Kendall Debate of 1949." *Studies in Intelligence* 35, no. 2 (Summer 1991): 37-49.

De Francesco, Henry F. *Quantitative Methods for Substantive Analysts*. Los Angeles: Melville Publishing Co., 1975.

Defense Intelligence Agency. *Methodology Catalog: An Aid to Intelligence Analysts and Forecasters*. DDE-2200-227-83. Washington, DC: DIA, December 1983.

DiPace, Tim. U.S. Atlantic Command Anti-Terrorism/Force Protection Officer. Interview by author, 19 March 1999.

"Don't Blame the CIA." *Economist*, 23 May 1998, 26.

Druzdzel, Marek J. "*Decision Analysis Software*," 5 September 1998. Decision Systems Laboratory. URL: <*http://www.lis.pitt.edu/~dsl/da-software.html*>. Accessed 17 February 1999.

Eales, Stewart Christopher. *Playing with Intelligence: Officer Application of Intelligence in the PURPLE SUNSET Wargame*. MSSI Thesis. Washington, DC: Joint Military Intelligence College, August 1997.

Finley, James P. "Intelligence Failure Matrix." *Military Intelligence Professional Bulletin* 20, no. 1 (January-March 1994): 14.

_____. "Nobody Likes to be Surprised: Intelligence Failures." *Military Intelligence Professional Bulletin* 20, no. 1 (January-March 1994): 15+.

Ford, Harold P. *Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating*. New York: University Press of America, 1993.

Graves, David Lawrence, Captain, USAF. *Bayesian Analysis Methods for Threat Prediction*. MSSI Thesis. Washington, DC: Defense Intelligence College, 1993.

Grunwald, Michael, and others. "CIA Halted Plot to Bomb U.S. Embassy in Uganda." *Washington Post*, 25 September 1998, A27+.

Hall, Wayne M., Lieutenant Colonel, USA. "Intelligence Analysis in the 21st Century." *Military Intelligence Professional Bulletin* 18, no. 1 (January-March 1992): 6-12.

Hammond, James D. *So You Want to be an Intelligence Analyst?* Research Paper. Washington, DC: Defense Intelligence College, October 1983.

Hayes, Richard E. President of Evidence-Based Research, Inc. Interview by author, 9 February 1999.

Henry, Ryan, and C. Edward Peartree. "Military Theory and Information Warfare." *Parameters* 28, no. 3 (Autumn 1998): 121-135.

Hilsman, Roger. "Does the CIA Still Have a Role?" *Foreign Affairs* 74, no. 5 (September/October 1995): 104-116.

Hulnick, Arthur S. "Managing Intelligence Analysis: Strategies for Playing the End Game." *International Journal of Intelligence and Counterintelligence* 2, no. 3 (Fall 1988): 321-342.

"Hypothesis Testing: A Technique for Structuring Analysis." Outline, Lesson Plan, and Workbook. N.p., n.d. Provided on 15 March 1999 By Morgan D. Jones.

Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal 1955-1992. Ed. H. Bradford Westerfield. New Haven: Yale University Press, 1995.

Jones, Morgan D. Former analyst for the Central Intelligence Agency and founder of Analytic Prowess, L.L.C. Interview by author, 15 March 1999.

_____. *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*. New York: Random House, Inc., 1998.

Kahaner, Larry. *Competitive Intelligence: From Black Ops to Boardrooms — How Businesses Gather, Analyze, and Use Information to Succeed in the Global Marketplace.* New York: Simon & Schuster, 1996.

Kam, Ephraim. *Surprise Attack: The Victim's Perspective*. Cambridge, MA: Harvard University Press, 1988.

Keithly, David M. "Leading Intelligence in the 21st Century: Past as Prologue?" *Defense Intelligence Journal* 7, no. 1 (Spring 1998): 78-88.

Kent, Sherman. *Strategic Intelligence For American World Policy.* Princeton, NJ: Princeton University Press, 1949.

Kifner, John. “Raids by U.S. Agents and Tirana Police Reportedly Thwart Attack on Embassy.” *New York Times*, 21 August 1998, A13.

Landers, Daniel F. “The Defense Warning System.” *Defense Intelligence Journal* 3, no. 1 (Spring 1994): 21-32.

Loeb, Vernon and Walter Pincus. “New Spy Satellites at Risk Because Funding Is Uncertain, Pentagon Told.” *Washington Post*, 12 November 1999, A7.

Manheim, Jarol B., and Richard C. Rich. *Empirical Political Analysis: Research Methods in Political Science*. New Jersey: Prentice-Hall, Inc., 1981.

Mann, Steven R. “Chaos Theory and Strategic Thought.” *Parameters* 22, no. 3 (Autumn 1992): 54-68.

Manthorpe, William H.J. Jr. “From the Editor.” *Defense Intelligence Journal* 7, no. 1 (Spring 1998): 3-5.

McCarthy, Mary. “The National Warning System: Striving for an Elusive Goal.” *Defense Intelligence Journal* 3, no. 1 (Spring 1994): 5-19.

Murray, Thomas H., Ph.D. Former analyst and trainer for the Central Intelligence Agency and Senior Vice President of Sequoia Associates, Inc. Interview by author, 18 January 1999.

Neustadt, Richard, and Ernest May. *Thinking in Time*. New York: The Free Press, 1986.

New York Times, 7 June 1998 and 21 August 1998.

Newing, Rod. “Consumer Information is the Fuel of a New Industrial Revolution.” *Financial Times*, 3 February 1999, B7.

Norusis, Marija J. *SPSS 8.0 Guide to Data Analysis*. Upper Saddle River, NJ: Prentice-Hall, 1998.

Nye, Joseph S. Jr. “Peering into the Future.” *Foreign Affairs* 73, no. 4 (July/August 1994): 82-93.

Nye, Joseph S. Jr., and William A. Owens. “America’s Information Edge.” *Foreign Affairs* 75, no. 2 (March/April 1996): 20-25.

“An Orderly Approach to Intelligence Analysis.” Instructor’s manual. N.p., n.d. Provided on 18 January 1999 by the Senior Vice President of Sequoia Associates, Inc., Thomas H. Murray.

Owens, William A. “Intelligence in the 21st Century.” *Defense Intelligence Journal* 7, no. 1 (Spring 1998): 25-45.

Peterson, John L. “Forecasting: It’s Not Possible.” *Defense Intelligence Journal* 3, no. 2 (Fall 1994): 37-45.

Pilzer, Paul Zane. *Unlimited Wealth*. New York: Crown Publishers, Inc., 1990.

Porteous, Samuel D. “Looking out for Economic Interests: An Increased Role for Intelligence.” *Washington Quarterly* 19, no. 4 (Autumn 1996): 191-204.

Quantitative Approaches to Political Intelligence: The CIA Experience. Ed. Richards J. Heuer Jr. Boulder: Westview Press, Inc., 1978.

Resch, David T., Captain, USA. “Predictive Analysis: The Gap Between Academia and Practitioners.” *Military Intelligence Professional Bulletin* 21, no. 2 (April-June 1995): 26-29.

Robbins, Carla Anne. “Intelligence Community is Criticized in Review.” *Wall Street Journal*, 3 June 1998, A8.

Schweizer, Peter. “Growth in Economic Espionage.” *Foreign Affairs* 75, no. 1 (January/February 1996): 9-14.

Schum, David A. *Evidence and Inference for the Intelligence Analyst*. Volumes I and II. Lanham, MD: University Press of America, 1987.

Shirley, Edward G. “CIA Needs Reform, Not New Missions.” *Wall Street Journal*, 19 November 1998, A22.

Seib, Philip. “Intelligence Gathering Remains a Vital Function,” 1 March 1999. *Dallas Morning News*. URL: *<http://www.dia.ic.gov/admin/EARLYBIRD/990302/ s199990302/ gathering.htm>*. Accessed 2 March 1999.

Siegel, Sydney. *Nonparametric Statistics For the Behavioral Sciences*. New York: McGraw-Hill Book Company, Inc., 1956.

Studeman, William O. “Leading Intelligence along the Byways of Our Future: Acquiring C4ISR Architectures for the 21st Century.” *Defense Intelligence Journal* 7, no. 1 (Spring 1998): 47-65.

Tellis, Ashley J., Thomas S. Szayna, and James A. Winnefeld. *Anticipating Ethnic Conflict.* Santa Monica, CA: The Rand Corporation, 1997.

Toffler, Alvin, and Heidi Toffler. *War and Anti-War: Survival at the Dawn of the 21st Century.* New York: Little, Brown and Company, 1993.

Tufte, Edward R. *The Visual Display of Quantitative Information.* Cheshire, CT: Graphics Press, 1983.

Turner, Michael A. “Issues in Evaluating U.S. Intelligence.” *International Journal of Intelligence and Counterintelligence* 5, no. 3 (Fall 1991): 275-284.

U.S. Commission on the Roles and Capabilities of the United States Intelligence Community. *Preparing for the 21st Century: An Appraisal of U.S. Intelligence.* Washington, DC: GPO, 1 March 1996. URL: <*http://www.access.gpo.gov/su_docs/dpos/epubs/int/int012.html*>.

Warning analyst at the National Warning Staff. Telephone interview by author, 5 November 1998.

Weiner, Tim, and James Risen. “Decision to Strike Factory in Sudan Based on Surmise: Inferred from Evidence.” *New York Times*, 21 September 1998, A1.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford, CA: Stanford University Press, 1962.

ABOUT THE AUTHOR

Master Sergeant Robert D. Folker, Jr. received the Master of Science of Strategic Intelligence degree from the Joint Military Intelligence College in 1999. He is currently Superintendent of the 325th Operations Support Squadron's Intelligence Flight at Tyndall Air Force Base, Florida. Since enlisting in the Air Force in 1986, MSgt Folker's assignments have included Non-Comissioned Officer in Charge (NCOIC), Special Intelligence Team at the Strategic Command's Intelligence and Warning Center, Offutt Air Force Base, Nebraska; NCOIC, Intelligence Element at the 80th Fighter Squadron, Kunsan Air Base, South Korea; and NCOIC, Mission Analysis Flight and Senior Analyst with the Contingency Airborne Reconnaissance Deployable Ground Station 2, Beale Air Force Base, California. MSgt Folker may be contacted at: <*robert.folker@tyndall.af.mil*>.

Joint Military Intelligence College

Occasional Papers

Unclassified papers are available through <***www.ntis.gov***>; selected papers are available through the U.S. Government Printing Office <***www.gpo.gov***>.

1. Classified paper.

2. *Getting Intelligence Right: The Power of Logical Procedure*, Capt (USAF) William S. Brei, 1996.

3. *An Office Manager's Guide to Intelligence Readiness*, Russell G. Swenson, 1996.

4. Classified paper.

5. *A Flourishing Craft: Teaching Intelligence Studies*, Papers Prepared for the 18 June 1999 JMIC Conference on Teaching Intelligence Studies at Colleges and Universities, 1999.

6. *Intelligence Essentials for Everyone*, Lisa Krizan, 1999.

7. *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods*, MSgt (USAF), Robert D. Folker, Jr., 2000.

This Page Is Intentionally Left Blank

Joint Military Intelligence College

June 1999

INTELLIGENCE ESSENTIALS FOR EVERYONE

Occasional Paper Number Six

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 1999		**00-00-1999 to 00-00-1999**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Intelligence Essentials for Everyone	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Joint Military Intelligence College,200 MacDill Blvd,Washington,DC,20340-5100**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**89**	

The Joint Military Intelligence College supports and encourages research on intelligence issues that distills lessons and improves support to policy-level and operational consumers.

This series of Occasional Papers presents the work of faculty, students and others whose research on intelligence issues is supported or otherwise encouraged by the Joint Military Intelligence College through its Office of Applied Research. Occasional Papers are distributed to Department of Defense schools and to the Intelligence Community, and unclassified papers are available to the public through the National Technical Information Service (www.ntis.gov).

Proposed manuscripts for these papers are submitted for consideration to the Applied Research Editorial Board. Papers undergo review by senior officials in Defense, Intelligence, and occasionally civilian academic or business communities. Manuscripts or requests for additional copies of Occasional Papers should be addressed to Defense Intelligence Agency, Joint Military Intelligence College, Office of Applied Research, MCE, Bolling AFB, Washington, DC 20340-5100.

Occasional Paper Number Six

INTELLIGENCE ESSENTIALS FOR EVERYONE

By Lisa Krizan

JOINT MILITARY INTELLIGENCE COLLEGE
WASHINGTON, DC
June 1999

The views expressed in this paper are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government

This paper has been approved for unrestricted public release by the Office of the Secretary of Defense (Public Affairs)

CONTENTS

Preface v

Foreword vii

Prologue: Intelligence Sharing in a New Light. 1

Part

I Intelligence Process 7

II Converting Customer Needs into Intelligence Requirements 13

III Collection 21

IV Processing Collected Information 25

V Analysis 29

VI Production 39

VII Managing the Intelligence Process 49

VIII Portrait of an Intelligence Analyst. 55

IX Defensive Measures for Intelligence 61

Epilogue 71

Glossary 72

Bibliography 75

About the Author 81

INTELLIGENCE ESSENTIALS FOR EVERYONE

Preface

The "importance of understanding" has become almost an obsession with significant portions of American business. There remain, however, many companies that attempt to operate as they traditionally have in the past — placing great faith in the owner's or manager's judgment as to what is required to remain competitive.

In this paper, the author has articulated clearly the fundamentals of sound intelligence practice and has identified some guidelines that can lead toward creation of a solid intelligence infrastructure. These signposts apply both to government intelligence and to business. Good intelligence should always be based on validated requirements, but it may be derived from a wide variety of sources, not all of which are reliable.

Understanding the needs of the consumer and the sources available enable an analyst to choose the correct methodology to arrive at useful answers. The author has laid out in clear, concise language a logical approach to creating an infrastructure for government and business. Every system will have flaws but this discussion should help the reader minimize those weaknesses. It is an important contribution to the education of government and business intelligence professionals.

James A. Williams, LTG, U.S. Army (Ret.)
Former Director, Defense Intelligence Agency

INTELLIGENCE ESSENTIALS FOR EVERYONE

Foreword

Decades of government intelligence experience and reflection on that experience are captured in this primer. Ms. Krizan combines her own findings on best practices in the intelligence profession with the discoveries and ruminations of other practitioners, including several Joint Military Intelligence College instructors and students who preceded her. Many of the selections she refers to are from documents that are out of print or have wrongly been assigned to a dustbin.

This primer reviews and reassesses Intelligence Community best practices with special emphasis on how they may be adopted by the private sector. The government convention of referring to intelligence users as "customers" suggests by itself the demonstrable similarities between government intelligence and business information support functions.

The genesis for this study was the author's discovery of a need to codify for the Intelligence Community certain basic principles missing from the formal training of intelligence analysts. At the same time, she learned of requests from the private sector for the same type of codified, government best practices for adaptation to the business world. As no formal mechanism existed for an exchange of these insights between the public and private sectors, Ms. Krizan developed this paper as an adjunct to her Master's thesis, *Benchmarking the Intelligence Process for the Private Sector.* Her thesis explores the rationale and mechanisms for benchmarking the intelligence process in government, and for sharing the resultant findings with the private sector.

The author and editor wish to acknowledge the constructive comments of two reviewers from the business community, representing the Amoco Corporation and DeGenaro and Associates, Inc. of Sarasota, Florida.

Comments on this paper are welcome, and should be directed to the Office of Applied Research, MCE-2, Joint Military Intelligence College, DIAC, Bolling AFB, Washington, DC 20340-5100. Telephone (202) 231-4193; DSN 428-4193; e-mail *AFswerg@dia.osis.gov.*

Dr. Russell G. Swenson, Editor and Director, Office of Applied Research

PROLOGUE: INTELLIGENCE SHARING IN A NEW LIGHT

Education is the cheapest defense of a nation.
— Edmund Burke, 18th-century British philosopher

National Intelligence Meets Business Intelligence

This intelligence primer reflects the author's examination of dozens of unclassified government documents on the practice of intelligence over a period of nearly seven years. For the national security Intelligence Community (IC), it represents a concise distillation and clarification of the national intelligence function. To the private sector, it offers an unprecedented translation into lay terms of national intelligence principles and their application within and potentially outside of government.[1] Whereas "intelligence sharing" has traditionally been a government-to-government transaction, the environment is now receptive to government-private sector interaction.

The widespread trend toward incorporating government intelligence methodology into commerce and education was a primary impetus for publishing this document. As economic competition accelerates around the world, private businesses are initiating their own "business intelligence" (BI) or "competitive intelligence" services to advise their decisionmakers. Educators in business and academia are following suit, inserting BI concepts into professional training and college curricula.[2]

Whereas businesses in the past have concentrated on knowing the market and making the best product, they are shifting their focus to include knowing, and staying ahead of, competitors. This emphasis on competitiveness requires the sophisticated production and use of carefully analyzed information tailored to specific users; in other words, intelligence. But the use of intelligence as a strategic planning tool, common in government, is a skill that few companies have perfected.[3]

Although BI practitioners refer to the national security model of intelligence, they do not seek to conduct secret intelligence operations, which are limited by law to government

---

[1] For the purpose of this study, the author includes in national security intelligence those analogous activities conducted by law enforcement personnel at the federal, state, and local levels. Readers seeking further information on law enforcement applications of intelligence may wish to read Marilyn Peterson, *Applications in Criminal Analysis* (Westport, Connecticut: Greenwood Press, 1994). An additional resource is the International Association of Law Enforcement Intelligence Analysts. Local IALEIA chapters are listed on the Association's web site: http://www.ialeia.org.

[2] An authoritative guide to business intelligence practices is found in Larry Kahaner, *Competitive Intelligence: From Black Ops to Boardrooms — How Businesses Gather, Analyze and Use Information to Succeed in the Global Marketplace* (New York, NY: Simon and Schuster, 1996).

[3] Richard D'Aveni, "Hypercompetition," briefing to SCIP Conference, Alexandria, VA, 28 March 1996.

authorities. The Society of Competitive Intelligence Professionals (SCIP), headquartered in the Washington, DC area, is an international organization founded in 1986 to "assist members in enhancing their firms' competitiveness through a greater... understanding of competitor behaviors and future strategies as well as the market dynamics in which they do business."[4] SCIP's code of conduct specifically promotes ethical and legal BI practices.[5] The main focus of "collection" is on exploiting on-line and open-source information services, and the theme of "analysis" is to go beyond mere numerical and factual information, to interpretation of events for strategic decisionmaking.[6]

Large corporations are creating their own intelligence units, and a few are successful at performing analysis in support of strategic decisionmaking. Others are hiring BI contractors, or "out-sourcing" this function. However, the majority of businesses having some familiarity with BI are not able to conduct rigorous research and analysis for value-added reporting. According to University of Pittsburgh professor of Business Administration John Prescott, no theoretical framework exists for BI. He believes that most studies done lack the rigor that would come with following sound research-design principles. By his estimate, only one percent of companies have a research-design capability exploitable for BI applications.[7] At the same time, companies are increasingly opting to establish their own intelligence units rather than purchasing services from BI specialists. The implication of this trend is that BI professionals should be skilled in both intelligence and in a business discipline of value to the company.[8]

On the other hand, as businesses come to appreciate the value of intelligence about their competitors, they are increasingly realizing their own vulnerability to similar scrutiny. The private sector can therefore benefit from IC expertise in disciplines complementary to active intelligence production, namely defensive measures. The whole concept of openness regarding intelligence practices may hinge upon the counter-balancing effect of self-defense, particularly as practiced through information systems security (INFOSEC) and operations security (OPSEC).[9] Because the IC seeks to be a world leader in INFOSEC and OPSEC as well as intelligence production, defensive measures are an appropriate topic for dialogue between the public and private sectors.

The U.S. government INFOSEC Manual sums up the relationship between offense and defense in a comprehensive intelligence strategy in this way:

> In today's information age environment, control of information and information technology is vital. As the nation daily becomes more dependent on

---

4 SCIP, *Competitive Intelligence Review*, 8, No. 3 (Fall 1997), unnumbered 8th page.

5 SCIP, *1995 SCIP Membership Directory* (Alexandria, VA: SCIP, 1995), xxvii.

6 Leila Kight, "Elements of CI Success," briefing to SCIP Conference, Alexandria, VA, 28 March, 1996.

7 John Prescott, Professor of Business Administration, University of Pittsburgh, "Research," briefing to SCIP conference, Alexandria, VA, 28 March 1996.

8 Jan Herring, "Strides in Institutionalizing BI in Businesses," briefing to SCIP Conference, Alexandria, VA, 28 March 1996.

9 These concepts are addressed in Part IX.

> networked information systems to conduct essential business, including military operations, government functions, and national and international economic enterprises, information infrastructures are assuming increased strategic importance. This has, in turn, given rise to the concept of information warfare (INFOWAR) — a new form of warfare directed toward attacking (offensive) or defending (defensive) such infrastructures.[10]

Giving citizens the tools they need to survive INFOWAR is one of the IC's explicit missions. This intelligence primer can assist that mission by offering a conceptual and practical "common operating environment" for business and government alike.[11]

Assessing and Exchanging Best Practices

In documenting the essentials of intelligence, this primer is an example of *benchmarking*, a widely used process for achieving quality in organizations, the use of which is a criterion for the business world's Malcolm Baldrige National Quality Award.[12] Benchmarking normally assesses best professional practices, developed and refined through experience, for carrying out an organization's core tasks.[13] An additional aim of benchmarking is to establish reciprocal relationships among best-in-class parties for the exchange of mutually beneficial information.[14] Because the IC is the *de facto* functional leader in the intelligence profession, and is publicly funded, it is obligated to lead both the government and private sector toward a greater understanding of the intelligence discipline.

In the mid-1990s, as national intelligence agencies began to participate in international benchmarking forums, individuals from the private sector began to request practical information on the intelligence process from IC representatives. The requestors were often participants in the growing BI movement and apparently sought to adapt IC methods to their own purposes. Their circumspect counterparts in the government were not prepared to respond to these requests, preferring instead to limit benchmarking relationships to common business topics, such as resource management.[15] Concurrently, the annual SCIP international conference highlighted the needs and capabilities of intelligence departments in the private sector.

---

[10] National Security Agency, *1995 INFOSEC Manual* (Ft. Meade, MD: NSA, 1995), para. C.1.

[11] Readers in doubt of the need for INFOSEC in the private sector may wish to study the real-world examples of INFOWAR battles and their implications for economic and personal security that author Winn Schwartau reveals in *Information Warfare: Chaos on the Electronic Superhighway*, (New York: Thunder's Mouth Press, 1994).

[12] A useful reference to benchmarking within the U.S. government is Jerry Frankenfield and Melissie Rumizen, *A Guide to Benchmarking* (Fort Meade, MD: National Security Agency (NSA), 12 July 1995). An overview of benchmarking in the private sector can be found in Dean Elmuti, Hanus Kathawaia, and Scott J. Lloyed, "The Benchmarking Process: Assessing Its Value and Limitations," *Industrial Management*, 39, No. 4 (July/August 1997): 12-19.

[13] Elmuti, Kathawaia and Lloyed, 12.

[14] Elmuti, Kathawaia and Lloyed, 13.

[15] Melissie C. Rumizen, Ph.D., Benchmarking Manager, National Security Agency, interview with the author, 2 April 1996.

Demand in the private sector for intelligence skills can be met through the application of validated intelligence practices presented in this document. Conversely, the business-oriented perspective on intelligence can be highly useful to government intelligence professionals. As a BI practitioner explains, every activity in the intelligence process must be related to a requirement, otherwise it is irrelevant.[16] Government personnel would benefit from this practical reminder in every training course and every work center. In the private sector, straying from this principle means wasting money and losing a competitive edge. The consequences of inefficient national intelligence can be costly on an even larger scale.

The basis for an IC benchmarking exchange with the private sector continues to grow. The Society of Competitive Intelligence Professionals is a clearinghouse for the review of private business intelligence practices, and therefore a champion of information sharing. Leading colleges and universities are beginning to offer coursework in intelligence methods, and in many cases intend to expand their offerings. Curriculum exchanges between private sector educators and the IC are encouraged by legislation and by Congressional Commission recommendations,[17] yet little such formal exchange has taken place.

Whereas government practitioners are the acknowledged subject-matter experts in intelligence methodology, the private sector offers a wealth of expertise in particular areas such as business management, technology, the global marketplace, and skills training. Each has valuable knowledge to share with the other, and experience gaps to fill. On the basis of these unique needs and capabilities, the public and private sectors can forge a new partnership in understanding their common responsibilities, and this primer may make a modest contribution toward the exchange of ideas.

The following chapters outline validated steps to operating an intelligence service for both the government and the private sector. In either setting, this document should prove useful as a basic curriculum for students, an on-the-job working aid for practitioners, and a reference tool for experienced professionals, especially those teaching or mentoring others. Although the primer does not exhaustively describe procedures for quality intelligence production or defensive measures, it does offer the business community fundamental concepts that can transfer readily from national intelligence to commercial applications, including competitive analysis, strategic planning and the protection of proprietary information. Universities may incorporate these ideas into their business, political science, and intelligence studies curricula to encourage and prepare students to become intelligence practitioners in commerce or government. For anyone outside of the

---

[16] David Harkleroad, “Actionable CI,” briefing to SCIP Conference, Alexandria, VA, 28 March 1996.

[17] For example, the 1991 National Security Education Act (P.L. 102-183), the 1993 Government Performance and Results Act (P.L. 103-62), and the Congressional Report of the Commission on the Roles and Capabilities of the U.S. Intelligence Community, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (Washington, DC: GPO, 1 March 1996), 87.

national security apparatus, this intelligence primer will shed light on why and how the government spends federal tax dollars on national intelligence.

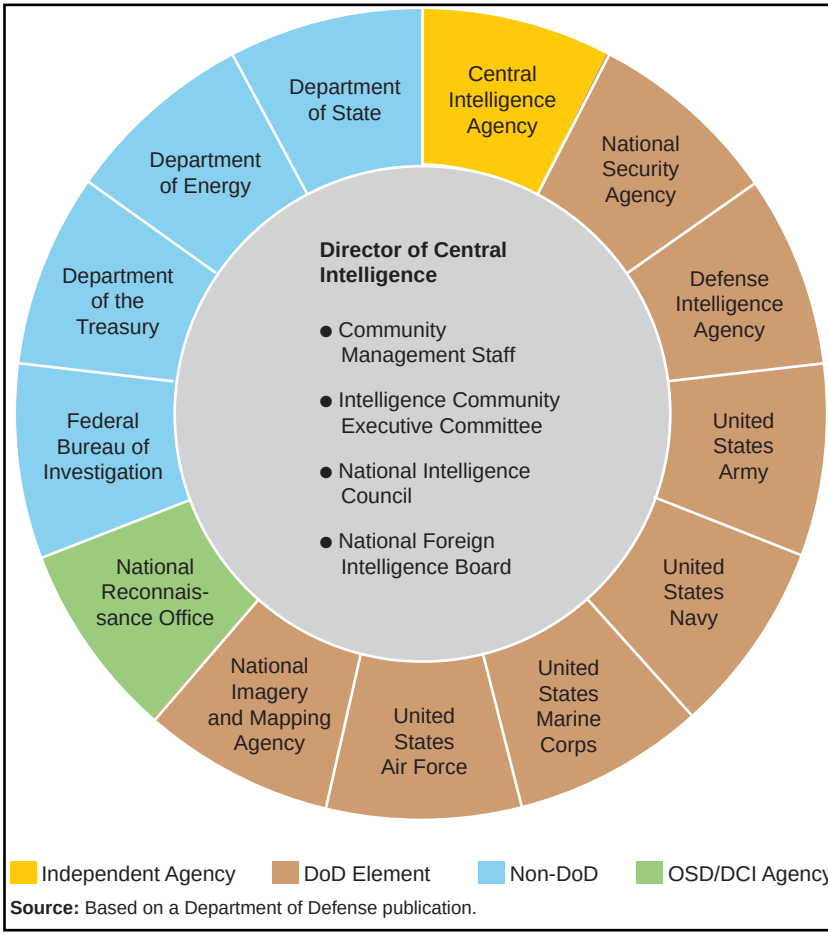


Figure 1: The National Intelligence Community.

PART I
INTELLIGENCE PROCESS

> [I]ntelligence is more than information. It is knowledge that has been specially prepared for a customer's unique circumstances. The word *knowledge* highlights the need for human involvement. Intelligence collection systems produce... data, not intelligence; only the human mind can provide that special touch that makes sense of data for different customers' requirements. The special processing that partially defines intelligence is the continual collection, verification, and analysis of information that allows us to understand the problem or situation in actionable terms and then tailor a product in the context of the customer's circumstances. If any of these essential attributes is missing, then the product remains information rather than intelligence.[18]

The intelligence profession, already well established within government, is growing in the private sector. Intelligence is traditionally a function of government organizations serving the decisionmaking needs of national security authorities. But innovative private firms are increasingly adapting the national security intelligence model to the business world to aid their own strategic planning. Although business professionals may prefer the term "information" over "intelligence," the author will use the latter term to highlight the importance of adding value to information. According to government convention, the author will use the term "customer" to refer to the intended recipient of an intelligence product — either a fellow intelligence service member, or a policy official or decisionmaker. The process of converting raw information into actionable intelligence can serve government and business equally well in their respective domains.

The Intelligence Process in Government and Business

Production of intelligence follows a cyclical *process*, a series of repeated and interrelated steps that add value to original inputs and create a substantially transformed product. That transformation is what distinguishes intelligence from a simple cyclical activity.[19] In government and private sector alike, analysis is the catalyst that converts information into intelligence for planners and decisionmakers.

Although the intelligence process is complex and dynamic, several component functions may be distinguished from the whole. In this primer, components are identified as Intelligence Needs, Collection Activities, Processing of Collected Information, Analysis and Production. To highlight the components, each is accorded a separate Part in this study. These

---

[18] Captain William S. Brei, *Getting Intelligence Right: The Power of Logical Procedure*, Occasional Paper Number Two (Washington, DC: Joint Military Intelligence College, January 1996), 4.

[19] Melissie C. Rumizen, Benchmarking Manager at the National Security Agency, interview by author, 4 January 1996.

labels, and the illustration below, should not be interpreted to mean that intelligence is a unidimensional and unidirectional process. "[I]n fact, the [process] is multidimensional, multidirectional, and — most importantly — interactive and iterative."[20]

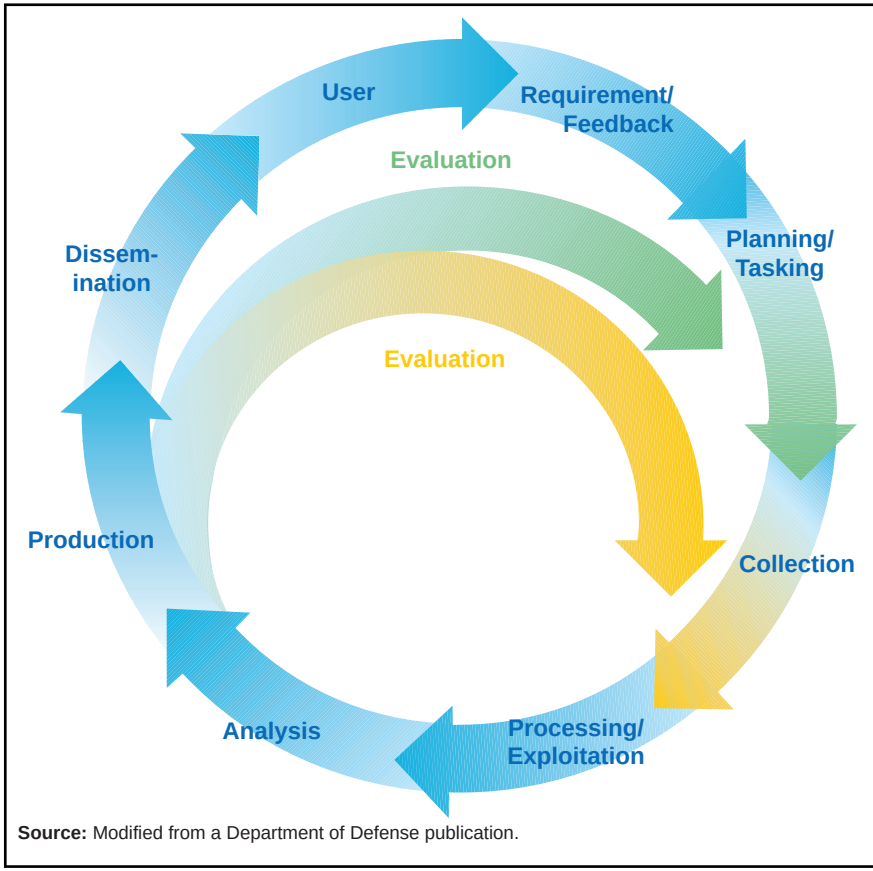


Figure 2: Process of Intelligence Creation and Use.

[20] Douglas H. Dearth, "National Intelligence: Profession and Process," in *Strategic Intelligence: Theory and Application*, eds. Douglas H. Dearth and R. Thomas Goodden, 2d ed. (Washington, DC: Joint Military Intelligence Training Center, 1995), 17.

The purpose of this process is for the intelligence service to provide decisionmakers with tools, or "products" that assist them in identifying key decision factors. Such intelligence products may be described both in terms of their subject content and their intended use.[21]

Table 1: Types of Intelligence Product Categories
Source: adapted from Garst, "Components of Intelligence"

By Subject	By Use
Biographic	Research
Economic	Current
Geographic	Estimative
Military	Operational
Political	Scientific and Technical
Sociological	Warning
Scientific and Technical	
Transportation and Communications	

Any or all of these categories may be relevant to the private sector, depending upon the particular firm's product line and objectives in a given industry, market environment, and geographic area.

A nation's power or a firm's success results from a combination of factors, so intelligence producers and customers should examine potential adversaries and competitive situations from as many relevant viewpoints as possible. A competitor's economic resources, political alignments, the number, education and health of its people, and apparent objectives are all important in determining the ability of a country or a business to exert influence on others. The eight subject categories of intelligence are exhaustive, but they are not mutually exclusive. Although dividing intelligence into subject areas is useful for analyzing information and administering production, it should not become a rigid formula. Some intelligence services structure production into geographic subject areas when their responsibilities warrant a broader perspective than topical divisions would allow.[22]

---

[21] Ronald D. Garst, "Components of Intelligence," in *A Handbook of Intelligence Analysis*, ed. Ronald D. Garst, 2d ed. (Washington, DC: Defense Intelligence College, January 1989), 1; Central Intelligence Agency, *A Consumer's Guide to Intelligence* (Washington, DC: Public Affairs Staff, July 1995), 5-7.

[22] Garst, *Components of Intelligence*, 2,3.

Similarly, characterization of intelligence by intended use applies to both government and enterprise, and the categories again are exhaustive, but not mutually exclusive. The production of basic research intelligence yields structured summaries of topics such as geographic, demographic, and political studies, presented in handbooks, charts, maps, and the like. Current intelligence addresses day-to-day events to apprise decisionmakers of new developments and assess their significance. Estimative intelligence deals with what might be or what might happen; it may help policymakers fill in gaps between available facts, or assess the range and likelihood of possible outcomes in a threat or "opportunity" scenario. Operational support intelligence incorporates all types of intelligence by use, but is produced in a tailored, focused, and timely manner for planners and operators of the supported activity. Scientific and Technical intelligence typically comes to life in in-depth, focused assessments stemming from detailed physical or functional examination of objects, events, or processes, such as equipment manufacturing techniques.[23] Warning intelligence sounds an alarm, connoting urgency, and implies the potential need for policy action in response.

How government and business leaders define their needs for these types of intelligence affects the intelligence service's organization and operating procedures. Managers of this intricate process, whether in government or business, need to decide whether to make one intelligence unit responsible for all the component parts of the process or to create several specialized organizations for particular sub-processes. This question is explored briefly below, and more fully in Part VII.

Functional Organization of Intelligence

The national Intelligence Community comprises Executive Branch agencies that produce classified and unclassified studies on selected foreign developments as a prelude to decisions and actions by the president, military leaders, and other senior authorities. Some of this intelligence is developed from special sources to which few individuals have access except on a strictly controlled "need-to-know" basis.[24] The four categories of special intelligence are Human Resources (HUMINT), Signals (SIGINT), Imagery (IMINT) and Measurement and Signatures (MASINT). The four corresponding national authorities for these categories are the Central Intelligence Agency (CIA), the National Security Agency (NSA), the National Imagery and Mapping Agency (NIMA) and the Defense Intelligence Agency (DIA). DIA shares authority for HUMINT, being responsible for Department of Defense HUMINT management. Along with these four agencies, other members of the Intelligence Community use and produce intelligence by integrating all available and relevant collected information into reports tailored to the needs of individual customers.

Private sector organizations use open-source information to produce intelligence in a fashion similar to national authorities. By mimicking the government process of translating customer needs into production requirements, and particularly by performing rigorous analysis on gathered information, private organizations can produce assessments that aid their leaders in

---

[23] CIA, *Consumer's Guide*, 5-7.
[24] CIA, *Consumer's Guide*, vii.

planning and carrying out decisions to increase their competitiveness in the global economy. This primer will point out why private entities may desire to transfer into their domain some well-honed proficiencies developed in the national Intelligence Community. At the same time, the Intelligence Community self-examination conducted in these pages may allow government managers to reflect on any unique capabilities worthy of further development and protection.

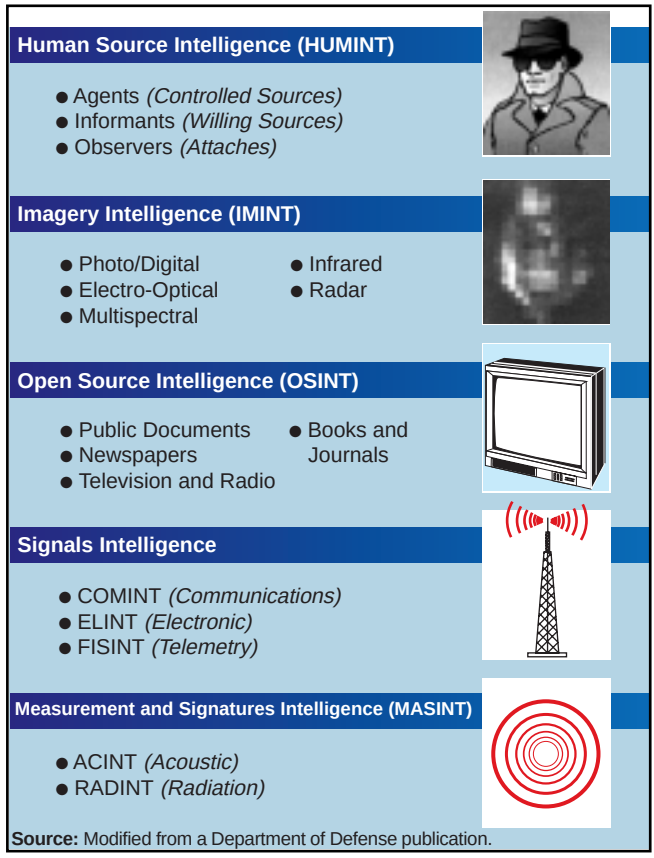


Figure 3: National Intelligence Production Resources.

PART II
CONVERTING CUSTOMER NEEDS INTO INTELLIGENCE REQUIREMENTS

> The articulation of the requirement is the most important part of the process, and it seldom is as simple as it might seem. There should be a dialogue concerning the requirement, rather than a simple assertion of need. Perhaps the customer knows precisely what is needed and what the product should look like. Perhaps... not. Interaction is required: discussion between ultimate user and principal producer. This is often difficult due to time, distance, and bureaucratic impediments, not to mention disparities of rank, personality, perspectives, and functions.[25]

Defining the Intelligence Problem

Customer demands, or "needs," particularly if they are complex and time-sensitive, require interpretation or analysis by the intelligence service before being expressed as intelligence requirements that drive the production process.[26] This dialog between intelligence producer and customer may begin with a simple set of questions, and if appropriate, progress to a more sophisticated analysis of the intelligence problem being addressed.

The "Five Ws" — *Who*, *What*, *When*, *Where*, and *Why* — are a good starting point for translating intelligence needs into requirements. A sixth related question, *How*, may also be considered. In both government and business, these questions form the basic framework for decisionmakers and intelligence practitioners to follow in formulating intelligence requirements and devising a strategy to satisfy them. Typically, government intelligence requirements are expressed in terms of foreign threats to national or international security. In business, requirements may be expressed in terms of the competitor's standing in the marketplace in comparison to one's own posture. Representative examples from each sector follow:

[25] Dearth, "National Intelligence," 17-18.
[26] Dearth, "National Intelligence," 18.

Table 2: Illustrative Definitions of Intelligence Problems and Customer Needs

Source: Author

A Government Scenario

The Intelligence Problem					
Who	***What***	***When***	***Where***	***Why***	***How***
A foreign president	Refusing to allow weapons sites to be inspected	Now; for several months	Country X	Unknown, possibly to hide illegal weapons	Barring access, destroying monitoring equipment
The Intelligence Need					
Who	***What***	***When***	***Where***	***Why***	***How***
U.S. President	Wants info on Country X President	Now, and update	White House	Determine power base and intent	All-source collection & analysis

A Business Scenario

The Intelligence Problem					
Who	***What***	***When***	***Where***	***Why***	***How***
Company X	Reorganizes production department	Sudden	Saturated market	Unknown	Unknown
The Intelligence Need					
Who	***What***	***When***	***Where***	***Why***	***How***
CEO of similar Company Y	Wants to know why and how Company X changed	ASAP	CEO's office	Determine if new structure gives advantage	Open source analysis; tailored, confidential report

Examination of these basic scenarios should inspire further development of the concept of determining customer needs in specific situations. The thoughtful researcher may propose, for example, ways to gather information on additional aspects of the problem (Who, What) and on customers (Who), as well as on the attendant motivations (Why) and strategies (How) of the target and the customer. Defining the intelligence problem in this manner paves the way for the next step in the intelligence process — the development of intelligence collection, analysis, and production *requirements*, explained later in this chapter.

Another, more complex model for defining intelligence scenarios employs the Taxonomy of Problem Types.[27] The table below illustrates the factors that customers and producers may take into account in articulating the nature of the intelligence problem and selecting a strategy for resolving it.

Table 3: Taxonomy of Problem Types

Source: Analysis course material, Joint Military Intelligence College, 1991

Characteristics	Problem Types				
	Simplistic	**Deterministic**	**Moderately Random**	**Severely Random**	**Indeterminate**
What is the question?	Obtain information	How much? How many	Identify and rank all outcomes	Identify outcomes in unbounded situation	Predict future events/ situations
Role of facts	Highest	High	Moderate	Low	Lowest
Role of judgment	Lowest	Low	Moderate	High	Highest
Analytical task	Find information	Find/create formula	Generate all outcomes	Define potential outcomes	Define futures factors
Analytical method	Search sources	Match data to formula	Decision theory; utility analysis	Role playing and gaming	Analyze models and scenarios
Analytical instrument	Matching	Mathematical formula	Influence diagram, utility, probability	Subjective evaluation of outcomes	Use of experts
Analytic output	Fact	Specific value or number	Weighted alternative outcomes	Plausible outcomes	Elaboration on expected future
Probability of error	Lowest	Very low	Dependent on data quality	High to very high	Highest
Follow-up task	None	None	Monitor for change	Repeated testing to determine true state	Exhaustive learning

[27] Morgan D. Jones, *The Thinker's Toolkit* (New York: Random House, 1995), 44-46, as elaborated by Thomas H. Murray, Sequoia Associates, Inc., Arlington, VA., in coursework at the Joint Military Intelligence College.

As with the "Five Ws," this model enables decisionmakers and analysts to assess their needs and capabilities in relation to a particular intelligence scenario. This ability to establish a baseline and set in motion a collection and production strategy is crucial to conducting a successful intelligence effort. Too often, both producers and customers waste valuable time and effort struggling to characterize for themselves a given situation, or perhaps worse, they hastily embark upon an action plan without determining its appropriateness to the problem. Employing a structured approach as outlined in the Taxonomy of Problem Types can help the players avoid these inefficiencies and take the first step toward generating clear intelligence requirements by defining both the intelligence problem and the requisite components to its solution. Following are example scenarios. The reader is encouraged to follow the scenarios down the columns of the taxonomy table, then generate new scenarios in similar fashion.

Intelligence Problem Definition

A Government Scenario

The Severely Random problem type is one frequently encountered by the military in planning an operational strategy. This is the realm of wargaming. The initial intelligence problem is to identify all possible outcomes in an unbounded situation, so that commanders can generate plans for every contingency. The role of valid data is relatively minor, while the role of judgment is great, as history and current statistics may shed little light on how the adversary will behave in a hypothetical situation, and the progress and outcome of an operation against that adversary cannot be predicted with absolute accuracy. Therefore, the analytical task is to define and prepare for all potential outcomes. The analytical method is role playing and wargaming: placing oneself mentally in the imagined situation, and experiencing it in advance, even to the point of acting it out in a realistic setting. After experiencing the various scenarios, the players subjectively evaluate the outcomes of the games, assessing which ones may be plausible or expected to occur in the real world. The probability of error in judgment here is inherently high, as no one can be certain that the future will occur exactly as events unfolded in the game. However, repeated exercises can help to establish a measure of confidence, for practice in living out these scenarios may enable the players to more quickly identify and execute desired behaviors, and avoid mistakes in a similar real situation.

A Business Scenario

The Indeterminate problem type is one facing the entrepreneur in the modern telecommunications market. Predicting the future for a given proposed new technology or product is an extremely imprecise task fraught with potentially dire, or rewarding, consequences. The role of valid data is extremely minor here, whereas analytical judgments about the buying public's future — and changing — needs and desires are crucial. Defining the key factors influencing the future market is the analytical task, to be approached via the analytical method of setting up models and scenarios: the if/then/else process. Experts in the proposed technology or market are then employed to analyze these possibilities. Their output is a synthesized assessment of how the future will look under various conditions with regard to the

proposed new product. The probability of error in judgment is extremely high, as the decision is based entirely on mental models rather than experience; after all, neither the new product nor the future environment exists yet. Continual reassessment of the changing factors influencing the future can help the analysts adjust their conclusions and better advise decisionmakers on whether, and how, to proceed with the new product.

Generating Intelligence Requirements

Once they have agreed upon the nature of the intelligence problem at hand, the intelligence service and the customer together can next generate intelligence *requirements* to drive the production process. The intelligence requirement translates customer needs into an intelligence action plan. A good working relationship between the two parties at this stage will determine whether the intelligence produced in subsequent stages actually meets customer needs. However, the differing perspectives that each side brings to the negotiation process can make cooperation between them a difficult feat.[28]

Customers want intelligence to guide them clearly in making policy and operational decisions. They may have little understanding of the intelligence process, and little patience for the subjectivity and conditionality of intelligence judgments. For customers, intelligence can be just one of many influences on their decisionmaking, and may be given little weight in comparison to other, more readily digested, familiar, or policy-oriented inputs. However, intelligence is neither designed nor equipped to meet these customer expectations.[29]

As a discipline, intelligence seeks to remain an independent, objective advisor to the decisionmaker. The realm of intelligence is that of "fact," considered judgment, and probability, but not prescription. It does not tell the customer what to do to meet an agenda, but rather, identifies the factors at play, and how various actions may affect outcomes. Intelligence tends to be packaged in standard formats and, because of its methodical approach, may not be delivered within the user's ideal timeframe. For all these reasons, the customer may not see intelligence as a useful service.[30]

Yet, somehow the intelligence producer and customer must reconcile their differing perspectives in order to agree on intelligence requirements and make the production process work. Understanding each other's views on intelligence is the first step toward improving the relationship between them. The next step is communication. Free interaction among the players will foster agreement on intelligence priorities and result in products that decisionmakers recognize as meaningful to their agendas, yet balanced by rigorous analysis.[31] In addition, as discussed below, customer feedback on production quality will lead to better definition of future intelligence problems and requirements.

---

[28] Arthur S. Hulnick, "The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach," *Intelligence and National Security*, 1, No. 2, (May 1986): 214-216.

[29] Hulnick, "Producer-Policy Consumer Linkage," 215-216.

[30] Hulnick, "Producer-Policy Consumer Linkage," 216.

[31] Adapted from Michael A. Turner, "Setting Analytical Priorities in U.S. Intelligence," *International Journal of Intelligence and CounterIntelligence*, 9, No. 3, (Fall 1996): 320-322.

Types of Intelligence Requirements

Having thus developed an understanding of customer needs, the intelligence service may proactively and continuously generate intelligence collection and production requirements to maintain customer-focused operations. Examples of such internally generated specifications include analyst-driven, events-driven, and scheduled requirements. The table below briefly describes them.[32]

Table 4: Types of Producer-Generated Intelligence Collection and Production Requirements

Source: Hulnick

Analyst-driven	Based on knowledge of customer and issues
Events-driven	In response to time-sensitive relevant events
Scheduled	Periodic activities to document and update target status

Further distinctions among intelligence requirements include timeliness and scope, or level, of intended use. Timeliness of requirements is established to meet standing (long-term) and *ad hoc* (short-term) needs. When the customer and intelligence service agree to define certain topics as long-term intelligence issues, they generate a standing requirement to ensure that a regular production effort can, and will, be maintained against that target. The customer will initiate an *ad hoc* requirement upon realizing a sudden short-term need for a specific type of intelligence, and will specify the target of interest, the coverage timeframe, and the type of output desired.

The scope or level of intended use of the intelligence may be characterized as strategic or tactical. Strategic intelligence is geared to a policymaker dealing with big-picture issues affecting the mission and future of an organization: the U.S. President, corporate executives, high-level diplomats, or military commanders of major commands or fleets. Tactical intelligence serves players and decisionmakers "on the ground" engaged in current operations: trade negotiators, marketing and sales representatives, deployed military units, or product developers.

Table 5: Types of Customer-Defined Intelligence Requirements

Source: Author

Timeliness	Short-term *(ad hoc)*	Long-term (standing)
Scope	Broad (strategic)	Narrow (tactical)

[32] Adapted from Arthur S. Hulnick, "Managing Intelligence Analysis: Strategies for Playing the End Game," *International Journal of Intelligence and CounterIntelligence* 2, No. 3 (Fall 1988): 327.

Ensuring that Requirements Meet Customer Needs

Even when they follow this method of formulating intelligence requirements together, decisionmakers and their intelligence units in the public and private sectors may still have an incomplete grasp of how to define their needs and capabilities — until they have evaluated the resultant products. Thus, customer feedback, production planning and tasking, as well as any internal product evaluation, all become part of the process of defining needs and creating intelligence requirements. However, when intelligence producers and users are not in nearly direct, daily contact, this process can consume a good deal of time. This is why the national Intelligence Community is experimenting with compressing both the accustomed time and spatial dimensions of the intelligence process through remote electronic collaboration and production methods.[33]

Whether in business or government, six fundamental values or attributes underlie the core principles from which all the essential intelligence functions are derived. The corollary is that intelligence customers' needs may be defined and engaged by intelligence professionals using these same values. Table 6 offers a brief explanation of how both intelligence customers and producers may use these values to evaluate how well they have translated needs into requirements that will result in useful products.[34]

Interpretation of these values turns a customer's need into a collection and production requirement that the intelligence service understands in the context of its own functions. However, illustrating the complexity of the intelligence process, once this is done, the next step is not necessarily collection.

Rather, the next stage is analysis. Perhaps the requirement is simply and readily answered — by an existing product, by ready extrapolation from files or data bases, or by a simple phone call or short desk note based on an analyst's or manager's knowledge. On the other hand, the requirement might necessitate laborious effort — extrapolation, collation, analysis, integration, and production — but still the product can be constructed and sent directly to the requester. Case closed; next problem.... Preliminary analysis might well show, however, that while much data exists, because the issue at hand is not a new one, gaps in information must be filled... Obviously, this calls for collection. This brings up an essential point: consumers do not drive collection *per se*; analysts do — or should.[35] Part III explores this next step in the intelligence process.

---

[33] The U.S. military has pioneered the concept of an electronic intelligence operating environment that transcends organizational boundaries. Congress has recommended that the IC adopt this *Joint Intelligence Virtual Architecture* model to take advantage of technological developments, reduce bureaucratic barriers, and thereby provide policymakers with timely, objective, and useful intelligence. See U.S. Congress Staff Study, House Permanent Select Committee on Intelligence, *IC21: The Intelligence Community in the 21st Century,* (April 1996): Section III, "Intelligence Requirements Process."

[34] The six values are adapted by Brei from an earlier version of U.S. Department of Defense, Joint Chiefs of Staff, Joint Pub 2-0, *Joint Doctrine for Intelligence Support to Operations* (Washington, DC: GPO, 5 May 1995), IV-15.

[35] Dearth, "National Intelligence," 18-19.

Table 6: Intelligence Values

Source: Brei

Accuracy: All sources and data must be evaluated for the possibility of technical error, misperception, and hostile efforts to mislead.
Objectivity: All judgments must be evaluated for the possibility of deliberate distortions and manipulations due to self-interest.
Usability: All intelligence communications must be in a form that facilitates ready comprehension and immediate application. Intelligence products must be compatible with a customer's capabilities for receiving, manipulating, protecting, and storing the product.
Relevance: Information must be selected and organized for its applicability to a customer's requirements, with potential consequences and significance of the information made explicit to the customer's circumstances.
Readiness: Intelligence systems must be responsive to the existing and contingent intelligence requirements of customers at all levels of command.
Timeliness: Intelligence must be delivered while the content is still actionable under the customer's circumstances.

PART III
COLLECTION

The collection function rests on research — on matching validated intelligence objectives to available sources of information, with the results to be transformed into usable intelligence. Just as within needs-definition, analysis is an integral function of collection.

Collection Requirements

The collection *requirement* specifies exactly how the intelligence service will go about acquiring the intelligence information the customer needs. Any one, or any of several, players in the intelligence system may be involved in formulating collection requirements: the intelligence analyst, a dedicated staff officer, or a specialized collection unit.

In large intelligence services, collection requirements may be managed by a group of specialists acting as liaisons between customers and collectors (people who actually obtain the needed information, either directly or by use of technical means). Within that requirements staff, individual requirements officers may be dedicated to a particular set of customers, a type of collection resource, or a specific intelligence issue. This use of collection requirements officers is prevalent in the government. Smaller services, especially in the private sector, may assign collection requirements management to one person or team within a multidisciplinary intelligence unit that serves a particular customer or that is arrayed against a particular topic area.

Regardless of how it is organized, the requirements management function entails much more than simple administrative duties. It requires analytic skill to evaluate how well the customer has expressed the intelligence need; whether, how and when the intelligence unit is able to obtain the required information through its available collection sources; and in what form to deliver the collected information to the intelligence analyst.

Collection Planning and Operations

One method for selecting a collection strategy is to first prepare a list of expected target evidence. The collection requirements officer and the intelligence analyst for the target may collaborate in identifying the most revealing evidence of target activity, which may include physical features of terrain or objects, human behavior, or natural and man-made phenomena. The issue that can be resolved through this analysis is “What am I looking for, and how will I know it if I see it”?

Successful analysis of expected target evidence in light of the customer’s needs can determine what collection source and method will permit detection and capture of that evidence. Increasingly sophisticated identification of evidence types may reveal what collectible data are essential for drawing key conclusions, and therefore should be given priority; whether the evidence is distinguishable from innocuous information; and whether the intelligence service has the skills, time, money and authorization to collect the data

needed to exploit a particular target. Furthermore, the collection must yield information in a format that is either usable in raw form by the intelligence analyst, or that can be converted practicably into usable form.

For example, in the case of the first business scenario presented in Part II, the CEO needs intelligence on why and how the similar, competitor company suddenly reorganized its production department. The collection requirement might specify that the intelligence unit give first priority to this new issue; it will focus on collecting information about the competitor's reorganization. A list of relevant evidence might include the following: changes in personnel assignments, changes in supply of production components, budget deficit or surplus, age of infrastructure, breakthroughs in research and development, and changes in the cultural or natural environment. To exploit this evidence, the intelligence service would thus need direct or indirect access to information on the company's employees, its previous production methods, its financial status, its physical plant, its overall functional structure and operations, and the consumer market. The collection unit would choose from among the sources listed in Table 7 below those most likely to provide timely access to this information in usable form.

Finally, upon defining the collection requirement and selecting a collection strategy, the intelligence unit should implement that strategy by tasking personnel and resources to exploit selected sources, perform the collection, re-format the results if necessary to make them usable in the next stages, and forward the information to the intelligence production unit. This aspect of the collection phase may be called collection operations management. As with requirements management, it is often done by specialists, particularly in the large intelligence service. In smaller operations, the same person or team may perform some or all of the collection-related functions.

The small, multidisciplinary intelligence unit may experience certain benefits and disadvantages in managing multiple phases of the intelligence process at the same time. In comparison to the large, compartmentalized service, the smaller unit will likely experience greater overall efficiency of operations and fewer bureaucratic barriers to customer service. The same few people may act as requirements officers, operations managers and intelligence analysts/producers, decreasing the likelihood of communication and scheduling problems among them. This approach may be less expensive in terms of infrastructure and logistics than a functionally divided operation. On the other hand, the financial and time investment in training each individual in every facet of the intelligence process may be substantial. Furthermore, careful selection and assignment of personnel who thrive in a multidisciplinary environment will be vital to the unit's success, to help ward off potential worker stress and overload. An additional pitfall that the small unit should strive to avoid is the tendency to be self-limiting: overreliance on the same customer contacts, collection sources and methods, analytic approaches, and production formulas can lead to stagnation and irrelevance. The small intelligence unit should be careful to invest in new initiatives that keep pace with changing times and customer needs.

Collection Sources

The range of sources available to all intelligence analysts, including those outside of government, is of course much broader than the set of restricted, special sources available only for government use. U.S. government collection of information for intelligence purposes is channelled through the recognized intelligence collection disciplines described in Part I. From a different perspective, four general categories serve to identify the types of information sources available to the intelligence analyst: people, objects, emanations, and records. Strictly speaking, the information offered by these sources may not be called intelligence if the information has not yet been converted into a value-added product. In the government or private sector, collection may be performed by the reporting analyst or by a specialist in one or more of the collection disciplines. The following table, derived from Clauser and Weir, illustrates the distinct attributes offered by the four sources of intelligence.[36]

Table 7: Categories of Intelligence Sources by Analytic Use

Source: Adapted from Clauser and Weir

Source	Related Collection Discipline(s) and Source Attributes	Analytic Use
People	HUMINT; subject-matter experts, professional researchers, information specialists, eyewitnesses or participants	Transfer of first-hand knowledge, referral to other sources
Objects	IMINT; physical characteristics of equipment, materials, or products, such as texture, shape, size, and distinctive markings	Basis for emotive but objective reporting on composition, condition, origin, or human purpose
Emanations	MASINT, SIGINT; detectable phenomena given off by natural or man-made objects; electromagnetic energy, heat, sound, footprints, fingerprints, and chemical and material residues	Scientific and technical analysis
Records	IMINT, SIGINT, symbolic (written and oral reports, numerical tabulations) or non-symbolic (images, electro-magnetic recordings of data)	Research, background information, translation, conversion to usable form

[36] Jerome K. Clauser and Sandra M. Weir, *Intelligence Research Methodology: An Introduction to Techniques and Procedures for Conducting Research in Defense Intelligence* (Washington, DC: Defense Intelligence School, 1975), 111-117.

The following table offers examples from government and business of each source type.

Table 8: Comparison of Illustrative Intelligence Sources from Government and Business

Source: Author

Source	Information Provided	Government	Business
People	Inadvertent or intentional revelation by a person in a casual encounter, official meeting, or informant relationship	A foreign diplomat	A fellow exhibitor at a trade show
Objects	Physical and functional characteristics of the item, discerned through physical or visual examination	Military equipment	Products or components
Emanations	Clues about the identity and activities of the originator	Intercepted communications	Trace chemicals in factory effluent
Records	Evidence of existence and characteristics of target entities	Imagery, telemetry, documents	Product literature

The collection phase of the intelligence process thus involves several steps: translation of the intelligence need into a collection requirement, definition of a collection strategy, selection of collection sources, and information collection. The resultant collected information must often undergo a further conversion before it can yield intelligence in the analysis stage. Processing of collected information into intelligence information is addressed in the following Part of this primer.

PART IV
PROCESSING COLLECTED INFORMATION

From Raw Data to Intelligence Information

No matter what the setting or type of collection, gathered information must be packaged meaningfully before it can be used in the production of intelligence. Processing methods will vary depending on the form of the collected information and its intended use, but they include everything done to make the results of collection efforts usable by intelligence producers. Typically, "processing" applies to the techniques used by government intelligence services to transform raw data from special-source technical collection into intelligence *information*.[37]

> While collectors collect "raw" information, certain [collection] disciplines involve a sort of *pre-analysis* in order to make the information "readable" to the average all-source analyst. For instance: imagery analysts "read-out" the basic information on the image; foreign language broadcasts must be literally translated by linguists and analyzed for linguistic "context"; electronic signals require sorting out to be intelligible to the uninitiated in that arcane art; agent reports also need literal translations and perhaps comments as to access, context, assumed or proven past veracity.[38]

In the private sector, some processing activities are analogous to those of the government. Interpreting and annotating open-source information for a business intelligence service may include: marking locations of interest on a map or photograph, "translating" press releases or technical reports, transcribing the words of a speaker from video or audiotape into text, or drafting a detailed commentary from a personal interview.

Another term for processing, *collation*, encompasses many of the different operations that must be performed on collected information or data before further analysis and intelligence production can occur. More than merely physically manipulating information, collation organizes the information into a usable form, adding meaning where it was not evident in the original. Collation includes gathering, arranging, and annotating related information; drawing tentative conclusions about the relationship of "facts" to each other and their significance; evaluating the accuracy and reliability of each item; grouping items into logical categories; critically examining the information source; and assessing the meaning and usefulness of the content for further analysis. Collation reveals information

---

[37] The Department of Defense defines intelligence information as "unprocessed data of every description which may be used in the production of intelligence." (Department of Defense, Joint Chiefs of Staff, Joint Pub 1-02, *Dictionary of Military and Associated Terms* (Washington, DC: 23 March 1994), 184.)

[38] Dearth, "National Intelligence," 19.

gaps, guides further collection and analysis, and provides a framework for selecting and organizing additional information.[39]

Examples of collation include filing documents, condensing information by categories or relationships, and employing electronic database programs to store, sort, and arrange large quantities of information or data in preconceived or self-generating patterns. Regardless of its form or setting, an effective collation method will have the following attributes:

1. Be impersonal. It should not depend on the memory of one analyst; another person knowledgeable in the subject should be able to carry out the operation.

2. Not become the "master" of the analyst or an end in itself.

3. Be free of bias in integrating the information.

4. Be receptive to new data without extensive alteration of the collating criterion.[40]

Evaluating and Selecting Evidence

To prepare collected information for further use, one must evaluate its relevance and value to the specific problem at hand. An examination of the information's *source* and *applicability* to the intelligence issue can determine whether that information will be further employed in the intelligence production process. Three aspects to consider in evaluating the relevance of information sources are reliability, proximity, and appropriateness.

Reliability of a source is determined through an evaluation of its past performance; if the source proved accurate in the past, then a reasonable estimate of its likely accuracy in a given case can be made. A human source's own testimony of reliability may also be taken into account; qualifiers such as "certain," "believe," and "guess" indicate how sure the source is of the information being conveyed. However, if the source is completely untested, then evaluation of the information must be done solely on its own merits, independent of its origin.[41]

Proximity refers to the source's closeness to the information. The direct observer or participant in an event may gather and present evidence directly, but in the absence of such firsthand information, the analyst must rely on sources with varying degrees of proximity to

---

[39] R.H. Mathams, "The Intelligence Analyst's Notebook," in *Strategic Intelligence: Theory and Application*, eds. Douglas H. Dearth and R. Thomas Goodden, 2d ed. (Washington, DC: Joint Military Intelligence Training Center, 1995), 85-86.

[40] Mathams, 86.

[41] adapted from Gary Harris, "Evaluating Intelligence Evidence," in *A Handbook of Intelligence Analysis*, ed. Ronald D. Garst, 2d ed. (Washington, DC: Defense Intelligence College, January 1989), 34-35. For an in-depth treatment of evidence evaluation techniques and factors, see David A. Schum, *Evidence and Inference for the Intelligence Analyst*, Vols. I and II (Lanham, MD: University Press of America, 1987).

the situation. A primary source passes direct knowledge of an event on to the analyst. A secondary source provides information twice removed from the original event; one observer informs another, who then relays the account to the analyst. Such regression of source proximity may continue indefinitely, and naturally, the more numerous the steps between the information and the source, the greater the opportunity for error or distortion.[42]

Appropriateness of the source rests upon whether the source speaks from a position of authority on the specific issue in question. As no one person or institution is an expert on all matters, the source's individual capabilities and shortcomings affect the level of validity or reliability assigned to the information it provides regarding a given topic.[43]

The following examples illustrate the use of reliability, proximity, and appropriateness to evaluate a source.

> The mail clerk at 3rd Army Headquarters told me that, according to the 1st Armored Division Supply Officer, the Division is being deployed to Site Y in three days.

The reliability of the mail clerk as a source (questionable), his proximity to the information (secondary), and the appropriateness of the Supply Officer as a source on the fact of deployment (uncertain), make this information of little value to the intelligence production process.

> A major national newspaper published an interview with the CEO of Big Company, quoting the CEO's announcement of a merger the company had just secretly concluded with Large Company.

The reliability of a major national newspaper as a source (good), its proximity to the information (secondary), and the appropriateness of the CEO as the source of the merger announcement (high) make this information of high value to intelligence production.

Three aspects of the information itself have a bearing on its applicability to intelligence issues: plausibility, expectability, and support. *Plausibility* refers to whether the information is true under any circumstances or only under certain conditions, either known or possible. *Expectability* is assessed in the context of the analyst's prior knowledge of the subject. *Support* for information exists when another piece of evidence corroborates it — either the same information from a different source, or different information that points to the same conclusion.[44]

For example, a source contends that the President of Country X recently died, but the death is being kept secret from all but a few members of his regime. Although unusual, this information is plausible, and even has precedent in history. The scenario may meet the expectability criterion, if the country or this particular regime is known to be

---

[42] Harris, 35.
[43] adapted from Harris, 36.
[44] adapted from Harris, 36-38.

extremely secretive and paranoid about being vulnerable to hostile internal or external takeover movements. Support for this information may come from the same source providing details on the President's secret burial ceremony, or a different source, such as an actor who was hired to play the part of the President in a false Presidential address televised to the nation.

All these factors of source and content contribute to an initial assessment of the value of a particular piece of information to the intelligence production process. Those pieces that are judged to be useful may then undergo further scrutiny in light of customer needs, while items of questionable value may be rejected or set aside for further processing and comparison with other information. This initial selection of intelligence information sets the stage for intelligence analysis and production, as explained in the following Parts of the primer.

PART V
ANALYSIS

> Analysis is the breaking down of a large problem into a number of smaller problems and performing mental operations on the data in order to arrive at a conclusion or a generalization. It involves close examination of related items of information to determine the extent to which they confirm, supplement, or contradict each other and thus to establish probabilities and relationships.
>
> — *Mathams, 88.*

Analysis is not merely reorganizing data and information into a new format. At the very least, analysis should fully *describe* the phenomenon under study, accounting for as many relevant variables as possible. At the next higher level of analysis, a thorough *explanation* of the phenomenon is obtained, through interpreting the significance and effects of its elements on the whole. Ideally, analysis can reach successfully beyond the descriptive and explanatory levels to synthesis and effective persuasion, often referred to as *estimation*.

The *purpose* of intelligence analysis is to reveal to a specific decisionmaker the underlying significance of selected target information. Frequently intelligence analysis involves estimating the likelihood of one possible outcome, given the many possibilities in a particular scenario. This function is not to be confused with prediction, as no one can honestly be credited with predicting the future. However, intelligence analysis does appropriately involve forecasting, "which requires the explicit statement by the analyst of the degree of confidence held in a certain set of judgments, based upon a certain set of explicit facts or assumptions."[45] Different levels of analysis result in corresponding levels of conclusions that may be traced along an "Intelligence Food Chain."[46] This concept, illustrated in the following table, is equally applicable in government and business intelligence.

Table 9: The Intelligence Food Chain

Source: adapted from Davis, Analytic Tradecraft

Facts	verified information related to an intelligence issue (for example: events, measured characteristics).
Findings	expert knowledge based on organized information that indicates, for example, what is increasing, decreasing, changing, taking on a pattern.
Forecasts	judgments based on facts and findings and defended by sound and clear argumentation.
Fortunetelling	inadequately explained and defended judgments.

[45] Dearth, "National Intelligence," 25.

[46] Adapted from Jack Davis, *Intelligence Changes in Analytic Tradecraft in CIA's Directorate of Intelligence*, (Washington, DC: CIA Directorate of Intelligence, April 1995), 6.

Intelligence analysts may use this Food Chain model to measure their adherence to rigorous analytic thought — how far to go with their analytic judgments, and where to draw the line. The mnemonic "Four Fs Minus One" may serve as a reminder of how to apply this criterion. Whenever the intelligence information allows, and the customer's validated needs demand it, the intelligence analyst will extend the thought process as far along the Food Chain as possible, to the third "F" but not beyond to the fourth.

Types of Reasoning

Objectivity is the intelligence analyst's primary asset in creating intelligence that meets the Four Fs Minus One criterion. More than simply a conscientious attitude, objectivity is "a professional ethic that celebrates tough-mindedness and clarity in applying rules of evidence, inference, and judgment."[47] To produce intelligence objectively, the analyst must employ a process tailored to the nature of the problem. Four basic types of reasoning apply to intelligence analysis: induction, deduction, abduction and the scientific method.

Induction. The induction process is one of discovering relationships among the phenomena under study. For example, an analyst might discover from systematic examination of media reports that Country "X" had been issuing aggressive statements prior to formally announcing an arms agreement with Country "Y." Or an analyst may notice that a characteristic sequence of events always precedes Country "Z's" nuclear weapons tests.[48] In the words of Clauser and Weir:

> Induction is the intellectual process of drawing generalizations on the basis of observations or other evidence. Induction takes place when one learns from experience. For example, induction is the process by which a person learns to associate the color red with heat and heat with pain, and to generalize these associations to new situations.
>
> Induction occurs when one is able to postulate causal relationships. Intelligence estimates are largely the result of inductive processes, and, of course, induction takes place in the formulation of every hypothesis. Unlike other types of intellectual activities such as deductive logic and mathematics, there are no established rules for induction.[49]

Deduction. "Deduction is the process of reasoning from general rules to particular cases. Deduction may also involve drawing out or analyzing premises to form a conclusion."[50] In the case of Country "Z" above, the analyst noted a pattern of events related to testing of nuclear weapons. Later, after noticing this series of events occurring in Country "Z," the analyst may conclude that another nuclear weapons test is about to take place in that coun-

---

[47] Davis, *Analytical Tradecraft,* 5.
[48] Clauser and Weir, 81.
[49] Clauser and Weir, 81.
[50] clauser and Weir, 81.

try. The first premise, that certain events were related to weapons testing, was derived inductively — from specific observations to a conclusion. The second premise, that another test was imminent, was derived deductively — from a generalization to a specific case.[51]

Deduction works best in closed systems such as mathematics, formal logic, or certain kinds of games in which all the rules are clearly spelled out. For example, the validity and truthfulness of the following conclusion is apparent to anyone with a knowledge of geometry: "This is a triangle, therefore the sum of the interior angles will equal 180 degrees." In closed systems, properly drawn deductive conclusions are always valid.[52]

However, intelligence analysis rarely deals with closed systems, so premises assumed to be true may in fact be false, and lead to false conclusions. For example, in the weapons testing case above, Country "Z" may have deliberately deceived potential observers by falsely staging activities similar to those usually taken before a real weapons test. A conclusion that observed activities signalled a real test would be false in this case. Thus, as human activities rarely involve closed systems, deduction must be used carefully in intelligence analysis.[53]

Readers interested in further study into the use of deductive logic in estimative intelligence may wish to read the work of Israeli intelligence analyst Isaac Ben-Israel on this subject.[54] At the Joint Military Intelligence College, one student, Navy Lieutenant Donald Carney, explored the application of deductive logic to intelligence collection and analysis decisions in estimating the disintegration of Yugoslavia. Carney showed that Ben-Israel's "critical method" of inquiry could be applied prospectively to the collection of information to refute specific hypotheses, allowing for an unusually definitive estimate of the likelihood of each outcome.[55]

Abduction. Abduction is the process of generating a novel hypothesis to explain given evidence that does not readily suggest a familiar explanation. This process differs from induction in that it adds to the set of hypotheses available to the analyst. In inductive reasoning, the hypothesized relationship among pieces of evidence is considered to be already existing, needing only to be perceived and articulated by the analyst. In abduction, the analyst creatively generates an hypothesis, then sets about examining whether the available evidence unequivocally leads to the new conclusion. The latter step, testing the evidence, is a deductive inference.[56]

---

[51] Clauser and Weir, 82-83.

[52] Clauser and Weir, 83.

[53] Clauser and Weir, 83-84.

[54] Isaac Ben-Israel, "Philosophy and Methodology of Intelligence: The Logic of Estimative Process," *Intelligence and National Security 4*, no. 4 (October 1989): 660-718.

[55] LT Donald J. Carney, USN, *Estimating the Dissolution of Yugoslavia*, Seminar Paper (Washington, DC: Joint Military Intelligence College, September 1991).

[56] David A. Schum, *Evidence and Inference for the Intelligence Analyst*, Volume I (Lanham, MD: University Press of America, 1987): 20.

Abductive reasoning may also be called intuition, inspiration, or the "Ah-ha!" experience. It characterizes the analyst's occasional ability to come to a conclusion spontaneously, often without a sense of having consciously taken definable steps to get there. While the abduction process may not be easily defined or taught, it may be encouraged by providing analysts with a wide array of research material and experiences, and by supporting the expenditure of time and energy on creative thinking.[57]

Examples of abductive reasoning in intelligence analysis include situations in which the analyst has a nagging suspicion that something of intelligence value has happened or is about to happen, but has no immediate explanation for this conclusion. The government intelligence analyst may conclude that an obscure rebel faction in a target country is about to stage a political coup, although no overt preparations for the takeover are evident. The business analyst may determine that a competitor company is on the brink of a dramatic shift from its traditional product line into a new market, even though its balance sheet and status in the industry are secure. In each case, the analyst, trusting this sense that the time is right for a significant event, will set out to gather and evaluate evidence in light of the new, improbable, yet tantalizing hypothesis.

Scientific Method. The scientific method combines deductive and inductive reasoning: Induction is used to develop the hypothesis, and deduction is used to test it. In science, the analyst obtains data through direct observation of the subject and formulates an hypothesis to explain conclusions suggested by the evidence. Experiments on the subject are devised and conducted to test the validity of the hypothesis. If the experimental results match the expected outcome, then the hypothesis is validated; if not, then the analyst must develop a new hypothesis and appropriate experimental methods.[58]

In intelligence analysis, the analyst typically does not have direct access to the observable subject, but gathers information indirectly. From these gathered data, the intelligence analyst may proceed with the scientific method by generating tentative explanations for a subject event or phenomenon. Next, each hypothesis is examined for plausibility and compared against newly acquired information, in a continual process toward reaching a conclusion. Often the intelligence analyst tests several hypotheses at the same time, whereas the scientist usually focuses on one at a time. Furthermore, intelligence analysts cannot usually experiment directly upon the subject matter as in science, but must generate fictional scenarios and rigorously test them through mental processes such as those suggested below.[59]

---

[57] The relationship of this type of reasoning to Eastern philosophy is addressed in LCDR William G. Schmidlin, USN, *Zen and the Art of Intelligence Analysis*, MSSI Thesis (Washington, DC: Joint Military Intelligence College, July 1993).

[58] Mathams, 91. A seminal contribution to understanding scientific method is Abraham Kaplan's *The Conduct of Inquiry* (San Francisco, CA: Chandler, 1964). The applicability of this method in social science, and therefore, in intelligence, is developed in Earl Babbie's *The Practice of Social Research* (Belmont, CA: Wadsworth Publishing Co, 1992).

[59] Mathams, 91.

Methods of Analysis

Opportunity Analysis. Opportunity analysis identifies for policy officials opportunities or vulnerabilities that the customer's organization can exploit to advance a policy, as well as dangers that could undermine a policy.[60] It identifies institutions, interest groups, and key leaders in a target country or organization that support the intelligence customer's objective; the means of enhancing supportive elements; challenges to positive elements (which could be diminished or eliminated); logistic, financial, and other vulnerabilities of adversaries; and activities that could be employed to rally resources and support to the objective.[61] Jack Davis notes that in the conduct of opportunity analysis,

> [T]he analyst should start with the assumption that every policy concern can be transformed into a legitimate intelligence concern. What follows from this is that analysts and their managers should learn to think like a policymaker in order to identify the issues on which they can provide utility, but they should always [behave like intelligence producers]. ... The first step in producing effective opportunity analysis is to redefine an intelligence issue in the policymaker's terms. This requires close attention to the policymaker's role as "action officer" - reflecting a preoccupation with getting things started or stopped among adversaries and allies.... It also requires that analysts recognize a policy official's propensity to take risk for gain....[P]olicymakers often see, say, a one-in-five chance of turning a situation around as a sound investment of [organizational] prestige and their professional energies....[A]nalysts have to search for appropriate ways to help the policymaker inch the odds upward - not by distorting their bottom line when required to make a predictive judgment, or by cheerleading, but by pointing to opportunities as well as obstacles. Indeed, on politically sensitive issues, analysts would be well advised to utilize a matrix that first lists and then assesses both the promising and discouraging signs they, as objective observers, see for... policy goals.... [P]roperly executed opportunity analysis stresses information and possibilities rather than [explicit] predictions.[62]

Linchpin Analysis. Linchpin analysis is one way of showing intelligence managers and policy officials alike that all the bases have been touched. Linchpin analysis, a colorful term for structured forecasting, is an *anchoring* tool that seeks to reduce the hazard of self-inflicted intelligence error as well as policymaker misinterpretation. At a minimum, linchpin tradecraft promotes rigor through a series of predrafting checkpoints, outlined below. Analysts can also use it to organize and evaluate their text when addressing issues

---

[60] Jack Davis, *The Challenge of Opportunity Analysis* (Washington, DC: Center for the Study of Intelligence, July 1992), v.

[61] Davis, *Opportunity Analysis*, 7.

[62] Davis, *Opportunity Analysis*, 12-13.

of high uncertainty. Reviewing managers can use — and have used — linchpin standards to ensure that the argument in such assessments is sound and clear.[63]

Table 10: Steps in Linchpin Analysis

Source: Davis, *Analytic Tradecraft*

1. Identify the main uncertain factors or key variables judged likely to drive the outcome of the issue, forcing systematic attention to the range of and relationships among factors at play.
2. Determine the *linchpin* premises or working assumptions about the drivers. This encourages testing of the key subordinate judgments that hold the estimative conclusion together.
3. Marshal findings and reasoning in defense of the linchpins, as the premises that warrant the conclusion are subject to debate as well as error.
4. Address the circumstances under which unexpected developments could occur. What *indicators* or patterns of development could emerge to signal that the linchpins were unreliable? And what *triggers* or dramatic internal and external events could reverse the expected momentum?

Analogy. Analogies depend on the real or presumed similarities between two things. For example, analysts might reason that because two aircraft have many features in common, they may have been designed to perform similar missions. The strength of any such analogy depends upon the strength of the connection between a given condition and a specified result. In addition, the analyst must consider the characteristics that are dissimilar between the phenomena under study. The dissimilarities may be so great that they render the few similarities irrelevant.

> One of the most widely used tools in intelligence analysis is the analogy. Analogies serve as the basis for most hypotheses, and rightly or wrongly, underlie many generalizations about what the other side will do and how they will go about doing it.[64]

Thus, drawing well-considered generalizations is the key to using analogy effectively. When postulating human behavior, the analyst may effectively use analogy by applying it to a specific person acting in a situation similar to one in which his actions are well documented: an election campaign or a treaty negotiation, for example. However, an assumption that a different individual running for the same office or negotiating a similar treaty would behave the same way as his predecessor may be erroneous. The key condition in this analogy is the personality of the individual, not the similar situations. This principle of appropriate comparison applies equally to government and business intelligence analysis.

---

[63] Davis, *Analytic Tradecraft*, 8-9.
[64] Clauser and Weir, 246-248.

> Analogies are used in many different kinds of intelligence analyses from military and political to industrial intelligence. For example, major U.S. auto makers purchase their competitors' models as soon as they appear in the showrooms. The new cars are taken to laboratories where they are completely and methodically disassembled. Reasoning by analogy, that is, assuming that it would cost one producer the same amount to produce or purchase the same components used by another, the major auto producers can estimate their competitors' per-unit production costs, any cost-saving measures taken, and how much profit is likely to be earned by the sale of a single unit.[65]

Customer Focus

As with the previous stages of the intelligence process, effective analysis depends upon a good working relationship between the intelligence customer and producer. A significant difference exists between the public and private sectors with regard to this customer-producer relationship. Government analysts typically benefit from close interaction with policymakers by virtue of their well understood institutional position. The same is not often true in the business world, where the intelligence analyst's role is not yet well institutionalized.

The government intelligence analyst is generally considered a legitimate and necessary policymaking resource, and even fairly junior employees may be accepted as national experts by virtue of the knowledge and analytic talent they offer to high level customers. Conversely, in the private sector, the intelligence analyst's corporate rank is generally orders of magnitude lower than that of a company vice-president or CEO. The individual analyst may have little access to the ultimate customer, and the intelligence service as a whole may receive little favor from a senior echelon that makes little distinction between so-called intelligence and the myriad of other decisionmaking inputs. When private sector practitioners apply validated methods of analysis geared to meet specific customer needs, they can win the same kind of customer appreciation and support as that enjoyed by government practitioners.

Statistical Tools

Additional decisionmaking tools derived from parametric or non-parametric statistical techniques, such as Bayesian analysis, are sometime used in intelligence. An exploration of them is beyond the scope of this study. Many of the statistically oriented tools continue to rely fundamentally on human judgment to assign values to variables, so that close attention to the types of reasoning and methods of analysis presented herein remain the fundamental analytical precondition to their use.[66]

---

[65] Clauser and Weir, 248-250.

[66] Editor's note: A former JMIC faculty member, Douglas E. Hunter, explores the intelligence applications of Bayesian Analysis in *Political/Military Applications of Bayesian Analysis: Methodological Issues* (Boulder, CO: Westview, 1984).

Analytic Mindset

Customer needs and collected information and data are not the only factors that influence the analytic process; the analyst brings his or her own unique thought patterns as well. This personal approach to problem-solving is "the distillation of the intelligence analyst's cumulative factual and conceptual knowledge into a framework for making estimative judgments on a complex subject."[67] Mindset helps intelligence analysts to put a situation into context, providing a frame of reference for examining the subject. Analysis could not take place if thinking were not bounded by such constructs. However, mindset can also lead analysts to apply certain viewpoints inappropriately or exclusively while neglecting other potentially enlightening perspectives on an issue. While no one can truly step outside his or her own mindset, becoming aware of potential analytic pitfalls can enable intelligence analysts to maximize the positive effects of mindset while minimizing the negatives.[68] Analysts can use the accompanying list of analytical pitfalls to determine which, if any, they may be applying in their work, and whether the relevant ones are accounted for in their analytic tasks.

Categories of Misperception and Bias[69]

Evoked-Set Reasoning: That information and concern which dominates one's thinking based on prior experience. One tends to uncritically relate new information to past or current dominant concerns.

Prematurely Formed Views: These spring from a desire for simplicity and stability, and lead to premature closure in the consideration of a problem.

Presumption that Support for One Hypothesis Disconfirms Others: Evidence that is consistent with one's preexisting beliefs is allowed to disconfirm other views. Rapid closure in the consideration of an issue is a problem.

Inappropriate Analogies: Perception that an event is analogous to past events, based on inadequate consideration of concepts or facts, or irrelevant criteria. Bias of "Representativeness."

Superficial Lessons From History: Uncritical analysis of concepts or events, superficial causality, over-generalization of obvious factors, inappropriate extrapolation from past success or failure.

Presumption of Unitary Action by Organizations: Perception that behavior of others is more planned, centralized, and coordinated than it really is. Dismisses accident and chaos. Ignores misperceptions of others. Fundamental attribution error, possibly caused by cultural bias.

---

[67] Jack Davis, "Combatting Mindset," *Studies in Intelligenc*e 35, no. 4 (Winter 1991): 13-18.
[68] Davis, "Combatting Mindset," 13-15.
[69] Excerpted from Dearth, "The Politics of Intelligence," 106-107.

Organizational Parochialism: Selective focus or rigid adherence to prior judgments based on organizational norms or loyalties. Can result from functional specialization. Group-think or stereotypical thinking.

Excessive Secrecy (Compartmentation): Over-narrow reliance on selected evidence. Based on concern for operational security. Narrows consideration of alternative views. Can result from or cause organizational parochialism.

Ethnocentrism: Projection of one's own culture, ideological beliefs, doctrine, or expectations on others. Exaggeration of the causal significance of one's own action. Can lead to mirror-imaging and wishful thinking. Parochialism.

Lack of Empathy: Undeveloped capacity to understand others' perception of their world, their conception of their role in that world, and their definition of their interests. Difference in cognitive contexts.

Mirror-Imaging: Perceiving others as one perceives oneself. Basis is ethnocentrism. Facilitated by closed systems and parochialism.

Ignorance: Lack of knowledge. Can result from prior-limited priorities or lack of curiosity, perhaps based on ethnocentrism, parochialism, denial of reality, rational-actor hypothesis (see next entry).

Rational-Actor Hypothesis: Assumption that others will act in a "rational" manner, based on one's own rational reference. Results from ethnocentrism, mirror-imaging, or ignorance.

Denial of Rationality: Attribution of irrationality to others who are perceived to act outside the bounds of one's own standards of behavior or decisionmaking. Opposite of rational-actor hypothesis. Can result from ignorance, mirror-imaging, parochialism, or ethnocentrism.

Proportionality Bias: Expectation that the adversary will expend efforts proportionate to the ends he seeks. Inference about the intentions of others from costs and consequences of actions they initiate.

Willful Disregard of New Evidence: Rejection of information that conflicts with already-held beliefs. Results from prior policy commitments, and/or excessive pursuit of consistency.

Image and Self-Image: Perception of what has been, is, will be, or should be (image as subset of belief system). Both inward-directed (self-image) and outward-directed (image). Both often influenced by self-absorption and ethnocentrism.

Defensive Avoidance: Refusal to perceive and understand extremely threatening stimuli. Need to avoid painful choices. Leads to wishful thinking.

Overconfidence in Subjective Estimates: Optimistic bias in assessment. Can result from premature or rapid closure of consideration, or ignorance.

Wishful Thinking (Pollyanna Complex): Hyper-credulity. Excessive optimism born of smugness and overconfidence.

Best-Case Analysis: Optimistic assessment based on cognitive predisposition and general beliefs of how others are likely to behave, or in support of personal or organizational interests or policy preferences.

Conservatism in Probability Estimation: In a desire to avoid risk, tendency to avoid estimating extremely high or extremely low probabilities. Routine thinking. Inclination to judge new phenomena in light of past experience, to miss essentially novel situational elements, or failure to reexamine established tenets. Tendency to seek confirmation of prior-held beliefs.

Worst-Case Analysis (Cassandra Complex): Excessive skepticism. Reflects pessimism and extreme caution, based on predilection (cognitive predisposition), adverse past experience, or on support of personal or organizational interests or policy preferences.

Because the biases and misperceptions outlined above can influence analysis, they may also affect the resultant analytic products. As explained in the following Part, analysis does not cease when intelligence production begins; indeed, the two are interdependent. The foregoing overview of analytic pitfalls should caution intelligence managers and analysts that intelligence products should remain as free as possible from such errors of omission and commission, yet still be tailored to the specific needs of customers. Consistently reminding intelligence producers of the dangers and benefits of mindset may help them avoid errors and polish their analytic skills. In addition, managers may conduct post-production evaluation of intelligence products, using the biases and misperceptions listed above to identify strengths and weaknesses in individual analysts' work, and to counsel them accordingly.

PART VI
PRODUCTION

Creating Intelligence

The previously-described steps of the intelligence process are necessary precursors to production, but it is only in this final step that functionality of the whole process is achieved. *Production* results in the creation of intelligence, that is, value-added actionable information tailored to a specific customer. In practical terms, production refers to the creation, in any medium, of either interim or *finished* briefings or reports for other analysts, or for decisionmakers or policy officials. As with elements of analysis developed in Part V, production principles described and explained here may apply to both government and private sector intelligence operations.

In government parlance, the term "finished" intelligence is reserved for products issued by analysts responsible for synthesizing all available sources of intelligence, resulting in a comprehensive assessment of an issue or situation, for use by senior analysts or decisionmakers. Creating finished intelligence for national and military customers is the role of CIA and DIA analysts, respectively. Analysts within an intelligence sub-discipline may also speak of a "finished" product from their point of view, meaning that intelligence from a single source, such as SIGINT, was interpreted as fully as possible in light of all other available intelligence from that source, plus any relevant published intelligence from other sources, and open source information. Analysts within the single-source intelligence agencies consider any information or intelligence not issued by their own organization to be "collateral."

Similar designations for finished intelligence products may apply in the business world. Particularly in large corporations with multidisciplinary intelligence units, or in business intelligence consulting firms, some production personnel may specialize in the creation of intelligence from a single source, while others specialize in finished reporting. For example, there may be specialists in library and on-line research, "HUMINT" experts who conduct interviews and attend conferences and trade shows, or scientists who perform experiments on products or materials. The reports generated by such personnel may be considered finished intelligence by their intended customers within subdivisions of the larger company. The marketing, product development, or public relations department of a corporation may consume single-source intelligence products designed to meet their individual needs. Such a large corporation may also have an intelligence synthesis unit that merges the reports from the specialized units into finished intelligence for use in strategic planning by senior decisionmakers. Similarly, in the intelligence consulting firm, each of the specialized production units may contribute their reports to a centralized finished intelligence unit which generates a synthesized product for the client.

Emphasizing the Customer's Bottom Line

The intelligence report or presentation must focus on the *results* of the analysis and make evident their significance through sound arguments geared to the customer's interests. In short, intelligence producers must BLUF their way through the presentation — that is, they must keep the "Bottom Line Up Front." This axiom applies not only to written expression, but also to oral briefings, or any other medium of expression used in the intelligence environment of government or business.

> It is often difficult for... intelligence [producers] to avoid the temptation to succumb to the Agatha Christie Syndrome. Like the great mystery writer, we want to keep our readers in suspense until we can deliver that "punch line." After we have worked hard on this analysis... we want the reader to know all the wonderful facts and analytical methods that have gone into our conclusions.... Most readers really will not care about all those bells and whistles that went into the analysis. ***They want the bottom line***, and that is what intelligence professionals are paid to deliver.[70]

Knowing the customer enables the producer to generate intelligence that highlights the bottom line. Some customers are "big picture" thinkers, seeking a general overview of the issue, and guidance on the implications for their own position and responsibilities. An appropriate intelligence product for such a customer will be clear, concise, conclusive, and free of jargon or distracting detail.[71] Conversely, some customers are detail-oriented, seeing themselves as the ultimate expert on the subject area. This type of customer needs highly detailed and specialized intelligence to supplement and amplify known information. The broad-brush approach to intelligence will not only miss the mark with this customer, but may actually be perceived as an insult, lessening the chances that future products by the offending producer will be accepted or used.[72] Producers should therefore tailor both the content and delivery of the intelligence to the customer. The following section provides guidelines for creating intelligence products that meet customer needs.[73]

Anatomy of an Intelligence Product

Whether it is produced within the government, or in the business setting, the basic nature of the intelligence product remains the same. The analyst creates a product to document ongoing research, give the customer an update on a current issue or situation, or

---

[70] James S. Major, *The Style Guide: Research and Writing at the Joint Military Intelligence College*, (Washington DC: Joint Military Intelligence College, August 1994): 345.

[71] Mathams, 88.

[72] Davis, *Analytic Tradecraft*, 7.

[73] The Central Intelligence Agency has published an unclassified collection of essays on techniques for producing finished national security intelligence. The purpose of the collection is to document best practices, and to reach out to academia and the public. Its title emphasizes the instrumentality of analysis to production. See Central Intelligence Agency, *A Compendium of Analytic Tradecraft Notes*, (Washington, DC, Directorate of Intelligence: February 1997).

provide an estimate of expected target activity. In general terms, the product's function is to cover one or more subject areas, or to be used by the customer for a particular application. Along with these aspects, additional dimensions of the intelligence product are summarized in the table below. They are more fully described in the following paragraphs.

Table 11: Dimensions of an Intelligence Product

Source: Author

Dimension Category	Dimension	Examples
Content	Subject	Biographical, economic, geographic, military, political, science and technology, sociology, transportation and communications
	Intended Use	Research, current, estimative, operational, science and technology, warning
Features	Timeliness	Short-/long-term, opportune, routine/priority
	Periodicity	Ad hoc/scheduled; analyst/customer-initiated
	Scope	Narrow/broad; detailed/summary; basic/exhaustive
Packaging	Medium	Hard/softcopy, written/oral, video
	Format	Formal/informal, textual/graphical
Customer	Relationship to producer	Intended/incidental recipient; internal/external; novice/expert
	Distribution method	Internal/external; direct/indirect; focused/broad

Content

Determination of product content is done in close cooperation with the customer, sometimes at the initiative of one or the other, often in a cycle of give-and-take of ideas. Formal intelligence requirements, agreed upon by both producer and customer in advance, do drive the production process, but the converse is also true. The intelligence unit's own self-concept and procedures influence its choice of which topics to cover, and which aspects to emphasize. As a result, the customer comes to expect a certain type of product from that unit, and adjusts requirement statements accordingly. In addition, the intelligence process may bring to light aspects of the target that neither the producer nor customer anticipated. When the parties involved have a close working relationship, either

one may receive inspiration from interim products, and take the lead in pursuing new ways to exploit the target.[74]

Often, this dialogue centers around the pursuit of new sources associated with known lucrative sources. Examples from government include HUMINT targeting of persons identified in SIGINT as having access to foreign leaders, and SIGINT targeting of communications equipment revealed in IMINT of a foreign military installation. Parallel business examples might include intelligence personnel following leads to new sources revealed in original research or a published report: A pharmaceutical industry analyst who reads a business intelligence report about current breast cancer treatments may then investigate how to access human and documentary sources mentioned in the report, for further information on new drug therapy options for the disease.

The basic orientation of the intelligence product toward a particular subject or application is also determined by the producer-customer relationship. Frequently, the intelligence service will organize the production process and its output to mirror the customer organization. Government production by the single-source intelligence agencies is largely organized geographically or topically, to meet the needs of all-source country, region, or topic analysts in the finished-intelligence producing agencies, such as DIA or the National Counterintelligence Center. In the private sector, some intelligence consultant firms are specializing in one subject area, and gearing all production to one customer set, such as the petroleum industry.

In terms of intended use by the customer, both business and government producers may generate intelligence to be applied in the current, estimative, operational, research, science and technology, or warning context. Serendipity plays a role here, because the collected and analyzed information may meet any or all of these criteria. A good example is warning intelligence. Military and political analysts are always alert for target indications that an emergency, such as outbreak of war, or a political coup, is imminent. Standing procedures dictate that routine operations switch to warning mode in this case, so that time-sensitive intelligence on the situation can be issued to all relevant customers. Business intelligence analysts may also find themselves in the warning role unexpectedly, when they make discoveries that have significant time-sensitive implications for customer decisions and actions.

Features

Three key features of the intelligence product are timeliness, scope, and periodicity. Timeliness includes not only the amount of time required to deliver the product, but also the usefulness of the product to the customer at a given moment. Scope involves the level of detail or comprehensiveness of the material contained in the product. Periodicity describes the schedule of product initiation and generation.

---

[74] Turner, 314-320.

In intelligence production, the adage "timing is everything" is particularly apt. When a customer requests specific support, and when actionable information is discovered through collection and analysis, the resultant intelligence product is irrelevant unless the customer receives it in time to take action — by adapting to or influencing the target entity. Timeliness therefore encompasses the short-term or long-term duration of the production process, and the degree to which the intelligence itself proves opportune for the customer. In addition, the relative priority of the intelligence contained in the product affects the timeliness calculus. For example, a business intelligence analyst conducting research for a consumer electronics corporation may produce short-term routine reports as new information becomes available. A long-term routine summary report may be the final output from this project. However, a short-term priority report may result at any time, if time-sensitive information on competitor capabilities or intentions comes to light.

The scope of an intelligence product describes both the amount of material it contains and the depth of coverage it provides on the topic. Its focus may be narrow or broad, and the content may be detailed or in summary form. The level of coverage may be basic or exhaustive. All of these aspects are determined by the customer's needs, and by the amount and extent of the source material available.

> The amount of detail distributed will depend on the circumstances and the requirements of the user. Time constraints often will determine how much detail is given. There may be such a wealth of detail on a particular subject that an analyst might spend a month or more making a detailed analysis, but the urgency of the need for the intelligence may be such as to make a brief survey, produced in two days, much more valuable. It is important to remember that many users of intelligence have neither the time nor the patience to read through a voluminous study, however excellent it may be, and would much prefer to have the essential elements of the analysis set down in a few succinct paragraphs. Some users, however, do require detail, and when that is the case it should be provided in a usable form.[75]

Periodicity is also linked to validated customer requirements. Intelligence products correspond to requirements that specify responsiveness criteria, thus production may occur on an *ad hoc* basis or on a schedule. Analysts may proactively generate products to meet known needs of specific customers, or they may respond to spontaneous customer requests for tailored intelligence. Furthermore, "analysts, as experts in their fields, are expected to initiate studies that address questions yet unformulated by [customers]."[76] By selecting from available source material, and determining when to issue an intelligence product, analysts have the potential to influence how their customers use intelligence to make policy decisions.[77] In the government, topic experts may become close advisors to National Intelligence Officers or directly to senior policymakers. In

[75] Mathams, 92.
[76] Turner, 319.
[77] Turner, 320.

the business world, a sharp intelligence analyst might be responsible for a dramatic change in a retail company's focus, by identifying emerging consumer trends and sensitizing management for the need to reorient the company. To effect this change, the company would become dependent on intelligence about competitors in the same industry. For example, an analyst's assessment of consumer interest in buying natural pet foods might stimulate requirements for further studies, and might lead a manufacturer to change its products to meet consumer demand, before another company captures that market.

Packaging

Government intelligence products are typically packaged as highly structured written and oral presentations, including electrical messages, hardcopy reports, and briefings.[78] Many organizations also generate video intelligence products, especially in the form of live daily "newscasts," or canned documentary presentations. However, the production landscape is being transformed by technology, and today, a wide range of options is available to both business and government. Modern telecommunications and software make possible a whole new world of intelligence production, in which all the players, including customers, are in constant interaction. The Department of Defense, for example, has devised the Joint Intelligence Virtual Architecture (JIVA) concept to accelerate and streamline the entire intelligence process. Under JIVA, intelligence personnel will use advanced communication and analysis tools to electronically collaborate with each other and their customers, resulting in improved timeliness and customization of Defense intelligence products.[79] Part of the JIVA concept is the use of on-line product modules that can stand alone as finished intelligence, or be synergistically combined with other modules for use by interim or ultimate customers.[80] Similar collaborative production techniques may be successful in large business intelligence units with geographically dispersed personnel and customers. However, the benefits offered by modern intelligence practices such as JIVA also present significant challenges, including the financial and political investment in new infrastructure, and the legal implications of the required cooperation between the government and technology firms.[81]

The format of the intelligence product, regardless of the medium used to convey it, affects how well it is received by the customer. Even in a multimedia presentation, the personal touch can make a positive difference. Therefore, the degree of formality, and the mix of textual and graphical material should match the customer's preferences. Some cus-

---

[78] A guide to orally presenting intelligence is found in James S. Major, *Briefing with Intelligence*, (Washington DC: Joint Military Intelligence College, August 1997).

[79] Defense Intelligence Agency, *Vector 21, A Strategic Plan for the Defense Intelligence Agency* (Washington, DC: Programs and Operations Staff, undated), 20.

[80] Louis E. Andre, "Intelligence Production: Towards a Knowledge-Based Future," *Defense Intelligence Journal* 6, no. 2 (Fall 1997): 41.

[81] William O. Studeman, "Leading Intelligence Along the Byways of Our Future: Acquiring C^4ISR Architectures for the 21st Century," *Defense Intelligence Journal* 7, no. 1 (Spring 1998): 52.

tomers want formal briefings, while others enjoy conversational give and take; some want a scheduled meeting, others want the analyst to be available at any time for impromptu consultation. Often, verbally oriented customers request one-on-one exchanges during official travel in automobiles or in airplanes. Conversely, the visually oriented customer may prefer video clips, graphs, charts, and photographs, accompanied by brief amplifying text. Many customers prefer written analyses, often in the form of concise executive summaries or point papers; some will ask for an in-depth study after consuming the initial or periodic assessment. However, producers should be aware of the potential pitfalls of relying on the executive summary to reach key customers. If the product does not appeal to the executive's staff members who read it first, it may never reach the intended recipient.[82]

Customer

In addition to understanding the customer's intelligence requirements, the producer may benefit from an awareness of the relationship between the customer organization and the intelligence service itself. Status issues between the two parties may influence the tone of the intelligence product. Aspects of the producer-customer relationship include whether the recipient is the intended or incidental customer, whether the customer is internal or external to the intelligence service, and whether the parties differ in their level of subject matter knowledge.

The intelligence producer selects the product content and format to suit a specific individual or customer set. However, the producer should beware of selecting material or phraseology that is too esoteric or personal for a potential wide audience. Intelligence products are official publications that become official records for use by all authorized personnel within the producer and customer organizations. They should focus on the primary customer's needs, yet address the interests of other legitimate players. Sometimes, when the producer is struggling with how to meet the needs of both internal and external customers, the solution is to create two different types of products, one for each type of customer. Internal products contain details about the sources and methods used to generate the intelligence, while external products emphasize actionable target information. Similarly, the producer adjusts the product content and tone to the customer's level of expertise. For example, a SIGINT producer may issue a highly technical and detailed product for fellow SIGINT service members, but for intelligence producers in a different agency, a less technical but still producer-oriented product may be appropriate. Similarly, the business intelligence producer within a marketing department may generate a highly specialized report for the head of the department, but may issue an executive summary for the company president.

Selection of the distribution method for the product is also closely tied to the relationship between producer and customer. The ability to deliver specific types of products to internal and external customers depends upon available infrastructure and

---

[82] Loch K. Johnson, *America's Secret Power, The CIA in a Democratic Society,* (New York: Oxford University Press, 1989): 98.

resources (telecommunications lines, transportation, media equipment). Politics affect whether intelligence can be delivered by the individual analyst directly to the customer, or only through a chain of command. Finally, the number of designated recipients is often determined by the sensitivity of the intelligence issue covered in the product. If the intelligence is highly sensitive, such as a report on threats to the president's life, then only the few involved persons (the president and a few key security personnel) will receive the report. A routine report may be broadly distributed to a large customer set. Thus, the choice of distribution method is more a marketing decision than a mechanical exercise.[83] Successful delivery of a truly useful intelligence product to a receptive customer is the result of communication and cooperation among all the players.

Customer Feedback and Production Evaluation

The production phase of the intelligence process does not end with delivering the product to the customer. Rather, it continues in the same manner in which it began: with dialogue between producer and customer.

> If the product is really to be useful for policy-making and command, dissemination involves feedback, which is part of the marketing function.... Ideally, the "marketer" who delivers the product is the same individual who accepts and helps to refine the initial requirement.[84]

Intelligence producers need feedback from end-users. If producers do not learn what is useful and not useful to customers, they cannot create genuine intelligence. Internal review procedures that focus on the format and style of intelligence products are not sufficient for producers to judge their performance; they must hear from customers on the intelligence value of their work. Then producers can modify their practices to further develop those activities that served the customer well, and improve or eliminate those that did not.

Feedback procedures between producers and customers should include key questions, such as: Is the product usable? Is it timely? Was it in fact used? Did the product meet expectations? If not, why not? What next? The answers to these questions will lead to refined production, greater use of intelligence by decisionmakers, and further feedback sessions. Thus, production of intelligence actually generates more requirements in this iterative process.[85] Producers and managers may use the framework developed by Brei and summarized below as an initial checklist for evaluating their own work, and as a basis for formal customer surveys to obtain constructive feedback.

Producers also need performance feedback from their own managers. Useful aspects of such an internal evaluation may include whether the output met the conditions set down by customers and producers in formal intelligence requirements, whether the intel-

---

[83] Johnson, 97.
[84] Dearth, "National Intelligence," 20.
[85] Dearth, "National Intelligence," 20.

ligence was indeed used by customers, and whether the product resulted from a high standard of analytic quality.[86] To establish a formal internal review process for monitoring the quality of analysis in intelligence products, managers could select experienced analysts to serve on a rotating basis as "mindset coaches" — reviewing assessments for issues of mindset, uncertainty, and policy utility, or consider pairing with another production division to swap personnel for this activity. As a rule, the less the critical reader knows about the substance of the paper the more he or she will concentrate on the quality of the argumentation. A reward for the best "mindset coaches" would be to make them branch chiefs.[87]

Table 12: A Framework for Intelligence Product Evaluation and Customer Feedback

Source: adapted from Brei

Accuracy: Were all sources and data free of technical error, misperception, and hostile efforts to mislead?

Objectivity: Were all judgments free of deliberate distortions and manipulations due to self-interest?

Usability: Was all production issued in a form that facilitated ready comprehension and immediate application? Were products compatible with the customer's capabilities for receiving, manipulating, protecting, and storing the product?

Relevance: Was information selected and organized for its applicability to a customer's requirements, with potential consequences and significance of the information made explicit to the customer's circumstances?

Readiness: Are intelligence systems responsive to the existing and contingent intelligence requirements of customers at all levels of command?

Timeliness: Was intelligence delivered while the content was still actionable under the customer's circumstances?

Management's role extends beyond fostering quality production, to bearing responsibility for organizing and administering the complete intelligence process. Managers make key decisions that mirror the intelligence process and make production possible. In conjunction with customers, managers determine what customer set the intelligence unit will serve; what sources it will exploit; what types of intelligence it will produce; and what methods of collection, processing, analysis, production, customer feedback, and self-evaluation it will use. The following Part of this primer explores best practices in managing the intelligence process.

[86] Arthur S. Hulnick, "Managing Intelligence Analysis," 338.
[87] Davis, "Mindset," 17.

PART VII
MANAGING THE INTELLIGENCE PROCESS

The Role of Management

> Another discipline integral to the intelligence profession — but worthy of special consideration in this context — is that of management. The effective administration and direction of intelligence activities can be regarded as the epitome of intelligence professionalism. Just as an untutored civilian cannot be expected competently to command [a military unit], so an untrained or inexperienced layperson cannot be expected effectively to direct [an intelligence operation]. But mastery of professional intelligence skills does not, in itself, ensure that a person is able to direct intelligence functions competently; expertise in administrative techniques and behavioral skills is also essential to managerial effectiveness. Some facility in these areas can be acquired through experience, but a professional level of competence requires familiarity with the principles and theories of management, and leadership.[88]

Moreover, supervisors and managers have a particular responsibility for ensuring the professional development of their subordinates. When all the members of the intelligence unit are competent, then the effectiveness of the group increases. Enabling subordinates also frees managers to thoroughly plan and administer the intelligence operation, instead of redoing the work of production personnel. Meanwhile, managers may continue to broaden their own knowledge of the intelligence process and its customer-service mission.[89]

Organizing the Intelligence Service

In the national Intelligence Community, federal laws form the basis for a centrally coordinated but functionally organized system. The Director of Central Intelligence (DCI) leads the community with the aid of the National Intelligence Council (NIC). Members of the NIC come from all the intelligence agencies plus academia and the private sector. The

---

[88] George Allen, "The Professionalization of Intelligence," in Dearth and Goodden, 1995, 37. Informed debate on the realities of analysts' and managers' intelligence responsibilities toward customers is ongoing in the *International Journal of Intelligence and CounterIntelligence.* Examples of this literature are: Michael A. Turner, "Setting Analytical Priorities in U.S. Intelligence," 9, no. 3 (Fall 1996): 313-327; H. Bradford Westerfield, "Inside Ivory Bunkers: CIA Analysts Resist Managers' "Pandering" Part I, 9, no. 4 (Winter 1996/97): 407-424; and H. Bradford Westerfield, "Inside Ivory Bunkers: CIA Analysts Resist Managers' "Pandering" Part II, 10, no. 1 (Spring 1997): 19-54.

[89] Russell G. Swenson, *An Office Manager's Guide to Intelligence Readiness,* Occasional Paper Number Three (Washington, DC: JMIC, December 1996), 3-5.

NIC manages the national Intelligence Needs Process and supervises the production of National Intelligence Estimates for senior policymakers. Other senior bodies advise or assist the DCI in matters of policy, resource management, performance review, coordination of elements, customer relations, and intra-community relations.[90] Four topical intelligence centers staffed by multiple agencies coordinate intelligence production for policymakers in the key areas of Counterterrorism, Counterintelligence, Counternarcotics, and Nonproliferation.[91] Crisis situations may spark the formation of a temporary special task force, integrating intelligence functions that are usually separate. Although the national Intelligence Community is centrally coordinated, each member organization develops some self-determined policies and procedures, and engages in competitive analysis with respect to the other organizations.

The unifying principle across government intelligence missions is the basic charter to monitor and manage threats to national interests and to the intelligence service itself. In both the national Intelligence Community and the business community, managers may make a distinction between self-protective intelligence activities and competitive intelligence activities. Self-protection involves gathering and analyzing data about threats to public, personal, or multinational mission members' security, whereas competitive activities involve gathering and analyzing data about adversary organizations or countries. In business, the two functions are sometimes undertaken by entirely different companies or groups within the same company.[92] Government subordinates both functions within the intelligence infrastructure.

Table 13: Three Contexts for Government and Business Intelligence Tasks

Source: Author and Editor

Contexts:	**Individual**	**Corporate**	**Global**
Government Tasks:	Diplomatic Security/ Force Protection	Foreign Capabilities Assessment	Strategic Warning from Intelligence
Business Tasks:	Threat Analysis, Personal Risk Analysis	Business/Competitive Intelligence	Business Scenario Planning

Threat analysis in the business environment depends on the open exchange of information between companies, as it is widely recognized that no one benefits from other companies encountering unnecessary risk or danger to their personnel. On the other hand, at the corporate level, competitive business intelligence relies on the protection or discovery of important corporate data. In the public security environment, diplomatic security and

[90] CIA, *Consumer's Guide*, 2-3.

[91] Davis, *Opportunity Analysis*, 8.

[92] Jonathan Tetzlaff, Area Director, Security Research and Analysis, Amoco Corporation, personal correspondence with editor, 24 October 1997.

force protection for a government's own citizens, and for personnel in multilateral operations, is in the best interests of all. Conversely, foreign capabilities assessment operates in the context of a zero-sum game among countries, with potential winners and losers of the tactical advantage.

When the very survival of a corporation or country is at stake vis-a-vis other players in their respective environments, a global or strategic model applies. At this level, strategic warning intelligence takes center stage in the government security setting, and its counterpart — strategic scenario planning — achieves value in the private sector. Scenario planning has been used advantageously by some companies. The Shell Oil Company, for example, used scenario planning to justify disinvestment in oil exploitation infrastructure prior to the worldwide fall in oil demand in the 1980s. The company rose from 14th to 2nd place among oil multinationals, as overinvested companies lost billions.[93] The alternative to taking global or strategic intelligence action is to allow threats to emerge and to bring company or government officials to the realm of crisis management. There, fundamental government or business interests are at stake, and the outcome is more likely to be left to the vagaries of impulse and chance than to the considered judgment and actions of corporate or government leaders.

Private sector intelligence services can consider which elements of the national intelligence model may apply in their own domain. Will the organization require central coordination of diverse elements as the national system does, or might the intelligence unit more closely resemble a single collector or producer agency with a simpler management structure? Will an advisory group mediate between intelligence producers and customers, and does the intelligence service require its own staff to coordinate operations? Will the service be organized functionally into collection and production elements, or perhaps topically? Is

---

[93] Robbie E. Davis-Floyd, "Storytelling Corporate Futures: The Shell Scenarios," *International Journal of Futures Studies* 1 (1995-1997), on-line at http://www.systems.org/HTML/journals.htm, accessed 3 December 1997. The purpose of scenario planning is to force business managers and executives to face future uncertainties squarely by elaborating and evaluating the likelihood and impact of alternative hypothetical business environments. Dissenters are valued, rather than avoided, and, as in government intelligence channels, information is proactively developed to champion and refute the various scenarios as "controllable" pathways to the future. Recent reviews of business scenario planning include Kathy Moyer, "Scenario Planning at British Airways — A Case Study," *Long Range Planning* 29, No. 2 (April 1996): 172-181; Francoise Hecht, "The Aha! Factor," *Director* 50, No. 12 (July 1997): 59; and Ian Smith, "Avoiding Future Shock," *Director* 50, No. 12 (July 1997): 56-59.

A seminal work on the analytical environment for strategic warning in government intelligence is Ephraim Kam, *Surprise Attack* (Cambridge, MA: Harvard University Press, 1988). Although Kam focuses on military attack scenarios, the arena for strategic warning in government intelligence work has expanded as international security concerns shift toward economic competition and away from military confrontation. The convergence of economics and security signals a need for benchmarking the intelligence process, and could presage an era of greater collaboration between cells of intelligence analysts and policymakers at the highest levels, not unlike the give and take that characterizes successful business scenario planning.

the intelligence service an independent organization with external customers, or does it operate within a parent organization? If the latter, does each department, such as Marketing, Planning, or Research require its own tailored intelligence support? Does the chief executive require a centralized intelligence service, by whatever name, to assist in corporate policy-making? Should the service develop contingency plans for providing time-sensitive support in a crisis situation? On a larger scale, should intelligence services within an industry pool their resources for mutual benefit in a crisis environment, or to proactively adapt to a changing environment, as does the national Intelligence Community? The answers to these questions may help private sector intelligence organizations determine how closely to pattern their structure after that of the national intelligence system.

Managing Analysis and Production

Intelligence managers in government and industry need to decide how to organize the production process just as they need to determine the structure of the intelligence service as a whole. Typical methods of assigning analysts are by target function, geographical region, technical subject, or policy issue. The intelligence service may task analysts to concentrate on one type of source information, or to merge all available sources to produce "finished" intelligence or estimates. Some industries will need analysts to specialize in certain technical subject areas or complex issues, while large corporations may assign intelligence analysts to each of several departments such as Research or Product Development. Small independent intelligence services may require personnel to perform all the functions of the intelligence process from needs assessment to production and performance evaluation. In that case, analysts might be assigned to a particular customer account rather than a specific topic area. Part VIII of this primer presents findings on the attributes of intelligence analysts that may prove useful in determining how to allocate human resources in the intelligence production process.

> Some characterizations of the analytic mission...seem to emphasize serving the policymaking process as an abstraction: to tell it like it is, to level the playing field, to keep the policymakers honest, to be right on the record.... But excessive adherence to these attributes can cause overproduction of assessments that feature what analysts think policy officials should want to know, and underproduction of assessments featuring what officials think they need from...analytic specialists.... To provide the requisite benefits for policymakers, the analytic assessments of the intelligence production unit have to deliver a high order of understanding and insight that can support sound decisionmaking. One should avoid a definition of effective analysis that emphasizes accurate prediction...or one that centers on whether or not a policy worked.[94]

> Furthermore, managers can take the initiative in transforming intelligence into a proactive service. Managers who are isolated from the intelligence customer tend to monitor the quantity of reports produced and level of polish in intelligence products, but not the utility of the intelligence itself.[95]

---

[94] Davis, *Opportunity Analysis*, 2-3.
[95] Davis, *Opportunity Analysis*, 10.

> But policy officials will seek information and judgment from the source that provides it at the lowest personal cost, including the mass media, no matter how much money the intelligence organization is spending to fund analysis on their behalf. Thus, managers need to learn to ask for and accept opportunity analysis included in intelligence products, not remove it as inappropriate during the review process. One way to ensure that analysts produce truly useful intelligence is for managers to take an inventory, say twice per year, of the specific professional interests of their key [customers]. Policy officials are more comfortable thinking in terms of outputs than of inputs. Thus, the inventory should be couched in terms of the policymakers' objectives — their hopes and fears — and not in terms of their "intelligence priorities."... The intelligence manager should then take responsibility for converting the inventory into signals for the restructuring of collection, research, and analytic production.[96]

Evaluating the Intelligence Process

Beyond organizing and monitoring intelligence production, an additional management responsibility is to evaluate the intelligence service's overall mission performance. From the manager's perspective, intelligence products are not the only output from the intelligence process; therefore, products are not the only focus of rigorous self-evaluation. In the course of its operations, the intelligence unit expends and generates significant amounts of financial and political capital. Careful examination of this commodity flow may yield key insights into process improvement. Internal review procedures may thus include measures of how well the intelligence service and its components organize their work, use funds, allocate materiel and human resources, and coordinate with parent and customer organizations, all from the self-interested perspective of the intelligence service itself. To assist them in this effort, managers may evaluate the sub-processes and interim products of the Needs Definition, Collection, Processing, Analysis, and Production phases of the intelligence process in terms of Brei's Intelligence Values: Accuracy, Objectivity, Usability, Relevance, Readiness, and Timeliness.

Furthermore, to put a human face on intelligence process, conscientious managers may wish to include in their internal review a frank analysis of their own personnel management record. Perhaps a new definition of "customer" is in order for carrying out this aspect of intelligence evaluation. Seeing the members of the intelligence service as customers of management, and of each other, can enable managers to create a work culture in which each person's needs and talents are respected and incorporated into the organization's mission. By subscribing to the philosophy that a happy workforce is a productive workforce, managers may also achieve the organizational goal of satisfying external customer requirements. With this purpose in mind, principles for matching intelligence personnel to appropriate job assignments are discussed in the next Part of this primer.

---

[96] Davis, *Opportunity Analysis*, 6.

PART VIII
PORTRAIT OF AN INTELLIGENCE ANALYST

The efficacy of the intelligence process described in the foregoing chapters depends upon personnel who are both able and willing to do the specialized work required. Through the findings of several government studies, this section presents the ideal characteristics of the central figure in value-added production — the intelligence analyst. According to these studies, the successful intelligence analyst brings to the discipline certain requisite knowledges and abilities, or has a high aptitude for acquiring them through specialized training; is able to perform the specific tasks associated with the job; and exhibits personality traits compatible with intelligence analysis work. This profile will remain valid in any setting modeled after the national security intelligence system.

The cognitive, performance and personality attributes of the intelligence analyst are explained below. Readers are encouraged to apply this information in accordance with their own particular circumstances. For example:

> Incumbents and individuals considering employment in intelligence analysis may deepen their self-awareness and assess their potential for success and satisfaction in this profession.
>
> Educators and recruiters may identify and prepare candidates for employment in intelligence analysis.
>
> Managers and supervisors may make enlightened decisions about selection, placement, tasking and evaluation of intelligence analysis personnel.

Cognitive Attributes

An individual's analytic skill results from a combination of innate qualities, acquired experience, and relevant education. Psychologists call these mental faculties cognitive attributes, and further divide them into two types: abilities (behavioral traits, being able to perform a task) and knowledges (learned information about a specific subject).[97] Whereas an individual's cognitive abilities are relatively fixed by the time he or she enters the job market, knowledges are situation-specific and can be acquired through training.[98]

According to a recent formal job analysis of selected intelligence analysts conducted by the NSA Office of Human Resources Services, important cognitive abilities for intelligence analysis include written expression, reading comprehension, inductive reasoning, deductive reasoning, pattern recognition, oral comprehension, and information

---

[97] Mark H. Haucke, Industrial Psychologist, NSA, interview with the author, 25 May 1995.
[98] Melissie C. Rumizen, Benchmarking Manager, NSA, interview with the author, 5 July 1996.

ordering.[99] Furthermore, both junior analysts and experienced analysts or supervisors agree that high levels of these abilities are necessary for performing the intelligence analysis job. The abilities are defined in the box below.

Cognitive Abilities Required of Intelligence Analysts[100]

Written Expression: The ability to use words and sentences in writing so others will understand. Involves knowledge of the meanings and distinctions among words, knowledge of grammar, and the ability to organize sentences and paragraphs.

Reading Comprehension: The ability to read and understand written sentences and paragraphs.

Inductive Reasoning: The ability to combine separate pieces of information, or specific answers to problems, to form general rules or conclusions. Involves the ability to think of possible reasons why things go together. Also includes coming up with a logical explanation for a series of events that seem unrelated.

Deductive Reasoning: The ability to apply general rules to specific problems to come up with a logical resolution. Involves deciding if the resolution makes sense.

Pattern Recognition: The ability to identify or detect a known pattern (a figure, word, or object) that is hidden in other material.

Oral Comprehension: The ability to listen and understand spoken words and sentences.

Information Ordering: The ability to follow a rule or set of rules in order to arrange things or actions in a meaningful order. The rule or set of rules to be used must already be given. The things or actions to be put in order can include numbers, letters, words, pictures, procedures, sentences, and mathematical or logical operations.

One set of junior analysts and another of supervisors were separately asked to judge the importance of each of these abilities in performing the intelligence analysis job (see Table 14). Junior analysts assign greater importance to two abilities (written expression and inductive reasoning), but significantly less importance to pattern recognition, than do their supervisors. These results have implications for staffing the intelligence analysis job in both the government and private sector. For example, if junior analysts place greater importance on written expression than their supervisors do, they may be frustrated to receive less training, tasking and recognition than needed for this aspect of their job. The discrepancies in the rankings among the five abilities judged most important by the two groups can be addressed individually by managers. However, the rankings provide some useful generalizations for identifying cognitive attributes applicable to any intelligence environment. In the case of the National Security Agency, the results presented here led

[99] Data were generated by Mark H. Haucke, Industrial Psychologist, using a Management Research Institute (MRI) survey instrument presented in *Ability and Knowledge Requirements* (Bethesda, MD: MRI, 1994).

[100] Adapted from MRI, *Ability and Knowledge Requirements.*

psychologists to design a job-relevant pre-employment aptitude exam for intelligence analysts.

Table 14: Comparative Ranking of Cognitive Abilities Thought to Be Required for Intelligence Analysis

(The lower the number on the 1 to 5 scale, the higher the perceived importance of the ability)

Source: Author and Haucke Study

Cognitive Ability	GROUP 1 (23 Junior Analysts - less than 7 years experience)	GROUP 2 (18 Supervisors — older generation; Ave. Years experience: 19)
Written Expression	1	3
Reading Comprehension	2	1
Inductive Reasoning	2	3
Deductive Reasoning	3	2
Pattern Recognition	3	1
Oral Comprehension	4	4
Information Ordering	5	4

Unlike the abilities categories, areas of knowledge for government intelligence specialists do not necessarily apply to their private sector counterparts. The formal job study of government intelligence analysts revealed that knowledge of military-related and technical subjects, not surprisingly, was prevalent among the individuals in the research group.[101] However, in either public or private sectors, managers can hire and train personnel to apply the requisite knowledges in a given job. A next logical step is to define the components of the intelligence analysis job, to be able to plan and assess individual job performance.

Performance Factors

Even as the analysis described above examined cognitive inputs to the job, a related performance review project, also at NSA, described intelligence analysts' output on the job. As part of this review, supervisors of intelligence analysts placed their subordinates' mission-essential job tasks into seven categories. Next, they evaluated the job performance of

[101] Data courtesy of Dr. Mark Haucke.

intelligence analysts according to those criteria. Researchers found a strong positive correlation between aptitude for intelligence analysis (as measured in the knowledges and abilities survey) and successful job performance (as rated by supervisors).[102] Following is a brief description of the seven intelligence analysis performance categories:[103]

Data Collection - Research and gather data from all available sources.

Data Monitoring - Review flow of scheduled incoming data.

Data Organizing - Organize, format, and maintain data for analysis and technical report generation.

Data Analysis - Analyze gathered data to identify patterns, relationships, or anomalies.

Data Interpretation/Communication - Assign meaning to analyzed data and communicate it to appropriate parties.

Computer Utilization - Use computer applications to assist in analysis.

Coordination - Coordinate with internal and external organizations.

This concise inventory echoes the intelligence process and illustrates the complexity of the intelligence analyst's job. It also serves as a blueprint for managers as they design intelligence organizations and individual personnel assignments. In particular, the analyst's job description should reflect these expected behaviors for purposes of recruitment, selection, placement, training, and performance evaluation. The intelligence organization should also be structured physically and logically to enable these functions to occur. Managers should consider how all these factors combine to determine the effectiveness of individual analysts, intelligence units, and even national agencies or private firms that produce and use intelligence.

Personality Traits

The third component of the intelligence analyst profile, personality traits, addresses the individual's preferences for behaving in certain ways under specific conditions. Adults tend to exhibit the same set of behavior preferences consistently in familiar situations. This behavior pattern may be identified as a personality type. One well-known instrument for identifying an individual's personality type is the Myers-Briggs Type Indicator (MBTI).[104] The following discussion of the intelligence analyst's personality is based upon MBTI research.

---

[102] Haucke interview, 13 June 1996.

[103] Standardized categories are presented in an MRI performance evaluation booklet, *Job Dimension Ratings* (Bethesda, MD: MRI, 1995).

[104] See Isabel Briggs Myers, *Introduction to Type*. (Palo Alto, CA: Consulting Psychologists Press, 1980), and Ronald D. Garst, *Intelligence Types: The Role of Personality in the Intelligence Profession*. 2d printing, (Washington, DC: Joint Military Intelligence College, August 1995).

> Personality types are associated with more or less predictable patterns of behavior — meaning that people of different personality types approach tasks differently and have different tastes, interests, likes and dislikes. For example, some people would rather work alone while others prefer to work with other people. Some enjoy working with concrete information, others with abstract information. Some decide on the basis of personal reasons, some on cold, hard logic. And finally, some people enjoy making decisions while others are reluctant to decide because of perceived information inadequacy.[105]

Research at the Joint Military Intelligence College (JMIC) demonstrates that intelligence professionals exhibit a pattern of personality traits that sets them apart from the U.S. population as a whole. In this regard, intelligence professionals are no different from many others, for every profession has its own distinct pattern of personality traits. A significant percentage (21 percent) of those who choose to pursue employment in national security intelligence tend to express the following behavior preferences: orientation to the inner world of ideas rather than the outer world of things and people, tendency to gather factual information through the senses rather than inspiration, proclivity to make decisions on the basis of logic rather than emotion, and an eagerness to seek closure proactively instead of leaving possibilities open. In contrast, researchers found that people who exhibit the opposite set of personality traits are almost non-existent among intelligence professionals. The chart below summarizes the terminology by which the MBTI describes personality traits. Note that the most frequently occurring type among the respondents to the JMIC survey exhibit the traits I, S, T and J.[106]

The JMIC data are based on a large sample of government intelligence students and practitioners. Persons engaged in the study or practice of other forms of intelligence, particularly in the private sector, should not expect their personality type to match the JMIC profile. However, intelligence practitioners who choose and successfully apply the intelligence methodology presented in this primer are likely to exhibit the same personality traits as those identified in government practitioners. Because people tend to be satisfied and productive in their work if their own personalities match the corresponding behaviors suitable to their jobs, this research tying personality traits to the intelligence profession can help individuals consider their general suitability for certain types of intelligence work.

---

[105] Garst, *Intelligence Types*, 1.
[106] Garst, *Intelligence Types*, 9.

Personality Aspects Measured by the MBTI[107]

Orientation to the world

E=Extraversion	**I=Introversion**
Orientation to the outer world of things and people, interacting with and affecting them	Orientation to the inner world of ideas and concepts, solitude and self-awareness

Perception: non-rational processes; awareness of things, people, events or ideas, selection of stimuli to attend to

S=Sensing	**N=Intuitive**
Gather information by physical sensation; oriented to facts, detail and the present	Gather information by inspiration, unconscious processes; oriented to possibilities, relationships, and the future

Judgment: ways of deciding, evaluating, choosing, selecting

T=Thinking	**F=Feeling**
Decide on basis of logic, impersonal objective criteria, cause and effect, laws and justice	Decide on basis of subjective, personal criteria and values, and how decisions affect other people and relationships.

Preference for Closure as manifested through behavior using S/N or T/F Functions

J=Judging	**P=Perceiving**
Want to have an issue or project completed so they can move on; work takes precedence over play; proactive	Leave decisions open to modify response in accordance with new information; use play to make work more enjoyable; reactive

[107] Compiled from Garst, *Intelligence Types*, 4-9.

PART IX
DEFENSIVE MEASURES FOR INTELLIGENCE

> [A]s information becomes more and more a factor of production, of tangible worth for its own sake, the value of the special knowledge that is the essence of intelligence will command a higher price in the global information age marketplace than will the generally available knowledge. Therein lies the most ancient and, at the same time, the most modern challenge to the future of intelligence — protecting it.
>
> *— Goodden, in Dearth and Goodden, 415.*

Beyond Intelligence Process: Protecting the Means and the Results

An intelligence organization's openness about its validated intelligence methods is of course tempered by self-defense considerations. Two arenas that are complementary to intelligence production, Operations Security (OPSEC) and Information Systems Security (INFOSEC), focus on how practitioners can avoid revealing proprietary or classified information. OPSEC measures protect the specific actions taken to produce intelligence, whereas INFOSEC protects from disclosure the intelligence information used in production, as well as the resulting intelligence products.

In government circles, standard procedures guide the implementation of OPSEC and INFOSEC measures. In the private sector, trial and error may predominate. Companies that emphasize methods for exploiting publicly available information about their competitors may show little regard for protecting themselves from being targeted by the same means they have employed to target others. Furthermore, the trend toward greater computerization of the workplace, including on-line information systems and networked services, makes both government and commercial organizations vulnerable to being exploited themselves.[108]

For example, the Boeing Corporation discovered in 1992 that amateur computer hackers had found their way into the company's computer network, and used stolen passwords to open pathways to proprietary information stored in other computers in industry, government, and education organizations.[109] Prosecuting this case cost Boeing, the FBI, and other law-enforcement authorities considerable time and money.[110] This case was trivial

---

[108] Keen insights into such vulnerabilities are presented in Ira Winkler, *Corporate Espionage: What It Is, Why It Is Happening in Your Company, What You Must Do about It,* (Rocklin, CA: Prima Publishing, 1997).

[109] Rhonda E. MacLean, Senior Manager, Boeing Computing and Communications Security, "The Boeing Hacker Incident," *DODSI Security Awareness Bulletin* Number 1-94 (Richmond, VA: Department of Defense Security Institute, August 1994), 19.

[110] MacLean, 20-21

compared to other well publicized security breaches in government and industry.[111] Yet, at the March 1996 international SCIP conference, of 72 presentations held during four days, only three specifically addressed counterintelligence or security.[112] One reason for this is that businesses may be reluctant to admit their own vulnerabilities in the presence of competitor firms. However, as a Boeing computer security officer has noted, corporations are beginning to realize that admitting flaws in information system defenses is the first step toward preventing future violations, and business and government should work together toward this goal.[113]

In light of the tendency to overlook OPSEC and INFOSEC implementation, the remainder of this section develops an instructional overview of the basic information that government and business personnel should know to protect their activities from unauthorized exploitation. Indeed, for the health of U.S. commerce and national security activities, everyone needs user-friendly information on how to protect proprietary information. Even the most sophisticated corporations have difficulty keeping up with the hazards of the information age; it was not until 1992 that Boeing mandated that all company computer users attend a security awareness briefing, and this was after the firm suffered a major breach of information security. Now Boeing sees "...the importance of information security to our company's long-term competitiveness..." and considers awareness activity as the cornerstone to a good security program.[114]

Operations Security

OPSEC is essential to the intelligence function in both the national security and business environments. OPSEC denies adversaries information about one's own operational capabilities and intentions by identifying, controlling, and protecting indicators associated with the planning and conduct of those operations and other related activities. An adversary is not necessarily a belligerent enemy: In OPSEC terms, an adversary is any entity that acts against one's own interest or actively opposes one's own goals.[115]

To protect an intelligence operation, practitioners can adopt an adversary's perspective. For example, factors at risk in one's own environment can be categorized into critical information, indicators, and vulnerabilities, described briefly below.

---

[111] Examples include those cited in Clifford Stoll, *The Cuckoo's Egg*, (New York: Pocket Books, 1990) and Winn Schwartau, *Information Warfare: Chaos on the Electronic Superhighway*, (New York: Thunder's Mouth Press, 1994).

[112] SCIP, *Conference Proceedings.* Annual International Conference & Exhibit, March 27-30, 1996, (Alexandria, VA: SCIP, March 1996).

[113] MacLean, 22.

[114] MacLean, 22.

[115] National Cryptologic School, Information Security Department, *Operations Security Fundamentals*, (Fort Meade, MD: 1994), 2.

Factors at Risk in Intelligence Operations	
Critical Information	Details of capabilities and operations directed against an adversary
Indicator	Detectable actions and publicly available information revealing critical information
Vulnerability	Conditions making exploitable information available to the adversary

Countermeasure options to prevent an adversary from exploiting these factors include: eliminating the indicators altogether, concealing indicator activities, disguising indicator activities, and staging deceptive (false) activities.[116]

The practice of OPSEC is so important to national security that a federal organization has been established as its advocate. As a result of the 1988 Presidential Directive on national operations security, the Interagency OPSEC Support Staff (IOSS) was formed, with the National Security Agency as its director. The core membership of the IOSS includes the Department of Defense, Department of Energy, Central Intelligence Agency, Federal Bureau of Investigation, and General Services Administration.[117] Other executive and national security bodies, including the military services, have representation on the National Operations Security Advisory Committee, which advises the Executive Branch on the practice of OPSEC.[118] The IOSS may be contacted for assistance at:

Interagency OPSEC Support Staff, 6411 Ivy Lane, Suite 400, Greenbelt, MD 20770-1405 Telephone (301) 982-2313/0323.

Information Systems Security

Information Systems Security (INFOSEC) refers to the protection of information that an organization uses and produces in the course of its operations. Today, this means protecting complex electronic networks. Government and business depend upon computerized systems for everything from banking, communications, and data processing to physical security and travel reservations. To the casual observer, INFOSEC may seem the domain of a few technical specialists, or the exclusive concern of the military or intelligence agencies. But INFOSEC is the responsibility of everyone who has ever used a telephone, computer, or automatic bank teller machine.[119]

---

[116] National Cryptologic School, 9.

[117] National Security Agency, Introduction.

[118] National Operations Security Advisory Committee, *National Operations Security Doctrine*, (Greenbelt, MD: Interagency OPSEC Support Staff, January 1993): unnumbered back of first and second physical pages from beginning.

[119] A basic reference on INFOSEC is the National Research Council book *Computers at Risk: Safe Computing in the Information Age*, (Washington, DC: National Academy Press, 1991).

> INFOSEC today [involves] significantly more than the traditional security offered by encryption. Network vulnerability to adversarial intercept, tampering, or destruction of data mandates INFOSEC solutions that ensure the authentication, integrity, and availability of classified and unclassified information created, stored, and processed on [information] systems. ... Such solutions must enable the interconnection of Command and Control, intelligence, and support systems and must allow for the commingling of critical information of different classification levels on a common transport backbone. INFOSEC solutions must be flexible, configurable, and result from a risk management scenario that balances the costs and availability of countermeasures against actual threats to, and vulnerabilities of, networks and systems. Finally, INFOSEC must accomplish all of this in an environment in which networks are neither owned nor controlled by [the government] and resources are severely constrained.[120]

Each intelligence organization and activity must tailor its INFOSEC measures to its particular technologies and operational practices, weighing the costs of such measures against their value in safeguarding the mission. A three-dimensional model of INFOSEC, illustrated below, may guide the intelligence service in implementing protective measures and assessing their adequacy. The first dimension addresses the need to understand the vulnerability of information as it passes through different stages of use. The second dimension includes the key characteristics of information that must be preserved for it to remain useful and secure. The third dimension covers the general categories of INFOSEC tools that the intelligence service may employ. Each element of the model is dependent on the others.[121] Together, these interlocking pieces make up a comprehensive INFOSEC strategy appropriate to the public or private sector.

Dimensions of INFOSEC[122]

Information States:	Transmission, Storage, Processing
Critical Information Characteristics:	Confidentiality, Integrity, Availability to Legitimate Users
Countermeasures:	Technology, Policy/Practice, Education

Role of the Federal Government

Federal agencies, including Intelligence Community members, play key roles in helping both government and businesses learn and practice INFOSEC. The two primary authorities for INFOSEC are the Department of Commerce and the Department of

[120] National Security Agency, Introduction, para. D.2.

[121] Lynn F. Fisher, "Defining the Threat to Information Systems," *DODSI Security Awareness Bulletin* 2-94, (August 1994), 4.

[122] Fisher.

Defense. Organizations within these departments provide INFOSEC services to their respective constituencies within the framework of national information policies established by the Executive Branch. The following overview begins with a summary of Executive Branch policy.

National Information Policy

> The vision of the National Information Infrastructure — or NII — is [as] a vast accessible network of networks that supports communications and information processing to create jobs, increase productivity, improve access to government services, and encourage community networking. The NII is also the wide array of information of all kinds within the networks, whether it is stored, processed, or communicated. Finally, it includes the people... who are today creating and using the NII.[123]

The federal government's role in the NII is to provide a sound legal and policy framework, in conjunction with state, local and Native American governments. Current initiatives include assuring universal service on the NII, thereby enabling open access to government information; protecting intellectual property rights; protecting the privacy of individual information; and stimulating the development of advanced information technologies, including security technologies.[124] The Office of Management and Budget's (OMB) national information security authority covers the development, promotion, implementation and evaluation of government policies and practices for information resource management.[125]

A multi-agency group, the national Information Infrastructure Task Force (IITF), coordinates the federal role in the NII through three committees: the Committee on Applications and Technology, the Telecommunications Policy Committee, and the Information Policy Committee. The OMB's Office of Information and Regulatory Affairs chairs the IITF's Information Policy Committee. As noted below, elements of the Commerce Department chair the other two IITF committees. In addition, the NII Security Issues Forum coordinates NII security activities throughout the IITF and the federal government.[126]

Commerce Department

The Commerce Department's Assistant Secretary for Communications and Information heads the National Telecommunications and Information Administration (NTIA).

---

[123] Sally Katzen, Administrator, Office of Information and Regulatory Affairs, U.S. Office of Management and Budget, Remarks prepared for delivery at the National Computer Security Conference, Baltimore, MD, 11 October 1994.

[124] Katzen.

[125] U.S. Congress, Office of Technology Assessment, *Information Security and Privacy in Network Environments* (Washington, DC: GPO, September 1994), 137.

[126] Katzen.

The NTIA's information security responsibilities include: serving as the principal executive adviser to the President on telecommunications and information policy; serving as the principal federal telecommunications research and engineering laboratory, through the Institute for Telecommunication Sciences in Boulder, Colorado; and providing grants to programs that promote the development and provision of advanced telecommunications technologies for the public. The NTIA chairs the IITF's Telecommunications Policy Committee.[127]

The Commerce Department's Technology Administration includes two components involved in information security, the Office of Technology Policy (OTP) and the National Institute for Standards and Technology (NIST).

> The primary role of the OTP is to offer assistance to private sector and government communities in advocating and pursuing policies that maximize the impact of technology on economic growth, and by exercising leadership to define the role of government in supporting U.S. industrial competitiveness in the post-cold war environment. ... NIST's primary mission is to promote U.S. economic growth by working with industry to develop and apply technology, measurements, and standards.[128]

NIST is the national authority for developing government-wide standards and guidelines for protecting unclassified but sensitive information, and for developing government-wide training programs.[129] NIST also chairs the IITF's Committee on Applications and Technology.[130] Finally, NIST maintains the Computer Security Resource Clearinghouse (CSRC) as a resource for anyone with an interest in computer security. It is available on-line 24 hours a day, seven days a week at no charge. The CSRC provides access to crisis response information on security-related threats, vulnerabilities, and solutions, and is a general index to computer security topics such as general risks, privacy, legal issues, viruses, assurance, policy, and training.[131]

Defense Department

The Secretary of Defense is the Executive Agent for National Security Telecommunications and Information Systems Security.[132] As a whole, Department of Defense (DoD) information and communications systems are termed the Defense Information Infrastructure (DII). Under the direction of the Secretary of Defense, three DoD agencies form the

---

[127] Katzen.

[128] Office of the Federal Register, National Archives and Records Administration, *The United States Government Manual 1995/96* (Washington, DC: GPO, 1 July 1995), 167-168.

[129] U.S. Congress, Office of Technology Assessment, 13.

[130] Katzen.

[131] Defense Information Systems Agency (DISA), "The NIST Computer Security Resource Clearinghouse," *DISSPatch* 4, no. 1 (3rd Quarter 1996): 6. See CSRC home page at: http://www.csrc.nist.gov.

[132] National Security Agency, Chapter 3, B.d.

core DII INFOSEC team: the Defense Intelligence Agency (DIA), the Defense Information Systems Agency (DISA), and the National Security Agency (NSA). Although notionally the DII is a dedicated system for proprietary and classified national defense information, in fact over 95 percent of its communications are carried on the public switched networks of the NII.[133] Thus, DoD expertise in information security doctrine and technology makes the organizations explained below key resources for other government organizations and for the private sector.

The Defense Intelligence Agency, as the central authority for military intelligence, provides INFOSEC threat analysis and support to the DII.[134] Another agency, DISA, is responsible for planning, developing, and supporting command, control, communications, and information systems that serve the needs of the National Command Authorities under all conditions of peace and war; it further ensures the interoperability of all DII systems and those national and/or international commercial systems that affect the DISA mission.[135] NSA acts as the National Manager for National Security Telecommunications and Information Systems Security in the name of the Secretary of Defense. In this capacity, NSA is the focal point for U.S. government cryptography and for the security of national security telecommunications and information systems.[136] NSA provides DISA with the tools, techniques, products, services, and security management structures to protect the DII, through its "V" Group, the customer service and engineering organization for information systems security.[137] Within NSA, the National Computer Security Center (NCSC) conducts technical evaluation of the protection capabilities of commercially produced and supported systems.[138] Through its Information Systems Security Research Joint Technology Office (ISSR-JTO), NSA coordinates with DISA and the DoD's Advanced Research Projects Agency on engineering INFOSEC technologies. The ISSR-JTO provides a first line of defense for defensive information warfare, and permits electronic commerce between DoD and its contractors. It also maintains research and technology interfaces with the military departments, national labs, universities, and industry.[139] NSA coordinates with the National Institute for Standards and Technology (NIST) in matters of common concern.[140] Together, DIA, DISA, and NSA operate the DoD Center for Information Systems Security.[141]

---

[133] LtGen Kenneth A. Minihan, "Intelligence and Information System Security," *Defense Intelligence Journal* 5, no. 1 (Spring 1996): 20.

[134] Defense Information Systems Agency, "INFOSEC and the DII," *DISSPatch* 4, No. 1, (3rd Quarter, CY 1996): 7.

[135] Office of the Federal Register, 234.

[136] NSA, Chapter 3, B.e.(2).

[137] DISA, "Introducing NSA's New and Improved V Group," *DISSPatch* 4, no. 3 (3rd Quarter 1996): 2.

[138] NSA, Chapter 6, para. 1.

[139] DISA, "V Group," 5.

[140] INFOSEC Program Management Office (IPMO), *DISSPatch*, May 97, 14.

[141] DISA, "INFOSEC and the DII," *DISSPatch* 4, No. 1 (3rd Quarter 1996): 7.

The Department of Defense's INFOSEC Program Management Office (IPMO) is a joint DoD/DISA/NSA organization charged with executing centrally managed INFOSEC functions within the DoD.[142] The IPMO provides operational protection and detection capability for the DII against information exploitation, manipulation, or destruction. It administers DoD-wide INFOSEC training and manages the DoD INFOSEC Technical Services Contract. The IPMO conducts vulnerability, threat, and operational analyses of the DII, provides security policy guidance and oversight to DISA programs, and certifies DISA and non-DISA systems that connect to the DII.[143] The IPMO also provides support to the Assistant Secretary of Defense for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (ASD/C4ISR).[144] Another DoD body, chaired by the ASD/C4ISR, also has a role in INFOSEC. Under the purview of the National Security Council, the National Security Telecommunications and Information Systems Security Committee (NSTISSC) advises Executive Branch agencies and Departments on the status of national security systems. Its two subcommittees focus on telecommunications security and information systems security, respectively. NSA provides the NSTISSC secretariat.[145]

In addition, the DoD Security Institute (DODSI) promotes security awareness and compliance with security procedures in DoD by offering training courses to security personnel in DoD and DoD-related industry, publishing security awareness bulletins, and disseminating information to security trainers on security and counterintelligence.[146]

INFOSEC for Everyone

The national authorities for INFOSEC described above evolved out of the need to protect the fundamental role of information in a democratic society and market economy. They help strike the balance between free exchange of information and privacy, and between free enterprise and regulation. Government-sponsored information policy and technology set the standards upon which nearly every facet of public and private life is based. Citizens receive basic services through government-created or -regulated information infrastructure, including automatic payroll deposit to employee bank accounts, cellular telephone service, electronic commerce via the Internet, air and rail traffic control, emergency medical services, and electrical power supply.

Such services contribute not only to the citizen's quality of life, but to the very functioning of the nation. Information is the lifeblood of society and the economy. Imagine the chaos that would reign if the government, the military, banks, businesses, schools, and hospitals could not communicate reliably. Life would come to a halt.

---

[142] IPMO, 14.
[143] DISA, "INFOSEC," 7.
[144] U.S. Department of Defense Security Institute (DODSI), *DODSI Security Awareness Bulletin* 2-94 (August 1994): 25.
[145] NSA, Chapter 3, B.a, B.b, and B.c.
[146] DODSI, front cover, 12, 18.

INFOSEC is designed to protect society from inadvertent or intentional harm to these key functions. The same free access to information that makes society flourish also makes it vulnerable to damage, attack or exploitation. For example, passive threats such as shoddy equipment, faulty software, or negligent personnel can disrupt service and destroy information. Hostile threats include thrill-seeking computer hackers and belligerent foreign adversaries who deliberately target sensitive government and public information networks with the aim of disrupting or destroying key operations, such as military projects or power grids.[147] Comparable scenarios within the business sector, to include information sabotage and deception actions against competitors, are at least plausible. Therefore, basic knowledge of INFOSEC may benefit citizens in all walks of life. Addresses and phone numbers for the INFOSEC agencies that can assist the public are listed at the end of this chapter.[148]

Government expertise in information technology and policy has made it the authority specifically on protecting intelligence operations. The private sector may also benefit from this expertise by applying INFOSEC measures in business intelligence. In brief, successful intelligence operations rely on secure transmission, storage, and processing of the information used. The information itself must be exchanged only among legitimate users, and it must retain its intended meaning and be available to users upon demand. Finally, intelligence information and products can be protected through technology (access control, encryption), through security policies and practices, and through educating the workforce, as with this document.

Points of contact:

Commerce Department:

NIST, Public Inquiries Unit, 100 Bureau Drive, Gaithersburg, MD 20899-0001; 301-975-6478 (voice); email: inquiries@*nist.gov*; Website: *http://www.nist.gov/*.

DoD:

IPMO, 5111 Leesburg Pike, Suite 100, Falls Church, VA 22014-3206; 703-681-7944/DSN761-7944 (voice); 703-681-1386/DSN 703-761-1386 (fax); e-mail: *cissa@ncr.disa.mil*, Website: *http://www.disa.mil/ciss*.

DISA, Public Affairs Office, 701 South Courthouse Road, Arlington, VA 22204-2199; 703-607-6900 (voice); Website: *http://www.disa.mil*.

DODSI, 8000 Jefferson Davis Highway, Building 33E, Richmond, VA 23297-5091; 804-279-5314/DSN 695-5314 (voice); 804-279-5239/DSN 695-5239 (fax).

---

[147] Gregory L. Vistica and Evan Thomas, "The Secret Hacker Wars, Behind the spreading battle over cyberterrorism," *Newsweek* (1 June 1998): 60.

[148] In addition, the National Counterintelligence Center provides support to the private sector regarding economic espionage, economic intelligence collection, and threat awareness. The NACIC website is *http://www.nacis.gov.*

NCSC, Suite 6765, 9800 Savage Road, Fort George G. Meade, MD 20755-6765; 20 410-859-4371 (voice); 410-859-4375 (fax).

NSA, Fort George G. Meade, MD 20755-6000, Attn: V1, Office of Customer Support Services; 410-859-4384/DSN 644-0111; 800-688-6115 (voice); Website: *http://www.nsa.gov:8080/*.

EPILOGUE

This primer has reviewed government intelligence production practices in building-block fashion. It has also explored the defensive measures comprising information security and operations security, which are integral to all the building blocks, and are equally applicable to private businesses and government organizations. Finally, the primer has drawn a cognitive, behavioral and personality profile of the central figure in intelligence production — the intelligence analyst. In the spirit of benchmarking, this document invites a reciprocal examination of best practices that may have been developed by private businesses, and of principles that may have been derived from other academic studies of intelligence-related processes.

Although this effort reflects a government initiative, in fact the government Intelligence Community may receive the greater share of rewards from benchmarking its own process. Potential benefits to the Community include an improved public image, increased self-awareness, more efficient recruitment through more informed self-selection by candidates for employment, as well as any resultant acquisition of specialized information from subject matter experts in the business and academic communities.

Primary advantages for the government's partners in the exchange of information on best practices could be greater understanding of how tax dollars are spent, and the opportunity to transfer an appreciation of government professional intelligence production, security, and staffing methods into academic curricula and business operations.

For all participants in benchmarking, releasing information is actually a way of controlling it, a way of depicting and fostering an accurate organizational image rather than allowing others to draw and disseminate erroneous characterizations. For the U.S. Intelligence Community in particular, any initiative in benchmarking the intelligence process fulfills a charge of the recently completed Report on the Community's Roles and Capabilities: to improve its performance through closer relationships with customers, including the private sector.

GLOSSARY

ASD/C4ISR	Assistant Secretary of Defense for Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
BI	Business Intelligence
CIA	Central Intelligence Agency
CISS	Center for Information Systems Security
CSRC	Computer Security Resource Center
DCI	Director of Central Intelligence
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DISA	Defense Information Systems Agency
DoD	Department of Defense
DODSI	Department of Defense Security Institute
FISINT	Foreign Instrumentation and Signature Intelligence
GPO	U.S. Government Printing Office
HUMINT	Human Intelligence
IC	Intelligence Community
IITF	Information Infrastructure Task Force
IMINT	Imagery Intelligence
INFOSEC	Information Systems Security
INFOWAR	Information Warfare
IOSS	Interagency OPSEC Support Staff
IPMO	INFOSEC Program Management Office
ISSR-JTO	Information Systems Security Research Joint Technology Office
JIVA	Joint Intelligence Virtual Architecture

JMIC	Joint Military Intelligence College
MASINT	Measurement and Signature Intelligence
MBTI	Myers-Briggs Type Indicator
MRI	Management Research Institute
NACIC	National Counterintelligence Center
NCSC	National Computer Security Center
NIC	National Intelligence Council
NII	National Information Infrastructure
NIMA	National Imagery and Mapping Agency
NIST	National Institute for Standards and Technology
NSA	National Security Agency
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NTIA	National Telecommunications and Information Administration
OMB	Office of Management and Budget
OPSEC	Operations Security
OSD	Office of the Secretary of Defense
OTP	Office of Technology Policy
SCIP	Society of Competitive Intelligence Professionals
SIGINT	Signals Intelligence

BIBLIOGRAPHY

Allen, George. "The Professionalization of Intelligence." In *Strategic Intelligence: Theory and Application*, 2d ed. Eds. Douglas H. Dearth and R. Thomas Goodden, 33-40. Washington, DC: Joint Military Intelligence Training Center (JMITC), 1995.

Andre, Louis E. "Intelligence Production: Towards a Knowledge-Based Future." *Defense Intelligence Journal* 6, no. 2 (Fall 1997): 35-45.

Babbie, Earl. *The Practice of Social Research.* Belmont, CA: Wadsworth Publishing Co, 1992.

Ben-Israel, Isaac. "Philosophy and Methodology of Intelligence: The Logic of Estimative Process." *Intelligence and National Security* 4, no. 4 (October 1989): 660-718.

Brei, Captain William S. *Getting Intelligence Right: The Power of Logical Procedure*. Occasional Paper Number Two. Washington, DC: Joint Military Intelligence College (JMIC), January 1996.

Carney, LT Donald J., USN. *Estimating the Dissolution of Yugoslavia*. Seminar Paper. Washington, DC: Joint Military Intelligence College, September 1991.

Central Intelligence Agency. *A Compendium of Analytic Tradecraft Notes*. Washington, DC, Directorate of Intelligence, February 1997.

_____. *A Consumer's Guide to Intelligence*. Washington, DC: Public Affairs Staff, July 1995. PAS 95-00010.

Clauser, Jerome K. and Sandra M. Weir. *Intelligence Research Methodology, An Introduction to Techniques and Procedures for Conducting Research in Defense Intelligence*. Washington, DC: Defense Intelligence School, 1975.

D'Aveni, Richard. "Hypercompetition." Briefing to SCIP Conference. Alexandria, VA, 28 March 1996.

Davis, Jack. "Combatting Mindset." *Studies in Intelligence* 35, no. 4 (Winter 1991): 13-18.

_____. *Intelligence Changes in Analytic Tradecraft in CIA's Directorate of Intelligence*. Washington, DC: CIA Directorate of Intelligence, April 1995.

_____. *The Challenge of Opportunity Analysis*. Intelligence Monograph. Washington, DC: Center for the Study of Intelligence, July 1992. CSI 92-003U.

Davis-Floyd, Robbie E. "Storytelling Corporate Futures: The Shell Scenarios." *International Journal of Futures Studies* 1 (1995-1997), on-line at http://www.systems.org/HTML/journals.htm, accessed 3 December 1997.

Dearth, Douglas H. “National Intelligence: Profession and Process.” In *Strategic Intelligence: Theory and Application*, 2d ed. Eds. Douglas H. Dearth and R. Thomas Goodden, 15-31. Washington, DC: JMITC, 1995.

_____. “The Politics of Intelligence.” In *Strategic Intelligence: Theory and Application*, 2d ed. Eds. Douglas H. Dearth and R. Thomas Goodden, 97-121. Washington, DC: JMITC, 1995.

Defense Information Systems Agency. “INFOSEC and the DII.” *DISSPatch* 4, no. 1 (3rd Quarter 1996): 7.

_____. “Introducing NSA’s New and Improved V Group.” *DISSPatch* 4, no. 1 (3rd Quarter 1996): 2, 5.

_____. “The NIST Computer Security Resource Clearinghouse.” *DISSPatch* 4, no. 1 (3rd Quarter 1996): 6.

Defense Intelligence Agency. *Vector 21, A Strategic Plan for the Defense Intelligence Agency.* Washington, DC: Programs and Operations Staff, undated.

Elmuti, Dean, and Hanus Kathawaia and Scott J. Lloyed. “The Benchmarking Process: Assessing Its Value and Limitations.” *Industrial Management*, 39, No. 4 (July/August 1997): 12-19.

Fisher, Lynn F. “Defining the Threat to Information Systems.” *DODSI Security Awareness Bulletin* 2-94 (August 1994): 3-10.

Frankenfield, Jerry and Melissie Rumizen. *A Guide to Benchmarking*. Fort Meade, MD: NSA, 12 July 1995.

Garst, Ronald D. “Components of Intelligence.” In *A Handbook of Intelligence Analysis*, 2d ed. Ed. Ronald D. Garst, 1-32. Washington, DC: Defense Intelligence College, January 1989.

_____. *Intelligence Types: The Role of Personality in the Intelligence Profession*. Washington, DC: Joint Military Intelligence College, August 1995.

Goodden, Royal Thomas. “Intelligence in the Information Age.” In *Strategic Intelligence: Theory and Application*, 2d ed. Eds. Douglas H. Dearth and R. Thomas Goodden, 409-416. Washington, DC: JMITC, 1995.

Harkleroad, David. “Actionable CI.” Briefing to SCIP Conference. Alexandria, VA, 28 March 1996.

Harris, Gary. “Evaluating Intelligence Evidence.” In *A Handbook of Intelligence Analysis*, 2d ed. Ed. Ronald D. Garst, 33-48. Washington, DC: Defense Intelligence College, January 1989.

Haucke, Mark H. Industrial Psychologist, National Security Agency. Interview with the author, 25 May 1995.

Hecht, Francoise. "The Aha! Factor." *Director* 50, No. 12 (July 1997): 59.

Herring, Jan. "Strides in Institutionalizing BI in Businesses." Briefing to SCIP Conference. Alexandria, VA, 28 March 1996.

Hulnick, Arthur S. "The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach." *Intelligence and National Security*, 1, No. 2, (May 1986): 212-233.

_____. "Managing Intelligence Analysis: Strategies for Playing the End Game." *International Journal of Intelligence and CounterIntelligence*, 2, No. 3, (Fall 1988): 321-343.

Hunter, Douglas E. *Political/Military Applications of Bayesian Analysis: Methodological Issues.* Boulder, CO: Westview, 1984.

Johnson, Loch K. *America's Secret Power, The CIA in a Democratic Society.* New York: Oxford University Press, 1989.

Jones, Morgan D. *The Thinker's Toolkit.* New York: Random House, 1995: 44-46.

Kahaner, Larry. *Competitive Intelligence: From Black Ops to Boardrooms*. New York: Simon and Schuster, 1996.

Kam, Ephraim. *Surprise Attack*. Cambridge, MA: Harvard University Press, 1988.

Kaplan, Abraham. *The Conduct of Inquiry.* San Francisco, CA: Chandler, 1964.

Katzen, Sally. Administrator, Office of Information and Regulatory Affairs, U.S. Office of Management and Budget. Remarks prepared for delivery at the National Computer Security Conference, Baltimore, Maryland, 11 October 1994.

Keesing, Hugo A. Instructor, Joint Military Intelligence College. Remarks to a meeting of the Communications Analysis Association, Fort Meade, MD, 6 November 1995.

Keirsey, David. *Portraits of Temperament*. Amherst, NY: Prometheus, 1987.

Kight, Leila. "Elements of CI Success." Briefing to SCIP Conference. Alexandria, VA, 28 March, 1996.

Macdaid, Gerald P., Mary H. McCaulley and Richard I. Kainz. *Myers-Briggs Type Indicator: Atlas of Type Tables*. Gainesville, FL: Center for Applications of Psychological Type, 1986.

MacLean, Rhonda E. "The Boeing Hacker Incident." *DODSI Security Awareness Bulletin* 2-94 (August 1994): 19-22.

Major, James S. *Briefing with Intelligence*. Washington DC: Joint Military Intelligence College, August 1997.

_____. *The Style Guide: Research and Writing at the Joint Military Intelligence College*. Washington DC: Joint Military Intelligence College, August 1994.

Management Research Institute (MRI). *Ability and Knowledge Requirements*. Bethesda, MD: MRI, 1994.

_____. *Job Dimension Ratings*. Performance evaluation booklet. Bethesda, MD: Management Research Institute, 1995.

Mathams, R. H. "The Intelligence Analyst's Notebook." In *Strategic Intelligence: Theory and Application*, 2d ed. Eds. Douglas H. Dearth and R. Thomas Goodden, 77-96. Washington, DC: JMITC, 1995.

Minihan, Lt. Gen. Kenneth A. Director, National Security Agency. "DIR Addresses the Future of NSA." *Communicator* 4, no. 20 (14 May 1996): 1-3.

_____. "Intelligence and Information System Security." *Defense Intelligence Journal* 5, no. 1 (Spring 1996): 13-23.

_____. "Winning the Information Game: NSA's Role in the 21st Century." *NSA Newsletter*, May 1996, 3.

Moyer, Kathy. "Scenario Planning at British Airways — A Case Study." *Long Range Planning* 29, No. 2 (April 1996): 172-181.

Murray, Thomas H. "Taxonomy of Problem Types." Analytic coursework material for the Joint Military Intelligence College, based upon Morgan D. Jones, *The Thinker's Toolkit.* New York: Random House, 1995: 44-46.

Myers, Isabel Briggs. *Introduction to Type*. Palo Alto, CA: Consulting Psychologists Press, 1980.

_____. and Mary H. McCaulley. *Manual: A Guide to the Development and Use of the Myers-Briggs Type Indicator.* Palo Alto, CA: Consulting Psychologists Press, 1985.

_____. with Peter Myers. *Gifts Differing*. Palo Alto, CA: Consulting Psychologists Press, 1980.

National Cryptologic School (NCS). Information Security Department, *Operations Security Fundamentals*. Fort Meade, MD: NCS, 1993.

National Operations Security (OPSEC) Advisory Committee. *National Operations Security Doctrine*. Greenbelt, MD: Interagency OPSEC Support Staff, January 1993.

National Research Council. *Computers at Risk: Safe Computing in the Information Age*. Washington, DC: National Academy Press, 1991.

National Security Agency. *1995 INFOSEC Manual*. Fort Meade, MD: NSA, 1995.

Office of the Federal Register. National Archives and Records Administration. *The United States Government Manual 1995/96*. Washington, DC: GPO, 1 July 1995.

P.L. 102-183. "David L. Boren National Security Education Act of 1991." Title VIII, Sections 801-802, 4 December 1991.

P.L. 103-62. "Government Performance and Results Act of 1993."

Peterson, Marilyn. *Applications in Criminal Analysis.* Westport, Connecticut: Greenwood Press, 1994.

Prescott, John. Professor of Business Administration, University of Pittsburgh. "Research." Briefing to SCIP Conference, 28 March 1996

Rumizen, Melissie C. Benchmarking Manager, National Security Agency. Interviews with the author, 4 January 1996 and 5 July 1996.

Schmidlin, LCDR William G., USN. *Zen and the Art of Intelligence Analysis*. MSSI Thesis. Washington, DC: Joint Military Intelligence College, July 1993.

Schum, David A. *Evidence and Inference for the Intelligence Analyst*. Volume I. Lanham, MD: University Press of America, 1987.

Schwartau, Winn. *Information Warfare: Chaos on the Electronic Superhighway.* New York: Thunder's Mouth Press, 1994.

SCIP. *1995 SCIP Membership Directory.* Alexandria, VA: SCIP, 1995.

_____. *Competitive Intelligence Review* 8, No. 3 (Fall 1997): unnumbered 8th page.

_____. *Conference Proceedings.* Annual International Conference & Exhibit, March 27-30, 1996. Alexandria, VA: SCIP, March 1996.

Smith, Ian. "Avoiding Future Shock." *Director* 50, No. 12 (July 1997): 56-59.

Stoll, Clifford. *The Cuckoo's Egg*. New York: Pocket Books, 1990.

Studeman, William O. "Leading Intelligence Along the Byways of Our Future: Acquiring C^4ISR Architectures for the 21st Century." *Defense Intelligence Journal* 7, no. 1 (Spring 1998): 47-65.

Swenson, Russell G. *An Office Manager's Guide to Intelligence Readiness*. Occasional Paper Number Three. Washington, DC: JMIC, December 1996.

Tetzlaff, Jonathan. Area Director, Security Research and Analysis, Amoco Corporation. Personal correspondence with editor, 24 October 1997.

Turner, Michael A. "Setting Analytical Priorities in U.S. Intelligence." *International Journal of Intelligence and CounterIntelligence* 9, no. 3 (Fall 1996): 313-327.

U.S. Congress, House Permanent Select Committee on Intelligence. *IC21: The Intelligence Community in the 21st Century.* Staff Study, April 1996: Section III, "Intelligence Requirements Process."

_____. Office of Technology Assessment. *Information Security and Privacy in Network Environments*. Washington, DC: GPO, September 1994. OTA-TCT-60

_____. *Preparing for the 21st Century: An Appraisal of U.S. Intelligence*. Report of the Commission on the Roles and Capabilities of the U.S. Intelligence Community. Washington, DC: GPO, 1 March 1996.

U.S. Department of Defense. DoD Security Institute (DODSI). *DODSI Security Awareness Bulletin* 2-94 (August 1994).

_____. Joint Chiefs of Staff. Joint Pub 1-02. *Dictionary of Military and Associated Terms*. Washington, DC: 23 March 1994: 184.

_____. Joint Chiefs of Staff. Joint Pub 2-0. *Joint Doctrine for Intelligence Support to Operations*. Washington, DC: GPO, 5 May 1995.

Vistica, Gregory L. and Evan Thomas, "The Secret Hacker Wars, Behind the Spreading Battle Over Cyberterrorism." *Newsweek* (1 June 1998): 60.

Westerfield, H. Bradford. "Inside Ivory Bunkers: CIA Analysts Resist Managers" Pandering' — Part I." *International Journal of Intelligence and CounterIntelligence* 9, no. 4 (Winter 1996/97): 407-424.

_____. "Inside Ivory Bunkers: CIA Analysts Resist Managers' "Pandering' — Part II." *International Journal of Intelligence and CounterIntelligence* 10, no. 1 (Spring 1997): 19-54.

White House. *National Operations Security Program*. Fact Sheet. Washington, DC: January 1988.

Winkler, Ira. *Corporate Espionage: What It Is, Why It Is Happening in Your Company, What You Must Do about It*. Rocklin, CA: Prima Publishing, 1997.

ABOUT THE AUTHOR

Lisa Krizan has been a researcher with the Department of Defense since 1987. She received a master's degree from the Joint Military Intelligence College in 1996 and developed many of the ideas for this paper as part of her thesis on benchmaking the intelligence process. A second-generation intelligence scholar, she follows the example set by her father, 1972 Defense Intelligence College graduate Allen J. Montecino, Jr., Colonel, USAF (Ret).

Joint Military Intelligence College
Occasional Papers

1. Classified paper.

2. *Getting Intelligence Right: The Power of Logical Procedure*, Capt (USAF) William S. Brei, 1996.

3. *An Office Manager's Guide to Intelligence Readiness*, Russell G. Swenson, 1996.

4. Classified paper.

5. *A Flourishing Craft: Teaching Intelligence Studies*, Papers Prepared for the 18 June 1999 JMIC Conference on Teaching Intelligence Studies at Colleges and Universities, 1999.

6. *Intelligence Essentials for Everyone*, Lisa Krizan, 1999.

This Page Is Intentionally Left Blank

BRINGING INTELLIGENCE ABOUT

Practitioners Reflect on Best Practices

With a Foreword by

Mark M. Lowenthal
Assistant Director of Central Intelligence

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAY 2003		**00-00-2003 to 00-00-2003**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Bringing Intelligence About Practitioners Reflect on Best Practices	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Joint Military Intelligence College,200 MacDill Blvd,Washington,DC,20340-5100**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**157**	

BRINGING INTELLIGENCE ABOUT

Practitioners Reflect on Best Practices

May 2003

Russell G. Swenson, Editor

With a Foreword by
Mark M. Lowenthal
Assistant Director of Central Intelligence

The Joint Military Intelligence College supports and encourages research on intelligence that distills lessons and improves support to policy-level and operational consumers, and that familiarizes the public with aspects of the intelligence profession.

Bringing Intelligence About: Practitioners Reflect on Best Practitioners

The title chosen for this book carries two meanings. The more straightforward interpretation of "Bringing Intelligence About," and the principal one, refers to the book's coverage of wide-ranging sources and methods employed to add value to national security-related information—to create "intelligence." A second meaning, not unrelated to the first, refers to the responsible agility expected of U.S. intelligence professionals, to think and act in such a way as to navigate information collection and interpretation duties with a fix on society's shifting but consensual interpretation of the U.S. Constitution.

A prominent individual and ideal intelligence professional who lived both meanings of "Bringing Intelligence About" was the late Lieutenant General Vernon A. Walters. As an intelligence officer, defense attache, ambassador-at-large and ambassador to Germany, his combination of skills—notably his language skills—made him the epitome of a professional. Beyond intelligence service in the Departments of Defense and of State, General Walters presided as Deputy Director of Central Intelligence during the Watergate episode, where he stood on principle and at odds with political figures in the Nixon administration. His mastery of intelligence collection, analysis and politically attuned synthesis, the full story of which has not yet been told, make him a near-mythic figure for aspiring intelligence professionals.

Although the talents and assignments of General Walters were extraordinary, his demonstration that intelligence aptitudes and skills are fungible across Departments and Agencies is a powerful suggestion that those separate institutions can also operate together as a professional community.

The papers in this publication are based exclusively on sources available to the public and the views expressed are those of the respective authors, and do not necessarily reflect the official policy or position of the Department of Homeland Security, the Department of Defense or the U.S. Government.

This publication has been approved for unrestricted distribution by the Office of the Secretary of Defense (Public Affairs). Copies of this publication are available in limited quantities to U.S. Government officials, and to the public through the National Technical Information Service (www.ntis.gov), or the U.S. Government Printing Office (www.gpo.gov).

Russell.Swenson@dia.mil
Editor

Library of Congress Control Number 2001-126998

ISBN 0-9656195-4-0

FOREWORD

There are two anecdotes from the world of entertainment that seem apt to introduce this book.

First: The great 19th-century Anglo-Irish actor Edmund Kean lay on his deathbed. A friend asked, "Is it hard, Edmund?"

"No," he replied. "Dying is easy. *Comedy* is hard."

Second: A Hollywood producer in the 1930s or 1940s was asked why a certain film succeeded at the box office but another did not. He replied, "If we knew the answer to that, we'd only make hits."

Similarly, the process of intelligence is easy; *good* intelligence is hard. And if we could figure out what made some intelligence "good" or "better" (which would require some further definition), then we would produce it more regularly.

We spend a lot of time in the Intelligence Community analyzing the various parts of the intelligence process and trying to define what makes some intelligence better than other intelligence. And yet, for all that intellectual effort, we still have not evolved a steady and reliable means of producing this "better" intelligence. We know when the process works and when it does not, but this knowledge does not turn into a formula for greater success.

Why is that? Are we unable to learn from our own successes and failures? Or does the process remain so intangible at core that it eludes us even when we have, on occasion, mastered it? My own view is that we have not yet (after more than 55 years) come up with a good picture in our minds—nor have we successfully enunciated—just what a professional intelligence analyst "looks like," and how we train and develop this analyst across his or her entire career—not just at the outset. Interestingly, we do know what the analyst's ethos is, but we remain fuzzy on the necessary professional underpinnings.

This volume helps us move down the long and difficult road of helping identify how to produce good or better intelligence—by which I mean intelligence that is of use to policymakers and is better than other intelligence by being so used. The authors have—across a range of areas of interest—identified some of the practices that work best to produce—or, more aptly, "to bring about"—good intelligence. Note that the preceding sentence said "some of the practices." Few books could expect to identify all of the practices that work and, as the authors of each chapter would undoubtedly concede, there will always be some variables and intangibles at work in intelligence: vagaries of time to perform collection and analysis; the quality of sources; the quality of the analysts; the nature and personality of the policymakers. Still, it is possible to identify the practices that work and the practices that have to be altered over time as conditions change.

I cannot help but think that if we were to take the various observations and recommendations of these chapters and shape them into a coherent program we would be well on our way to producing better intelligence on a more consistent basis. Of course, we would still face the issue of where that program should exist and how it should be imparted because, for all of the improvements we have made in training and developing analysts, we still do this in vertical, agency-dominated stovepipes. We have a variety of courses that seek to train (or inculcate) people into the broader Community aspects of intelligence, but training remains a series of isolated enterprises. Thus, even if we accept the many good ideas in this book, getting them to all of the people who might benefit from them remains typically problematic.

Finally, it is also important to understand that this book focuses on the issue of analysis. I am admittedly prejudiced in my views, but I believe that analysis is the main goal of any intelligence enterprise: putting informed judgments in front of policymakers to help them make decisions. This is not meant to demean clandestine activities in the field, or the designing and operation of collection systems, or any of the other necessary parts of the broader intelligence function. But, at the end of the day, the most consistent service intelligence provides is analysis, whether it is a one-line warning or a detailed estimate. The Infantry likes to call itself "the Queen of Battle." This is how I feel about analysis in the world of intelligence. This book helps analysis remain firmly placed on her throne.

Mark M. Lowenthal
Assistant Director of Central Intelligence for
Analysis and Production
Vice-Chairman for Evaluation, National Intelligence
Council

BRINGING INTELLIGENCE ABOUT
PRACTITIONERS REFLECT ON BEST PRACTICES

Contents

Introduction
Russell G. Swenson 1

The Intelligence Pro and the Professor: Toward an Alchemy of Applied Arts and Sciences
Pauletta Otis 7

Via the Internet
John Turner 19

Visit to Mazagon Dockyard, Bombay
F.G. Satterthwaite 29

Improving CIA Analysis by Overcoming Institutional Obstacles
Stephen Marrin 41

Appraising Best Practices in Defense Intelligence Analysis
Thomas A. Garin 61

Core Competencies for Intelligence Analysis at the National Security Agency
David T. Moore and Lisa Krizan 95

The U.S. Coast Guard Joins the Intelligence Community
Michael E. Bennett LT, USCG 133

Index 141

List of Figures

Map of India 30
Author talks with an Indian Navy captain on board a third-party vessel 32
The Gateway to India and naval facilities in Bombay 33
Author and son visiting with a Hindu holyman at a curio shop in Bombay 34
There is life after naval service in India 37
Author with makeshift head covering for visiting at Hindu temple 38
Functional core competencies for intelligence analysis 96
An intelligence evaluation scheme 101
Measures of success for intelligence products 103
Characteristics of successful intelligence analysts 106
Abilities required for successful intelligence analysis 107
Skills required for successful intelligence analysis 112
Knowledge required for successful intelligence analysis 120
U.S. Coast Guard missions 133
Coast Guard civil/military authorities 134

ABOUT THE AUTHOR

Dr. Russell G. Swenson directs the Center for Strategic Intelligence Research at the Joint Military Intelligence College. His initial exposure to the world of intelligence was as an Air Force linguist in the mid-1960s. He holds undergraduate degrees from the University of Kansas, and graduate degrees in Geography from the University of Wisconsin-Milwaukee. At the JMIC since 1988, he has taught the course on strategic warning from intelligence, as well as thesis research and writing seminars. He also teaches a course on intelligence issues in Latin America. His research interests include the application of analytic methods and the comparative study of intelligence practices, especially in the Western Hemisphere.

INTRODUCTION

Russell G. Swenson
with David T. Moore and Lisa Krizan

This book is the product of studious self-reflection by *currently serving* intelligence professionals, as well as by those who are in a position, with recent experience and continuing contacts, to influence the development of succeeding generations of intelligence personnel. Contributors to this book represent eight of the fourteen organizations that make up the National Foreign Intelligence Community. A positive image of a community of professionals, engaged in public service, and concerned about continuous self-improvement through "best practices," emerges from these pages.

Practitioners anywhere in this Community are professional by any definition of the term. Their work requires extensive education and specialized training, and at their best, personnel exhibit highly innovative approaches to collection and analysis. Differences in focus among the principal Intelligence Community partners are sometimes sharp, but similarities in techniques do exist, particularly at the "working level." Community partners, such as the Central Intelligence Agency (CIA), Defense Intelligence Agency (DIA), the National Security Agency (NSA), and the State Department's Bureau of Intelligence and Research (INR), for example, share responsibilities for national security issues that allow individual collectors, analysts, issue managers and offices to work together on interagency task forces.

However, commonalities may decrease farther afield, for example between the agencies with a strategic focus and those involved in tactical or law-enforcement intelligence. Not the least of these differences is that, with its strategic focus, the Intelligence Community expects to be forward-looking, envisioning future developments and their repercussions, whereas law enforcement intelligence efforts have typically focused on exploiting pattern analysis to link together the extralegal behavior of individuals and organizations with clear and legally acceptable evidence. Some overlap of intelligence applications already occur, especially in the areas of crime and narcotics, where interagency task forces work from both ends of the problem—the predictive and the reactive—so that a facile claim of significant differences between law enforcement and national security intelligence may hold up to scrutiny only in terms of the scale of operations supported rather than professional intelligence techniques employed. [1] We may infer from these observations that the principles of intelligence collection and analysis addressed in this book will apply to intelligence creation in the broadly overlapping cultures of law enforcement and national security intelligence.

---

[1] Two works that document the evolution of criminal or law enforcement intelligence, both in the U.S. and internationally, are 1) *Intelligence 2000: Revising The Basic Elements: A Guide for Intelligence Professionals*, Marilyn Peterson, ed. (n.p.: Law Enforcement Intelligence Unit, California, and International Association of Law Enforcement Intelligence Analysts, 2000), and 2) Don McDowell, *Strategic Intelligence: A Handbook for Practitioners, Managers and Users* (Cooma, NSW, Australia: Istana Enterprises Pty, Ltd, 1998). These books provide evidence of a convergence, in both instructional and professional standards of practice, between law enforcement and national security intelligence.

The concept of a *Community* of professional intelligence collectors and analysts persists, despite the specialized character of much of their work. Further, the National Foreign Intelligence Community does not remain static, as shown by its recent (2001), formal incorporation of the U.S. Coast. The Coast Guard combines its new intelligence focus with its traditional broad responsibilities in law enforcement, in paramilitary operations, and in public safety. As a new, young member, and a bridge between national security and law enforcement spheres, the USCG is in position to help rejuvenate the community by exemplifying the ideal of sharing both information and assessments.

The U.S. Intelligence Community was subject during the 1990s to a congressionally mandated reduction in Intelligence Community personnel levels.[2] This reduction occurred despite numerous small wars and the continuation of international criminal activity during the decade. When dissenters, such as former Director of Central Intelligence James Woolsey, "talked about the proliferators, traffickers, terrorists, and rogue states as the serpents that came in the wake of the slain Soviet dragon, [they were] accused of 'creating threats' to justify an inflated intelligence budget."[3] Even government reports such as that of the United States Commission on National Security (commonly referred to as the Hart-Rudman Report), which warned of catastrophic attacks against the American homeland and a need for vigilance, were dismissed.[4]

Intelligence collectors and analysts have at times been subject to personnel retrenchment, a situation favoring current operations support, and leading to the neglect of individual and corporate succession planning—to capture and pass on institutional and target knowledge. Today, collection and analysis tradecraft remain neglected phenomena—the focus of very few self-studies.[5] Naturally, some literature known to "insiders" is not made available to the general public because of the admonition not to disclose "sources and

[2] John E. McLaughlin, CIA Deputy Director of Intelligence, notes that the reduction was 22 percent. See McLaughlin's "The Changing Nature of CIA Analysis in the Post-Soviet World," remarks as prepared for delivery at the Conference on CIA's Analysis of the Soviet Union, 1947-1991, 9-10 March 2001 (Princeton, NJ: Princeton University, 2001), URL: <http://www.cia.gov/cia/public_affairs/speeches/archives/2001/ddci_speech_03092001.html>, accessed 22 December 2002. Cited hereafter as McLaughlin.

[3] McLaughlin.

[4] U.S. Commission on National Security/21st Century, *New World Coming: American Security in the 21st Century*, The Phase I Report on the Emerging Global Security Environment for the First Quarter of the 21st Century, Supporting Research and Analysis (Washington, DC: GPO, 15 September 1999), 49.

[5] The few works that do address intelligence practices in informed detail have become classics, and are widely cited. They include Sherman Kent's *Strategic Intelligence For American World Policy* (Princeton, NJ: Princeton University Press, 1949); Roger Hilsman, *Strategic Intelligence and National Decisions* (Glencoe, IL: The Free Press, 1956); Washington Platt, *Strategic Intelligence Production: Basic Principles* (New York: Frederick A. Praeger, 1957); Bruce D. Berkowitz and Allen E. Goodman, *Strategic Intelligence for American National Security* (Princeton, NJ: Princeton University Press, 1989); Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999) and Lisa Krizan, *Intelligence Essentials for Everyone*, Occasional Paper Number Six (Washington, DC: Joint Military Intelligence College, 1999).

methods." However, even though collection methods are often arcane, methods of analysis are not very esoteric. Analytic methods used by intelligence analysts are readily available to specialists in the academic world.[6] The commonalities that do exist among collectors and analysts across the Community have rarely been noted in intelligence literature. The essays in this book will help fill that gap, and should illuminate for non-specialists the important role of self-reflection among intelligence professionals who remain in government service.

The contributors to this book share an interest in exploring and explaining intelligence collection and analysis practices.

Pauletta Otis, whose work has acquainted her with both the Intelligence Community and academia, outlines from experience the numerous similarities and differences between communities of academics and intelligence professionals. Her reminder that academics tend to be "contrarian" points up the value of academics having continual interaction with intelligence experts, in support of the Community's ideal, "nonmonastic" (not following the party line) approach to issues.

In the next essay, retired Navy Captain George Satterthwaite recounts how persistence and creativity when coupled with serendipity can contribute to gathering unique information that may thereby yield valuable intelligence. By taking advantage of his responsibilities as Defense Attaché to host official U.S. delegations, he gained access to important facilities in India for insight into Indian nuclear and naval capabilities. Intelligence professionals can readily relate to his spirited interaction with bureaucratic and political colleagues in the U.S. Embassy and the host country.

It may now be true that the value of intelligence to consumers is more dependent on the evaluation of information (grappling with mysteries) than on discovering "secrets."[7] If so, then the evaluation of social trends in various regions might best begin with systematic exploitation of authentic or "grass-roots" reporting from newspapers and other mass media. In the third essay, John Turner, senior Middle East and North Africa analyst at the U.S. European Command's Joint Analysis Center, illustrates his facility with exploiting multilingual electronic news media from North Africa. Translation and reporting by the Foreign Broadcast Information Service from such media is selective rather than comprehensive, and selections are not tailored for individual analysts, who are removed from first-hand screening of the sources. Therefore, language capabilities are indispensable for any country's intelligence personnel who seek insights through indigenous mass media. Language capabilities must mirror those tongues used across the electronic media that represent the target entities. Further, as noted in a recent news

[6] Many if not most analysts have been exposed, by training or experimentation, to such techniques as link analysis, the Delphi technique, and analysis of competing hypotheses. Morgan D. Jones, former CIA analyst, has distilled the less structured techniques that intelligence analysts may employ in *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving* (New York: Times Business, Random House, 1995 and 1998).

[7] For an "insider's" comparison of secrets" and "mysteries" see John C. Gannon, CIA Deputy Director for Intelligence, speech before the World Affairs Council, 20 March 1996. URL: *http://www.cia.gov/cia/public_affairs/speeches/archives/1996/ddi_speech_032096.html.*

report, the U.S. experience is that non-native, academically trained linguists who have lived abroad typically outperform native linguists in intelligence assignments that depend on language ability.[8] Dr. Turner's essay, with its emphasis on his own familiarity with North African news media reporting, illustrates that point.

Stephen Marrin reflects on his experiences as a new CIA analyst as he addresses whether and how formal training programs can impart the specialized knowledge, skills, and abilities necessary for meaningful intelligence analysis. He examines how the customary activity, processes, and organization of intelligence may have contributed to some failed aspects of intelligence prior to the events of 11 September 2001. He then suggests some specific ways to reinvent certain aspects of the national intelligence mission to allow analysts to bring greater persuasiveness to their value-added information.

U.S. Air Force Lieutenant Colonel Tom Garin examines how dignity and self-respect among professionals may be fostered within an intelligence organization. Garin defines the intelligence corporation in terms of a "learning organization" and then applies external standards from the Baldrige National Quality Program to selected intelligence-producing offices within the Defense Intelligence Agency. This benchmarking study not only identifies best practices, but also shows how such professional standards could be used to identify exemplary offices or individuals across the entire Intelligence Community.

Available literature does not yet address the question of what knowledge, skills and abilities are required, from the point of view of front-line managers, to support and sustain the evolution of intelligence tradecraft. David Moore and Lisa Krizan define a graduated set of criteria to calibrate an individual's suitability for an analytic position. Given the current Intelligence Community hiring surge, the set of core competencies they identify for NSA also provides a guide for the larger Intelligence Community to improve the professional stature of its workforce by defining who the analysts of the present and future ought to be.

The last essay reveals how the U.S. Coast Guard, having only recently joined the Intelligence Community, has already adjusted its organizational structure and its personnel system, expanded its participation in multi-agency initiatives, and developed procedures for more effective management of its unique position between civilian and military worlds. These rapid developments, stimulated by membership in the Community of Intelligence professionals, should enable the Coast Guard to anticipate and meet the requirements of both law enforcement and national security intelligence. As a fresh-faced affiliate of the Intelligence Community, the Coast Guard can inject an uncompromised determination to help the community live up to its name.

The essays collected here only begin to illustrate the potential of self-reflective writing by intelligence practitioners. If a communitarian ethos distinguishes intelligence professionals from their more individualistic and self-absorbed brethren in academia, then self-reflection among intelligence practitioners can also easily become a communal good. Tension between a communitarian and individualistic ethos can resolve itself among

---

[8] Susan Schmidt and Allan Lengel, "Help Still Wanted: Arabic Linguists," *Washington Post*, 27 December 2002, A23.

intelligence professionals through the strength of their bureaucratic (Weberian), nonmonastic tradition. The essays in this volume illustrate how, through self-reflection, that tension may be resolved. For example, individual professionals can easily spell out connections among these essays that would quickly move the discussion to a classified realm—into their "culture." That culture is typically characterized by fast-moving events and requirements that preclude introspection about the phenomena of intelligence collection and production.

Self-reflection not only allows the various agency sub-cultures to be displayed, as portrayed here, but also allows "insiders" to realize the subtle connections of their individual work to the overall enterprise. As a further illustration of this principle, the intense intellectual effort that characterized earlier eras of intelligence production and that continues as a part of the enduring culture, is evoked by the observations of William Millward, a World War II intelligence analyst at the UK's Bletchley Park:

> [Analysis] means reviewing the known facts, sorting out significant from insignificant, assessing them severally and jointly, and arriving at a conclusion by the exercise of judgment: part induction, part deduction. Absolute intellectual honesty is essential. The process must not be muddied by emotion or prejudice, nor by a desire to please.[9]

National intelligence collection management and intelligence analysis remain inherently government functions, and privatized intelligence—with its prospect of reduced congressional oversight—is even more antagonistic to the communal sharing of information than are the more stringently overseen bureaucratic fiefdoms.[10] In this environment, to "bring intelligence about" from the point of view of the American people requires peeling back some of the thick mantle of secrecy that has shrouded individual initiatives and management approaches—Community best practices—employed in the execution of ordinary and extraordinary tasks. Readers who look closely at the observations set down by the authors here will find a serviceable tool for unwrapping some of the otherwise enigmatic enthusiasms and motivations of government intelligence professionals.

---

[9] William Millward, "Life in and out of Hut 3," in F.H. Hinsley and Alan Stripp, *Codebreakers: The Inside Story of Bletchley Park* (Oxford, UK: Oxford University Press, 1993), 17.

[10] Across the Intelligence Community, the proportion of private, "contract" employees of all categories now stands at about 30 percent, and is growing. Few of these individuals are "independent" contractors, the great majority being associated with small or large private enterprises. Although most such contractors hold high-level security clearances based upon background investigations, the proprietary interests of their "parent" organizations can be at odds with an ethos of uninhibited sharing of information and perspectives. For an exploration of these issues, see James R. Sutton, *Subversion of a Government Monopoly: The Privatization of Intelligence Services* (n.p.: Research Intelligence Consortium, Inc., 2000). For information about the author, see http://www.trinitydc.edu/academics/depts/ Interdisc/International/Jim_Sutton.htm.

ABOUT THE AUTHOR

Pauletta Otis is Professor of Political Science and International Studies at the University of Southern Colorado. Her Ph.D. was awarded from the Graduate School of International Studies at the University of Denver in 1989. Dr. Otis held the position of Distinguished Visiting Professor of International Security Studies at the Joint Military Intelligence College in 1998 and then was Visiting Scholar for the National Security Education Program 1999, under the auspices of the National Defense University. She continues to teach summer sessions at JMIC and contributes to a number of defense research efforts. Dr. Otis maintains an active speaking schedule and has been guest speaker at a number of prestigious meetings including those held by the National War College, National Intelligence Council, Defense Intelligence Agency, Central Intelligence Agency, National Security Agency, U.S. Marine Corps, the Denver Committee on Foreign Relations, and other private and public venues.

Dr. Otis has special expertise in the study of sub-national violence and combines theoretical (from graduate degrees in Anthropology, Political Science, and International Studies) with operational experience and expertise. She has conducted field research in conflict situations in South Asia, Latin America, the Middle East, and the eastern Mediterranean.

THE INTELLIGENCE PRO AND THE PROFESSOR: TOWARD AN ALCHEMY OF APPLIED ARTS AND SCIENCES

Pauletta Otis

Recent events have led to an increasing realization that all of the resources of the American public must be engaged in support of national security. The U.S. academic community and the U.S. National Foreign Intelligence Community are institutional managers of "information as power." Yet their potential for useful cooperation and collaboration is unrealized and the relationship between the communities continues to be somewhat strained. This relationship has been the topic of discussions for many years in a somewhat benign security environment. With dramatic changes in that environment in late 2001, maximizing resources through enhanced cooperation and collaboration assumes critical importance. How can the Intelligence Community (IC) and the academic community best cooperate in support of national security? What are the inherent risks and challenges?

The theoretical challenge is of primary concern. Basic assumptions about the nature of democracy and the nature of secrecy are foundational to each of the communities' view of itself and of the other. The major theoretical concern for both intelligence and academic communities is the apparent contradiction between secrecy and democratic governance. From the academic's point of view, the U.S. Government's stability and its concern for the common welfare derive from the First Amendment. If a stable democracy depends on an informed public, the public cannot make good decisions without accurate and timely information. Without the "self-correcting" mechanism of free speech, a government tends to be subject to centrifugal forces, to spin on its own axis, and to become an entity quite separate from the citizenry.

Yet, on a practical level, we need to "keep secrets" from U.S. enemies, however they may be defined. A certain level of secrecy is required to protect national interests. How much secrecy is "best" in a democracy is subject to ongoing debate.[11] The pendulum swings over time and in response to perceived threats to national security. Subsequent to 11 September 2001, an acceptance of "more secrecy" has accompanied public support for the IC's enhanced role in homeland security. It may also be assumed that eventually a public reaction to perceptions of "too much" secrecy will move the pendulum back toward an historical center. Compromise between requirements to keep secrets must be balanced with the requirements of free speech inherent in the very definition of democracy. CIA Director Stansfield Turner (1977-1981), when he was at the center of the secrecy maelstrom, simply stated: "Accommodating secrecy in a democracy requires compromises with the theory of full freedom of speech, inquiry, and endeavor."[12] The problems inherent to this balancing act

---

[11] Pat M. Holt, *Secret Intelligence and Public Policy: A Dilemma of Democracy* (Washington, DC: CQ Press, 1995), see especially chapter 1.

[12] Stansfield Turner, *Secrecy and Democracy: the CIA in Transition*. Boston, MA: Houghton Mifflin Company, 1985), 112.

have been apparent in all aspects of contemporary American life, yet nowhere so fraught with difficulty as in the relationship between academia and the national security community. This tension, albeit normal, natural, and expected, is often most apparent and most difficult in the relationship between academe and intelligence professionals.[13]

The special caveat is that patriotism is not at issue: degree of commitment to this country is an individual attribute. Whereas the intelligence professional may work on a daily basis with threats to this country, the academic may work on supporting the values and attitudes necessary to sustain democratic life. One focuses on external threat, the other on the internal maintenance of the democratic system itself.

COMMONALITIES

Both the IC and the academic community work in the world of word-power. Both are populated by dedicated and committed Americans. In most cases, cooperative efforts have yielded the "best" for the United States in terms of public policy and decisionmaking. Yet, at other times, the communities have been at serious odds. The ensuing problems have been of significant concern to the attentive public and detrimental to the common good. These problems emanate not only from the theory of democracy but from competition over the nature of truth and value for the country. They can also be traced to concern about the nature and processes of intelligence gathering.

The IC and the academic community have much in common: both realize that information is power and that power comes in the form of words. These words form the basis of cultural assumptions, common concepts, and grand theory. In terms of information handling minutiae, intelligence specialists and academic scholars do much the same thing. They research, write, explain, and predict with excruciating self-consciousness and realization of the power of words. Intelligence professionals and academics contribute to public discussion in both oral forums and in written format. Intelligence professionals and academics are valued and participant citizens: They attend common religious services, participate in the education of children, contribute to community service organizations, and talk to neighbors. At this level, both are truly in the same "game." In the public domain, both intelligence professionals and academics contribute information, analysis, and opinions. These are read and integrated by the public, by policymakers, and by the "other" community. This common body of public information and analysis is at the core of intelligent decisionmaking in the United States.

For 50-plus years, relations between the IC and academia have wavered between cooperation and competition. The basic tension inherent in keeping "secrets in a democracy" has been played out in specific activities and attitudes. These can be seen at the individual, institutional, and political levels. At the individual and institutional levels, no doubt in part because of the strong influence of Ivy League academics in World War II intelligence

[13] Robert M. Gates, as CIA Deputy Director for Intelligence in 1986, addressed the John F. Kennedy School of Government at Harvard University on the relationship between the IC and academe. His address was published as "CIA and the University," in *Studies in Intelligence* 30, no. 2 (Summer 1986): 27-36.

(especially in the Office of Strategic Services), considerable rapport between academe and government intelligence was maintained.[14] Universities and study centers were also involved in the ongoing relationship between the intelligence and academic communities. Between 1939 and 1961, Yale University was overtly supportive of the IC.[15] Students and faculty were participants in intelligence collection and analysis. Study centers were financially supported and professional journals published. Information was collected and archived (including the Human Relations Area Files). The money was channeled to individuals or to institutions but seemed to raise few concerns.[16] At the political level, the existence of a "community" of intelligence-related agencies and offices has been noted in legislation, suggesting wide acceptance of the idea of government intelligence operations as regularized institutions with special taskings in support of U.S. national security.[17]

CONTINUITY, CHANGE, AND THE DEVELOPMENT OF DIFFERENCES

The "position descriptions" of an intelligence specialist and of an academic are polar opposites: The basic job of an academic is to find information, collect factoids whether they are useful or not–and scatter the information to the winds hoping and praying to make more sense of the ensuing chaos. Intelligence specialists collect similar factoids for very specific productive purposes. Whereas the academic is spreading information, the intelligence professional is collecting, narrowing, and refining data to produce reports, even if at the same time continuing an academic interest in the subject. The academic may learn for the fun of it; the intelligence professional prefers, or learns to be able to actually *do* something with the information. In the long run, the academic must write, produce, and contribute to the body of professional literature, but there is not the pressure for immediate production that the intelligence professional must face. The academic can say "that is interesting"; the intelligence professional must certify that "it is important."

---

[14] For example, see Roger Hilsman's *Strategic Intelligence and National Decisions* (Glencoe, Il: The Free Press, 1956), 7, 10. A Princeton academic, he explores the notion that "scholars could in some respects take the place of spies," and that academics, especially social scientists, could in the IC "find their real home within the formal structure of government."

[15] Norman Holmes Pearson, Yale graduate and former OSS official, suggested that the CIA recruit its younger personnel from universities and urged that each university have informal talent spotters who would forward names of likely candidates. See Robin W. Winks, *Cloak and Gown: Scholars in the Secret War, 1939-1961* (New York: William Morrow Publishing Company, 1987), 315.

[16] Winks, 14-19, notes that Nathan Hale, a Yale graduate, is of special interest as the first "spy" executed for his work. Other noted Yale personages involved with intelligence activities include: Arnold Wolfers, Sherman Kent, Chester B. Kerr, James Angleton, C. Bradford Wells, Norman Holmes Pearson, Dean Acheson and Richard Bissell.

[17] Edward F. Sayle, "The Historical Underpinning of the U.S. Intelligence Community," *International Journal of Intelligence and Counterintelligence* 1, no. 1 (Spring 1986): 1-17.

Another point of conversation and contention is the responsibility for the ultimate use of information power, whether of technical or human origin. Is the individual who has the information and gives it to the "government" responsible for the ultimate use of that information? Referring to scientific advances in weaponry during World War II: Was a scientist who invented a weapon responsible for the ultimate use of that weapon? If the academic-scientist gave information to the government, did the very nature of government absolve him from guilt if it were to be used in a way not foreseeable by the scientist? Did it matter whether the government was a "dictatorship" or a "democracy"? On the human intelligence side: Were doctors and scientists, conducting scientific experiments on human populations in concentration camps and under the direction of government officials, responsible for the use of that information? What if the information eventually saved lives, albeit those of a Fascist regime? During the Vietnam era, the question was raised in another context: Information concerning populations in Laos, Cambodia, and Vietnam, collected by anthropologists, was subsequently used in support of the war effort. What was the ethical and moral responsibility of the information gatherer? Did they "sell out"? And, if so, what did they sell out to? Is final use of HUMINT the combined responsibility of the collector and disseminator? The ensuing and subsequent debates have been acrimonious, difficult, and divisive.

On the West Coast, and during the Cold War, the strain between academics and the IC contributed to a number of very ugly scenes. Distinctions were made between those academics who were "patriotic, loyal, and anti-communist," and those who challenged authority in any context. Simple questioning became a sign of disloyalty. Universities were increasingly supported by public funding, and administrators were increasingly drawn from a professional management pool rather than from the scholarly community, resulting in a view that universities were simply another form of business enterprise. Administrators were often afraid to allow challenges to government on the part of the faculty out of fear of losing funding. The divisiveness of this period cannot be overemphasized in explaining the nature of the contemporary public university. Administrative penalties for individual scholars included blacklisting, failure to get tenure, lack of research support, and even dismissal from teaching positions. The public presentation of "truth" was simple: teaching loyalty to the country was the real job of the teacher/ academic. Anything contrary was a serious and significant challenge to the future of the nation. And, if the public supported the university both financially and with its "children," it in turn should be able to expect loyalty on the part of its faculty employees. The long-term effects of this controversy were devastating: a certain level of self-censorship on the part of academics, serious mistrust between university administrators and faculty, and reluctance of faculty members to cooperate with intelligence agencies. The communities became unnecessarily, but understandably, polarized.[18]

---

[18] Ellen W. Schrecker, *No Ivory Tower: McCarthyism and the Universities* (New York: Oxford University Press, 1986).

A significant problem for both communities is the strangulation that can occur through bureaucratic-institutional rigidities. The academic community is quite aware that real education *could be* much better but that the *status quo* supports the professoriate; that is, change is always a bit dangerous as it usually means a diminishment of academic independence and an enhancement of administrative power. The IC also would admit to bureaucratic complacency in times of peace. Changes incur costs either in the diminution of capability or loss of institutional "territory." Both the intelligence professional and the academic are, to some extent, prisoners of their own bureaucracies and are habitually resistant to change.

There is an attendant problem: Neither of the communities is monolithic, although that stereotype persists. Most academics do not know the difference between the CIA and DIA nor the nature of their specific mandates from Congress, except perhaps in "wartime," when such differences become more widely known through media coverage. Similarly, intelligence professionals often lump all colleges and universities and hence the professoriate into one big resource group. Intelligence professionals make it their business to know their colleagues in other agencies; academics know who is working on "what," the relative integrity of individuals and institutions, and the unwritten division of labor in the university system. This information is buried in the collective consciousness of each community and remains difficult to exhume—hence the persistence of the monolithic stereotype

Each community has a body of common knowledge which it assumes everyone working within the institutional framework knows and accepts. Because common knowledge is "common," it is not self-conscious and most individuals do not even realize that basic assumptions are seldom challenged. For example: the academic community assumes that books are good and thus libraries should have them. Individuals in the IC often assume that books are inherently historical and that current information and intelligence must be "near-real-time" and continually refreshed. There is a distinct attitude of arrogance when these individuals discuss the currency of information with academics. What is not at issue, of course, is that the intelligence professional has to produce and is charged with an indications and warning responsibility mandating inclusion of current information.

Academics are known for jargon and obfuscation; the IC is known for producing acronyms seemingly at leisure. The tribal languages are difficult to learn without a willing translator. Such facilitators may be hard to find because language serves to define the in-group and the out-group and what can or should be communicated within the organization and to outsiders. To illustrate, the academic community believes that the title "doctor" is best reserved for a medical professional and that the title of "professor" connotes sufficient recognition of achievement. However, the military and intelligence communities rigidly and habitually call academics "doctor," sometimes embarrassing both parties. At the same time, the IC has a specific ranking for directors, analysts, collectors, and techies, and for military and civil service personnel. These are totally obscure for the academic working within the community. They don't know the differences and often do not want to take the time to learn.

Rules of interaction for each group differ significantly. Academics are notoriously fractious and democratic. Anyone can challenge anyone on any idea at any time–and do so. Sometimes it is not very polite or courteous even when the comment begins with: "I understand your premise, *but*, have you considered.....?" Bloodletting is the rule rather than the exception. Members of the IC appear to be more polite although "outsiders" may assume that they derive enjoyment from more discreet disagreement. The various forms of interaction are notable when individuals from the IC quietly participate in sections of the International Studies Association or the Political Science Association, or when academics vociferously contribute to conferences held under the auspices of the IC.

Prejudices and stereotypes held by each group toward the other are often very funny and uncomfortably accurate. The intelligence professional hides in a secure building; the academic retreats to the pie-in-the-sky ivory tower. The intelligence professional is not excessively talkative; the academic cannot be bridled. It is assumed that academics and scholars are in never-never land with theory that cannot be proved or disproved. The intelligence professional is said to live in a land of basic facts without understanding the "big picture." When specifically challenged, both sides recognize that one cannot have facts without theory nor theory without supporting evidence. Yet the stereotypes remain and there is misunderstanding and misinformation on both sides and few venues to correct those that cause problems in communication.

There is further the problem of "group-think" on both sides. Each assumes not infrequently that they have a lock on reality and often simply refuse to be open-minded. This occurred during the Vietnam era when the IC felt itself misunderstood and abused, and the academic community believed that its information and personnel were being used by intelligence agencies in ways of which academe did not approve. The complexity of the story is well-known but the mythology remains extant.[19] Part of the mythology is that intelligence agencies will collect information from academics but not return or share information in a collegial manner. On the other side, the assumption on the part of intelligence professionals is that the academics have a bad attitude and misunderstand or undervalue the IC contribution to national well-being. The academic community believes that it is not afflicted with the IC's tunnel vision and can contribute to lateral thinking that supports enhanced problem-solving capabilities.

THE ACADEMIC'S DECISION

The motivations for an academic to work for the IC are, of course, individualistic and mixed. He or she may simply want a "steady" job that pays well–even if only working over the summer break. There can also be an ego boost when intelligence experts value the information and assessment done by an academic in a particular field. The value attached to being "appreciated" for the information and analysis cannot be overstated as there is very little of that inherent in the academic community. It is also possible that an

[19] Note the references to news reports and other material on websites devoted to the use and abuse of intelligence during the Vietnam Era.

academic simply wants a new and important challenge and seeks to contribute to a group effort designed to enhance national security.

A number of problems may emerge if an academic goes to work for the IC, becomes a contractor, or produces information that can be used by that community. He may "go native," that is, become more "intelligence-centric" than the IC needs or desires, all in an attempt to "belong." There is a tendency for self-delusion and thinking that the information contributed is going to "make a difference." Sometimes it does; sometimes it is just part of the package provided for a specific tasking. The academic really has no way of knowing what impact his or her work is having.

There are special areas in which the academic can contribute to the IC. A primary contribution is in the collection of facts and information using sources that the IC is precluded from using. Academics can generally travel more easily than intelligence analysts and can establish human networks across international boundaries that can be very useful especially in times of crisis. Academics generally are trained in the development of analytical frameworks and employ them with a degree of ease and clarity. Many academics contribute a unique ability to critique or evaluate projects based on a wide reading of the literature combined with "on the ground" experience. The good academic is always a perverse thinker–looking to examine the null hypothesis or suggesting alternative explanations. They tend not to accept the "generally accepted explanation." This habit can make them a bit difficult as conversationalists especially if "critique" is translated as "criticism." A good academic scholar will insist on "rigor," as in following the requirement to test basic assumptions, validate criteria used in hypothesis building, monitor the internal validity of hypotheses, and pinpoint the public implications of certain theories. Academic rigor mandates "elegance"; that is, a hypothesis must be important, clear, and predictive. Even in descriptive analysis, an academic insists on looking at a range of possible alternative choices and at the internal coherence of the final product.

There is another caveat: most academics believe that intelligence professionals are better paid and have more job security for doing similar work. This may imply that academics will skew their work in order to get the "big bucks" that the IC is assumed to have sitting in a back room. The serious implication is that there is a potential for academics to give up academic integrity and play to the audience in order to get government contracts. On the other hand, if it is only supplemental income for the professors, the extra income can be very supportive of the academic profession at large. It is worth noting that salaries of academics vary hugely across the spectrum of colleges and universities and in different regions of the country.[20] It must also be noted that if academics are taking up intelligence taskings, they are not generally able at the same time to write for publication in scholarly journals. Participation in conferences is also limited and inter-academic communications suffer as a consequence.

---

[20] Approximately forty percent of all U.S. academic positions are adjunct or part-time. These pay somewhere in the range of $1,500 to $3,000 per class, which roughly translates as $24,000 a year for someone with an advanced, terminal degree.

There are a number of roles that academics can have in the IC: teaching, conducting research, consultation on specific issues, monitoring, evaluating programs, collaborating with other professionals on special projects, and holding conversations on issues of mutual concern. Most of these areas have been exploited to one degree or another. An area that is often overlooked is that of professional development. After all, many professors have spent a great deal of time teaching, testing, and designing learning materials. Not all are good at it–but many have considerable skills that could be tapped. Another specific area is in the teaching of research methodology and specialized writing. Intelligence professionals are sometimes criticized on their ability to effectively and efficiently engage the audience in oral presentations of their ideas and materials. Perhaps specific individuals in the academic community would be helpful in teaching and supporting that skill development.

The ultimate caveat: it is hard to explain to professional colleagues that "I am not a spy." The mystique outlives the reality. It can be overcome with honesty and some degree of good humor.

There are specific benefits to the IC if academics and scholars are employed wisely. One of the often-heard criticisms of the IC is that it has a special susceptibility to "group-think" because analysts seldom have internal challenges. Projects, after all, are group-produced and tend to reduce an individual's unique contribution in favor of the final product. The academic, simply by the nature of the job, challenges the norms, supports individual initiative and creativity, and values novel or unconventional thinking.

SUGGESTIONS FOR MUTUAL SUPPORT AND MUTUAL BENEFIT

For all of the reasons just noted, it is important that the IC encourage the participation of academics. Academics can make significant contributions in creative thinking, rigor of analysis, and professional presentation of products.

But the choice of which academic to invite as a participant and the venue for participation are not givens. The IC might do well to choose individual academics not for their geographic convenience, near to the Washington or New York areas, but for the written scholarly work produced in their "home environment." Some of the work is apparent at professional conferences such as those of the International Studies Association and the Political Science Association. Some academics, however, do not "conference." They do, however, write and produce articles for journals and books for publication. These individuals can be found by reputation in the community, in reading lists, and in lists of current publications provided by commercial book publishers. Another often-neglected academic source is the database developed by University Microfilms International (UMI) of Ann Arbor, Michigan. Its widely available "Dissertation Abstracts International" indexes over 1.5 million dissertations from the U.S. and some other English-speaking countries.[21]

It matters little whether the academic is familiar or comfortable with intelligence or intelligence agencies: what matters most is honest and clear communication. In the

author's first association, I was promised that all materials could and should be "open source" and that I had final say on what information went into the project. Because I was aware of the potential for harm to informants in an ethnic violence situation, this became critical support for my contribution to a specific project.

Think tanks are very peculiar instances of hybridization. What the IC does not often realize is that Rand, Hoover, and Carnegie are assigned specific status by academics. It is assumed that "since they get their money directly from the government," they are somehow tainted. Research is suspect and academic integrity is assumed to have been compromised. Nevertheless, the tanks pay very well and very fine academics contribute substantially to critically needed and specifically targeted research.

Universities are not monolithic. Many will support technical research financed by the U.S. Government, but distance themselves from government "intrusion" in the social sciences. This is understandable but can be challenged if those interested in "public-private" interchange develop or appeal to a board of monitors or research advisors.[22] The IC is not precluded from supporting social-cultural research. There have been any number of works emanating from political science departments on topics relating to democracy and development. Economics departments are enthusiastic contributors to development projects and economic distribution issues. Most universities are giving increased attention to environmental issues including environmental security.[23]

Another touchy but important area is in the potential contribution of information and understanding by visiting foreign students and visiting professors. It is well recognized that using undergraduate students in this sense remains fairly unproductive. There is an ongoing debate about getting information about, tracking, or using graduate students. Certainly the base of internationally focused information available on university cam-

---

[21] The University of Minnesota maintains a database for U.S. Master's theses and Ph.D. dissertations These are abstracted and available through the UMI system. Further information can be found on their respective websites: http://www.lib.umn.edu and http://www.lib.umi.com/dissertations.

[22] Widely used "Institutional Research Boards," for example, could address ethical and other issues even before they arise. For a useful discussion of the role of IRBs, see Bruce L. Berg, *Qualitative Research Methods for the Social Sciences*, 3rd ed. (Boston, MA: Allyn and Bacon, 1998), chapter 3.

[23] Although there is no evidence of specific linkages between the IC and the following examples, these academic authors are often quoted by the IC in support of new models relating intelligence requirements to a broadened definition of security: Jack Snyder, *From Voting to Violence: Democratization and Nationalist Conflict* (New York: W. W. Norton, 2000); Georg Sorensen, *Democracy and Democratization: Processes and Prospects in a Changing World* (Boulder: Westview Press, 1998); James G. March and Johan P. Olsen, Democratic Governance (New York: Free Press, 1995). On environment issues related to security, see *Environmental Conflict*, Paul F. Duiehl and Nils Petter Gleditsch, eds. (Boulder: Westview Press, 2001) and *Ecoviolence: Links among Environment, Population, and Security*, Thomas Homer-Dixon and Jessica Blitt, eds. (Boulder, CO: Rowman & Littlefield Publishers, Inc., 1998).

puses could be more usefully (and publicly) exploited. In the current environment, most universities have been encouraged to check on the legal status of their international students, especially those coming from countries known to support international terrorism. International student offices and university administrators have had mixed reactions. The international students are a source of out-of-state tuition and contribute to the overall diversity of a campus. International student counselors and offices have historically acted as advocates for the guest students. There is some reluctance to take on a "law enforcement" function, however much individuals may support anti-terrorism efforts.

Specific programs have been developed by the CIA and DIA for encouraging academic participation with the IC. These efforts need to be encouraged, regularized, institutionalized, and adequately financed. The Scholars-in-Residence program of the Central Intelligence Agency is well known.[24] The Fulbright Senior Fellowship program, funded through the Department of State, is invaluable. Most informal or formal interaction takes place through individual consulting, sponsorship and organization of topical conferences, funding of individuals for specific research of mutual interest and concern, funding and support for research centers, and informal conversations at any one of the periodic, internationally focused academic conferences. This interaction can be highly productive because both parties tend to focus on international issues of mutual concern, and bring special expertise to bear for creative and constructive problem solving.

CONCLUSION

Academics and intelligence professionals are concerned with much the same set of problems. The approaches to problem solving may differ but certainly the practices inherent in American democratic tradition have constructed the intellectual environment so as to provide common definitions of contemporary threats and challenges. Both communities agree that liberty, democracy, freedom, equality, law, and property are defensible American values. Cooperation between the IC and academics, and specific contributions that academics can make to the production of good intelligence, can and must be further supported. It would be foolish to waste available skills and talent. There is too much at stake.

BIBLIOGRAPHY

Berg, Bruce L. *Qualitative Research Methods for the Social Sciences*, 3rd ed. Boston, MA: Allyn and Bacon, 1998.

Duiehl, Paul F. and Nils Petter Gleditsch, eds. *Environmental Conflict*. Boulder, CO: Westview Press, 2001.

---

[24] See Gates, 1986. A more recent status report on ties between CIA and professional academics is in Lloyd D. Salvetti, Director, Center for the Study of Intelligence, "Teaching Intelligence: Working Together to Build a Discipline," in *Teaching Intelligence at Colleges and Universities*, Proceedings of the18 June 1999 JMIC Conference (Washington, DC: JMIC, 1999), 12-24.

Gates, Robert M. "CIA and the University," *Studies in Intelligence* 30, no. 2 (Summer 1986): 27-36.

Hilsman, Roger. *Strategic Intelligence and National Decisions*. Glencoe, IL: The Free Press, 1956.

Holt, Pat M. *Secret Intelligence and Public Policy: A Dilemma of Democracy*. Washington, DC: CQ Press, 1995.

Homer-Dixon, Thomas and Jessica Blitt, eds. *Ecoviolence: Links among Environment, Population and Security*. Boulder, CO: Rowman and Littlefield Publishers, 1998.

March, James G. and Johan P. Olsen. *Democratic Governance*. New York: Free Press, 1995.

Salvetti, Lloyd D. "Teaching Intelligence: Working Together to Build a Discipline." In *Teaching Intelligence at Colleges and Universities*, Proceedings of the 18 June 1999 JMIC Conference. Washington, DC: JMIC, 1999.

Sayle, Edward F. "The Historical Underpinnings of the U.S. Intelligence Community." *International Journal of Intelligence and Counterintelligence* 1, no. 1(Spring 1986): 1-17.

Schrecker, Ellen W. *No Ivory Tower: McCarthyism and the Universities*. New York: Oxford University Press, 1986.

Snyder, Jack. *From Voting to Violence: Democratization and Nationalist Conflict*. New York: W.W. Norton, 2000.

Sorensen, Georg. *Democracy and Democratization: Processes and Prospects in a Changing World*. Boulder, CO: Westview Press, 1998.

Turner, Stansfield. *Secrecy and Democracy: The CIA in Transition*. Boston, MA: Houghton Mifflin Company, 1985.

Winks, Robin W. *Cloak and Gown: Scholars in the Secret War*, 1939-1961. New York: William Morrow Publishing Company, 1987.

ABOUT THE AUTHOR

Dr. John Turner is the senior Middle East and North Africa analyst at the U.S. European Command's Joint Analysis Center, where he is responsible for strategic estimates. His past assignments concerned with the Middle East and Africa region include estimative, counterintelligence, and current intelligence analytical postings in the U.S. and Europe. He has traveled widely in the Middle East and Africa. Dr. Turner earned degrees in Near Eastern Languages and Literatures from the University of Michigan and Yale University.

VIA THE INTERNET: NEWS AND INFORMATION FOR THE ANALYST FROM NORTH AFRICAN ELECTRONIC MEDIA

John Turner

The remarkable growth of electronic media over the past decade in Francophone North Africa provides specialists in the region with a wealth of news and other information. This survey and analysis of the French-language media of Algeria, Morocco, and Tunisia examines how these media go about providing information on North African politics, economics, and culture in a way that does take account of expatriates, who make up an important sector of the politically active population. For "outsiders" who specialize in the interpretation of the region, news media offer a "grass-roots"-based prism through which future developments may be anticipated.[1] Observable trends in the North Africa media, when carefully documented and placed in context, validate the contention of various authors, from Robert Steele and Gregory Treverton to Arthur Hulnick, who have addressed the promises and perils of devoting a greater share of intelligence resources to the exploitation open-source information. They have found much more promise than peril.[2]

REGIONAL MEDIA CULTURE

The political context in which North African media have evolved over the past three decades is chiefly one of centralized governments tending toward authoritarianism, be it oligarchical in the case of Algeria, monarchical in the case of Morocco, or presidential in the case of Tunisia. The political institutions of each country developed separately in the post-colonial period and in each country a different media culture exists that has until now clearly defined the role of the broadcast and print media. However, through the 1990s, as Internet access and use spread to the region, the public in each country, as well as the expatriate North African communities in Europe and elsewhere are proving to be a major

---

[1] An early and prescient example of this approach to "futurology" is in John Naisbitt's *Megatrends* (New York: Warner Books, 1982). Naisbitt's approach to trendspotting was to scan thousands of local newspapers in the U.S. and to extrapolate trends unobtrusively from those "grass roots" sources. This approach is explained in pages 8-9 of the book.

[2] For example, see Steele's *On Intelligence: Spies and Secrecy in an Open World* (Fairfax, VA: AFCEA International Press, 2002); Treverton's *Reshaping National Intelligence for an Age of Information* (Cambridge, UK: Cambridge University Press, 2001), chapter Four; Hulnick, "The Downside of Open Source Intelligence," *International Journal of Intelligence and CounterIntelligence* 15, no. 4 (Winter 2002-2003): 565-579.

new political factor.[3] This development results from the web's provision of news, including both analysis and opinion, as well as useful business information. Governments now experience strong competition from non-state run media due in large part to the use by the latter of the Internet.[4]

The political and business elites in Algeria, Morocco, and Tunisia have spearheaded the public demand for information to support their routine decisionmaking. Exposed increasingly over the past four decades to European and other media, North Africans desire that their domestic media mirror standards set elsewhere in the region and the world. It is in the electronic versions of the region's print media that this expectation has been most fully realized. Since the late 1990s a host of daily and weekly periodicals have developed electronic news sites, most backed by their parent print news organizations. Although the discussion here focuses on the French-language dimensions of this phenomenon, the reader should be aware that in each country a rapidly growing Arabic electronic media culture exists as well.

SURVEY OF NORTH AFRICAN ELECTRONIC NEWS MEDIA

Algeria

Algeria's electronic media culture is dominated by Internet versions of the country's French and Arabic-language newspapers. For the former, there are a dozen Algiers-based dailies and one Oran-based daily that cater to audiences in Algeria and Europe (see table below). Electronic versions of Algerian newspapers began in the early 1990s to provide the Algerian community abroad, especially in France, with news.[5] As of late 2002 thirteen dailies[6] are available on the Internet, all regularly maintained and updated daily. Algerian dailies are increasingly user-friendly and most have undergone facelifts as they make a bid for an increasingly sophisticated audience at home and abroad. Generally these

[3] Naturally, this development is recognized by those predisposed to shape public opinion. On the information-media contest between religious and secular forces, see Dale F. Eickelman, "The Coming Transformation in the Muslim World," *Current History* 99, no. 633 (January 2000): 16-20. For further background, see Eickelman's book, *New Media in the Muslim World: The Emerging Public Sphere* (Bloomington, IN: Indiana University Press, 1999).

[4] For discussions of the pre-Internet media in North Africa during the Cold War era, see especially the U.S. Army publications *Algeria: A Country Study*, fourth edition, 1985, 268-271; *Morocco: A Country Study*, fifth edition, 1985, 277-280; and *Tunisia: A Country Study*, third edition, 1986, 249-252. For coverage of post-Internet media developments, see *http://www.hrw.org/advocacy/internet/mena/index.htm*.

[5] See Elias Hanna Elias, *La Presse arabe* (Paris: Maisonneuve & Larose, 1993), 94. The government press monopoly was only ended in 1988. A snapshot of the evolving press culture in Algeria in the early 1990s is given in the fifth edition of *Algeria: A Country Study*, 1994, 218-220.

[6] One of them, *L'Expression*, was dormant for most the month of November 2002, reappearing at the end of the month after a remake (*www.lexpressiondz.com*). Such episodes are common with other electronic dailies in Algeria, which can unexpectedly be down for long periods of time while their web sites are redesigned.

changes have seen progressive upgrades in graphics quality, reliability of links, and web page format. In late 2002 alone, two dailies, *Liberte* and *Le Soir d'Algerie,* have both undergone major changes in the "look and feel" of their web sites.

Name	Internet address	Remarks
L'Actualitie	*www.lactualite-dz.com*	Independent; pdf format only
L'Authentique	*www.authentique-dz.com*	Independent
L'Expression	*www.lexpressiondz.com*	Independent; connections with government
Horizons	*www.horizons-dz.com*	Independent
Le Jeune Independant	*www.jeune-independant.com*	Independent
Liberte	*www.liberte-algerie.com*	Independent
Le Matin	*www.lematin-dz.com*	Connections with Interior Ministry
Al-Moudjahid	*www.elmoudjahid-dz-com*	Newspaper of the FLN, the ex-state party
La Nouvelle Republique	*www.lanouvellerepublique.com*	Independent
Le Quotidien d'Oran	*www.quotidien-oran.com*	Independent; main French-language daily in Western Algeria; published in Oran.
Le Soir d'Algerie	*www.lesoirdalgerie.com*	Independent; principal independent evening French daily
La Tribune	*www.latribune-online.com*	Independent
El Watan	*www.elwatan.com*	National daily of record; connections to Army

Algerian French-Language Daily Newspapers on the Internet

In contrast to the wealth of dailies represented in the electronic media, there is a dearth of Algerian weeklies available on the Internet. Some of the daily web sites have "weekend"-oriented articles appearing in their Thursday or Saturday editions (Algerian papers and their electronic counterparts are not issued on Friday). However, only three of them at the time of writing had multimedia "magazine" supplements.[7]

Algeria's government news site is the Algerian Press Service (APS),[8] which has web pages in Arabic, French, English, and Spanish. APS has news offices throughout Algeria and updates its web page of news items daily. Many of the news dailies discussed below use APS reports. However, most have their own network of reporters throughout Algeria and rely upon APS and international wire services for foreign news.

Daily press summaries are provided on two independent web sites. The first is offered by Agence Algerienne d'Information (AAI),[9] which has a detailed daily press review covering the headlines of the nation's French and Arabic language newspapers. A briefer ver-

[7] These were the *Jeune Independant* ("JI Multimedia"), *Le Matin* (*MultiM@tin*), and *La Tribune* ("*La Tribune Multimedia*"). In addition, *Le Matin* had a topical section updated every several weeks.

[8] *www.aps.dz.*

[9] *www.aai-online.com/revu.*

sion of the country's daily press offering is found on the website of the "Algeria Guide."[10] *El Watan*[11] is one of the oldest of the electronic dailies appearing on the web, and caters to a French-speaking audience at home and abroad. El Watan is widely cited as a news daily of record.

In addition to the French-language dailies noted in the table, one cannot ignore Algeria's leading Arabic language daily, *El Khabar*.[12] Starting in 2001, daily editions of this paper in Arabic have been supplemented by English and French headlines pages.[13] Each consists of a brief summary of the daily print and electronic edition's major stories. Although the English and French sites are similar, the choice of items for summarization from the Arabic original is not all-inclusive. Nevertheless, these pages are important for non-Arabic readers as an insight into the reporting focus of Algeria's largest daily.

Morocco

In contrast to Algeria's thriving daily Internet news culture, Moroccan electronic news media represent a combination of daily and weekly web sites. The daily print news providers and their electronic web sites (see table below) are dominated by four major papers. However, the news culture of Morocco is also marked by a strong showing of news weeklies, many of which are relatively new since the end of the 1990s and the accession of the present monarch, King Mohamed VI, to the throne.

Name	Internet address	Remarks
Al-Bayane	*www.casanet.net.ma/albayane/*	Casablanca; French-language daily of the PPS
Liberation	*www.liberation.press.ma*	Casablanca; French-language daily of the USFP
Le Matin du Sahara et du Maghreb	*www.lematin.ma*	Casablanca; government/royalist news daily
L'Opinion	*www.lopinion.ma*	Casablanca; French-language daily of the Istiqlal
L'Economiste	*www.leconomiste.com*	Casablanca; independent daily specializing in business and commercial news
Le Quotidien du Maroc	*www.casanet.net.ma/quotidien*	Casablanca; Independent daily

Moroccan French-Language Daily Newspapers on the Internet

Moroccan dailies have been appearing in electronic form since 1998, when the semi-official *Le Matin du Maghreb et du Sahara* began Internet publication. *Le Matin* was later followed by the newspapers of three of the political parties of the center-left Koutla coalition in the parliament. These papers still form the backbone of the electronic daily publi-

[10] *www.algerie-guide.com/actualitie.*

[11] *El Watan: Le Quotidien Independant, http://www.elwatan.com.*

[12] *www.elkhabar.com*. Links to the French and English headline pages are found on the main page of the daily edition.

[13] *www.elkhabar.com/html/pageAnglais.html* and *www.elkhabar.com/html/pageFrancais.html*

cation, joined only by the independent *L'Economiste* and *Le Quotidien du Maroc*. Morocco's news dailies are still largely the domain of its political parties.[14]

Morocco's national news agency is the *Maghreb Arabe Pres*se (MAP),[15] which has web sites in English, French, Arabic, and Spanish. MAP, as well as international wire services, provides domestic news dailies with foreign news and some domestic news items. MAP hosts a French web site that provides a daily press review of nineteen French and Arabic dailies.[16]

Le Matin du Maghreb et du Sahara has the largest print circulation and its web version also dominated the electronic media after its 1998 launch. However, the first web site was extensively overhauled in September 2001, changing from one primarily mirroring the print edition to one with distinctive content that was also distinguished with a distinct name—*Le Matin.ma*[17]—to emphasize its web status.

Tunisia

Tunisia's electronic press remains restricted compared to that in Algeria and Morocco, with the country's Internet activity subject to close government scrutiny. The paucity of news dailies (see table below) and the availability of foreign print media at the present time combine with government controls to produce an electronic media culture that focuses heavily on business and commerce, as well as non-controversial domestic and foreign news items.

Name	Internet address	Remarks
La Presse du Tunisie	*www.tunisie.com/LaPresse/index.html*	Principal French-language daily; government connections
Le Renoveau	*www.tunisieinfo.com/LeRenoveau/*	French-language daily of the RCD, the dominant political party in Tunisia.
Le Temps	*www.tunisie.com/Assabah/Alternate: www.lapress.tn*	French daily published by Dar es-Sebah, Tunis

Tunisian French-Language Daily Newspapers on the Internet

Tunisia's news dailies are heavily controlled by the government, with even the country's largest non-government press house, Dar es-Sebah, having to keep within unofficial but very real constraints.[18]

[14] Elias, 109.

[15] *www.map.co.ma*.

[16] *www.map.co.ma/mapfr/fr.*

[17] *www.lematin.ma*.

[18] See Elias, 108-109, for the major Tunisian press enterprises, of which *Dar es-Sebah* is one.

MEDIA ISSUES: OBJECTIVITY AND ACCURACY

The political heritage of North Africa and its impact on the region's media culture together raise the inevitable questions of editorial freedom, objectivity and accuracy. The ideal standard for North African publications, as in other countries, is one of adherence to strict standards of reporting and analyzing events in a climate of universal press freedom. However, "red lines'' exist in editorial freedom, objectivity, and accuracy that are perilous to cross. North African media have suffered negative sanctions imposed by government officials as the result of reporting that has broken taboos.[19]

Objectivity is a concern for analysts and researchers in a media culture where most papers, not only those owned by manifestly political groups, but also the independent press, are controlled by interests that have a marked political agenda. Nevertheless, in both Algeria and Morocco a system of checks and balances exists, with daily and weekly print media and their electronic counterparts in vigorous competition for the domestic and foreign market. These publications maintain high standards of journalism, and are normally quite open about their particular biases or journalistic objectives. Such competition and declared interests ensure a degree of confidence in political and economic analysis that allows a high degree of confidence among business and government consumers who seek information for decisionmaking. Tunisia, with its dearth of news dailies and strong government influence in the media, remains problematic for the area specialist seeking in-depth analysis of some events, although most economic and business reporting remains of high quality and supports its citizens' decisionmaking effectively.[20]

Accuracy has historically been less of a concern. A flourishing media culture and rivalry among news dailies and weeklies in Algeria and Morocco ensures a degree of competition that normally means news items are reliable; that is, consistently reported in different publications with a sufficient degree of detail and verification of factual data to make them satisfactory records of events. In such an information-rich climate, attempts by government or private parties to plant stories would be subject to immediate scrutiny and detection by the press. The latter frequently analyzes government reporting on an issue and takes it to task for various shortcomings, thereby ensuring, through the resulting reliability, that validity or accuracy is also addressed.

NORTH AFRICAN MEDIA AS A SOURCE OF INFORMATION

The electronic media in Algeria, Morocco, and Tunisia remain tied to their print media roots. This is an economic necessity, as too few in these countries lack the disposable income to rely on the Internet as their main source of information. Printed newspapers,

[19] Recent problems encountered by journalists include cutoff of advertising support in Tunisia (*El Maoukif*, 21 December 2001), as well as outright government seizure of publications in Morocco (*Al Mostaqil*, 1 May 2002).

[20] For the Arab world as a whole, these observations are supported by Dale F. Eickerman, "The Arab 'Street' and the Middle East's Democracy Deficit,'' *Naval War College Review* 55, no. 4 (Autumn 2002): 39-48.

either daily or weekly, are relatively cheap and widely available, and within the means of most of the region's population. So long as the region's economic problems continue, there will be limits on disposable income that impact the ability of the electronic media to be of practical use to its intended audience.

Databases, and their extent and degree of searchability, remain issues for the researcher. In terms of media-based interpretation of North African countries, there is little consistency in whether or not an electronic daily or weekly has links to past editions, and how easily they can be accessed and searched. The majority of electronic news media still offer no search capability, forcing readers to access past editions one by one in the hope of finding specific news items. Media storage capabilities often limit web sites from offering more than a few months' worth of past issues. Certain publications, such as those of the Moroccan *L'Economiste, La Vie Economique*, and *Maroc Hebdo*, are prominent exceptions. But with most other electronic publications from the region, the researcher's quest is often frustrated by lack of archival depth and broken links. Remedies to the current deficiencies will be slow in coming and dependent on additional data storage availability and improved website management.

Reporting of events, as noted above, is as objective and accurate as that found anywhere in the world. The electronic media in Algeria and Morocco are often the single best source of news for outside researchers who try to interpret the climate of opinion and incipient trends that exist in the interior of these large and increasingly complex countries. Local news is a growth industry in Morocco, but has yet to become well-established in Algeria or Tunisia. However, the steady growth of electronic media and the institutionalization of its culture as a normal supplement to the print world promises that local newspapers will soon be much more available in electronic form via the Internet. Such sites, however, are as likely to be in Arabic as in French, depending upon the local population and the degree to which the outlet has an expatriate readership.

Electronic news media are slowly but certainly being augmented by independent Internet sites. Such sites are still relatively few due to their lacking a solid print media base to finance electronic editions. However, the provisional success of *CasaNet* in Morocco[21] and *Cirta* in Algeria[22] probably indicate a proliferation of these sources.

[21] *www.casanet.net.ma* is the web site address of *Menara: La Portail du Maroc*, hosted by Morocco's largest telecommunications company, Maroc Telecom. Menara previously hosted the Moroccan electronic dailies *Liberation* and *al-Bayane*, but both now have their own independent sites.

[22] *www.cirtaonline.com/news/* has a constantly updated listing of world, national, and local news. Despite its name (Cirta is the old Roman name for the eastern Algerian city of Constantine), the site is national in scope, leaving local news to the Arabic-language daily *an-Nasr* (*www.an-nasr.com*).

It remains uncertain whether electronic news dailies or weeklies will come to dominate the Internet news market in North Africa. Much depends on the fortunes of their parent print media companies, trends in the news-reading public's interests, and the rate of growth of the local economies in North Africa and the amount of disposable income available to the general population to sustain further growth of the electronic media. Until personal computers and affordable Internet access is commonly available, most North Africans will still rely on the print and broadcast media as their primary forms of news information. In this situation, access by the public to the Internet will remain largely confined to the "Internet Cafes" that are burgeoning throughout the region. Such a situation will sustain only modest electronic media growth.

Under these circumstances, it is likely that one of the key factors in the growth of North African electronic media is likely to be the expatriate community in Europe.[23] The latter enjoy sufficient disposable income and have the motivation to make use of the Internet to follow events in their countries of origin, including at the local or community level. The increased interest by European business and government professionals in North African affairs also provides a potential growth market for electronic media. These professionals often seek and indeed require more information beyond the apparent wealth of data currently available. Catering to such audiences—the expatriate and foreign business/government community—will tend to ensure that in the electronic media world French (and possibly English) news availability will dominate, despite likely future gains by Arabic in the print media world in North Africa itself.

OUTLOOK: INCREASED COVERAGE, GREATER DEPTH

In general, North African, electronic French-language news media still follow the lead of their print counterparts. This is due to the limited access of the population to computers and the Internet, and the continued reliance of the public on broadcast and print media. Further, most media advertisers remain wary of investment in Internet sites, a factor that limits them to being sponsored by established media interests, such as the print media. Nevertheless, the growing number of home computers and Internet connections is bringing the first steps of transformation.

For observers of North African affairs, trends in the French-language electronic news media are reassuring for the near future. Area specialists and other interested professionals will have a steadily growing body of information from which they can draw

---

[23] The North African community in Western Europe numbers approximately two million. For details on numbers and other particulars, see Sarah Colinson, *Shore to Shore: The Politics of Migration in Euro-Maghreb Relations* (London: Royal Institute for International Affairs/Middle East Programme, 1996), especially the table on page102; and *Migration aus Nordafrika: Ursachen und Problem*, ed. Michaela Koller (Martinsried, Germany: Ars Una, 2000), especially 8ff. and 60ff.

for a reasonably authentic representation of social trends. If political, economic, and social information remains readily available without the geographic limitations associated with print media distribution, the confidence level in information associated with this region among government and business interests worldwide will continue to improve. The ability of North African intelligence specialists to take advantage of multiple rather than single-source information to provide analysis to decisionmakers will, however, increasingly have to take account of Arabic-language media as well as independent Internet news sites in order to ensure a more complete picture of events.

ABOUT THE AUTHOR

Early in his career, as operations officer on the WWII Fletcher-Class destroyer USS *Benham* (DD796), **CAPT George Satterthwaite** became intrigued by the international aspects of being a U.S. Navy officer. The Benham was about to be transferred to Peru under the Military Assistance Program, and he was to accompany a Peruvian crew to Norfolk for underway training, and then go on to Callao where the re-christened *Villar* was to be the flagship of the Peruvian Navy. But he was transferred instead to the Naval Academy to teach calculus. After a tour on a diesel submarine, he left active service, and joined the inactive reserves. Twenty-two years later, in 1986, he discovered that the Navy was looking for individuals to serve attaché duty in hard-to-fill jobs in the Third World. Peru was on the list, and he soon began training and education to become Navy DATT/ALUSNA (Defense Attaché/American Legation U.S. Naval Attaché) in Lima. As he was about to enter Spanish language training, his assignment to Latin America was cancelled, and he was reassigned to be ALUSNA New Delhi where he served for four years from 1988 to 1992.

Having enjoyed his tour in India immensely, CAPT Satterthwaite asked to be reassigned to another Defense Attaché Office (DAO), and was sent to Jakarta for three years (1993 to 1996). During his last year in Jakarta he remarked to his Navy personnel detailer that he had enjoyed the 10 years of active duty time despite the fact that he did not get to go to Peru. The detailer exclaimed that he was having a very tough time filling the DATT/ALUSNA job in Lima, and asked CAPT Satterthwaite to apply once more. At age 60 CAPT Satterthwaite and his wife entered language training for the third time and, after a few months at the Defense Language Institute, went to Lima for a two-year assignment. UNITAS, the large Western Hemisphere, Navy-to-Navy exercise, was inaugurated in the year CAPT Satterthwaite was originally supposed to go to Peru (1960). In 1998 and 1999 he oversaw the planning and implementation of the 38th and 39th cruises. He ended his career as a Naval Attaché in a ceremony officiated by the Chief of Staff of the Peruvian Navy, who had been on the Villar (ex-Benham) as a junior officer. Also in attendance at that ceremony was CAPT Satterthwaite's relief on the Benham, VADM (Ret) Daniel Mariscal. Coincidentally, VADM Mariscal was a 1954 graduate of the U.S. Naval Academy, and CAPT Satterthwaite's father had been his sponsor.

Between active duty assignments, CAPT Satterthwaite had a varied and diverse career. In 1979, he earned a Ph.D. in Public Administration and later taught at The American University, the Naval War College and the Monterey Institute of International Studies. He was also an operations research analyst at the Johns Hopkins University Applied Physics Laboratory, and has served as a consultant to federal, state, local and tribal governments. He now teaches occasionally at the Defense Resource Management Institute, volunteers his time teaching math in a local high school, and is a member of the Monterey County, California, Civil Grand Jury.

VISIT TO MAZAGON DOCKYARD, BOMBAY

F.G. (George) Satterthwaite, CAPT, USNR (Ret.)

Often there are many interesting places an attaché wants to see in the host country, but sometimes the host government is not willing to grant permission for the visit. Sometimes it is a matter of equity. Sometimes permission is not granted because the host has a memorandum of understanding with another country to forbid others to see mutual development projects. At other times the host just considers the places to be visited too sensitive to allow foreigners to see what they are up to.[1] At still other times denial of permission to visit is due to a "we've never done that before, so why let someone do it now" syndrome. The story related here is an example of that kind of response.

During my tour as DATT in Lima, I struck up a friendship with the Commander of the Peruvian Submarine Force. He had just returned from Germany where he had been the Defense and Naval Attaché. He understood the value of promoting good will with others by permitting foreign attachés to observe military operations of a training nature. He knew his attaché in Washington had been taken aboard U.S. nuclear submarines, and had visited the National Training Center at Fort Irwin. He wanted to reciprocate and offered me an eight-hour training ride on one of the Peruvian submarines. He made this offer on the spur of the moment without checking with his Director of Naval Intelligence. He probably thought, as I did, that because Peru has U.S. submarines, allowing a U.S. Naval Attaché on a U.S.-produced submarine would not be a violation of their security rules. The Admiral's offer was made in the weeks just before tensions between Peru and Ecuador heated up, during the summer of 1998. When I called to find out when the trip was scheduled, the Admiral's aide said that all the subs were on alert and he didn't know when the next training ride would take place. This was a totally expected and reasonable response given the operational situation.

---

[1] Defense Attaché officers are bound by the "Vienna Convention on Diplomatic Relations and Optional Protocols[,] Done at Vienna [Austria] on 18 April 1961, U.N.T.S. Nos. 7310-7312, vol. 500, 95-239 (see copy at URL: *http://www.fletcher.tufts.edu/multi/texts/BH408.txt*). These guidelines allow for accredited embassy officials, including military attachés, to engage in "ascertaining by all lawful means conditions and developments in the receiving State, and reporting thereon to the Government of the sending State (Article 3), and provide for freedom of movement except in specifically denied areas (Article 26). For a thorough overview of the "Defense Attaché System," see the Defense Intelligence Agency's *Communique* 12, no. 5 (September/October 2000).

As soon as the hostilities were brought to a peaceful conclusion on 26 November 1998, I tried to find another date for the promised submarine ride. The Admiral's aide told me they were trying to find a time and he would get back to me soon. He kept putting me off. As my tour wound down and my relief came to Lima for an orientation to the environment and to the job, I planned a reception and invited the Submarine Commander, among others whom my relief would need to know after he relieved me. The Admiral told me at that time that the visit was a "go," and that it would happen in the final week of my tour. During the last week of my tour the Foreign Liaison Officer took me out to lunch and he told me that the Director of Naval Intelligence (DNI) had countermanded the submarine Admiral's kind offer to let me ride on a Peruvian submarine. The reason given was it

would be counter to the national security interests of Peru. The Admiral was totally embarrassed as was the Foreign Liaison Officer, and the Peruvian Navy did not get to show the flag to a friend. The idea of reciprocity did not seem to enter the DNI's mind. Building a good service-to-service relationship moves ahead when friendly attachés are allowed to see how the host services train and operate.

How does an attaché allay either national security concerns or wrong thinking on the part of host-country foreign intelligence officials? In my experience, it is useful to take advantage of visits by "high rollers" to the country. A high roller is a flag or equivalent-level civilian who comes either invited by the host or self-invited by the U.S. Government. Generally, combatant command commanders self-invite themselves once every year or so to the countries in their Area of Responsibility. Fleet commanders of forward-deployed ships also like to visit countries in their operations area that have ports or navies. Self-invited visits generally result in gaining access to military units, which the attaché may have had difficulty visiting on his own. Superior to the self-invited visit is the visit sponsored by the host. Counterpart visits by chiefs of service fall under this heading. Here the host country is usually trying to put a best foot forward to impress the visitor with the capabilities of the host military and may be more amenable to showing off new capabilities and units.

Because the attaché is in a position to recommend an itinerary in both the invited and self-invited visits to the invitee as well as the host, he or she can influence the visit by recommending interesting places for that visitor to see. The only times I was able to see India's Mazagon Dockyard was when the U.S. Chief of Naval Operations (CNO) visited on two different occasions (host-invited visits), and when the staff of the Senate Select Committee on Intelligence (on a self-invited visit) traveled to India to investigate high-tech developments there. The Government of India accepted both of the CNO visits to the dockyard to see submarine developments as natural requests, because both CNOs were submarine officers (ADM Trost and ADM Kelso). I accompanied both CNOs on these visits and had a firsthand look at the Indian Navy's first submarine construction project. There were no repercussions in making these two visits. In fact, the Indian Navy asked me afterward what the CNO thought about their capability to build submarines. They were looking for acceptance as a modern and capable navy from the chief of the world's most modern navy. It was the self-invited visit by the Senate Select Committee on Intelligence staff to Mazagon Dockyard that gave me heartburn.

Several months before the Gulf War it was announced during the embassy's country team meeting that three members of the staff of the Senate Select Committee on Intelligence planned to visit India to see firsthand evidence of India's shipbuilding, aircraft building, atomic research, and space research programs. The staff members were senior U.S. Government employees, at least one of whom was a senior executive civil service or, in military terms, a flag-level visitor. Typically in U.S. embassies around the world, visits by congressional members or staff are under the auspices of the Political Section. This was the case for the Senate Select Committee Staff visit. A control officer from the Political Section was assigned the task of coordinating the visit. His job was to find out what the Staff wanted to accomplish in India, and then present a proposed program agenda to

the Foreign Ministry expressing the desires of the self-invitees. After informal acceptance of the proposal, the control officer drafted a diplomatic note and passed it around the embassy for coordination. It was at this point that I learned the visitors would be traveling to Bombay to see the Mazagon Dockyard and Bhaba Atomic Research Laboratory. From Bombay they would travel to the South India version of Silicon Valley at Bangalore, and visit Hindustan Aeronautics Ltd, and the Indian Space Research Organization (ISRO).

Author talks with an Indian Navy captain on board a third-party vessel.
This and other photos courtesy of the author.

I called on the control officer and found he was not overly excited about his responsibilities. He didn't want to travel with the visitors and complained of having too many other responsibilities. Also, the Department of State budget was very tight that year, and the Political Counselor didn't know where the money for travel was going to come from. I immediately interpreted the control officer's protests as a plea to pass the baton of handling this group to someone else. I told him I would be more than happy to take the burden from him. My boss and his agreed to the switch, and I drafted a change to the diplomatic note indicating I would be the new control officer. I did not realize at that time that to propose something to the Indian Foreign Ministry that was a little different from their expectations would make them attribute suspicious intentions to me. I'm sure the old India hands in the embassy, like the Deputy Chief of Mission, had experience with the mindset of Indian bureaucrats, but they did not advise me about the potential for Indian xenophobia to be translated into casting a pall over my bona fides.

I went about coordinating the visit by contacting the visitors and making arrangements for their travel and transportation within India. They arrived in country a week later and

we consolidated the plans for the trip to Bombay and Bangalore. Early on a Monday morning we departed from Indira Ghandi International Airport on an Indian Airlines flight to Bombay. Until this point everything was going as planned. Upon arrival in Bombay we hired a cab and took the 25-kilometer ride to the Taj Intercontinental Hotel, past the two million people in the city's slums and over the series of interconnected islands that make up Greater Bombay. We checked into the very posh Taj Intercontinental Hotel, which overlooks the Gateway to India, a memorial to the visit of King George V completed early in the 20th century. I asked for my usual room on the 14th floor, because besides overlooking the *Gateway of India*, it has a panoramic view of Bombay harbor. Fortunately, the room was vacant, and it was assigned to me. After checking in and unloading my suitcase, I peered out the window to see what there was to see in the harbor.

I always looked forward to trips to Bombay because my favorite restaurant there was the Nanking. It was a Chinese restaurant specializing in seafood dishes at very reasonable prices. It was on the ground floor in the same building as the Royal Bombay Yacht Club, and it was only a short walk from the hotel. Their crab with lobster sauce was especially delicious.

The Gateway to India and naval facilities in Bombay.

Author and son visiting with a Hindu holyman at a curio shop in Bombay.

The service in the Nanking was superb. My meal of crab with lobster sauce lived up to expectations, and after a cup of green tea I left the restaurant.

Later that day we visited the Bhaba Atomic Research Center located about mid-way between the hotel and Mazagon Dockyard. We were given the regular visiting-fireman type of tour. We did not observe any advanced research projects, but we did see a reactor used for medical isotope development and were given a watered-down briefing covering the entire research program. Even though we weren't shown the whole nine yards, so to speak, the staffers were impressed at the level of technical sophistication and knowledge of the researchers at the lab. Because their mission was to gauge overall technical competence and not specific programs, the visit to the Bhaba Atomic Research Center was successful.

The next morning we were escorted to the Dockyard, and got a windshield tour of the production facilities by company car. We also saw the work in progress on Soviet-designed destroyers and fast patrol boats. Modular construction of the destroyer was very impressive, and we were also given a status report on the production schedule. Submarine construction was left off the tour, but the chief executive officer of all the Indian-owned shipyards briefed us. He told us of the highlights and shortcomings of the entire Indian shipbuilding industry (military and commercial). All in all, the entire visit to Bombay was more than I had hoped for. One more night in teeming Bombay and we would be off to Bangalore in the morning.

We took the morning Indian Airlines flight to Bangalore, aboard an Airbus 320, of the same type that had crashed a year or so earlier due to a faulty fly-by-wire system. We were fortunate this time. The plane was on time and the flight uneventful.

Bangalore is a much less hectic city than Bombay. It also is populated with a large middle class of educated professionals. Unlike Bombay with some very rich and millions of poverty-stricken citizens, Bangalore is more homogeneous in terms of the standard of living. It is also the hub of technical innovation in India. Many computer firms, to include Hindustan Aeronautics Ltd. and the Indian Space Research Organization (ISRO) are the main centers of technology there. Because of the high density of well-educated and sophisticated people in Bangalore, one finds more Western style retail business establishments there as well. Many of the professional class were educated in the UK or the U.S. and have acquired tastes for Western food and clothing. The *sari* is still commonly worn; hence adoption of Western clothing style is limited to the male population. Bangalore is located in Karnataka State in South India and the local language is Kanada. Kanada, like other South Indian languages, is very different in sound, vocabulary and grammar from the interrelated languages of the North (Hindi, Punjabi, Marathi, Bengali, Bihari, and the like). Hindi speakers cannot understand Kanada speakers and vice versa, so communication between them is usually in English.

We checked into the Taj West End hotel, a member of the same chain as the Taj Intercontinental in Bombay and Taj Village in Goa. It is a one-story series of motel-like suites, and the layout and amenities have a Southern California look about them. We had nothing official on the agenda this day, so we lounged around the pool that afternoon and shared sea stories.

After a breakfast of very strong coffee, *somvar* and *idli* (spicy chutney and mushy rice), a traditional South Indian dish, we met our car and driver which had been prearranged by the Ministry of External Affairs (Foreign Ministry), and headed off to ISRO and Hindustan Aeronautics Ltd.

Our visit to ISRO was interesting. The Indian Government has a very sophisticated research program directed at putting satellites in stationary orbit above India. We learned, for example, that they had the capability to locate areas in India where ground water was prevalent and also where the vegetation was rapidly dying. This information, if used properly, could support the management of scarce potable water and forest resources. The Indian mindset, however, appeared to be focused on the technology itself and not on solving critical environmental problems. There was no effort to integrate the technology with the problems of the Home Ministry (Interior Ministry). It seemed that the Indians felt a lot of pride about being a member of the club of nations who have the ability to develop very sophisticated technology.

Next we visited Hindustan Aeronautics Ltd. (HAL). During WW II the predecessor to HAL had been a facility built by the U.S. to repair and assemble aircraft, which were being used in the China-Burma-India Theater of the war. After the war the Indian Govern-

ment took it over and converted the facility to an aircraft production facility. At the time of our visit they were building or conducting concept design on British Tornadoes under license from the UK, small Bell-type helicopters of indigenous design, and a new light combat aircraft, also of indigenous design. We toured the plant and were given a short briefing on future plans. I was especially interested in HAL because it was there that the LM 2500 General Electric gas turbine engines would be fabricated under license to be installed in the Indian Taruntul seagoing patrol craft. East would meet West in India when the U.S. LM2500 would power the Soviet-designed Taruntul! That project was mentioned in the brief, but the international agreements had not yet been signed so no production activity had been started. After a luncheon with the public affairs folks at HAL we departed for the airport for a flight back to New Delhi.

From my point of view spending DAO travel funds on this trip was a good investment. I was able to visit places by piggy-backing or "strap-hanging" on the visit of the Senate staffers—places that I would unlikely have been able to visit on my own, except perhaps for HAL. After the staffers departed, I busily documented the trip and fired off the resulting report to headquarters. About one week later the real fun began. I was looking forward to the next project, wondering what could top the trip to Bombay and Bangalore, when I was called into the Deputy Chief of Mission (DCM's) office. The DCM told me that the Joint Secretary for the Americas Division of the Ministry of Foreign Affairs had formally requested that I meet with him to explain my role in the Bombay and Bangalore trip. I asked what this was all about, and the DCM said he didn't have a clue. The change to the diplomatic note spelled out my role in the visit, and since the Government of India had approved the visit, he could not figure out why such a high-ranking official would summon me to his office. A Joint Secretary is equivalent in rank to an Assistant Secretary of State. The incumbent was in charge of international relations with Mexico, Canada, and the U.S. He had formerly served as the minister counselor (similar to a DCM) in the Indian Embassy in Washington and presumably knew how the U.S. Government was organized and operated. I had met him briefly at a fourth of July party, so I was not walking in on a complete stranger. My recollection was that he thoroughly enjoyed his tour in Washington, and his family was eager to return. I made an appointment to see the Joint Secretary the following week.

There is life after naval service in India.

On the appointed day I took the route to the foreign ministry that passes by all the apartments set aside for members of Parliament. Since Parliament was in session, there was much activity in the area. Clothes just washed were being hung out to dry and some Parliamentarians dressed in *dhotis* were gathered outside their apartments having morning *chai*. The Foreign Ministry was located in South Block, as was Naval Headquarters and the Ministry of Defense, except that the entry to the Foreign Ministry was on the opposite side of the fortress-like building from the Navy entrance. Upon entering, guests were asked to sign in and show their carnet (diplomatic I.D.), and then asked to wait in a musty but elegant anteroom until their point of contact could be reached. After about fifteen minutes, and still puzzled by the purpose of the summons, I was escorted to the Joint Secretary's office.

After a few introductory remarks about the cold winter weather in New Delhi and a cup of *chai*, I was bluntly asked why I was doing the work of the CIA, whose task it was to handle visitors from the U.S. National Foreign Intelligence Community? I retorted that Senate staffers are not from the Intelligence Community. They only conduct oversight with respect to the Community. In addition, the staffers mainly wanted to visit military production facilities here in India, and the military was definitely the bailiwick of the DAO. The Joint Secretary said, "Yes, I know how it works in Washington, but how do I answer the Parliament, whose members will presume you work for the CIA?" "Tell the truth," I said. He retorted, without further explanation, that this would put him in a very difficult position. I explained that what I did was a natural and reasonable thing to do given my responsibilities as a military attaché. I wondered at that point if I was going to

be expelled from India because of the Parliament's perception that I was doing something inconsistent with my diplomatic status as a military attaché. I kept thinking to myself, "How can we be having this conversation, when they (the Government of India) officially and in writing gave us permission to make the trip? This question could have been raised before the official notification of approval, and the Joint Secretary would not be in this 'difficult position.'"

Author with makeshift head covering for visiting a Hindu temple.

The issue was not resolved during the meeting. I suppose the Joint Secretary was reacting to questions from Parliament members, and had to go through the motions of calling me in and upbraiding me. I chalked it up to some communist sympathizer either in the Foreign or Defense Ministry who probably put the idea of my not being a "real" attaché into the bonnet of some receptive and Soviet-sympathizing Parliamentarian.

The price I paid for visiting some high-tech centers in India was that I was painted with a brush of suspicion. In my mind it was worth the embarrassment of being chewed out by the foreign ministry. I was not declared *persona non grata* and did not have to uproot my family. The U.S. Government was not embarrassed by the episode. We had followed the prescribed process of submitting a diplomatic note covering the trip and therefore the Government of India could only give me a verbal demarche instead of expulsion. The experience enlightened me about the complexity of Indian attitudes toward American diplomats. At one level it was all right to let U.S. officials see their facilities because of the Indian enjoyment of being thought of as avant-garde

or modern. At another there was still the lingering animosity and suspicion of Westerners promoted by the long-standing competition for the "hearts and minds" of the Indians by the U.S. and USSR. It would take some time to undo the effects of the Cold War that was waged hotly in the Third World.

ABOUT THE AUTHOR

Stephen Marrin is a graduate student specializing in intelligence studies at the University of Virginia, and he developed the ideas for this paper as part of his Master's thesis assessing the impact of the CIA's Kent School on analytic quality. He has also participated in CIA's analytic process in three different capacities: in 1996 and 1997 as a leadership analyst for CIA's Office of Near East, South Asia, and Africa; in 1998 as a project assistant for a group in the Office of Transnational Issues; and in 1999 and 2000 as a team leader for a contractor supplying analytical support to the Office of Transnational Issues. As required, this paper has been reviewed by CIA's Publication Review Board, which has no security objection to its dissemination. Their review does not confirm the accuracy of the information nor does it endorse the author's views.

IMPROVING CIA ANALYSIS BY OVERCOMING INSTITUTIONAL OBSTACLES

Stephen Marrin

The accuracy of CIA intelligence analysis depends in part upon an individual analyst's expertise, yet programs implemented to increase this expertise may not be sufficient to increase the accuracy of either an individual's analysis or the institution's output as a whole. Improving analytic accuracy by increasing the expertise of the analyst is not easy to achieve. Even if expertise development programs were to result in greater regional expertise, language capability, or an improved application of methodological tools, the production process itself still takes place within an institutional context that sets parameters for this expertise. The agency's bureaucratic processes and structure can impede an analyst's acquisition and application of additional expertise, preventing the full realization of the potential inherent in expertise development programs. Therefore, any new reform or program intended to improve analytic accuracy by increasing the expertise of its analysts should be supplemented with complementary reforms to bureaucratic processes — and perhaps even organizational structure — so as to increase the likelihood that individual or institutional improvement will occur.

The interplay between analyst and institution within the Intelligence Community remains poorly studied. As Columbia University's Robert Jervis has observed, "perhaps the intelligence community has paid too [little attention] ...to how the community's internal structure and norms might be altered to enable intelligence to be worth listening to."[1] CIA's intelligence production may be subject to improvement, but making that a reality requires a sophisticated understanding of how an analyst operates within the Directorate for Intelligence's [DI's] institutional context. However, empirical verification of this hypothesis is impossible since, as Jervis notes, "[r]igorous measures of the quality of intelligence are lacking" and are insurmountably difficult to create.[2] Under these circumstances, this essay is a conceptual "what-if" exploration into the interplay between the acquisition and application of expertise on three levels: that of the individual, bureaucratic processes, and organizational structure.

THE GOAL: IMPROVING CIA'S ANALYSIS

Improving the accuracy of CIA's finished intelligence products could make an immediate and direct improvement to national security policymaking as well as reduce the frequency and severity of intelligence failures. The CIA's DI—like other intelligence

---

[1] Robert Jervis, "What's Wrong with the Intelligence Process?" *International Journal of Intelligence and Counterintelligence* 1, no. 1 (1986): 41.

[2] Jervis, 30

agencies — ideally provides policymakers with "timely, accurate, and objective" finished intelligence analysis tailored to the needs of the national security policymaker.[3] In the author's experience and observation, a DI analyst interprets the international environment through an information-processing methodology approximating the scientific method to convert raw intelligence data into finished analysis. The traditional "intelligence cycle" describes how an analyst integrates information collected by numerous entities and disseminates this information to policymakers. As William Colby—former Director of Central Intelligence (DCI) and veteran operations officer — notes, "at the center of the intelligence machine lies the analyst, and he is the fellow to whom all the information goes so that he can review it and think about it and determine what it means.[4] Although this model depicts the process in sequential terms, more accurately the analyst is engaged in never-ending conversations with collectors and policymakers over the status of international events and their implications for U.S. policy. As part of this process, intelligence analysts "take the usually fragmentary and inconclusive evidence gathered by the collectors and processors, study it, and write it up in short reports or long studies that meaningfully synthesize and interpret the findings," according to intelligence scholar Loch Johnson.[5]

Intelligence failures of every stripe from the trivial to the vitally important occur every day for a variety of reasons, including the mis-prioritization of collection systems, hasty analysis, and inappropriately applied assumptions. In the mid-1970s Richard Betts effectively settled the academic question of causes of failure by arguing that intelligence failures will be inevitable due to many inherent limitations in the analytic process.[6] Administrators at the Joint Military Intelligence College note that "analysis is subject to many pitfalls — biases, stereotypes, mirror-imaging, simplistic thinking, confusion between cause and effect, bureaucratic politics, group-think, and a host of other human failings."[7] Yet most intelligence failures do not lead to direct negative consequences for the U.S. primarily because the stakes of everyday policymaking are not high, and errors in fact and interpretation can be corrected as the iterative process between intelligence

[3] CIA website, "The Role and Mission of the Directorate of Intelligence," URL: *http://www.odci.gov/cia/di/mission/mission.html*., accessed October 2001.

[4] William Colby, "Retooling the Intelligence Industry." *Foreign Service Journal* 69, no. 1. (January 1992): 21.

[5] Loch K. Johnson, "Making the Intelligence 'Cycle' Work." *International Journal of Intelligence and Counterintelligence* 1, no. 4 (1986): 11.

[6] Richard K. Betts, "Analysis, War and Decision: Why Intelligence Failures Are Inevitable," *World Politics* 31, no. 1 (October 1978): 61-89.

[7] Ronald D. Garst and Max L. Gross, "On Becoming an Intelligence Analyst." *Defense Intelligence Journal* 6, no. 2 (1997): 48. See also: Richards Heuer, Psychology of Intelligence Analysis (CIA, Center for the Study of Intelligence, 1999); Ralph K. White, "Empathy as an Intelligence Tool," *International Journal of Intelligence and Counterintelligence* 1, no. 1 (Spring 1986): 57-75. Richards Heuer, "Improving Intelligence Analysis: Some Insights on Data, Concepts, And Management in the Intelligence Community" *The Bureaucrat* 8, no. 1 (Winter1979/80): 2-11.

and policy develops. As a result, most failures or inaccuracies are eventually corrected and usually never even noticed. However, sometimes intelligence failure is accompanied by either great policymaker surprise or serious negative consequences for U.S. national security, or both.

The CIA's May 1998 failure to warn American policymakers of India's intentions to test nuclear weapons is an illustration of both kinds of failure. This lapse — widely criticized by foreign policy experts and the press — highlighted intelligence limitations such as the DI's inability to add together all indications of a possible nuclear test and warn top policymakers. According to New York Times correspondent Tim Weiner, these indicators included "the announced intentions of the new Hindu nationalist government to make nuclear weapons part of its arsenal, the published pronouncements of India's atomic weapons commissioner, who said...that he was ready to test if political leaders gave the go-ahead, and ...missile tests by Pakistan that all but dared New Delhi to respond."[8] CIA's inability to integrate these indicators — a failure of analysis — led to charges of "lack of critical thinking and analytic rigor."[9] Admiral David Jeremiah—who headed the official investigation into the failure—concluded that intelligence failed to provide warning in part because analysts "had a mindset that said everybody else is going to work like we work," otherwise known as mirror-imaging.[10] He then "recommended hiring more analysts, improving their training and increasing contact with outside experts to challenge conventional wisdom," according to The Wall Street Journal's Carla Robbins.[11]

CIA's search for ways to improve analytic accuracy and prevent intelligence failure—if successful—could have a positive impact on national security policymaking. The CIA is arguably the centerpiece of the United States' fourteen-agency intelligence community (IC) and "has primary responsibility for all-source intelligence analysis in the [IC] and the preparation of finished national intelligence for the President and his top policymakers," according to former CIA Inspector General Fred Hitz.[12] If CIA analysis does have this kind of central role in influencing policy, improving its accuracy should provide policymakers with the opportunity to create or implement policies that more effectively protect national security and advance national interests.

---

[8]Tim Weiner, "U.S. Blundered on Intelligence, Officials Admit," *New York Times*, 13 May 1998, A14..

[9]James R. Asker, "Same Ol', Same Ol'," *Aviation Week and Space Technology*, 8 June 1998: 21.

[10]CIA website, "Jeremiah News Conference," URL: http://www.cia.gov/cia/public_affairs/press_release/archives/1998/jeremiah.html, accessed October 2001.

[11]Carla Anne Robbins, "Failure to Predict India's Tests Is Tied to Systemwide Intelligence Breakdown," *Wall Street Journal*, 3 June 1998, A8.

[12]For further information on the IC see CIA's website, "United States Intelligence Community," URL: http://www.odci.gov/ic/, accessed October 2001. Also see Frederick P. Hitz, "The Future of American Espionage," *International Journal of Intelligence and Counterintelligence* 13, no. 1 (2000):3.

THE METHOD: INCREASING ANALYTIC EXPERTISE

Improving the capabilities and knowledge of the individual CIA analyst through programs reflecting Admiral Jeremiah's recommendation, is one way to improve the accuracy of intelligence analysis. An analyst's expertise, defined as "the skill of an expert," [13] is a crucial component for the production of accurate intelligence analysis. "In the lexicon of US intelligence professionals, 'analysis' refers to the interpretation by experts of unevaluated ['raw'] information collected by the [IC]," according to Loch Johnson.[14] The presumption is the more "expert" an analyst is the more accurate the resulting interpretation will be. In May 2000, DCI George Tenet described the importance of an analyst's expertise in this manner:

> In our [DI] it is not enough just to make the right call. That takes luck. You have to make the right call for the right reasons. That takes expertise. It is expertise—built up through study and experience—that combines with relevance and rigor to produce something that is very important: insight....[O]ur analysts blend a scholar's mastery of detail with a reporter's sense of urgency and clarity. At its best, the result is insight. And it is insight that wins the confidence of our customers and makes them want to read our publications and listen to our briefings."[15]

Analytic expertise is a multi-faceted concept because CIA uses a complex web of analytic specialties to produce multi-disciplinary analysis. Not hired directly by the CIA or even the DI, most analysts are hired by the individual DI offices and assigned to "groups" that cover specific geographic areas, and are then assigned a functional specialty—"discipline" or "occupation" in DI terminology—such as political, military, economic, leadership, or scientific, technical, and weapons intelligence, according to CIA's website.[16] An analyst's expertise can vary depending on his or her relative degree of regional knowledge, familiarity with disciplinary theory, and with intelligence methods in general:

- Regional expertise is essentially area studies: a combination of the geography, history, sociology, and political structures of a defined geographic region. The DI's regional offices are responsible for an analyst's regional expertise and develop it by providing access to language training, regional familiarization through university courses, or in-house seminars.

---

[13] Merriam-Webster online, URL: *http://www.m-w.com.*

[14] Loch K. Johnson, "Analysis For a New Age." *Intelligence and National Security* 11, no. 4 (October 1996): 657.

[15] CIA website: "Remarks of the Director of Central Intelligence George J. Tenet at the Dedication of the Sherman Kent School, 4 May 2000," URL: *http://www.cia.gov/cia/public_affairs/speeches/archives/2000/dci_speech_05052000.html*, accessed October 2001.

[16] On the CIA website, see "Intelligence Disciplines" at URL: *http://www.odci.gov/cia/di/work/disciplines.html*; also see on the CIA website, "Directorate of Intelligence Organizational Components, Council of Intelligence Occupations," URL: *http://www.cia.gov/cia/di/mission/cioc.html*, accessed October 2001.

- Disciplinary expertise relates to the theory and practice that underlies the individual analytic occupations. For example, economic, military, political and leadership analysis are built on a bed of theory derived from the academic disciplines of economics, military science, political science, and political psychology, respectively. Disciplinary expertise can be acquired through previous academic coursework, on-the-job experience, or supplementary training.

For the most part each CIA analyst possesses a very small area of direct responsibility defined by a combination of regional area and discipline as they work in country teams with analysts of other disciplines and interact with other regional or disciplinary specialists as the need arises. CIA's small analytic niches create specialists, but their specialties must be re-integrated in order to provide high-level policymakers with a bigger picture that is more accurate and balanced than that arising from the limited perspective or knowledge of the niche analyst. This process of re-integration—known as "coordination" in DI parlance—allows analysts of all kinds to weigh in with their niche expertise on pieces of finished intelligence before they are disseminated. According to CIA analyst Frank Watanabe: "We coordinate to ensure a corporate product and to bring the substantive expertise of others to bear."[17] Accordingly, the bureaucratic norm is for an analyst to make every effort to coordinate a draft with other analysts in related regional or disciplinary accounts prior to submitting the draft to management for editing and dissemination. As a result, whereas the expertise of the primary drafter of the piece usually has primary influence on the accuracy of the final piece, the coordination process exerts a strong influence as well.

Insufficient analytic expertise can cause inaccuracies in intelligence analysis. Robert Jervis points out that "a grav[e] danger lies in not having sufficient expertise about an area or a problem to detect and interpret important trends and developments. To make up for such deficiency, analysts tend to impose on the information the concepts, models, and beliefs that they have derived elsewhere."[18] In addition, in 1991 former DCI Stansfield Turner noted that "[a]nother reason for many of the analytic shortcomings is that our analytical agencies do not have an adequate grasp of the cultures of many countries with which we must deal."[19] Seven years later the CIA failed to provide policymakers with warning of India's nuclear tests for this very reason. To bolster CIA's weaknesses, in 1991 Turner suggested that analysts should be provided with "a better opportunity to attend academic institutions, participate in professional conferences, travel and live abroad, acquire language skills and thus become true experts in their areas."[20] Yet in

[17] Frank Watanabe, "Fifteen Axioms for Intelligence Analysts." *Studies in Intelligence*, unclassified edition (1997), URL: *http://www.odci.gov/csi/studies/97unclass/axioms.html*, accessed October 2001.

[18] Jervis, 32.

[19] Stansfield Turner, "Intelligence for A New World Order," *Foreign Affairs* 70, no. 4 (Fall 1991): 163.

[20] Turner, 164.

1998 former CIA officer Robert Steele observed that "[t]he average analyst has 2 to 5 years' experience. They haven't been to the countries they're analyzing. They don't have the language, the historical knowledge, the in-country residence time or the respect of their private-sector peers," as reported by Tim Weiner.[21]

CIA has recently implemented programs to increase analytic expertise. In 2000, then-Deputy Director for Intelligence (DDI) and current Deputy Director of Central Intelligence (DDCI) John McLaughlin created the Sherman Kent School for Intelligence Analysis, which was "designed to give new employees a rigorous, 26-week overview of intelligence analysis" [22] as well as provide training in CIA's analytic disciplines to officers of all levels. In addition, McLaughlin said that CIA is "going all out to achieve greater analytic depth. We are providing incentives for analysts to stay on their accounts longer. We are affording our analysts greater opportunities to travel and to broaden their experience. Because we claim no monopoly on wisdom, we are bringing in outside experts for short tours as scholars-in-residence. We also are encouraging our analysts to expand their contacts with specialists elsewhere in government, in the private sector and in academia."[23]

Increasing expertise may not be sufficient to produce accuracy or prevent failure. As Jervis notes, "experts will [not] necessarily get the right answers. Indeed, the parochialism of those who know all the facts about a particular country that they consider to be unique, but lack the conceptual tools for making sense of much of what they see, is well known."[24] In addition, "[e]ven if the organizational problems...and perceptual impediments to accurate perception were remedied or removed, we could not expect an enormous increase in our ability to predict events" because "(t)he impediments to understanding our world are so great that... intelligence will often reach incorrect conclusions."[25] That is because human cognitive limitations require analysts to simplify reality through the analytic process, but reality simplified is no longer reality. As a result, "even experts can be wrong because their expertise is based on rules which are at best blunt approximations of reality. In the end any analytic judgment will be an approximation of the real world and therefore subject to some amount of error"[26] and analytic inaccuracies—and sometimes intelligence failure—will be

[21] Quoted in Tim Weiner, "Naivete at the CIA: Every Nation's Just Another U.S.," *New York Times Week in Review*, 7 June 1998, 5.

[22] Vernon Loeb, "CIA's Analysis Becomes Transnational," *Washington Post Online*, 2 April 2001, URL: *http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A16925-2001Mar30*

[23] CIA website, "Remarks of the Deputy Director..., Princeton," URL: *http://www.cia.gov/cia/public_affairs/speeches/ddci_speech_03092001.html*

[24] Jervis, 31-32.

[25] Jervis, 28, 30.

[26] Stephen Marrin, "Complexity is in the Eye of the Beholder," DI Discussion Database (an internal CIA bulletin board), 6 May 1997.

inevitable. Therefore, although increasing expertise is a goal, it cannot be the only goal for increasing DI capabilities.

Nevertheless, the DI leadership has created multiple expertise development initiatives to counter perceptions of analytic inadequacy and increase the DI's core capability — its analytic expertise. The unanswered question is whether the analyst can acquire and apply relevant expertise within the institutional constraints of the DI.

FIRST INTERVENING FACTOR: BUREAUCRATIC PROCESSES

Bureaucratic processes can impede the acquisition or application of expertise gained in expertise development programs, thereby limiting any potential improvement in overall analytic accuracy. The DI is a bureaucracy, and like every bureaucracy creates "standard operating procedures" (SOPs) which are necessary for efficient functioning but over time usually prove to be rigid in implementation.[27] As former DDI Doug MacEachin noted in 1994: "We have all been a part of what has been good and of what needs changing. Some of the practices needing change came into being as the unforeseen result of efforts undertaken for sound constructive reasons, judged by participants at the time to have been fully valid and usually aimed at correcting deficiencies of the time. But collectively, with time and bureaucratic evolution, they turned out to be counterproductive."[28] Some of the DI's SOPs prevent analysts from applying the tradecraft standards and other forms of expertise learned elsewhere. Jack Davis, a former DI officer and analytic methodologist, observed that "examples of what MacEachin would label as poorly substantiated analysis are still seen (after training). Clearly, ongoing vigilance is needed to keep such analysis from finding its way into DI products."[29] Such vigilance includes assessing the bureaucratic context for obstacles preventing tradecraft application.

Analysts must have the opportunity to apply newly acquired expertise back at their desks in the DI for any improvement to result. However, if analysts do not have the opportunity to apply this expertise, it will likely wither for lack of practice. The DI produces many types of finished intelligence — some reportorial, some analytical, and some estimative—to meet policymakers' varying needs for information. In addition to daily updates on developments worldwide, policymakers and their staffs also use information and analyses when crafting policy and monitoring its implementation. Obstacles to the development of expertise appear when shorter product types are emphasized over longer more

[27] If bureaucracies stultify good ideas by turning them into "standard operating procedures" regardless of situation — as Graham Allison's organizational process model in his *Essence of Decision* implies — then a bureaucracy is forever in a state of flux, somewhere along the pendulum from one bureaucratized extreme to the other.

[28] Douglas J. MacEachin and others, *The Tradecraft of Analysis: Challenge and Change in the CIA* (Washington, DC: Consortium for the Study of Intelligence, 1994), 1.

[29] Jack Davis, "Improving Intelligence Analysis at CIA: Dick Heuer's Contribution to Intelligence Analysis," in "Introduction" to *Psychology of Intelligence Analysis*, Richards J. Heuer (Washington, DC: Center for the Study of Intelligence, 1999), xix.

research-oriented ones. Short turnaround products—including daily updates known as "current" intelligence — have at times been emphasized over other products for their greater relevancy to policymakers, but this emphasis at the same time has reduced the expertise of the DI writ large because they require different kinds of mental operations that reduce the scope and scale of an analyst's research and knowledge. Robert Jervis once observed that "the informal norms and incentives of the intelligence community often form what Charles Perrow has called 'an error-inducing system.' That is, interlocking and supporting habits of the community systematically decrease the likelihood that careful and penetrating intelligence analyses will be produced and therefore make errors extremely likely."[30] Bureaucratic processes can contribute to the creation of this kind of "error-inducing system."

The Swinging Pendulum

For much of the DI's history, analysts acquired expertise by writing long reports. As former CIA officer Arthur Hulnick notes: "a great deal of research was being done, but ...much of it was done to enable the analyst to speak authoritatively on a current issue, rather than for publication."[31] Loch Johnson agrees, saying that "[t]he preparation of longer reports...is important, too, as ... a vital learning experience for analysts."[32] He adds that "[I]ntellectually most satisfying to the intelligence analyst is the full-blown research project, for it allows more room for the tracing of nuances. ... Under the Reagan administration, the [DI] established a research program...[in which] each of the ten [DI] offices...was told to redouble its efforts to produce solid research papers. In one nine-month period, more than 900 such reports were in progress... .[A]s Gates has claimed, 'the CIA is the only place where long-range research on national security issues is being done—two, five, ten, twenty years down the road. The Department of State Planning Staff conducts this kind of research only sporadically.'"[33]

By the early 1990s, however, long papers had become bureaucratized. In a 1993 article, former analyst Jay Young argued that "the needs of the policy-maker too often get lost in the time-consuming, self-absorbed and corrosive intelligence research production process. The DI's research program is run with the same rigid attention to production quotas as any five-year plan in the old USSR. ... This fixation on numerical production leads managers to keep analysts working away on papers whose relevance may be increasingly questionable. ... In short, too much of the Agency's longer-term research is untimely, on subjects of marginal importance and chock-full of fuzzy judgments." [34] He went on to

[30] Jervis, 34.

[31] Arthur S. Hulnick, "Managing Intelligence Analysis: Strategies for Playing the End Game," *International Journal of Intelligence and Counterintelligence* 2, no. 3 (1988): 322-323.

[32] Loch K. Johnson, "Analysis For a New Age," 665.

[33] Loch K. Johnson, "Making the Intelligence "Cycle" Work," 6-7.

[34] Jay T. Young, "US Intelligence Assessment in a Changing World: The Need for Reform," *Intelligence and National Security* 8, no. 2 (April 1993): 129, 134.

advocate a reduction in the number of long papers published each year. In short, although longer papers helped develop analytic expertise, bureaucratic tendencies had made their production increasingly irrelevant to policymakers.

In response to such criticisms, DI managers dictated that relevancy required shorter papers. In 1994, then-DDI Doug MacEachin limited "most DI analytical papers ... to 3 to 7 pages, including graphics and illustrations."[35] Shorter reports made the DI's analytical output more useful for policymakers, but analysts acquired less expertise on each topic. As a result, while the papers were more targeted, they contained fewer insights for the policymaker. Predictably, complaints then arose that the DI lacked the expertise necessary to do quality analysis. According to former DI analyst John Gentry in 1995:

> For reasons that heavily reflect its changing internal culture, CIA has begun to think much more myopically. It even claims now that it is emphasizing ''tactical'' projects and largely eliminated ''strategic'' work. In the DI, these terms are new ones for what formerly were ''current intelligence'' and ''research,'' respectively... The change is major and is formal policy...In other words, CIA has given up its former mission of trying to develop the analytic expertise and the information assets to forecast another Pearl Harbor in favor of collecting information to serve the analytic priority of drafting the short, pithy pieces for the National Intelligence Daily (NID) and other current intelligence publications...This change is enormous — and it is enormously irresponsible. ...[T]he failure to devote resources to long-term collection and to the development and maintenance of analytical expertise risks major surprises — and major intelligence failures — in the future.[36]

By 1997, DI management had admitted that the pendulum had swung too far and they were making efforts to address the decreased level of expertise. In 1997, then-DDI John McLaughlin noted that the DI's recent "impressive record of supporting the current intelligence needs of senior policymakers" made "an enormous claim on our personnel and resources" and the DI was "trying to balance the need for current support against the need to look ahead."[37] Since then the DI has emphasized acquisition of expertise, and funded opportunities for analysts to gain it by arguing that "[a]nother priority for intelligence analysis is to deliver a product that adds context and meaning to the raw intelligence. ...

---

[35] Center for Security Policy, "'Say It Ain't So, Jim': Impending Reorganization of CIA Looks Like Suppression, Politicizing of Intelligence," Publication No. 94-D74, 15 July 1994, URL: *http://www.security-policy.org/papers/1994/94-D74.html*, accessed October 2001.

[36] John A.Gentry, "A Framework for Reform of the U.S. Intelligence Community," 6 June 1995, remarks prepared for presentation to congressional intelligence committees, presented by the Federal of American Scientists at URL: *http://www.fas.org/irp/gentry/*, accessed October 2001.

[37] John E. McLaughlin, "New Challenges and Priorities for Analysis," *Defense Intelligence Journal* 6, no. 2 (Fall 1997): 17.

One of the ways to stay relevant is to build and maintain subject matter expertise, continuity, and depth within the analytical ranks."[38]

Losing Expertise to Gain Relevance

The swing of the pendulum that emphasizes policymaker relevance over analytic depth causes the DI to produce a large amount of current intelligence that prevents the acquisition and application of analytic expertise. Many analysts are facile data interpreters able to integrate large volumes of new information with existing knowledge, and interpret—based on underlying conceptual constructs — the significance of the new data in terms of its implications for U.S. foreign policymaking. This process provides policymakers with exactly what they are looking for from intelligence analysis. However, if provided with minimal time in which to integrate and process the information, the intelligence analyst by necessity cuts corners. When the DI emphasizes intelligence "on-demand," analysts meet the much shorter deadlines by reducing the scope and scale of their research as well as sidestepping the more laborious tradecraft procedures by not rigorously scrutinizing assumptions or comparing working hypotheses to competing explanations. Many times current intelligence analysis consists of a single hypothesis — derived within the first hour of the tasking — that the analyst intuitively believes provides the best explanation for the data. Current intelligence as a product has a lesser chance of being accurate because it lacks the self-conscious rigor that tradecraft entails even though it is the best that can be done under the press of quick deadlines.

The production of a single piece of current intelligence has limited effect on expertise because it draws on the knowledge and tools that an analyst has developed through training and prior analysis. However, if over time the analyst does not have the time to think, learn, or integrate new information with old to create new understandings, knowledge of facts and events may increase but the ability to interpret these events accurately decreases.

In a production environment attuned to the policymaker's current need for information, analysts will fail to apply the newly acquired expertise and instead will fall back to providing intuitive rather than structured analysis. Intelligence scholar Robert Folker observed that in his interviews of intelligence analysts a "repeated complaint was the analyst's lack of time to devote to thoughtful intelligence analysis. In a separate interview at CIA it was revealed that [intelligence analysts]... spend little time or effort conducting analysis."[39] Therefore, the effectiveness of expertise development programs in improving analytic accuracy may depend in part on whether the CIA is able to redress the overemphasis on short-term analysis. Balancing the swinging pendulum is easier to recom-

[38] McLaughlin, 18.

[39] Robert D. Folker, *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods*, Occasional Paper Number Seven (Washington, DC: Joint Military Intelligence College, January 2000), 12.

mend than to do since production of both extremes—long-term research and current intelligence support—may be necessary.

A Structural Fix?

If the DI remains true to form, at some time in the future the pendulum will swing too far toward knowledge-creation, papers will become longer and less relevant to policymakers. Perhaps there is a way to diagnose more accurately the cause of this swing and find a middle-ground that balances the trade-offs. The answer, however, does not lie in directives from the top that emphasize the utility or desirableness of one product type over another. These will likely just be encapsulated into the DI's SOPs and move the pendulum too far in the opposite direction. Instead, if CIA were to bifurcate its intelligence production system to specialize both in long-term research and current intelligence support, it would side-step the trade-offs between timeliness and accuracy that ultimately cause the pendulum to swing, and make the best use of any expertise-development program. Underlying this suggestion is a more strategic and nuanced approach to human resources management than CIA currently uses.

Just as there are different kinds of intelligence products requiring different levels of analytic ability, individual analysts possess varying cognitive strengths and weaknesses. As a senior DI analyst noted in an internal computer discussion in 1997, there may be two types of cognitive preferences — not "mutually exclusive"—that differentiate one kind of analyst from another: "Some people are better at...a broad range of issues, areas, and disciplines. These make the best current intelligence analysts because they generally are quick to learn an account. ... In simple terms, these are the people who are good at crafting a coherent story from a jumble of seemingly disconnected parts. ... Becoming an expert at this kind of analysis requires a great deal of experience. ... An expert of this type needs to continuously cast a net over a greater range of evidence and then relate it." He then goes on to add that it is better if this kind of analyst has experience on multiple accounts. Then he contrasts this expert generalist to "the other type of expert analyst...who concentrates on learning as much as possible about their chosen subject, area, or discipline. These are our specialists. They do the basic research, build our corporate knowledge base, and concentrate on depth rather than breadth. In the old days in the DDI, managers used to call these analysts the investors. They put money in the bank account which the current intelligence analysts draw out to spend. ... University study, technical training, language proficiency, and several years on an account are a necessity for developing the type of analytical expertise we need for our specialists."[40]

The DI appears to be remarkably blind to differentiation in both analysis and analysts, perhaps because it assigns tasks to "analysts" and equates the output with "analysis." As a result, "[w]e do not and never have used the term 'analysis' rigorously in the [IC]" according to Robert Bovey, formerly a special assistant to a DCI.[41] Robert Jervis

[40] CIA officer, "Two Types of Expert Analyst," DI Discussion Database, 28 March 1997.

illustrated the problems of equating the two in 1988 by arguing that "most political analysis would better be described as political reporting" and that instead of following an analytical approach "the analyst is expected to summarize the recent reports from the field—"cable-gisting." ... [T]he reporting style is not analytical—there are few attempts to dig much beneath the surface of events, to look beyond the next few weeks, to consider alternative explanations for the events, or to carefully marshal evidence that could support alternative views."[42] Jervis correctly differentiated the analytical intelligence product from its non-analytic cousin, but failed to distinguish between the analysts best suited for each. The DI — instead of differentiating between analysts — uses a one-size-fits-all recruitment, placement, training, and promotion strategy, and for the most part views analysts as interchangeable. As a result it has perennially had difficulty creating an appropriate mix of analytic abilities and skills for intelligence production when an issue or crisis develops. In particular, over time the shift in expertise corresponding to a preference for longer papers or shorter more current pieces is especially noticeable.

An intelligence production system bifurcated by product type would likely eliminate many of the problems inherent in the current system. In the early 1950s CIA intelligence production was organized by product type. The Office of Research and Reports produced basic intelligence, the Office of National Estimates provided forward-looking estimates, and the Office of Current Intelligence "produce[d] the President's daily intelligence publication," [43] according to the Agency's website. Resurrecting an Office of Current Intelligence to handle immediate requests and an Office of Research and Reports to do longer-term analytic papers could provide a self-selection mechanism useful for targeting an individual's cognitive strengths at the policymakers' intelligence needs. This structure would not promote the loss of expertise because different kinds of expertise would be applied to appropriate product types. However, this organizational structure would also require trade-offs-examined below—that would reduce regional expertise on the margins at the same time as it would allow the experts to increase theirs.

SECOND INTERVENING FACTOR: ORGANIZATIONAL STRUCTURE

The DI's organizational structure also influences which kind of analyst expertise is acquired and applied in finished intelligence products. Political scientist Thomas Hammond argues that organizational structure impacts analytic output. He employs information-flow models to demonstrate that—given the same information—one group of intelligence analysts organized by discipline would produce different analytic output than another group organized by region. He also concludes that it is impossible to

[41] Robert Bovey, "The Quality of Intelligence Analysis." *American Intelligence Journal* 3, no. 4 (Winter 1980-81): 7.

[42] Jervis, 34-35.

[43] CIA website, "Key Events in DI History," URL: *http://www.cia.gov/cia/di/history/*, accessed October 2001.

design a structure that does not impact output.[44] If we accept his argument, then organizational structure always affects internal information flows, and likely outputs as well. Theoretically, therefore, an organizational structure divided along disciplinary lines will accentuate learning of political, economic, military, or leadership methodologies through constant, interactive contact and awareness of the projects of other analysts.

However, regional or country knowledge is sacrificed due to the lack of such contact. In an office structured along geographic lines, the emphasis will be reversed. The 1998 India intelligence failure provides a good illustration of how organization can affect expertise. Prior to the 1996 creation of the National Imagery and Mapping Agency, imagery analysts had been distributed, by affiliation at least, throughout the Intelligence Community.[45] According to former CIA analyst Melvin Goodman, "the consolidation of all analysis of satellite imagery in (NIMA)...contributed to the intelligence failure. By placing all analysis of imagery inside the Department of Defense...there would be a minimum of the critical cross-discipline analysis required for difficult regional problems such as the political and military frictions in South Asia."[46] This episode may be considered an illustration of how trade-offs in expertise inherent in organizational structure can affect the DI as well.

Over the past 50 years the DI has been structured by product type, by discipline, and by region. From approximately the early 1960s to 1981, the DI was structured primarily by discipline with political, economic, military, and leadership offices each subdivided by geography. In 1981 "(a) (DI)-wide reorganization...shuffled most analysts and created geographically based, or "regional" offices out of the previous organization."[47] According to former CIA officer Arthur Hulnick: "These [new] offices combined political, economic, military, and other kinds of research under "one roof," thus making more detailed analytic research feasible. After some grumbling, the new offices began to turn out the in-depth products consumers had been seeking, while still providing current intelligence materials."[48] This integration of analytic disciplines in regional offices provided a more productive interpretation of the forces at work within a target country or region but also negatively affected the DI's ability to maintain disciplinary knowledge.

The 1995 dismantling of the DI's Office of Leadership Analysis (LDA) provides a good case study into the trade-offs between disciplinary and regional expertise resulting from differing organizational arrangements.[49] Since at least 1963 the CIA has consolidated biographic information on foreign leaders, and over time the value of leadership analysis as a complement to political, economic, and military analysis became evident.[50]

---

[44] Thomas H. Hammond, "Agenda Control, Organizational Structure, and Bureaucratic Politics" *American Journal of Political Science* 30, no. 2 (May 1986): 379-420.

[45] CIA website, "National Imagery and Mapping Agency," URL: *http://www.cia.gov/ic/nima.html*, accessed October 2001.

[46] Melvin A. Goodman, "US Intelligence Failure Shows Need for Reform," *Christian Science Monitor*, 18 May 1998, URL: http://www.csmonitor.com/durable/1998/05/18/p11s1.htm, accessed October 2001.

[47] Gentry, URL: *http://www.fas.org/irp/gentry/*, accessed October 2001.

[48] Hulnick, 323.

Analysis grounded in the theory of political psychology provided insight into a leader's behavior above and beyond the limited biographic scope of a leadership profile.[51] LDA was thus created to develop and consolidate the discipline of leadership analysis and put it on a near-equal basis with the other established analytic disciplines. However, in 1994, then-DDI Doug MacEachin reorganized LDA — the only disciplinary office left — out of existence as part of "downsizing the DI."[52] Political factors may have played a part in this decision. The Clinton Administration's Haiti policy was greatly complicated by partisan opposition in the wake of a leaked leadership profile produced by LDA that questioned the psychological stability of Jean Bertrand Aristide.[53] In any case, LDA's elimination had an impact on the expertise of the DI's leadership analysts.

The regional offices swallowed LDA as its component units were assigned to the relevant regional office. Some regional offices kept leadership analysts together as a team so as to maintain the disciplinary knowledge developed in LDA. Other offices broke leadership teams apart and assigned individual analysts to join multi-disciplinary country teams. The distribution of what had previously been centralized knowledge of analytic tools, specialized product formats, and disciplinary theory throughout the DI meant that new leadership analysts were not well trained in their discipline. These new analysts relied solely on the fast-dissipating knowledge of the handful of former LDA officers who happened to be assigned to their team or issue. In addition, actual physical co-location did not occur for months — and in some cases years — due to lack of space in CIA's overcrowded headquarters building. As a result of being "out of sight, out of mind," leadership analysts were frequently not informed of ongoing projects, briefings, and meetings, and such incidents had a negative impact on the finished analytical product. When leadership analysts were not included in briefings, the DI risked failing to keep its consumers fully informed of both leadership dynamics and changes within the country or region. In addition, products published and disseminated without coordination at times contained factual errors such as the wrong names or positions for foreign government officials, or distortions in analysis due to the lack of leadership analyst input. However, once re-organization occurred, regional counterpart analysts became team members, and after a shaking-out period began to incorporate leadership analyst contributions into their products more easily. In fact, the close interaction with other members of the regional team led to a better incorporation of leadership analysis into regional products than had occurred during the heyday

[49] The information herein on LDA is derived from personal experience as a leadership analyst from 1996 to 1998.

[50] CIA website, "Key Events In DI History," URL: *http://www.odci.gov/cia/di/history/index.html*, accessed October 2001.

[51] Thomas Omestad, "Psychology and the CIA: Leaders on the Couch," *Foreign Policy* 95 (Summer 1994): 105-122.

[52] CIA website, "Key Events In DI History," URL: *http://www.odci.gov/cia/di/history/index.html*, accessed October 2001.

[53] Center for Security Policy, URL: *http://www.security-policy.org/papers/1994/94-D74.html*, accessed October 2001.

of LDA. Therefore, the elimination of a leadership analysis-based office resulted in both increased incorporation of leadership analysis and insight into the regional teams' products, and decreased corporate knowledge and expertise in leadership analysis as a discipline. The same occurred for the other disciplines when their respective offices were eliminated in 1981.

PUTTING THE PIECES TOGETHER AGAIN

By the mid-1990s DI analysts were realizing that while multi-disciplinary analysis on country teams made for better integration of disciplines, it also led to the dissipation of disciplinary knowledge. Former LDA analysts' efforts to sustain their hold on disciplinary knowledge triggered similar efforts by political, economic and military analysts to both sustain and reconstruct occupational-specific knowledge. Without the framework of structural organization to bind each discipline together, over time they had each grown apart.

To rectify this loss of disciplinary expertise, in 1997 the DI created the "senior-level" Council of Intelligence Occupations (CIOC) with the initial intent of disciplinary "workforce strategic planning...in the areas of recruitment, assignments, and training" as well as "identify[ing] core skills and standards for expertise in the [DI]."[54] In practice, CIOC became a home for senior analysts interested in learning and teaching their discipline's methodologies. They "establish[ed] a professional development program for all DI employees that provides explicit proficiency criteria at each level so that everyone can see the knowledge, skills, and experiences required for advancement within each occupation or across occupations."[55] All this was done—according to the CIA website — "so that the DI has the expertise needed to provide value-added all-source analysis to its customers."[56] CIOC emphasized disciplinary training as a method to achieve this goal. As the CIA's website notes, "(t)he Council views learning and skills development as an essential part of work and the means whereby employees can respond to changes in customer priorities and the external environment."[57] In 2000, CIOC was disbanded although its training functions have been incorporated into the DI's Kent School and its other knowledge has been distributed elsewhere within the DI.

There may be no easy solution to the expertise trade-offs inherent in organizational structure. By definition, the structure will create synergies in the areas emphasized but the opportunity cost of doing so means losing the synergies in other areas. At bottom this

---

[54] McLaughlin, 18.

[55] CIA website, "Directorate of Intelligence Organizational Components, Council of Intelligence Occupations," URL: *http://www.cia.gov/cia/di/mission/cioc.html*, accessed October 2001.

[56] CIA website, "Directorate of Intelligence Organizational Components, Council of Intelligence Occupations," URL: *http://www.cia.gov/cia/di/mission/cioc.html*, accessed October 2001.

[57] CIA website, "Directorate of Intelligence Organizational Components, Council of Intelligence Occupations," URL: *http://www.cia.gov/cia/di/mission/cioc.html*, accessed October 2001.

is a prioritization issue: the organizational structure should reflect the dynamic that the DI leadership believes will most directly benefit its policymaker consumers. Establishing secondary institutions like CIOC or disciplinary training through the Kent School to bolster the lost expertise may be the only way to preserve knowledge that otherwise would be lost.

TO THE FUTURE

Expertise-development programs that create the potential to improve overall analytic accuracy—such as formal training in methodologies, regions, disciplines, or languages, or informal training resulting from greater overseas experience—do not provide much in the way of improvement if in fact the DI's business practices prevent application of this hard-earned expertise. CIA's leaders should continue to pursue ways to increase analyst expertise, for they could contribute to increased analytic accuracy. Yet at the same time the DI must adapt its practices to leverage the potential improvements of these programs if the CIA is to provide its policymaking customers with the intelligence they need now and in the future. The creation of a bifurcated production process might remove an impediment preventing acquisition and application of expertise, but other reforms may be necessary as well.

The CIA was created in the wake of the Japanese attack on Pearl Harbor to coordinate and integrate intelligence information and provide strategic warning should any foe of the United States choose to attack. With respect to the September 2001 attacks on the U.S.—it is still too soon to determine whether the CIA's failure to provide specific warning lay in organizational inefficiencies, collection gaps, analytic missteps, or in some combination of the three. Regardless, improvements in intelligence analysis must occur so as to provide policymakers with warning of any potential future attacks while preventing surprises on issues of national security importance. Managing the DI so that it can produce accurate intelligence will require an accurate assessment of the DI's current capabilities, an understanding of its limitations, and creative approaches to overcome them. Current DI business practices entail tradeoffs that prevent full actualization of the DI's potential. Perhaps through serious study the constraints that the DI's working environment imposes on analytic expertise will be understood and overcome. As Robert Jervis declares, "(w)e will never be able to do as well as we would like, but this does not mean that we cannot do better than we are doing now."[58]

BIBLIOGRAPHY

Asker, James R. "Same Ol', Same Ol'." *Aviation Week and Space Technology*, 8 June 1998: 21.

Betts, Richard K. "Analysis, War and Decision: Why Intelligence Failures Are Inevitable. *World Politics* 31, no. 1 (October 1978): 61-89.

Betts, Richard K. "Policy-Makers and Intelligence Analysts: Love, Hate or Indifference?'"

[58] Jervis, 30.

Intelligence and National Security 3, no. 1 (January 1988): 184-189.

Bovey, Robert. "The Quality of Intelligence Analysis." *American Intelligence Journal* 3 no. 4 (Winter 1980-81): 6-11.

Center for Security Policy. "'Say It Ain't So, Jim': Impending Reorganization of CIA Looks Like Suppression, Politicizing of Intelligence." Publication No. 94-D74, 15 July 1994. Available at URL: *http://www.security-policy.org/papers/1994/94-D74.html*. Accessed October 2001.

CIA officer. "Two Types of Expert Analyst," DI Discussion Database, 28 March 1997.

CIA website. "Directorate of Intelligence Organizational Components, Council of Intelligence Occupations," URL: *http://www.cia.gov/cia/di/mission/cioc.html*. Accessed October 2001.

CIA website. "Intelligence Disciplines." URL: *http://www.odci.gov/cia/di/work/disciplines.html*. Accessed October 2001.

CIA website. "Jeremiah News Conference." URL: *http://www.cia.gov/cia/public_affairs/press_release/archives/1998/jeremiah.html*. Accessed October 2001.

CIA website. "Key Events In DI History." URL: *http://www.odci.gov/cia/di/history/index.html*. Accessed October 2001.

CIA website. "National Imagery and Mapping Agency." URL: *http://www.cia.gov/ic/nima.html*. Accessed October 2001.

CIA website. "Remarks of the Deputy Director of Central Intelligence John E. McLaughlin at the Conference on CIA's Analysis of the Soviet Union, 1947-1991, Princeton University 9 March 2001." URL: *http://www.cia.gov/cia/public_affairs/speeches/ddci_speech_03092001.html*. Accessed October 2001.

CIA website. "Remarks of the Director of Central Intelligence George J. Tenet at the of the Sherman Kent School, 4 May 2000." URL: *http://www.cia.gov/cia/public_affairs/speeches/archives/2000/dci_speech_05052000.html*. Accessed October 2001.

CIA website. "The Role and Mission of the Directorate of Intelligence." URL: *http://www.odci.gov/cia/di/mission/mission.html*. Accessed October 2001.

Colby, William. "Retooling the Intelligence Industry." *Foreign Service Journal* 69, no. 1 (January 1992): 21-25.

Davis, Jack. "Improving Intelligence Analysis at CIA: Dick Heuer's Contribution to Intelligence Analysis," in "Introduction" to *Psychology of Intelligence Analysis*, Richards J. Heuer, Jr. (Washington, DC: Center for the Study of Intelligence, 1999), xix.

Folker, Robert D. *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods*, Occasional Paper Number Seven (Washington, DC: Joint Military Intelligence College, January 2000).

Garst, Ronald D and Max L. Gross. "On Becoming an Intelligence Analyst." *Defense Intelligence Journal* 6, no. 2 (1997): 47-59.

Gentry, John A. "A Framework for Reform of the U.S. Intelligence Community." Remarks prepared for presentation to congressional intelligence committees, 6 June 1995. Available on the Federation of American Scientists webpage at URL: *http://www.fas.org/irp/gentry/*. Accessed October 2001.

Goodman, Melvin A. "US Intelligence Failure Shows Need for Reform." *Christian Science Monitor*, 18 May 1998, 11. URL: *http://www.csmonitor.com/durable/1998/05/18/p11s1.htm*. Accessed October 2001.

Hammond, Thomas H. "Agenda Control, Organizational Structure, and Bureaucratic Politics." *American Journal of Political Science* 30, no. 2 (May 1986): 379-420.

Heuer, Richards J. Jr. "Improving Intelligence Analysis: Some Insights on Data, Concepts and Management in the Intelligence Community." *The Bureaucrat* 8, no. 1 (Winter 1979/80):2-11.

Hitz, Frederick P. "The Future of American Espionage." *International Journal of Intelligence and Counterintelligence* 13, no. 1 (2000): 1-20.

Hulnick, Arthur S. "Managing Intelligence Analysis: Strategies for Playing the End Game." *International Journal of Intelligence and Counterintelligence* 2, no. 3 (1988): 321-343.

Jervis, Robert. "What's Wrong with the Intelligence Process?" *International Journal of Intelligence and Counterintelligence* 1, no. 1 (1986): 28-41.

Johnson, Loch K. "Analysis For a New Age." *Intelligence and National Security* 11, no. 4 (October 1996): 657-671.

_____. "Making the Intelligence 'Cycle' Work." *International Journal of Intelligence and Counterintelligence* 1, no. 4 (1986): 1-23.

Loeb, Vernon. "CIA's Analysis Becomes Transnational." *Washington Post Online*, 2 April 2001. URL: *http://www.washingtonpost.com/ac2/wp-dyn?pagename=article&node=&contentId=A16925-2001Mar30*

MacEachin, Douglas J. and others. *The Tradecraft of Analysis: Challenge and Change in the CIA*. Washington, DC: Consortium for the Study of Intelligence, 1994.

McLaughlin, John E. "New Challenges and Priorities for Analysis." *Defense Intelligence Journal* 6, no. 2 (Fall 1997): 11-21.

Marrin, Stephen. "Complexity is in the Eye of the Beholder," DI Discussion Database, 6 May 1997.

Omestad, Thomas. "Psychology and the CIA: Leaders on the Couch." *Foreign Policy* 95 (Summer 1994): 105-122.

Robbins, Carla Anne. "Failure to Predict India's Tests Is Tied to Systemwide Intelligence Breakdown." *Wall Street Journal*, 3 June 1998, A8.

Turner, Stansfield. "Intelligence for A New World Order." *Foreign Affairs* 70, no. 4 (Fall 1991): 150-166.

Watanabe, Frank. "Fifteen Axioms for Intelligence Analysts." *Studies in Intelligence*. Unclassified edition, 1997. Available at URL: *http://www.odci.gov/csi/studies/97unclass/axioms.html*. Accessed October 2001.

Weiner, Tim. "Naivete at the CIA: Every Nation's Just Another U.S." *New York Times: Week in Review*, 7 June 1998, 5.

Weiner, Tim. "U.S. Blundered on Intelligence, Officials Admit." *New York Times*, 13 May 1998, A1, A14.

White, Ralph K. “Empathy As an Intelligence Tool.” *International Journal of Intelligence and Counterintelligence* 1, no. 1 (Spring 1986): 57-75.

Young, Jay T. “US Intelligence Assessment in a Changing World: The Need for Reform.” *Intelligence and National Security* 8, no. 2 (April 1993): 125-139.

ABOUT THE AUTHOR

Lt Col Tom Garin, an Air Force officer assigned to the National Reconnaissance Office (NRO), arrived at the Joint Military Intelligence College in September 1999 to occupy the General Thomas S. Moorman, Jr. Chair for National Reconnaissance Systems. He has taught graduate-level core and elective courses on missiles and space systems, structured techniques for intelligence analysis, and research methodologies, as well as an undergraduate core course on space systems. Prior to this post, Lt Col Garin was Chief, Organizational Development at the NRO. There, he used a balanced scorecard approach to link human resource policies with the overall NRO mission. He also worked part-time for Vice President Gore's National Performance Review on a performance measurement benchmarking study team to help government agencies prepare for the Government Performance and Results Act. In addition, he completed special projects as directed by the Assistant Secretary of the Air Force for Space.

Lt Col Garin received a B.S. in Operations Research (OR) from the United States Air Force Academy in 1982, a M.S. in OR from the Air Force Institute of Technology in March 1990, and a Master of Public Administration from the University of Southern California (USC) in May 2001. He is currently in the Doctorate of Public Administration program at USC.

APPRAISING BEST PRACTICES IN DEFENSE INTELLIGENCE ANALYSIS

Thomas A. Garin, Lt Col, USAF

An adaptable organization is one that has the capacity for internal change in response to external conditions. To be adaptable, organizations must be able to learn. Organizations can learn by monitoring their environment, relating this information to internal norms, detecting any deviations from these norms, and correcting discrepancies. The National Foreign Intelligence Community at large learns by collecting necessary information, analyzing the information, and disseminating it to users who in turn hold the option to influence collection decisions. A telling aspect of any knowledge organization is the way in which it manages its information.

Knowledge management can equip intelligence organizations for the fast-paced, high-technology information age. By building upon the best aspects of total quality management, and observing the criteria for performance excellence adopted for the Baldrige National Quality Program, managers can theoretically lead professionals to work together effectively as a group in a situation in which their dealings with one another affect their common welfare. In this paper, Baldrige criteria guide an "insider's" exploration of how a set of senior intelligence officers of the Defense Intelligence Agency do intelligence analysis.[1]

STUDY DESIGN

The DIA is expected to ensure the satisfaction of the full range of foreign military and military-related intelligence requirements of defense organizations, UN Coalition Forces, and non-defense consumers, as appropriate. Specifically, DIA supports: (1) joint military operations in peacetime, crisis, contingency, and combat; (2) service weapons acquisition; and (3) defense policymaking. In the past fifteen years, several analysis and production units within DIA have received prestigious awards demonstrating the confidence and appreciation that senior U.S. leaders have in the agency's performance. On the basis of these observations, a case could be made that DIA has become a world-class organization for meeting U.S. military intelligence requirements. Clearly, the DIA is a worthy organization to examine for evidence of how quality intelligence analysis can be carried out.

---

[1] The three essential characteristics of operations research are (1) systems orientation, (2) use of interdisciplinary teams, and (3) adaptation of the scientific method. The Baldrige criteria provide a similar function for assessing information organizations. From a systems perspective, the Baldrige criteria focus on a leadership triad and a results triad. Activity by leadership affects results and the results, in turn, affect the future activity of leadership. From a team perspective, the Baldrige criteria focus on the multiple lens of leadership, the customers or consumers, and the analysts to gain a complete understanding of its operations. Lastly, the Baldrige criteria focus on information and analysis, emphasizing a fact-based, scientific approach, to serve as a foundation for the performance management system.

A Typical Office

A typical analysis office consists of a manager, the senior intelligence officer (SIO), analysts, liaison officers, and administration/technical support staff. The manager handles a set of processes common to many organizations such as planning, organizing, staffing, directing, coordinating, reporting, and budgeting. The SIO is a senior analyst, a subject matter expert on a grand scale, and is responsible for the content of the analytical product. A typical SIO approves all finished intelligence products, coordinates budget to contract external studies, and is the unit's chief training officer. Analysts tend to be subject matter experts and are accustomed to using technology to support analysis. Liaison officers connect the analysis office either to operational forces in the field or to other organizations in the Intelligence Community. The administration/technical support staff provide a variety of functions such as disseminating the finished intelligence product, providing graphic support, and arranging travel.

Consumer Groups

Analysts produce intelligence for a number of different consumer groups.[2] These consumer groups include: (1) civilian and military policymakers; (2) military planners and executors; (3) acquisition personnel responsible for force modernization; (4) diplomatic operators; and (5) intelligence operators. Consumer groups specific to DIA analysts include (1) DIA leadership such as the Director, DIA, and the Director of Intelligence (DI); (2) Pentagon senior leadership such as Generals on the Joint Staff, other Generals in the Pentagon, and senior civilians; and (3) senior leadership in the field such as the Combatant Commanders.

Participants

This intelligence analysis benchmarking study is the result of a class project for the Joint Military Intelligence College's graduate-level course ANA 635, "Structured Techniques for Intelligence Analysts." This course helps students understand and apply descriptive and quantitative methodologies to intelligence analysis. Students were from the U.S. Air Force, U.S. Army, U.S. Navy, National Reconnaissance Office, National Imagery and Mapping Agency, and Defense Intelligence Agency. The study team worked

---

[2] A useful distinction may be drawn between "consumers" and "customers" of intelligence. Customers are those who must "pay" for the intelligence service by providing liaison officers or participating in the intelligence process in a way that drains away part of their own organization's resources. Consumers are those who are entitled to receive either standard or tailored analytic products, including briefings, but who do not find it necessary to obligate any of their own resources to its production. DIA offices typically do not recognize this distinction, and individual analysts are known to scoff at the notion that anyone for whom they provide an analytic product is a "customer" because of a perception that those who use a product are "professionals" in a sense that transcends the representation of value in dollar terms.

with five analytic units within DIA that have demonstrated excellence. The SIOs and others who met with the research team had a combined total of over 100 years of experience in intelligence analysis or related areas.

Process

The team followed established benchmarking procedures in conducting this study, which included on-site visits and interviews with members of each unit. The study team adopted a "systems" perspective that isolated the concepts of leadership, strategic planning, consumer focus, information and analysis, people and resources, process management, and mission accomplishment. Taken together, these seven elements define an organization (or a unit within a larger organization), its operations, and its performance. The information and analysis category is especially critical to the effective management of an information organization like DIA.

Exemplary Intelligence Offices

Based on their experiences, members of the JMIC faculty recommended a number of offices in the Defense Intelligence Agency as suitable interview venues for this project. The students in a structured analytic techniques class chose a subset of the organizations based on their interest in the organization. The class size limited the number of organizations that could be included in the study. Also, once officials became aware of the project and the nature of the information required, certain offices deselected themselves from the project based on their estimated lack of ability to contribute in a meaningful way. Other organizations were not available to meet with us during our limited schedule, the last few weeks of the spring quarter.

The study team visited a total number of five analysis-related organizations. Three of the organizations reside in the Directorate for Intelligence (DI). The J-2 representative who was interviewed was from a fairly small office within a much larger J-2 analysis office. He had experience in other DIA analysis offices. The JMIC respondent represented a relatively small number of faculty members with past analysis experience. Of the three DI offices, the TWC is a relatively large analysis office. The OICC, on the other hand, is a relatively small analysis-related shop that draws from the analysts within the DI to meet its mission requirements in a crisis situation. Like the OICC, the OSJ-2 is a relatively small analysis shop.

1. **Directorate for Intelligence (J2):** JCS/J-2 provides indications and warning, crisis and current intelligence support to the Office of the Secretary of Defense (OSD), the Chairman of the Joint Chiefs of Staff (JCS), Joint Staff offices, and to the Unified Commands. The J2 represents intelligence requirements of the Unified Commands, writes joint intelligence doctrine, and directs intelligence, surveillance, and reconnaissance-based assessments for the Joint Requirements Oversight Council, and the Joint Staff Director-led Joint Warfighter Capabilities Assessment teams that perform detailed assessments of programmatic alternatives, tradeoffs, risks, and effectiveness.

2. **Joint Military Intelligence College (JMIC):** The College educates military and civilian intelligence professionals and conducts and disseminates intelligence-related research.

Directorate for Intelligence Production (DI): This division manages the production of military intelligence throughout the General Defense Intelligence Program. Its products respond to intelligence needs of the OSD, JCS, Unified Commands, military services, and other U.S. government agencies. Specifically, offices for which information is developed here are:

3. **Office for Counterterrorism Analysis (TWC):** Supports the Transnational Warfare Group's efforts to detect, characterize, and assess vulnerabilities of adversary capabilities for emergent counterterrorism opportunities. TWC manages and produces all-source-intelligence in support of warfighter, policy, and acquisition communities.

4. **Operational Intelligence Coordination Center (OICC):** Exists as the focal point for crisis and contingency intelligence production within the DI. In this capacity, the OICC operates around the clock and supports the timely production and dissemination of all-source intelligence for DIA's strategic, operational, and tactical-level consumers. This effort includes the management of all intelligence taskings, requests for information, and personnel augmentation requests.

5. **Operational Environment Analysis Division (OSJ-2):** Initiates, oversees, and coordinates all-source military geographic (terrain, cultural and demographic) intelligence analysis and production required to support crisis, operational, and contingency planning efforts of the National Command Authorities (Secretaries of Defense and State), the JCS, Unified Commands, and deployed forces.

THE EVALUATION CRITERIA

The Malcolm Baldrige National Quality Improvement Act of 1987, Public Law 100-107, provides for the establishment and conduct of a national quality improvement program under which awards are given to organizations that practice effective quality management. The Act established the Malcolm Baldrige National Quality Award. In implementing this Act, the National Institute of Standards and Technology makes available guidelines and criteria designed for use by business, education and health care organizations for self-evaluation and improvement of their competitive positions.[3] In this paper, the NIST criteria are applied to DIA, under the premise that a U.S. government organization, through its component offices, could benefit from a systematic evaluation of its "competitive" position; namely, its ability to develop and maintain agility in a change-intensive environment.

---

[3] For background information, please see the website at URL: http://www.quality.nist.gov/.

LEADERSHIP

Leaders influence others to accomplish a mission by providing purpose, direction, and motivation. Baldrige leadership criteria apply to how the analysis organization's leader assigns tasks, interacts with analysts, and provides feedback. Within these three aspects of leader-analyst relationship, there appears to be a tension between initiative on the part of the analyst and direction on the part of the leader.

Task Assignment

Initiative. In many offices, analysis is self-generated. The office leader assigns each analyst to an area of the world and constantly pushes for finished products. The analyst is expected to act on his own initiative, do the analysis, and produce articles. In this scheme, there really is no clear top-down tasking process. One subject observed that leaders need to do a better job of prioritizing analysts' work because, even as analysts assemble data to put in databases, create briefings and produce finished intelligence products, they often write on relatively insignificant items. Their workload is usually events-driven. Consumers call in to their office and request certain information. The analysts attempt to tell the consumer what they don't already know. Their work may not always reflect the consumer's interests. To counter this tendency, some subjects maintain, managers need to incorporate a perspective on vital national interests into their analysts' tasks.

Another subject identified two ways in which analysis tasks are self-generated. In one, the analyst submits a formal proposal to do general research and, if approved, then does the work. In the second, the analyst submits a more structured proposal to study a region of the world by looking forward perhaps about 10 years. If approved, the analyst in this case identifies problems, examines them, and synthesizes them into most important issues. A problem and its attendant issues could become the basis for a National Intelligence Estimate (NIE).[4]

One subject noted that in a crisis situation, the analyst who answers the phone gets the job. For example, if the phone call comes at 1600 hours on Friday, then the analyst who has answered the phone would work with the consumer through the weekend if necessary. The study team thought that it might be difficult getting an individual to answer the phone on Friday afternoon. The subject, however, assured us that that was not the case. Indicative of the personal sense of responsibility and initiative felt by analysts, he asserted that they would actually want to get the phone call regardless of the time.

The self-generated analysis may have certain implications. First, the analysts may be doing analysis that serves the personal interest of the analyst, but does not meet a military leader's or other policymaker's requirements. Second, the analyst may be focusing atten-

[4] It is not uncommon for one of the National Intelligence Officers, who are the senior Intelligence Community experts on discrete topics, and who coordinate the production of NIEs, to visit with an individual analyst, or with small groups of analysts, to discuss such problems and issues.

tion on analysis projects that are the easiest or quickest to publish, satisfying a need of the analysis office, rather than producing analysis that is most beneficial to the Intelligence Community. Third, the analyst may focus on easier problems that reside in the short-term instead of tougher future-oriented problems in order to give the appearance of being more productive by producing more intelligence.

Directive. Each office leader tends to have a different method for assigning analysis tasks. In one office, the division chief ultimately assigns all tasks, regardless of the way the request comes into the subordinate office. Tasks come into an office through a "world-wide" collection management system, through internal DIA processes, through informal telephone calls from consumers, and through person-to-person memoranda. This practice may at times introduce some confusion in the office. For example, the leader may have a problem deciding whom to task. It may be appropriate to task the in-house analyst working in that area of the world, a member of a crisis response team, or a terrorist analyst.

There are certain implications when a leader directs an analyst to work a certain issue or problem. First, the leader may not be able to assign the "best" analyst because of workload. The best analyst may simply have too many projects on his or her plate or may have some other reason for making himself or herself unavailable. Second, the leader may assign a project to the wrong individual. The leader may not know who the right analyst is for a certain type of problem or issue. Third, the leader, by being too directive, may stifle the analysts' own creativity or initiative by keeping the analyst too busy.

Leader and Analyst Interaction

Initiative. Most interview subjects agreed that leaders from inside or outside their office do not interfere with the analyst's work. They provide oversight only when the analyst asks for it because analysts do not like to be micro-managed. Each manager considers his or her analysts subject matter experts. They may ask the analyst, "are you finished yet?" or "do you need help on A/B/C?" For additional support, analysts often appeal to other experts as needed.

The SIO for an office gets involved only if an analyst brings an issue or question to him. Sometimes, the SIO walks around the office, talks to the analysts, and looks for ways to help obtain certain information. The SIO gets formally involved in the analytic process, however, when the analyst has created the final product. Usually, it has been coordinated through the analyst's peers before it gets to the SIO. The SIO makes any substantive reformatting corrections before the final product can leave the office.

Directive. Usually during a crisis situation, there is face-to-face interaction between an office leader and analysts from the moment the requirement appears until it is met. One subject agreed that there should be a constant exchange of information between the leader and the analyst even during routine analysis. Some leaders are better at it than others. The lower level managers in their office worked directly with the analysts. Usually, they assign an analyst a project, discuss with them how to do it, and continually ask them how they are doing. Another subject described the production process this way: the analyst

produces, the boss does a sanity-check review; the analyst coordinates his or her work with other staffs, and they suggest changes.

Feedback

Initiative. The interaction between leadership and the analyst during feedback sessions varies from office to office. It usually follows a similar pattern: the analyst produces his or her findings, managers review the work; analysts make the recommended changes, and analysts coordinate the work with appropriate offices. In some cases, the analyst decides who should coordinate on his or her analysis. Competition between offices impedes the coordination process. One subject regrets that neither top-down guidance nor tools exist to support the coordination process.

One subject said all input from leaders and peers comes after the analysis is done. As a result, the usual case is for the assessment in the final product to be conceptually close to the analyst's own findings. Once the feedback process concludes, analysts are free to post their finished products on the electronic "broadcast" media. It is usually the case that one person from an office will post products on Intelink.[5] One office included in this study posts approximately 100 products per year on Intelink. An analyst may also send a copy directly to the consumer, or may inform specific consumers of its URL. As feasible, the product will be "downgraded" to a lower classification level by obscuring sources or methods to enable it to reach a wider audience on different electronic systems.

In one office, analysts put together products on an ad hoc basis to answer requirements from consumers. Finished products are normally briefings with supplemental documents—like maps or targeting materials—published either on the shop's website or forwarded to the consumer by email or hard copy. Another method of answering a requirement is to post the answer back into the production requirements system. In one office, leaders do not actively provide formal feedback to the analyst who puts the package together. Informally, however, the shop's leader will likely be tracking the progress the analyst is making in completing the tasking by checking the finished product before it is published in any format.

Directive. After completing the analysis, the analyst will normally present his or her information to a team chief or SIO for coordination. After considering the revisions, the SIO will give the analyst permission to send written findings forward. Because this information may appear unaltered in the U.S. President's read book, an SIO does not hesitate to "wordsmith. This feedback may be frustrating and humiliating for the analyst. The SIO may direct the analyst to fix the logical development of an argument or to present more and better data. Some analysts will simply rework their product and resubmit it to the SIO. Others, however, will discuss the comments with the SIO. The SIO typically prefers the latter method because the analyst will usually understand the comments better and

[5] Intelink is the Community's intranet, hosting "value-added" intelligence products.

will learn more from the experience. Almost all of the products go to their consumers; only rarely will a product be killed within the analyst's office.

Leaders tend to squelch any negative commentary on U.S. information operations (IO) issues. Their attitudes reflect an Intelligence Community-wide aversion to discussing IO problems associated with the U.S. or "blue" force. Intelligence analysts are free to discuss "red" force issues, but only military operations officers or "operators" are free to discuss "blue" force issues. As a result, decisionmakers must learn to seek information about the "blue" force from one source and information about the "red" force from another. They must combine the information themselves in order to get a full picture of the situation.

One subject suggested that ideally the analyst can encourage short, regular feedback sessions from the manager on an informal basis. For example, if the boss wanted a briefing for a future meeting, the analyst could give him some draft charts well ahead of time and expect nearly immediate feedback. In practice, however, the boss often edits only the final charts and returns them to the analyst who is forced under pressure of time to make the necessary changes. Interview subjects frequently alluded to this problem, and opine that such feedback issues remain a problem. Interview subjects nevertheless offered the following examples of good, direct feedback. First, an individual who was quite good at making changes would eliminate unnecessary words, shortening the report and making the wording much tighter. The analysts expressed appreciation of this feedback because of the value added to the product. In the second example, a manager was very good at grooming new managers. He would receive an analyst's report, then hand it to another analyst to review and comment. In this way, subjects noted, he was developing new leaders.

Comments

Good leadership demands high quality products to inform warfighters and policymakers. Leaders need analysis to answer tough questions. At the same time, managers need to keep in mind important questions about the analysis process itself:

- Are military leaders able to do their job better because of their analyst's product?
- Are the benefits of doing the analysis outweighing the costs?
- Are we doing risk analysis? That is, are we attempting to understand the balance between threat and vulnerabilities by examining local trade-offs?

Good leadership ensures a value-added coordination process. Analysts often find the coordination process tough. One subject said that before the first draft, the analyst's job was the best job. After the first draft, however, the analyst's job was difficult. Another subject called into question the coordination process because of the low quality of finished products posted in the database. Another subject said the coordination process is a humbling experience for the analyst because it is tough to get back your paper marked up with corrections. One subject said a co-worker tested the system. He worked really hard on one project and sent it forward. Next time, he slapped something together and sent it forward.

He noticed that it didn't make any difference either way. He was devastated. There was no motivation to excel. From these testimonials, one could conclude that unsystematized (non-standard) coordination may hinder the work of analysts.

Good leadership theoretically removes such barriers to effective use of analytical resources by providing leading-edge administrative and computer support; quick-turn-around graphics support for urgent tasks; and hassle-free travel support. One subject compared DIA administrative support unfavorably with what he grew to expect when he worked for the Central Intelligence Agency. He could drop something off at 5PM for graphics support and pick it up when he got to work in the morning. When he traveled, his proactive travel office would remove some of the hassles associated with traveling. He would tell someone in the travel office where he needed to go. They would call him back a short time later with all the information he needed to know about the trip. Then, when he got back from his trip, he told them what he did and they reimbursed him. There were no required travel reports and no receipts. In fact, they told him to get rid of all his receipts. In case he was caught; it would be better for no one else to know where he had been! One reason the DIA may be different is the fact that the CIA focuses more on covert operations than the DIA. Another reason is that DIA, a DoD organization, has stricter accountability rules and regulations than the CIA. As a result, the DIA analysts must do a better job of documenting their trip for accountability purposes. It would probably not be possible for the DIA to adopt the CIA process without some changes in the laws that govern travel accountability.

Good leadership intervenes to handle sensitive, political aspects of a job. Leaders may be able to supply the needed leverage or "muscle." For example, a limited number of analysts may be qualified to handle issues in a crisis situation. A trade-off may need to be negotiated between support for the warfighter and support for senior policymakers in the Pentagon, all within the Department of Defense. Further, leaders may need to intervene to facilitate interaction between the analyst and consumers in order to ensure that analysts anticipate and meet their consumers' priorities.

Summary

Leadership is a critical aspect in determining the success of the intelligence analysis process. Leadership demands high-quality products, ensures a value-added coordination process, removes technical or administrative barriers, and intervenes when needed. Some leaders assign tasks directly to the analysts. Others rely on the Senior Intelligence Officer (SIO) to assign tasks or rely on the initiative of the analysts themselves to seek out the right problems and analyze them. Leadership tends to provide little or no interaction during the analysis process except if and when the analyst seeks it. Analysts do not like to be micro-managed. In a crisis situation however, the leader takes a more direct and hands-on approach. Although feedback varied from office to office, ideally the analyst should seek short, regular feedback on an informal basis with the office leader.

STRATEGIC PLANNING

Baldrige criteria compel an examination of how an analysis office prepares for future challenges, records its institutional history, and uses academic or professional sources. Within the category of future challenges, a distinction may be made between *capability* and *issue* challenges. Future *capability* challenges deal with the people and process issues. Future *issue* challenges, on the other hand, are country- or target-dependent. These challenges deal specifically with the emerging threat to U.S. interests. Although none of the offices has a written, formal strategic plan, in most, leaders claimed to have thought about strategic planning issues and were working toward a future vision. Their daily mission though was to "get the right information to the right people at the right time."

Future Challenges

Capability Challenges. Organizational capability centers on people and processes. For those subjects who indicated that they have thought about the future in strategic planning terms, leaders recognized that the commitment of their people to an organizational ideal is a necessary ingredient for success. In practice, then, organizational capabilities must support strategic planning. Analysis organizations need to consider their staff capabilities and ensure that staffs have the necessary knowledge, skills, and tools for success. Our study subjects generally favored a team approach for intelligence analysis. Leaders wanted analysts to consult with experts and coordinate with stakeholders before sending the final product to consumers.

Most office representatives said they had just the right mix of people for their mission. In one instance, an office had been given an abundance of people and other resources. However, if some other offices only had a few more people or more resources, then they too would be able to do much more for their consumers. Since they were already meeting their mission requirements, they did not expect to have additional people bestowed on them. In fact, office leaders reported that they had to fight annually to maintain their personnel resources, as many capabilities are fungible from one office to another. One office among those examined expected to hire several more entry-level people. An advantage of this approach is that new people tend to be more computer-literate than older staff members. An unsurprising tradeoff is that new people also tend to be less well-educated, in a professional sense, in their specialty. Another subject said there was no real future planning for their office personnel. The objective was to get analysts through identified training requirements so they could produce reports in order to fill databases.

Since none of the subjects claimed to use a formal strategic planning process, our study team could not discuss the process with them in detail. A generic strategic planning process, however, should include (1) doing advanced planning, (2) performing an environmental scan based on external and internal information, (3) setting a strategic direction using the vision statement, (4) translating the strategic direction into action via an implementation plan, and (5) making a performance evaluation. A performance evaluation or assessment should include (1) defining goals, (2) describing success, (3) set-

ting targets, (4) measuring performance, and (5) adjusting goals based on performance. The DIA has a formal process to do strategic planning, but it was not clear to the study team how the organizational strategic planning process might be linked to the lower levels of the organization.

Issue Challenges. Concern about issues centers on the mission of each analysis office. Evidence from this study indicates that an SIO often thinks about future issues. For example, he may hire external contractors to investigate an area of interest. One office recently commissioned a study to look out 5-10 years and make recommendations on a specific issue. Those recommendations addressed the question of what they needed to do now in order to prepare themselves for the envisioned future. One subject stressed the extant ability of his office to remain flexible and to evolve thoughtfully, guided by its own resources and instincts. As evidence in support of such confidence, he noted the office's demonstrated ability to anticipate warfighter needs. Another subject asserted that his office simply follows issues (in the widest "all-source" sense) as they are developing so when they are called to support a requirement, they are aware of what is going on and may have some work completed already.

One subject offered an example of an office in CIA that he was invited to join a few years ago. It was a new organization and analysts joined it by invitation only. Analysts regarded it as a fun place to work because they had an opportunity to be innovative. The office wanted to look at the world in a new way. One type of project associated with this office was a study of demographic changes and political instability within the major cities of a certain foreign country. He said they wrote five case study documents covering these places of interest in considerable detail. Such detail on individual cities was unusual for an Intelligence Community product, and at the same time greatly appreciated by consumers. According to our subject, this office no longer exists in the CIA. When offering it as an example of good intelligence, he implied that it may be worthwhile for DIA to stand up an office like the former CIA office to deal with today's complex issues.

Institutional History

Most subjects said they did not have a written institutional history. There exist no formal analyses of their office's strengths or weaknesses. The office does rely, then, on retaining experienced individuals for its corporate memory.[6] Some offices maintain briefings about their office's operations as a surrogate for a written institutional history. Anyone assigned to an analytic unit is expected to set about building connections and learning operations and systems. Only one subject said they had formed a history office to record significant events for their office, beginning in the late 1990s. Even this admirable initiative, however, with its focus on events, rather that process itself, would fail to capture the nuances of truly useful and recoverable institutional history.[7]

Academic or Professional Sources

In the interviews, office leaders tended to support academic training, attendance at professional conferences and conventions as experiences useful to the development of professional expertise. However, there exist at the office level no guides or plans for such professionalization opportunities.[8] Within an office, professionalization appears to be driven from the bottom up. If an analyst learns about a class or other certifiable learning opportunity, the agency's training center resources can assist with financial support, assuming office politics and workload do not intervene. Interviews revealed that little

---

[6] DIA does operate a mentoring program to ensure that some corporate memory is passed to younger analysts. Facilitated mentoring can cut on-the-job training time by up to half and may be a key factor in the retention of entry-level hires. However, participation in the mentoring program is relatively small compared to the entire workforce. Even if some employees enter into a mentoring relationship, there is no guarantee that the process will be successful. Potential pitfalls include: unrealistic expectations, supervisor unsupportive, relationship derails, shortage of good mentors, differences (style, ethnicity, gender, age) interfere, and relationship is a poor fit. Although U.S. Government and Department of Defense regulations do require that agency, and by extension, office products and communications be preserved as official records, the combined procedural and target knowledge required to create actionable intelligence typically escapes being recorded in the impersonal domain of such records.

[7] One exception to this rule is the Agency's *Military and Geographic Intelligence Cookbook*. The Joint Military Intelligence College also offers an exception to this state of affairs, with its publications *Writing with Intelligence* (August 1995), *Briefing with Intelligence* (August 1997) and *Research: Design and Methods* (September 2000), which capture the combined experience of student and faculty interaction in teaching and learning about intelligence studies.

[8] Career development is a continuous career-long process of self-assessment and planning that helps employees integrate their career goals with their organization's mission and needs. The DIA Career Development System (CDS) is designed to assist employees in career planning and development. Components of the CDS include: entry level development program, designed to train and develop entry-level employees, and the career service program, designed to enhance DIA's work environment and improve employee productivity.

emphasis is likely to emanate from office or division managers. Most requests are driven by personal interest and are authorized so long as funds exist to support it.

Each analysis office uses academic and professional sources in a different way. One office hires contractors to provide them with computer support. Another office employs over 100 contractors and academics to perform tasks in an external research program. In this case, according to interview testimony, analysts are able to integrate the outside research into their daily operations only with some difficulty. For example, analysts in this unit had to learn how to integrate data on cyber-terrorism and IO into counterterrorism analysis. Representatives from one office visited Unified Command Joint Intelligence Centers to learn to do this better. Another office used the *Military and Geographic Intelligence Cookbook* (MAGIC) to inform their analysts of "everything they needed to know to do their job." If the analysts had not used a specific tool in a while, then they consulted MAGIC to refresh their memory.

Richards J. Heuer, Jr., a senior CIA analyst, has tried to acquaint analysts at that agency with methodological developments in socio-political analysis that were being developed and tested in the academic world. He had to keep at it for more than a decade to be heard.[9] He has often met with strong resistance. Only a few academics willingly come to the agency to talk with the analysts. "Factions," an analytical tool developed at CIA for systematic analysis of political instability, is a good example of research and development (R&D) work done in collaboration with members of the academic community.[10] In the 1980s there was no particular pressure or encouragement across the Community to use structured analytic methods. Analysts gathered the facts, looked at them in their uniquely "logical" way, and came to some conclusions. Some DIA analysts use structured techniques to do intelligence analysis. The subjects we spoke to, however, described their analytical process as gathering facts, examining them logically and drawing some conclusions. More emphasis on structured techniques at DIA may be appropriate.

Summary

Although none of our subjects had a written, formal strategic plan, most of them had thought about strategic planning issues and were working toward a future common vision

[9] Finally, on 20 June 2000, at the inauguration of CIA's Sherman Kent School, which features a curriculum for new analysts, Heuer's campaign reached a pinnacle of acceptance by the agency, evidenced by his book's, *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999), being the focus of remarks by invited speakers. Another senior CIA analyst, Morgan Jones, had a few years earlier published a compact summary of "Fourteen Powerful Techniques for Problem Solving," some of them having been developed exclusively by agency analysts, in *The Thinker's Toolkit* (New York: Random House, Times Books, 1995), reprinted in a slightly revised edition in 1998 by Random House's Times Business division..

[10] Stanley A. Feder, "Factions and Policon: New Ways to Analyze Politics,'' reprinted from CIA's *Studies in Intelligence in* H. Bradford Westerfield's *Inside CIA's Private World* (New Haven, CT: Yale University Press, 1995), 274-292.

among the personnel in their office. Office leadership is often engaged with senior leadership about future issues. Managers know the direction they want to go in and recognize the need to support a strategic plan. Furthermore, a focus on important future issues such as which country is most problematic clearly makes an analysis shop proactive and saves time in crisis situations.

Theoretically, the strategic management process includes (1) advanced planning; (2) an environmental scan that includes a review of internal and external information; (3) setting a strategic direction; (4) translating the strategic direction into action; and (5) evaluating performance. Consumers, stakeholders, and subjects influence the process by stating their requirements, receiving products and services, and providing feedback. Information and analysis influence each step of the process by providing management with important information, data, and feedback.

Most of our subjects relied on the corporate memory of senior analysts instead of maintaining a recorded institutional history. As senior analysts approach retirement age and leave government service, analysis offices will lose a great deal of expertise. Some offices maintained a written office history or had on file significant briefings about their office's operations. All of our subjects used academic or professional sources to develop their capabilities as needed. They also knew what commercial tools were available to help them to do more for their consumers.

CONSUMER FOCUS

The Baldrige criteria applicable to a consumer focus suit the DIA case very well. As an information organization, this agency is obligated, through its analysis units, to discern consumers' requirements. A key question for this study is whether relationships with consumers tend to be *ad hoc* or the result of a deliberate strategy.

Consumer Requirements

Consumers make their requirements known through a formal production database, telephone calls, individual initiatives, by e-mail, and through personal visits. They make their initial requirements known primarily on an *ad hoc* basis. The most meaningful requirements are informal because the analyst gets to talk directly to the consumer. Subsequently, the analyst can help the consumer refine the formal request in the Community's intelligence production database. Some consumers make telephone calls to analysts that require an answer in two hours or less. This can make the analyst's job very stressful. Consumers use emails, on the other hand, as a secondary contact medium and mostly for follow-up activities. On occasion, a consumer will come to the analyst's office to maximize the opportunity to gain a very specific pre-deployment, contextual understanding of target information. One subject noted that although most analytic tasks are management-driven, there are also many self-generated products. The latter could have a positive effect, especially in promoting analyst self-esteem, so long as the self-generated products are of interest to the entire Community. In one case made known to the study team, an office leader asked analysts simply to produce products for their databases. As a result,

analysts chose subjects that they could write about more easily in order to meet their deadlines, rather than picking topics that represent the "tough questions" and that would be most useful to the Community in general.

Consumer and Analyst Interaction

The different frames of reference that one might expect to characterize any interaction between analysts and consumers are on vivid display in anecdotes related by most interview subjects. Much of the time, consumers appear to shy away from direct interaction with an analyst. On occasion, the consumer's rank is too far above that of the analyst to allow an analyst to directly approach an individual consumer, especially in an organization like DIA, often still characterized by a culture that finds meaning in and derives behavioral clues from a hierarchy of authority. Occasionally, however, informal interaction does occur, to include face-to-face conversations or telephone calls to enhance clarity of requirements. One subject noted that his contact with consumers is mainly personal and direct. This analyst works with consumers to build training products that look as much as possible like the real world. Toward that end, an analyst might attend survival school as a student, rather than as a VIP, in order to absorb and then re-create more realistically some part of that training environment. On issues related to training, analysts tend to go to wherever their consumers are located. There, they interact directly and build products together. Consumers also come to DIA. For example, one analyst recounted his experience with a Navy SEAL who sat next to the analyst during the production process. In another example, one analyst worked closely with an Air Force consumer on a downed pilot evacuation and recovery area study.

Some subjects claimed to have little or no interaction with consumers. One subject said there was some consumer support at the analyst-to-analyst level and through informal channels. As a general rule, however, there is no regular contact with a consumer. Therefore, the role of consumer often is represented by whoever becomes a reader of a particular publication.[11] Production tasking usually passes through bureaucratic levels at both the producer and consumer ends, which reinforces pre-existing tendencies keeping analysts and consumers away from each other. Suddenly, an answer to a formal or informal request simply appears. A general absence of feedback from consumers characterizes the intelligence production process in the offices included in this study. Any interaction with consumers that does occur happens on an *ad hoc* basis.

---

[11] Because most products are published electronically on systems such as Intelink, it is possible for the agency to track in considerable detail the organizations and even particular analysts that access and explore particular documents. In practice, however, this is rarely done at the level of detail that allows an analyst to be certain who the consumer really may be. Even if one accepts the concept that within the Department of Defense, information becomes actionable intelligence mainly through the briefing process, it is wise to remember that cognitive processes do depend ultimately on purposeful information-seeking activity, which can hypothetically be tracked in such detail as to inform intelligence producers exactly who their true consumers really are.

Feedback

Analysts provide finished products to their consumers in a variety of ways: through the formal production requirements management database, in hard copy, posted to a website, or by email. Sometimes, depending on the size of the electronic file, analysts post a product on a "hidden" URL. Then, they call a known consumer to let them know where they have posted the product. Once the consumer has the product, the analyst can delete it from the system. Feedback appears in many forms. In one office, informal feedback predominates through personal contact with the consumers. Another office obtains consumer feedback either via the office web site's "feedback" button, or via a verbal response from the consumer that the product met or did not meet the need. Hard copies automatically include a publication office's formal feedback form. All products do not get this form. One subject said a team in their division uses a questionnaire to find out if their consumers liked their product. One office maintains a sizable travel budget so analysts may travel to their consumer's office regularly.

Sometimes analysts are told when they did a good job. They are also told when they could have done better, a phenomenon that has become more common with the advent of impersonal electronic communication. Consumers can be very specific. Analysts provide briefings to their consumers and they attend briefings by consumers. They may get a phone call saying either "great job," or that the Admiral wants to know why the analyst came to a certain conclusion. Sometimes, the analyst writes for a specific individual. The individual consumer almost always responds positively in this scenario. If the product goes directly from the analytic office to an individual, then there are not many levels of review. In such a case, reviewers will include a (1) branch chief, (2) the DIA Office of Research, and (3) the Division Chief. If, however, the analysis office broadcasts the product, then the review process can reach extremes of review and coordination.

Marketing a product can attain great importance. An analyst typically does not want his or her finished product to sit on the table in the J-2's office. The usual desire is for the information to reach much lower levels, where the material remains actionable information, which may only later become actionable *intelligence*. They do this by using different means of communication. For example, they publish their results using different media such as in the *Military Intelligence Digest*, which features strategic or operational assessments; the general finished intelligence database, known as Intelink; serialized DIA publications, and informal contacts with consumers around the world. The analyst who writes the product can market it by mailing hard copies, by telling people where to find it on Intelink or by responding to specific requests by sending email attachments or making a personal phone call.

Summary

Building relationships with consumers tends to be more *ad hoc* than the result of a deliberate strategy. Although consumer feedback varies from office to office, most of the subjects said that "working-level" consumers support their intelligence analysis process. Some got feedback from an office web site. Others got it through verbal interaction. If

funding is available, then analysts visit their consumers often to learn about their requirements and get feedback about past performance. Often these consumers will visit the shop to let them know what they need and to describe how particular, related products have been used in similar situations in the past.

Likewise, the way consumers make their requirements known varies from office to office. Consumers continuously provide information as they themselves move along in the analysis process.[12] Analysts preferred a phone call from the consumer first so they could coach the consumer through the process of documenting their needs in the COLISEUM database. Once the analyst completes the product, they market their work. Analysts used different methods to make their products available, improve their chances of getting their information to the appropriate consumers, and ensure consumers have an opportunity to use their product.

INFORMATION AND ANALYSIS

Information and analysis criteria address the question of how well DIA offices are meeting challenges in this core functional area, and reveal whether a meaningful approach is being taken by the organization for measuring product quality. Representatives of most of the analysis offices indicated that they are meeting the requirements embodied in these criteria. Informal means for measuring analysis performance included counting products, meeting production schedules, regularly updating databases, answering key consumer-oriented questions, and gauging performance based on "perception."

Meeting Current Analytic Challenges

Specific indicators of success that were quickly asserted by interview subjects included the following:

1. Positive comments or lack of negative comments from consumers;
2. Evidence of consumer use of intelligence products;
3. Knowledge of the number of terrorist attacks averted;
4. A downward trend in the number of requests for information (RFI);
5. Evidence of improvement of analysts' capabilities based on accumulated experience.

---

[12] DIA has begun serious promotion of collaborative intelligence production across the defense intelligence agencies, military service intelligence production facilities and among Unified Command Joint Intelligence Centers through the Joint Intelligence Virtual Architecture Program (JIVA). This program allows individual analysts from across the defense intelligence community to rapidly find, access, and use trusted information of all types and classification, without knowing its location or format, and to do their jobs easier, faster and better. JIVA provides a virtual, interactive environment for the development and exchange of responsive, tailored all-source Intelligence and value-added analysis.

Subjects easily enumerated evidence associated with each of these indicators. For example, if consumers are satisfied with the analyst's work, then they provide positive feedback via any number of methods. The amount of positive feedback, however, is usually meager. Not surprisingly, a tendency exists for a dissatisfied consumer to be more vocal. A lack of negative comments from consumers is therefore considered a positive indicator of success. Consumers never want DIA to stop sending them daily intelligence products. Even if routine DIA assessments are only placeholders, the consumer still expresses a demand for the products because one article could change everything.

Whether the consumer uses the intelligence product is another indicator of success. Analysts do need to know how many consumers read DIA products and find them useful. In actuality, a production office is only rarely able to gauge the use and impact of either particular products, or the office's overall production. Ideally, the office's products are suited for use without modification, as formal or informal coordination is expected to contribute meaningfully to the production of each item. The concept of usability depends on being able to measure whether information embodied in the office's products are "actionable." Measurement of actionability is never easy because often no recordable action is required, and the producer faces the difficult task of determining whether the product has simply influenced the way a consumer views an important issue. No one from among the offices under study here claims to have an answer to this difficult issue.

Likewise, a great indicator of success would be the number of terrorist attacks averted. It is rare, however, for DIA to learn about a terrorist cell whose members talk about an act of terrorism, prepare the attack, and then stop as a result of DIA's informing the specific target or the larger public. With continued capabilities to collect information without the target's knowledge, measurement of such occurrences is certainly feasible. With increased emphasis on collaborative counterterrorism analysis, some of the best minds in the Intelligence Community are now addressing this very problem.

DIA analysts often find themselves responding to formal Requests for Information (RFIs) from consumers. Another positive measurement standard, then, although an indirect one with the potential for unknown intervening variables, is a downward trend in the number of RFIs. Analysts do assume they are doing something right if the number of RFIs from active consumers are declining in number. Of course, if only a few RFIs make up this measurement, then some means of weighting the breadth of the requests needs to be considered. Over the course of a year, however, the substantial number of RFIs would allow the laws of probability to operate in support of attaching meaning to a statistically significant decline in overall RFI numbers. Nevertheless, at least among the offices in this study, no such statistically based measurement is practiced.

A different type of indicator of success is the level of improvement in analyst savvy, given the accumulation of experience. An office's SIO is in a good position to determine whether the analyst is making improvement. Comments from the SIOs contacted in the course of this study indicate that they examine the analyst's work with a critical eye to determine whether the analyst is growing in the job. If it is determined that the analyst is in fact getting better at doing analysis, then the SIO rewards the analyst with more work

and more challenging jobs. The SIO also rewards the analysts with an appropriate performance review. If however, the analyst does not show improvement in the current task, then the SIO working with the analyst and manager will attempt to diagnose the problem and provide appropriate training to improve proficiency in doing analysis.

One indicator of success that is not appropriate is that associated with a specific forecast of events. One subject noted that one must be cautious in making such a forecast, and then watching to see if the projection is correct. Office representatives observe that this approach does not constitute a good indicator of success because it may be misleading to track, as analysts have the opportunity to continually reshape their forecasts and analysts and professionals do not like the idea of being graded on their own judgment calls. To illustrate, one time an analyst wrote a paper on Kenya. The prediction was that Kenya would be stable over the next five years. In the third year, however, a destabilizing coup was attempted. The analyst had failed to account for a coup attempt, but since the coup failed, the analyst's judgment was confirmed—he was correct. But were the analyst and his product really successful?

A Standard Approach to Measuring Quality

No subject claimed to have plans to implement any kind of standard approach to measure analytic quality. One subject said he was not opposed to some standard for measuring quality. He has not, however, seen a useful measure for it. In another office, analysts "just publish in order to keep their database filled." Little or no attention is given to quality. Either the product meets the requirement or it doesn't. Another subject said even if he thought measuring analytic quality was a good idea, no one in his office would do it. Managers in his office, however, are examining ways to do things more effectively without destroying the office's "can-do" ethos.

Comments

All of the subjects said they had no formal performance measurements, but neither did they employ informal means. To justify this situation, one subject said intelligence analysis is purely subjective. There are no numbers to count. If analysts meet their production schedule, then they are considered to be successful. If analysts get all of their work done, then they have met the minimum success requirement. If analysts get all of their work done and they are also able to get *ad hoc* work done too, then they are considered more successful. No one interviewed would accept the idea that there may exist valid quantitative measures of analytical success.

Managers of intelligence analysis are ambivalent about managing for results. Though interested in demonstrating success, they are uneasy about being held accountable for poor organizational performance. There are severe problems in measuring performance in practice: (1) problems in getting agreement on what good performance means for intelligence analysis; (2) intelligence analysis goals are unreasonable compared with available resources; (3) key performance indicators are unavailable or too costly to collect; and (4) management is unwilling to make necessary changes to improve intelligence analysis.

Informal evaluation of analytical quality of course does occur. In many cases, an office SIO is expected to contribute to an analyst's performance evaluation. For example, the SIO might show the division chief examples of the analyst's work and point out what is good about it, what is a problem or an opportunity for improvement, and whether the analyst has learned from experience. Office leaders appear to be most interested in how many products the analyst finished, even though this crude measure is not supplemented with any method for independently weighting the relative value of those products.

One subject noted that his office does track certain indicators of quality, such as whether the consumer liked the product. A subsidiary indicator lies in evidence of whether the consumer responded to the product. Did anyone else want a copy of the product? Some have developed a measure of the significance of the problems they analyze. For example, an imminent terrorism problem, compared to a future military planning problem is more significant and would fit on of the high end of their measurement scale. The SIO or division chief for this office would maintain a matrix of products by author and subject.

One subject prefers using the term "gauge" instead of "measure" because "measure" assumes some sort of reasoned technique. Often, there is a bit of a "gut check" in any office with respect to how well managers perceive their office to be meeting its mission. Most of the measurement comes in the form of *ad hoc* consumer feedback. A well-executed mission, like a successful noncombatant evacuation operation (NEO) for instance, tells the office that they are doing a good job.

Summary

Informal means for measuring analysis performance included counting products, meeting production schedule, updating databases, answering key consumer-oriented questions, and gauging performance based on perception. Two common ways for analysts to know if they are meeting their consumer's needs are by a lack of negative feedback and by an increase in product use. Our subjects do not keep track of forecast accuracy because it is too difficult to track. Instead analysts individually keep a mental checklist on any forecasts they make and how the situation developed over time. Although none of our subjects planned to implement any standard approach to measure analytic quality in the near future, they continue to examine ways to do analysis more effectively without destroying their organization's "can do" ethos.

PEOPLE AND RESOURCES

The people and resources category offers criteria to examine the knowledge, skills, and experiences of the analysts and the availability of analysts' tools. Leaders can improve the quality of a product by promoting greater expertise among the intelligence analysts and by inducing analysts to take advantage of information found in open sources. Study subjects said they need analysts who think across interdisciplinary boundaries and they prefer analysts who have military operations experience.

Most of our subjects assert that they are well-qualified to perform their mission. One office was gaining personnel resources quickly because their issue is very visible. In the recent past, the boss would train the new analysts. Today, however, the office that has grown so rapidly finds that even the bosses are all new. They appear to need a formal training program targeted at the office level, rather than merely at individuals.[13] Another office whose personnel resources were static considered itself successful because they are meeting their requirements. They could be better if they had better tools and if they had a few more people in the office. They note that static personnel resourcing makes them less successful than they could be, but not unsuccessful. Another office claimed to be understaffed. To make matters worse, they suggest that they have the "wrong" people in management positions. Even within the small sample of offices in this study, there appeared some examples of high-interest areas where analysts whose experience had been gained in other functional areas are now "parked" pending retirement. This is clearly a poor management practice. It is the result of an archaic government personnel system and is common practice throughout government.

Knowledge, Skills, and Experience

According to representatives of the five offices in DIA, analysts bring with them or develop certain skills to help them perform their analysis and at the same time they must develop an awareness of how certain analytic pitfalls may influence their work. The analytic skills include: (1) technical or topical expertise; (2) knowledge of the target, sources, and analytic techniques; (3) ability to search and organize data; (4) ability to synthesize data or use inductive reasoning; and (5) ability to express ideas. The analytic pitfalls include: (1) personal biases or inexperience; (2) lack of data or access to data; (3) asking the wrong question;[14] (4) misunderstanding data; (5) flaws in logic; (6) no review or evaluation process; (7) denial and deception by the target; (8) politicization or non-objectivity; (9) groupthink; and (10) mirror imaging.

A synthesis of interviews conducted for this study suggests that analysts need to learn how to think across disciplinary boundaries. As a general rule, analysts do not learn to think across disciplinary boundaries in school. One subject suggested that analysts could take (remedial) philosophy courses in order to learn how to think across disciplinary boundaries. Another subject suggested that cross-disciplinary education continued in their

---

[13] Joint Military Intelligence Training Center courses are designed for students who have no experience or have limited previous experience in intelligence at the joint, combined, or national levels and have job-related requirements for knowledge of intelligence at the national or strategic levels.

[14] The problem of asking the wrong, or the right, question is especially noticeable in strategic analysis, the type of analysis produced by DIA in support of the Chairman of the JCS and the National Command Authorities. This problem has been addressed succinctly and with examples in Patrick J. Haney, "Soccer Fields and Submarines in Cuba: The Politics of Problem Definition," *Naval War College Review* 50, no. 4 (Augumn 1997): 67-84.

shop because personnel possess deep knowledge in history, political science, and economics. These people also had computer skills, and 5 to 25 years of intelligence analysis experience each. One subject added that the people in their office who started DIA employment in the 1980s had fewer computer skills, but knew more about their subject matter. Younger people tend to be gifted at using digits to display information. Their elders claim that they lack the skills necessary to infuse meaning into the displays.

One subject said they have area specialists, social scientists, former military personnel, former law enforcement agents, active-duty military professionals, and reservists with long active-duty backgrounds. They like having an office filled with people who have the different perspectives. They have senior people with lots of experience. Then there is a big drop-off in experience among the lower level staff members. One problem frequently voiced is that new hires top out in four years at the GS-13 level, then they have to move out of the office to continue advancing in their career. A consensus exists among office managers that any office struggles to maintain their analysis capability as people move to better jobs for promotion. Having people who are career intelligence officers, especially if they also possess a military operations background, is commonly cited as a key to a quality staff.

Tools

Subjects of this study reported using a variety of common tools to accomplish their missions. These tools included:

- COLISEUM (Community On-Line Intelligence System for End Users and Managers--an intelligence production requirements database);
- JWICS (Joint Worldwide Intelligence Communications System--featuring Intelink, the Community's finished intelligence database), Websafe (a message handling system) and VTC (Video Teleconferencing) to communicate with consumers;
- SIPRNET (Secret Internet Protocol Router Network);
- OSIS (Open Source Information System), and NIPRNet (Non-classified Internet Protocol Router Network);
- DITDS (Defense Intelligence Threat Data System);
- DIA and DODIIS (DoD Intelligence Information System) e-mail.

Analysts use a variety of techniques and tools to produce intelligence. Techniques include pattern analysis, systems analysis, quantitative analysis, modeling, and inductive reasoning. Analysts use tools specific to their form of analysis. These tools include the following:

- *The Analyst's Notebook*, featuring visual investigative analysis software that assists analysts by uncovering, interpreting, and displaying complex information in easily understood chart form. It includes a link notebook for link analysis and a case notebook for time-event analysis.
- *Hugin Expert* is artificial intelligence software based on Bayesian analysis. Bayesian analysis is a compact model for representing reasoning under uncertainty.

- *ESRI* (Environmental Systems Research Institute) GIS (Geographic Information System) is a core set of application tools for organizing and analyzing geographic information. *ArcView* includes powerful visualization tools to create maps.

Summary

Analysts need to be able to think across interdisciplinary boundaries and have military operations experience. Senior analysts tend to be subject matter experts. Newer analysts, however, tend to be more computer literate. Our subjects liked having staffs with a diverse mix of experiences. They recommended tools such as the analyst's notebook which features time-event analysis and link-analysis; *Hugin Expert* which features Bayesian network analysis; and *ESRI GIS* which contains ARC-View. They also use numerous intelligence-related classified databases and other open sources.

PROCESS MANAGEMENT

Process management criteria apply to information handling, intelligence analysis, and collaboration. Processes associated with the dissemination of information and intelligence are beyond the scope of this study, but in this area, the advent of online publication and the loosening of "need to know" rules governing access to sensitive information have relieved some classic dissemination bottlenecks.[15] Good analysts are commonly characterized by DIA officials as "focused freethinkers." Other commonly acknowledged maxims are that the analysis process is a highly competitive process, and that analysts rush to be first to publish vital intelligence findings. At the same time, analysts must work together by collaborating with other analysts to ensure accuracy.

None of our subjects said they observed a formal or structured process in doing intelligence analysis. One subject summed up this approach as simply "sitting down and going to work." A second subject claimed to use an informal and semi-structured, term research process. In this mode, the analyst first has an idea related to their "account." They discuss with their team chief the problem they are interested in solving. If they get permission, then they do the research. Another subject added that, likewise, he does not have a "hardwired" approach, yet applies a routine to the process. One subject said his office has a process that only remains in the mind of each of the office's analysts. It is, in the estimation of this subject, an application of the scientific method or at least a disciplined thought process. In this scheme, managers give the analyst a problem, and the analyst does research to determine what they have and what they need. If there is time, he or she will request collection of certain data. The analyst reviews the data and answers the question. Sometimes, the analyst will get feedback (either good job or please do better next time). Typically across the offices examined here, there is no standardized way of conducting

[15] Modification of the "need to know" principle as it applies to information systems has been accompanied by the use of effective counterintelligence tools that allow detailed tracking of actions taken by individual analysts in the handling of sensitive information.

analysis. This situation may be a tacit response to the philosophy expressed by office leaders that they try to encourage "out-of-the-box" thinking.

Information Handling

Analysts do their own fieldwork to gather any information beyond that from routinely available, written sources. One SIO emphasized that his analysts "gather" information, they do not "collect" it. For example, they do not have diplomatic immunity when they are visiting other countries; they must get specific permission from the country to be there. Standard Community information is derived from imagery, signals, human resources, "open" sources, and other technical means. The kind of information that analysts use is problem-dependent. They may use operations-support products such as maps, imagery, and target materials. Some analysts tend to use information from the source with which they feel most comfortable. For example, some like using signals information and rely solely on it. Office leaders typically try to accustom analysts to using multiple sources of information including the Internet.

Analysts report that they try to lay down the steps of their analysis in a logical way. For example, they use several paths to move from general information to more specific information. Some analysts write their papers as if they were doing research in a graduate school. Others write products that look like newspaper articles. Analysts tend to protect their sources in a manner similar to the way newspaper reporters protect the identity of their sources. They use a general description to protect the identity of the informant. For example, a writer may attribute a quote to a high level authority in a specific DoD organization such as the Pentagon. The reader may judge for him or herself whether the source is reliable, but is unable to precisely identify the source.

Intelligence Analysis Process

The analysis process includes (1) problem identification; (2) data gathering; (3) analysis, synthesis, collaboration, and examination of alternative propositions using all sources of data; and (4) direct support to consumers with briefings and publications. In the end, analysts make an assessment of what the data probably mean or what the data could mean. General Colin Powell (USA, Ret.) sums up his expectations as a consumer of intelligence in this way: "Tell me what you know, what you don't know, and what you think—in that order." In this oft-quoted dictum, he suggests that analysts can best convey what is known about the problem, evaluate the completeness of their knowledge, and interpret its meaning. It remains unclear whether the same guidance is as suitable for written products as for oral briefings. In the course of analysis, whether presented in written or oral format, it is important for the analyst to answer for himself certain key questions:

1. What do you know about the issue?
2. What is a logical, sequential way to present the facts?
3. What conclusions or implications can be drawn from these facts?

Analysts generally find it distasteful to coordinate their products with members outside of their team. Nonetheless, when the "corporate" analysis process works as it can, all of the teams contribute to the analyst's final product and, as a result, the analyst produces a superior product. Managers do want analysts to exchange information with each other. They have a distaste for competition among analysts. The analysts' rationale for resisting widespread coordination is that they consider themselves subject matter experts.

Beyond the thicket of coordination and collaboration, the analysis process becomes tough to execute when the office finds that several consumers demand attention all at once. When this occurs, the office's cradle-to-grave, face-to-face, and surge-flexible process becomes overwhelmed. One subject acknowledged that the tension between higher and lower echelon consumers and the tension between two or more concurrent contingencies gave them the most concern. Consumers typically ask the office's leaders to intervene when they believe the office is not meeting their requirements. As a result, the analyst can expect to have to shift priorities and perform many tasks under a great deal of stress.

Collaboration and Competition

Collaboration. If analysts choose not to collaborate with other Community experts, then the SIO may force them to do so during the coordination and review process. Managers want analysts to verify the validity of all of their information in a manner similar to the way that they feel compelled to check and verify human-resource information. They also need to confirm source reliability, be able to articulate the method they used to derive the information, and to confirm the information's contextual accuracy.

Competition. Collaboration among intelligence analysts is always a problem because analysts, like many school children, tend to be competitive with each other. The acknowledged lack of coordination within DIA is not a new or exceptional phenomenon. New analysts may not know who to talk to on a particular subject or where to go to get useful information. A more senior mentor or manager can usually provide the analysts with that kind of information, but the exchange of information between analysts doesn't normally happen in the unsupervised work environment. Analysts are very competitive within the office and especially with other agencies in the IC. There is a strong desire to publish first, a tendency that inhibits full disclosure to competing analysts. Other intelligence agencies usually have more resources than DIA and can report an item more quickly than DIA. From another perspective, one subject reflected on how analysis was done at the CIA many years ago. He said CIA analysts would initiate collaboration when necessary and had occasional meetings to share information. They had mixed luck with people external to their organization. Academics sometimes refused to talk to them. One time an ambassador was reluctant to talk with them. Overall, he concludes that there was very little collaboration "back then." He provided two examples:

First, all cross-office work was called "collaboration-by-staple." One person would write the first half of the paper and the other person from a different office wrote the second half. A person from a neutral third office would edit the entire paper. Then they would

staple it together and send it out. A more truly collaborative work environment would have made it easier for the analysts to bounce ideas off of each other and test their assumptions. Back then, everything was much more competitive even than today.

Second, message traffic came into the office mainly in paper format, rather than the electronic format of today. One clever analyst would come into the office each day much earlier than anyone else. He would review the message traffic, take the good papers, and then produce analysis on interesting topics that he would present later in the morning to his office leaders. Others in the office would be left to report on the remaining message traffic that was less interesting. In this subject's view, the office leaders unfortunately let this go on without intervention.

Summary

Good analysts are "focused freethinkers." Nevertheless, "out-of-the-box"-type thinking needs to be tempered by using an informal, disciplined thought process and collaborating with other analysts The scientific method is a streamlined process that ensures the analyst doesn't wander too far. Use of information is problem-dependent. There is, however, a general consensus among our subjects that analysts should use everything they can get their hands on. Analysts also need to assess the reliability of their sources and at the same time, protect the identity of sensitive sources. Collaboration tends to vary by organization and by issue. Collaboration tends to be better between analysts within DIA than between analysts from different parent organizations such as between CIA and DIA. There tends to be a competitive nature among analysts to be the first to publish their product.

MISSION ACCOMPLISHMENT

The mission accomplishment category examines the analyst's definition of success, and proceeds to secure an estimate of the percentage of time analysts believe they are successful.

Definition of Success

All of our subjects agreed that success is a difficult concept to define. Our subjects did, however, agree that it might be possible. First, success is positive feedback from consumers. If they do not provide explicit positive feedback, then the analysis shop can look for indirect indicators. For example, if the consumers keep coming back for more analysis, then analysts consider their products successful. Another informal way of measuring success was to count complaints.

Second, an intelligence analysis success occurs when a unit that is known to depend on DIA products completes its military operation successfully. If, however, there is loss of life during a mission, then the analysts are greatly disturbed. Their product may have in some way contributed to the lack of success for the military operation.

Third, success is obtaining an expanding budget and a growing workforce. These developments indicate that the topic focus is perceived as interesting by agency leadership. One subject labeled this type of success as "bureaucratic success."

Fourth, success to some analysts means that evidence indicates that they are able to look at things in the open sources and link them in ways others could not envision. The analyst would observe a situation, notice a trend, and take a position on a tough issue. The following descriptions are examples of good analysis written during the 1980s:

- The analyst's bosses didn't want a paper on the future of Lebanon written because it was a tough issue. When the analyst completed the paper, the director of the agency wanted to see it. The bosses fought among themselves to see who would take it to him. After reading it, the director wanted 20 copies to give to the Secretary of State.
- An analyst identified a high level of tension among the cultural groups living in Yugoslavia. The analyst reasoned that strong suppression was holding these cultures in check. When Tito dies, the analyst warned, "Look Out!" This example indicates that estimative studies should not be dismissed out of hand.[16]
- An analyst identified problems in African cities because of a certain mix of people living there. The paper predicted that similar problems would happen in suburbs as the suburbs began to get the same mix of people. As it turned out, the analyst was correct.

Fifth, a representative from one office defined success as a function of terrorist attacks. If no terrorist attacks happened, then they would consider themselves successful. However, terrorist attacks could potentially happen anytime, and if one happens, then the shop would consider itself unsuccessful.

Sixth, analysts in general put out a lot of paper and products in support of military "force protection," and to support the senior intelligence officers (J-2s) of the JCS and of the Unified Commands. DIA analysts consider themselves successful if their consumers change their behavior by doing things differently as a result of information provided.

Percent Successful

Study subjects clearly struggled to answer the question of how often they are successful. One subject said he had no answer: "Sometimes you will never know whether or not you were successful." He could confirm in any given case that no negative response had come from stakeholders, yet he could not be sure that the consumers considered their products successful. One subject said success for his office was at 90 percent. However, he could not elaborate.

---

[16] Perhaps the clearest exposition of how estimative intelligence can be accomplished in a way to discourage the work's being easily dismissed is provided by Isaac Ben-Israel in "Philosophy and Methodology of Intelligence: The Logic of Estimate Process," *Intelligence and National Security* 4, no. 4 (October 1989): 660-718.

One subject said that by his personal definition, all analyses were successful. His criterion for success was to go beyond the status quo, to clearly articulate views to real consumers, and to establish a feedback loop on utility of products. He admitted there was no readily accepted measure and no guidance concerning success. One way for an analyst to be successful was to get his work published. At least that would get his boss off his back for a certain amount of time! Still another subject said all products were in some sense successful. To be successful, he continued, it is important for someone to look at the products. One possible way to measure success is to count the number of electronic hits on a particular document on a database. If consumers are asking questions, then analysts can feel they are being helpful. An informal summary metric, then, is the measure of information flow out of the office.

Summary

Intelligence analysis supports DoD organizations and warfighter operations. Mission success is positive feedback from consumers or a successful completion of military operations. Bureaucratic success, on the other hand, results in more money to spend and more analysts to do the job. Analysts consider themselves successful if their consumers changed their behavior based on the information they provided to them. For example, successful analysts warn unit commanders of a possible terrorist attack and as a result of their work, the commander takes the appropriate steps to improve unit force protection.

STRATEGIES FOR SUCCESSFUL INTELLIGENCE ANALYSIS

"What is good intelligence analysis?"

Good or useful intelligence analysis may be best defined by its opposite. Bad intelligence does not specify what the threat is or how it will manifest itself. For example, the analyst may conclude there will be a 50 percent chance of a chemical weapons attack against the U.S. in the next 10 years. That conclusion is not meaningful or helpful to planners and users of intelligence.[17] In another example, the analyst may conclude that all ports are dangerous to U.S. ships. This analysis is impractical because ships have to use ports occasionally.

In positive terms, good intelligence analysis enlightens commanders or consumers. It doesn't necessarily have formal probabilities. Instead it communicates to the commander some level of likelihood. For example, if the commander implements plan X, then a terrorist group in this location is likely to react in the following manner. This information is

---

[17] Richards Heuer, 155, reproduces a table illustrating the different numerical probabilities that intelligence analysts and consumers associate with common word descriptions of probability. The message is that neither form of presentation expresses probability in a reliable fashion. The table appeared originally in Sherman Kent, "Words of Estimated Probability," in Donald P. Steury, ed., *Sherman Kent and the Board of National Estimates: Collected Essays* (CIA: Center for the Study of Intelligence, 1994), 133-137.

valuable to the commander because it gives him or her the opportunity to change plans based on the analysis. It enlightens the commander of the current situation. Good intelligence analysis takes a position on an issue. Some current intelligence products fail to say anything of substance because they use normative words such as "would," "could," "should," "will likely," "might, "may," and "can be." These products have limited value to the consumer. A remaining question is "How can intelligence products be made more useful?"

Good analysts use quantitative data when appropriate. Over time there has been a rise in the use of statistics in intelligence products. One subject observed that many years ago analysts rarely used statistics in their analysis. Then, some analysts used statistics, but they didn't write about it in their papers. He recognized statements made in the paper that would require use of a certain structured technique. He would call the author(s) to inquire about the technique. Usually, he was right. The author(s) had used the technique. After a while, some authors put the data in the appendix of their paper so others might replicate their work. Then, analysts began to put their statistical analysis in the text portion of their papers. These products became more like academic research papers than they had been in the past. Analysts tend to respond favorably to any form of rigor in intelligence products.

Richard K. Betts says intelligence failures are most often caused by decisionmakers who consume the products of intelligence service. The use of intelligence depends less on the bureaucracy than on intellect. Therefore, one can only get modest improvement by altering the analytic system.[18] Jay T. Young, on the other hand, sees barriers to more effective analysis that could be corrected by managerial, personnel, and training reform. He believes that an overhaul of the U.S. intelligence community's analysis effort can improve its effectiveness while reducing its overall size and cost.[19]

In government work, the applied nature of intelligence production would seem to offer the opportunity to develop and apply consistent measures of productivity and quality, just because the products are indeed used by specific consumers. If this is true, then there is room to bring "operations research" into play as well as the Baldrige criteria, to encourage the development and collection of carefully codified, surrogate measures of productivity and quality. Successful use of these tools does not remove from the manager the task of decisionmaking but rather it requires of him or her rather different kinds of decisions. In other words, using operations research tools provides managers with extra insight into their particular subject and hence leads them into much more difficult but fruitful areas. Consultants with scholarly backgrounds could come into the intelligence analysis work environment and make vast improvement to the intelligence analysis capability using such tools to assist them, in the author's opinion.

---

[18] Richard K. Betts, "Analysis, War, and Decision: Why Intelligence Failures are Inevitable," *World Politics* 31, no. 1 (October 1978): 61-89

[19] Jay T. Young, "US Intelligence Assessment in a Changing World: The Need for Reform," *Intelligence and National Security* 8, no. 2 (April 1993): 125-1390

QUESTIONS FOR FUTURE RESEARCH

Our subjects offered the following questions for future study:

1. Does DIA prepare analysts for their work by acquainting them with the use of analytic tools? Does DIA provide adequate analysis training?

2. What are the implications of the substantial difference between the ideal way for doing analysis and the way DIA analysts actually do it? For example, data are often contradictory and vague. They do not point in any particular direction. Yet the analyst knows he must draw conclusions at the end of the study. Can anyone conclude anything from such data?

3. If you could have any tool (real or imaginary) to help do your analysis better, what would that tool be? For example, some people like having fancy graphics in their papers or as part of their analysis.

4. What attitudes characterize DIA analysts? Do DIA analysts have a tendency to be more receptive to collaboration, or more competitive than government analysts in other agencies?

NOT AN END, BUT A BEGINNING

This report does not represent the end of the intelligence analysis benchmarking study; rather it creates a platform for a wide range of beginnings. The approaches identified in this report will come to life by being shared, debated, and implemented in the context of Department of Defense and Intelligence Community realities. Then, where appropriate, they may be used and expanded upon. Intelligence analysts throughout the intelligence community can establish their own analysis networks and working groups to share their own best practices and lessons learned with each other.

	Benchmarking Offices				
	1	2	3	4	5
1. Does your office leadership support analysis process?	Y/N	Y	Y	Y	Y/N
Usually leader assigns tasks		Y	Y		
Usually analysts perform self-generated tasks	Y		Y		Y
Analysts usually respond to crises			Y	Y	
Little or no interaction during analysis process	Y	Y			Y
Some interaction if asked			Y	Y	
Tend to put products on electronic media	Y	Y			
Tend to put products in many different forms			Y	Y	Y
Formal feedback and coordination process at end	Y	Y	Y		Y
Informal feedback prior to finished product				Y	Y
2. Does your office have a written strategic plan?	N	N	N	N	N
Able to meet future capability challenges	N	Y	Y	Y/N	Y
Able to meet future issues challenges	N	Y	Y	Y/N	Y
Recorded lessons learned	N	N	Y/N	Y/N	N

	Benchmarking Offices				
	1	2	3	4	5
Use academic or professional sources	Y	Y	Y	Y	Y
3. Do your consumers support the analysis process?	Y/N	Y	Y	Y	Y
Requirements through COLISEUM & phone calls	Y	Y	Y	Y	Y
Little or no interaction during the analysis process	Y		Y		Y
Some informal interaction if appropriate		Y		Y	
Electronic publications and/or hard copies	Y	Y		Y	Y
Use multiple methods to market products			Y		
Little or no formal feedback	Y	Y	Y/N	Y/N	Y/N
4. Do you measure your analysis performance?	N	N	N	N	N
Lack of negative feedback from consumers			Y	Y	
Consumers find product useful			Y	Y	
Analysts show improvement over time		Y			
Don't track forecast accuracy					Y
Use or plan to use standard metrics	N	N	N	N	N
5. Do you have the right people and resources?	Y/N	Y	Y	Y	Y
Need to think across interdisciplinary boundaries	Y				
Need balance between computer skills & being SME		Y			Y
Need diverse mix of experiences			Y		Y
Need military operations experiences				Y	
Want analysts to develop and use toolbox	Y	Y	Y	Y	Y
6. Do you have a formal process for doing analysis?	N	N	N	N	N
Does informal process inhibit good analysis?	Y	Y/N	N	Y/N	
Use all information you can get		Y			
Use creativity to make-up for resource shortages	Y				
Use open-source data more	Y	Y	Y		
Information use is problem dependent			Y	Y	
Assess reliability of sources					Y
Do your analysts collaborate with other analysts?	N	Y/N	Y/N	Y	Y/N
7. Does your office make a positive contribution?	Y	Y	Y	Y	Y
Use consumer feedback		Y		Y	Y
Contribute to mission accomplishment		Y		Y	
Expand budget and grow workforce	Y				
Consumer changes behavior based on analysis			Y		
Successful most of time	Y	Y	Y	Y	

Responses to Interview Questions, by Office.

The purpose of the matrix is to summarize what was learned during the interviews. The author constructed the matrix after the interviews took place. All of the responses in a single column are directly related back to a specific interviewee. If the respondent referenced a specific item in his response and indicated yes or no to that item, then that response is recorded on the line related to that item in the matrix. If the box is blank, then the respondent did not refer to that item in his response. In other words, the author is uncertain what the respondent would say concerning the item in the matrix. The interviewer asked each subject the first question in the series of items directly. As a result, each box for the first question in the series of items is complete. No item in the matrix has a completely blank line because someone had to refer to the item in his response in order to get the item listed in the matrix. The matrix provides a frequency count of items mentioned in response to the topic being discussed.

BIBLIOGRAPHY

Allison, Graham. *Essence of Decision: Explaining the Cuban Missile Crisis*, Little Brown, 1971.

Ben-Israel, Isaac. "Philosophy and Methodology of Intelligence: The Logic of Estimate Process." *Intelligence and National Security* 4, no. 4 (October 1989): 660-718.

Betts, Richard. "Analysis, War and Decision: Why Intelligence Failures Are Inevitable." *World Politics* 31, no. 1 (October 1978): 61-89.

Brei, William S. *Getting Intelligence Right: The Power of Logical Procedure*. Occasional Paper Number Two. Washington, DC: JMIC, January 1996.

Clark, Robert M., *Intelligence Analysis: Estimation and Prediction*. Baltimore: MD: American Literary Press, 1996.

Folker, Robert D., Jr. *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods*. Occasional Paper Number Seven. Washington, DC: JMIC, January 2000.

Heuer, Richards J., Jr. *Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence, 1999.

Hogarth, Robin. *Judgement and Choice*, John Wiley, 1987.

Jervis, Robert. *Perception and Misperception in International Politics*. Princeton, NJ: Princeton University Press, 1977.

Jones, Morgan. *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*. New York: Random House, Inc., 1995.

Kam, Ephraim. *Surprise Attack*. Cambridge, MA: Harvard University Press, 1988.

Krizan, Lisa. *Intelligence Essentials for Everyone*. Occasional Paper Number Six. Washington, DC: JMIC, June 1999.

Kuhn, Thomas. *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press, 1970.

May, Ernest. *"Lessons" of the Past: The Use and Misuse of History in American Foreign Policy*. New York: Oxford University Press, 1973.

Merom, Gil. "The 1962 Cuban Intelligence Estimate: A Methodical Perspective," *Intelligence and National Security* 14, no. 3 (Autumn 1999): 48-80.

Platt, John R. "Strong Inference," *Science* 146, no. 3642 (16 October 1964): 347-353.

Russo, J. Edward, and Paul J. H. Shoemaker. *Decision Traps: Ten Barriers to Brilliant Decision-Making and How to Overcome Them*. New York: Simon and Schuster, 1989.

Young, Jay T. "US Intelligence Assessment in a Changing World: The Need for Reform," *Intelligence and National Security* 8, no. 2 (April 1993): 125-139.

ABOUT THE AUTHORS

David T. Moore is a senior technical leader at the National Security Agency. During 18 years of Intelligence Community service he has completed a variety of assignments in the Washington, DC area and overseas. These assignments enabled Mr. Moore to earn credentials in technical communications analysis, intelligence analysis, and intelligence research. He has created and taught intelligence analysis courses for NSA's National Cryptological School as well as for other government agencies. His most recent assignment was in the Art and Science of Analysis organization where his work focused on improving methodologies for intelligence analysis. He holds a B.A. in sociology/anthropology from Washington and Lee University and an M.S. in Strategic Intelligence from the Joint Military Intelligence College.

Lisa Krizan is a senior technical leader at the National Security Agency. A self-described "intelligence brat," she was introduced to the field by her father, Col. Allen J. Montecino, Jr., USAF, retired. Through diverse experience in intelligence support and production assignments, Ms. Krizan has earned credentials in technical communications analysis, intelligence research, and foreign language analysis, and has created and taught intelligence analysis courses for the National Cryptologic School. She received a B.S. degree in Business and Management from the University of Maryland and an M.S. in Strategic Intelligence from the Joint Military Intelligence College. Her master's thesis, "Benchmarking the Intelligence Process for the Private Sector" was the result of combining her studies in best business practices with her Intelligence Community work. Ms. Krizan is also the author of *Intelligence Essentials for Everyone*, published in June 1999 by the JMIC as Occasional Paper Number Six.

Mr. Moore and Ms. Krizan's current work on core competencies arose from their continuing advocacy for best practices in intelligence analysis, as members of the Art and Science of Analysis organization.

CORE COMPETENCIES FOR INTELLIGENCE ANALYSIS AT THE NATIONAL SECURITY AGENCY

David T. Moore and Lisa Krizan

Seekers of Wisdom first need sound intelligence.

— Heraclitus[1]

What makes an intelligence analyst successful in the profession? This question strikes at the heart of the National Foreign Intelligence Community's mission to provide actionable information to national leaders and decisionmakers. The imperative to answer this question stems from two types of pressures, external and internal. Externally, the component agencies face a world that demands responsiveness, agility, and flexibility. [2] Internally, they are charged with transforming outdated Cold War organizational structure, mentality, and methods. [3] This paper argues that, at least at the National Security Agency, identifying core analytic competencies that can be translated into managerial strategies is the surest way to ensure that intelligence analysts are successful.

As a member of the Intelligence Community (IC), the National Security Agency (NSA) is now pursuing an ambitious campaign to modernize its intelligence production mission and to mold its workforce accordingly.[4] Part of the modernization campaign is a new organizational model that places all intelligence analysts under the purview of an analytic deployment service. In this paradigm, individual analysts are assigned to specific production lines based on the capabilities of the former and the needs of the latter. However, for this model to work, staffers need to know what assets the analysts in the work force possess. Similarly, when intelligence agencies use precious few hiring allocations to bring in new intelligence analysts, they must maximize those opportunities, and only hire qualified personnel. But what is a qualified intelligence analyst?

---

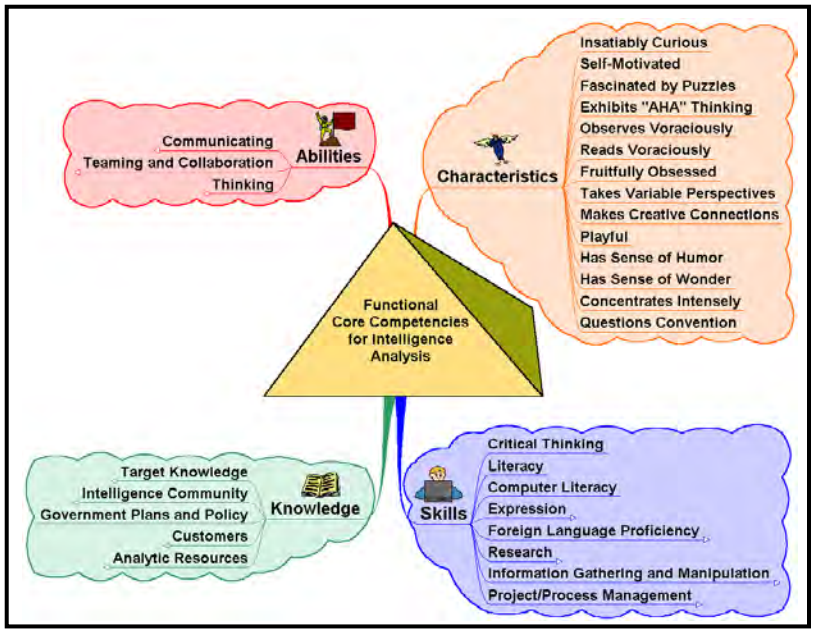
[1] From Brooks Haxton, translator, *Fragments, the Collected Wisdom of Heraclitus* (New York: Penguin, 2001), 33.

[2] John Gannon and others, National Intelligence Council, *Global Trends 2015: A Dialogue About the Future with Nongovernment Experts* (Washington DC: National Foreign Intelligence Board, 2000), 41, URL: *http://www.cia.gov/cia/publications/globaltrends2015/;* hereafter cited as National Intelligence Council. For other views of security threats to America see also Loch Johnson, *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security* (New York: New York University Press, 2000); and Robert D. Kaplan, *The Coming Anarchy: Shattering the Dreams of the Post-Cold War* (New York: Random House, 2000).

[3] George W. Bush, "National Security Presidential Directive 5," 9 May 2001. This directive instructs the Director of Central Intelligence to conduct a comprehensive review of U.S. intelligence. The order gives the DCI a broad mandate to "challenge the status quo."

[4] See URL: *http://www.nsa.gov/releases/nsa_new_enterprise_team_recommendations.pdf*, 1 October 1999, 16, accessed 3 November 2001. In this document, it is implicit that the Director, NSA recognizes that the agency's responsibility for the "production of signals intelligence" extends beyond "technical analysis of data" to "all-source" analysis of the context and implications of those data, especially but not exclusively for use within the agency itself.

In this paper the authors propose a set of functional core competencies for intelligence analysis, shown in the figure below, which provides a starting point for answering fundamental questions about the nature of ideal intelligence professionals, and how analysts who share these ideals can go about doing their work. Keeping in mind the complex nature of the threats to U.S. national security, we argue that the strategy for deploying intelligence analysts and for carrying out intelligence production must become more rigorous to keep pace with 21st Century foes, and to defeat them.



Functional core competencies for intelligence analysis..

The authors began exploring the art and science of intelligence analysis at their agency as part of a corporate initiative to add rigor to its analytic practice. Comments presented here on analytic thinking, its associated culture and processes, and its related technologies reflect conversations with intelligence experts both within and outside of government, and observation of analysts considered by their peers to be successful. We realized that definitions and descriptions of common characteristics, skills, knowledge, and abilities required for successful intelligence analysis were lacking, not only within our own agency but across the field of intelligence. We developed a set of functional core competencies for intelligence analysis that seem to apply across the intelligence profession in the government setting, not just for the types of analysis done at NSA. Our work has been reviewed by personnel in our agency as well as by individuals outside government, including academic experts on intelligence and

intelligence analysis.[5] They have made helpful suggestions for our model of functional core competencies.

Sherman Kent, who helped shape the national peacetime intelligence community, argues that intelligence requires its own literature. According to Kent, a key purpose of this literature is to advance the discipline of intelligence. Kent believed "[as] long as this discipline lacks a literature, its method, its vocabulary, its body of doctrine, and even its fundamental theory run the risk of never reaching full maturity."[6] Through the publication of articles on analysis and subsequent discussion, "original synthesis of all that has gone before" occurs.[7] In keeping with Kent's mandate to develop an intelligence literature that provokes discussion and further methodological development, we seek comment and further discussion among scholars of intelligence studies.

DEFINITIONS AND CONTEXT

> *Intelligence refers to information that meets the stated or understood needs of policymakers.... All intelligence is information; not all information is intelligence.*
>
> *— Mark Lowenthal*[8]

Intelligence is timely, actionable information that helps policymakers, decisionmakers, and military leaders perform their national security functions. The intelligence business itself depends on professional competencies, what John Gannon, former Chairman of the National Intelligence Council, refers to as "skills and expertise." He notes that "this means people—people in whom we will need to invest more to deal with the array of complex challenges we face over the next generation."[9] Analysis is the process by which

---

[5] The authors wish to acknowledge individuals within the Department of Defense who challenged our ideas and critiqued our work. Thanks also are due to James Holden-Rhodes, University of New Mexico; Robert Heibel, Mercyhurst College; Hugo Keesing, Joint Military Intelligence Training Center; Marilyn Peterson, Financial Analysis Coordinator, New Jersey Division of Criminal Justice; Adam Pode, formerly of Mercyhurst College; Robert David Steele, CEO, Open Source Solutions; and Russell Swenson, Joint Military Intelligence College. Colleagues in the international Generic Intelligence Training Initiative, sponsored by the U.S. Drug Enforcement Administration, also provided valuable comments.

[6] *Sherman Kent and the Board of National Estimates: Collected Essays,* Donald P. Steury, ed., (Washington DC: Center for the Study of Intelligence, Central Intelligence Agency, 1994), 14.

[7] See Sherman Kent, "The Need for an Intelligence Literature," *Studies in Intelligence*, Spring, 1955 (reprinted in Studies in Intelligence, 45th Anniversary Special Edition, Washington DC: Government Printing Office, 2001), 1-11.

[8] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, DC: CQ Press, 2000), 1-2.

people transform information into intelligence. Ultimately, analysis leads to synthesis and effective persuasion, or, less pointedly, estimation.[10] It does so by breaking down large problems into a number of smaller ones, involving "close examination of related items of information to determine the extent to which they confirm, supplement, or contradict each other and thus to establish probabilities and relationships."[11]

Since the advent of the Information Age, "[collecting] information is less of a problem and verifying is more of one."[12] Thus the role of analysis becomes more vital as the supply of information available to consumers from every type of source, proven and unproven, multiplies exponentially. Intelligence analysts are more than merely another information source, more than collectors and couriers of information to consumers. Further,

> [the] images that are sometimes evoked of policymakers surfing the Net themselves, in direct touch with their own information sources, are very misleading. Most of the time, as [policymakers'] access to information multiplies, their need for processing, if not analysis, will go up. If collection is easier, selection will be harder.[13]

At its best, the results of intelligence analysis provide just the right information permitting national leaders "to make wise decisions—all presented with accuracy, timeliness, and clarity."[14] The intelligence provided must "contain hard-hitting, focused analysis relevant to current policy issues....Therefore, analysis of raw information has the most impact on the decisionmaker and [therefore] producing high-quality analytical product should be the highest priority for intelligence agencies."[15]

Intelligence is judged, then, on its usefulness. But what criteria define "useful?" Amos Kovacs asserts that useful intelligence makes a "difference" to policymakers.[16] There is also an expectation that intelligence should be unbiased, although analysts with concerns

---

[9] Director of Central Intelligence National Security Advisory Panel, *Strategic Investment Plan for Intelligence Community Analysis* (Washington DC: Central Intelligence Agency, 2000), URL: *http://www.cia.gov/cia/publications/unclass_sip/index.html*, 11, accessed 29 September 2001.

[10] Lisa Krizan, *Intelligence Essentials for Everyone*, Joint Military College Occasional Paper Number Six (Washington DC: Joint Military Intelligence College, 1999), 29.

[11] R. H. Mathams, "The Intelligence Analyst's Notebook," in *Strategic Intelligence: Theory and Application*, 2d. ed. Douglas H. Dearth and R. Thomas Goodden, eds. (Washington, DC: Joint Military Intelligence Training Center, 1995), 88.

[12] R. H. Mathams, 88.

[13] R. H. Mathams, 88; Gregory F. Treverton, *Reshaping National Intelligence For an Age of Information* (Cambridge, UK; Cambridge University Press, 2001), 10.

[14] Loch K. Johnson, "Analysis for a New Age," *Intelligence and National Security* 11, no. 4 (October 1996): 658.

[15] Kevin P. Stack, "Competitive Intelligence," *Intelligence and National Security* 13, no. 4 (Winter 1998): 194.

about outcomes do influence the product by selecting which inputs to analyze.[17] Finally, as Michael Turner points out, analysts "from below" now join senior government officials in "setting the analytical agenda."[18] All policymakers and their subordinates are free to reject intelligence findings, no matter how persuasively argued they may be.

To say that policymakers may dismiss intelligence that doesn't support their presuppositions and policy objectives is to tell only half the story. There may be numerous reasons why policymakers do not accept intelligence. Gregory Treverton, former Vice-Chair of the National Intelligence Council, indicates that intelligence is ignored both when it brings inconvenient news and when it offers nothing new. In writing about the U.S. policy failures of the first Bush administration during the Balkan crisis, Treverton wonders, "If, in retrospect, the intelligence seems on the mark, did the policy failure derive from intelligence unheeded, or was the intelligence heeded but either not new or not really actionable?"[19]

Treverton adds that intelligence must anticipate the needs of policy. "By the time policy knows what it needs to know, it is usually too late for intelligence to respond by developing new sources or cranking up its analytic capacity."[20] A former policymaker himself, he asserts that intelligence is useful to policy at three stages during the life of an issue:

- If the policymakers are prescient, when the issue is just beginning; however there is likely to be little intelligence on the issue at that point.
- When the issue is "ripe for decision." Here policymakers want intelligence that permits alternatives to be considered; however, intelligence often is only able to provide background information necessary for understanding the issue.
- When the policymakers have made up their minds on the issue, but only if intelligence supports their view. They will be uninterested or even hostile when it does not support their view.[21]

These limitations notwithstanding, Treverton suggests that policymakers can and should establish a symbiotic relationship with the intelligence analysts who advise them:

> [If] you call them in, face to face, they will understand how much you know, and you'll have a chance to calibrate them. You'll learn more in fifteen minutes than you'd have imagined. And you'll also begin to target those analysts to your concerns and your sense of the issue.[22]

---

[16] Amos Kovacs, "Using Intelligence," *Intelligence and National Security* 12, no. 4 (October 1997): 148.

[17] Lowenthal, 4.

[18] Michael A. Turner, "Setting Analytical Priorities in U.S. Intelligence," *International Journal of Intelligence and Counterintelligence* 9, no. 3 (Fall 1996): 314.

[19] Treverton, 178.

[20] Treverton, 179.

[21] Treverton, 183-185.

Similarly, the analyst has responsibilities to the policymaker. In commenting on this relationship, Sherman Kent asserts

> [intelligence] performs a service function. Its job is to see that the doers are generally well informed; its job is to stand behind them with a book opened at the right page to call their attention to the stubborn fact they may be neglecting, and—at their request—to analyze alternative courses without indicating choice.[23]

In Kent's view, the intelligence analyst is required to ensure, tenaciously, that policymakers view those "right" pages, even when they may not wish to do so.

MEASURING SUCCESS IN INTELLIGENCE ANALYSIS

> *Intelligence must be measured to be valued, so let us take the initiative and ask our management, [and] the users, to evaluate us and our products.*
>
> *— Jan P. Herring*[24]

Any observer can expect that a successful intelligence analyst will have certain personal characteristics that tend to foster dedication to the work and quality of results. Such an analyst will also have specific abilities, skills, and knowledge to perform intelligence work. Finally such an analyst will have productive relationships with consumers. But how can success in intelligence analysis be measured?

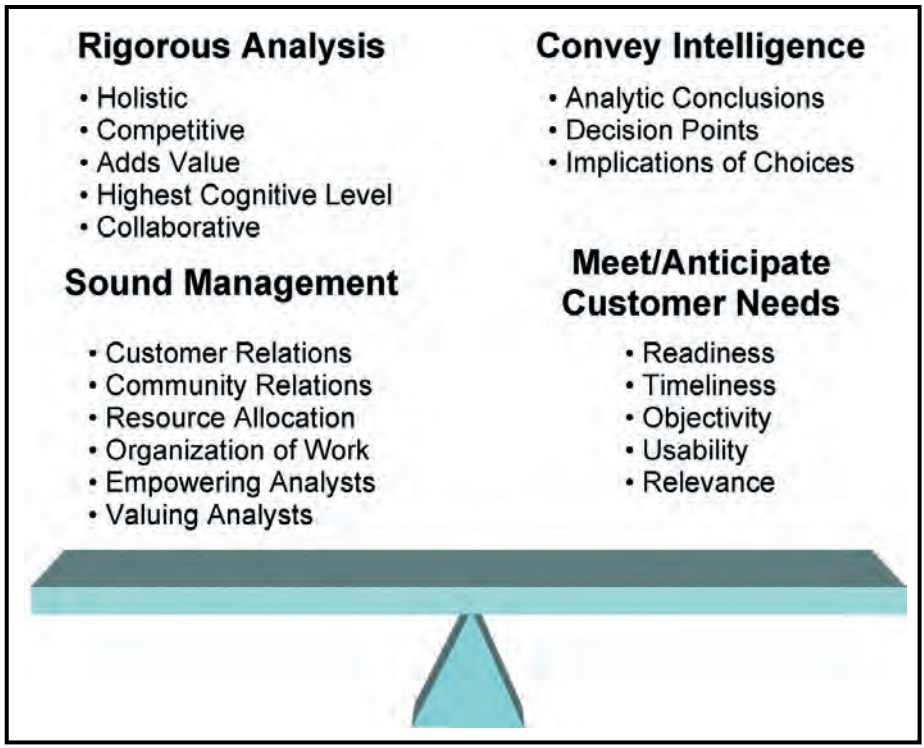
Measures of success have been based on job performance, including numbers of reports issued; volumes of raw data processed; or degree of consumer reliance on, or satisfaction with, products or services. However, these are measurements of outcome, only one facet of success. When analysis follows a rigorous process that allows an analyst to "add value" to information, and that results in timely, actionable intelligence used by consumers, then it may be judged successful. Thus, an assessment of success may be made by balancing measures of two basic criteria: intelligence process (processing and adding value to information) and intelligence product (meeting consumer needs). As depicted in the figure below, each can keep the other in balance, curbing any tendency toward "analysis paralysis"[25] on one side, and countering an assembly-line mindset on the other.

---

[22] Treverton, 191.

[23] Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton: Princeton University Press, 1949), 182.

[24] Jan P. Herring, *Measuring the Effectiveness of Competitive Intelligence: Assessing and Communicating CI's Value to Your Organization* (Alexandria, VA: Society of Competitive Intelligence Professionals, 1996), 63.



An intelligence evaluation scheme.

Intelligence Process

Successful intelligence analysis is a holistic process involving both "art" and "science." Intuitive abilities, inherent aptitudes, rigorously applied skills, and acquired knowledge together enable analysts to work problems in a multidimensional manner, thereby avoiding the pitfalls of both scientism and adventurism. The former occurs when scientific methodology is excessively relied upon to reveal the "truth"; the latter occurs when "inspiration [is] unsupported by rigorous analysis."[26]

[25] One potential pitfall of the analytic profession is the tendency to pursue analysis for its own sake, continually seeking more information, becoming locked into analysis and failing to reach conclusions. Rigorous methodology that emphasizes adding value to information and making it actionable for a specific consumer can break the cycle of such paralysis.

[26] Steven R. Mann, "Chaos Theory and Strategic Thought," *Parameters* 22, no. 3 (Autumn 1992): 67. Quoted in MSgt Robert D. Folker, Jr., *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods*, Occasional Paper Number Seven (Washington DC: Joint Military Intelligence College, 2000), 13.

A vital contributor to the analytic process is a spirit of competition, both within an intelligence-producing agency and especially between intelligence agencies. There is a tendency for analysts working together to develop a common mindset. This trap occurs typically when analysts fail to question their assumptions about their role in the intelligence process and about the target. The Council on Foreign Relations' independent task force on the future of U.S. intelligence recommends that "competitive or redundant analysis be encouraged" precisely for these reasons.[27]

Successful analysis adds value—to the information itself, to institutional knowledge, to fellow intelligence professionals, to the process, and to the institution or unit itself—in terms of reputation and the degree to which good analytic practices endure despite changes in target, consumer, and personnel. Successful analysts are those whose work, whenever possible goes to the level of making judgments or estimating. The analysts' risks in doing so are carefully calculated, for successful analysts rely on critical thinking. Nor do successful analysts settle for the first answer their analysis reveals. Rather they employ rigorous methods to push beyond the obvious conclusions. However, tendencies toward arrogance in trend-spotting analysis are tempered by self-awareness of biases and assumptions, strengths and weaknesses. And most importantly, successful analysts collaborate at every opportunity. Such measures ensure that analytic results, even if controversial, remain grounded in reality.

What role does management play in ensuring analytic success? First and foremost, management effectively uses financial and political capital to ensure that analysts have access to consumers, and to the resources they require to answer those consumers' intelligence needs. This includes the organization of the work itself, allocation of materiel and personnel, and coordination with consumers and other producers. When management is successful, the analyst has the necessary tools and the correct information for successful intelligence analysis. Good morale among analytic personnel becomes an indicator of effective management. A good understanding of the unit's mission and the analysts' own satisfaction with his or her performance naturally produces a feeling of empowerment and a belief that the organization places great value on analytic talent.

Intelligence Product

The products of successful analysis convey intelligence that meets or anticipates the consumer's needs; these products reveal analytic conclusions, not the methods used to derive them. Intelligence products are successful if they arm the decisionmaker, policymaker or military leader with the information and context—the answers—needed to win on his or her playing field. Such intelligence enables consumers to be more effective by making them smarter than they were before, smarter than the people they play with, and smarter than those they play against. Successful intelligence enables consumers to outwit

---

[27] Council on Foreign Relations, *Making Intelligence Smarter: The Future of U.S. Intelligence: A Report of an Independent Task Force*, 11, URL: *http://www.fas.org/irp/efr.html*, accessed 4 June 2001.

opponents, protect U.S. persons, bring aid to the nation's allies, or to judge levels of trust. It does so by revealing decision points, actions or choices available to a consumer, and the implications of choosing one over another.

Yet, consumers rarely acknowledge explicitly the role that good intelligence plays in their own success. While they may be quick to bring intelligence failures to the attention of the producing organization, consumers do not always give feedback on successful outcomes enabled by intelligence. Thus intelligence analysts and their management historically have looked within the production organization for ways to measure success, falling into the trap of "bean-counting." But there is a better way.

Readiness: Intelligence systems must be responsive to existing and contingent intelligence requirements of consumers at all levels.

Timeliness: Intelligence must be delivered while the content is still actionable under the consumer's circumstances.

Accuracy: All sources and data must be evaluated for the possibility of technical error, misperception, and hostile efforts to mislead.

Objectivity: All judgments must be evaluated for the possibility of deliberate distortions and manipulations due to self-interest.

Usability: All intelligence output must be in a form that facilitates ready comprehension and immediate application. Intelligence products must be compatible with the consumer's capabilities for receiving, manipulating, protecting, and storing the product.

Relevance: Information must be selected and organized for its applicability to a consumer's requirements, with potential consequences and significance of the information made explicit to the consumer's circumstances.

Measures of success for intelligence products[28]

Six "underlying ideas or core values" for intelligence analysis, identified by William Brei for operational-level intelligence, and shown in the figure above, establish the analyst's "essential work processes."[29] Since they are defined in terms of the consumer, they also can be used as a checklist to rate the quality of products provided to the consumer. Brei asserts that they "provide specific qualitative objectives for managers and leaders, and a framework for standards against which intelligence services should be judged."[30] While qualitative feedback from consumers aids evaluation of some of these objectives, the absence of consumer input does not prevent their being used in self-evaluation.

---

[28] William S. Brei, Captain, USAF, *Getting Intelligence Right: The Power of Logical Procedure*, Occasional Paper Number Two (Washington DC: Joint Military Intelligence College, 1996), 6.

[29] Brei, 6.

[30] Brei, 5.

The principles of Readiness and Timeliness evaluate the intelligence service's basic ability to perform intelligence production. These two principles are limiting factors affecting what the producer can do to "achieve accurate data, objective judgments, usable formats, and relevant products."[31] Once production Readiness and Timeliness are evaluated, the other four of Brei's fundamental principles then can be arranged in a checklist or a series of questions about intelligence products. Typical questions might include:

- Was the reported intelligence accurate? (*Accuracy*)
- Are there any distortions in the reported judgments? (*Objectivity*)
- Is the reported intelligence actionable? Does it facilitate ready comprehension? (*Usability*)
- Does it support the consumer's mission? Is it applicable to the consumer's requirements? Has its significance been made explicit? (*Relevance*)

These four principles also overlap, and poor quality in one can affect the quality of another. Brei asserts that accurate data provide the foundation for subsequent objective judgments, and the expression of objective judgments in a usable form provides much of the basis of a relevant product. Thus, unverified data cannot only cost an intelligence product its Accuracy, but also damage its Relevance to the customer.[32]

Although Brei's principles do not require consumer input in the evaluation of intelligence, the process of measuring the effectiveness of a product is enhanced with consumer participation. Brei suggests: "[L]isten to their complaints."[33] However, this does not guarantee that the responses will address the product of interest. Rather, the analyst needs to ask directly for specific feedback from the consumer. This is most effective if the analysts and managers have collaborative relationships with consumers. Lacking such relationships, producers may attach survey questions to intelligence products, prompting consumers to respond regarding the utility of the service provided. Admittedly, this elicitation may be disturbing, as consumers are more likely to respond when they are unhappy with the product than when they are pleased. Further, regardless of the assessment of worth or value, some consumers will never respond.

Brei's principles provide a means for evaluating a given intelligence product based on the meaning it conveys and the value of that intelligence to the consumer. His approach, when combined with an "insider's" view of the intelligence production process, analytic methods and personnel management practices, makes a comprehensive evaluation of intelligence analysis appear possible. In the sections to follow, the concept of core competencies for intelligence analysis is developed, from which may emerge some useful suggestions for operationalizing the concept of an "art and science" of intelligence analysis.

[31] Brei, 6.

[32] Brei, 6.

[33] Brei, 5.

CHARACTERISTICS OF SUCCESSFUL INTELLIGENCE ANALYSTS

> A sophisticated intelligence analyst is one who is steeped in the history and culture of a region, has lifelong interest in the area, and approaches the study of the region as a professional responsibility, and probably as an avocation as well.
>
> *— Ronald D. Garst and Max L. Gross*[34]

Who are the most successful intelligence analysts? What makes them successful? In setting forth the functional core competencies for successful intelligence analysis we observe there are characteristics which, while not necessary for successful intelligence analysis per se, do seem to be associated with analysts considered to be the most successful at their trade.[35] It should be noted, however, that not all successful analysts exhibit all these characteristics. The characteristics highlighted in the graphic below are a representative superset, and while individual analysts do seem to share certain characteristics, they do not share all of them in equal measure.

Probably the most indispensable characteristics of successful intelligence analysts are high self-motivation and insatiable curiosity. Analysts want to know everything they can about the objects under their scrutiny. Reading and observing voraciously, they ferret out every possible piece of information and demonstrate a sense of wonder about what they discover. As new fragments appear, novel connections are discovered between the new and older information as a result of intense concentration leading to epiphanous moments of "aha" thinking. The most successful analysts tend to enjoy their work—"It's play, not work." Indeed, they often will stay late at the office to pursue a thorny problem or an engaging line of reasoning.

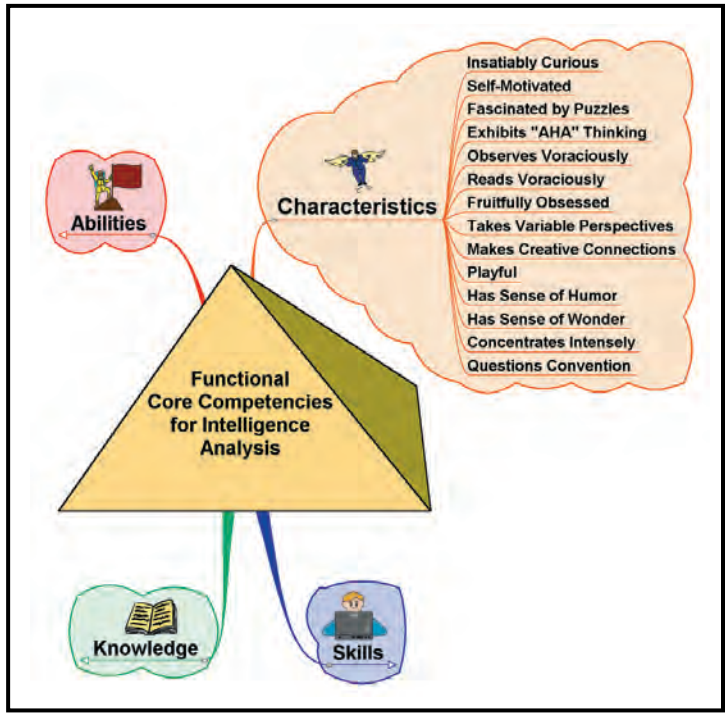
These characteristics also describe the values, standards, and beliefs of a dynamic, living analytic culture. As such, they may be used as preliminary indicators during the hiring process to identify prospective employees. A person with many of the characteristics listed may be predisposed to being a successful analyst, if the appropriate skills, abilities, and

---

[34] Ronald D. Garst and Max L. Gross, "On Becoming an Intelligence Analyst," *Defense Intelligence Journal* 6, no. 2 (Fall 1997): 55.

[35] The authors base their establishment of core competencies primarily on two initiatives taken as NSA in recent years. The first is an extensive formal job analysis conducted by industrial psychologists in the mid-1990s. Identification of some of the knowledge areas, skills and abilities required for intelligence analysis came out of that study, which is cited extensively in Lisa Krizan, *Intelligence Essentials for Everyone*, JMIC Occasional Paper Number Six (Washington, DC: JMIC, 1999). The second initiative is the ongoing work of the Arts and Science of Analysis research organization established at NSA in early 2000. As members of that organization, the authors participated in studies and interviews yielding insights into the behaviors applied by NSA intelligence analysts on the job.

necessary knowledge to perform the work are also present. Employee orientation programs that acknowledge these characteristics may be most successful in initiating new employees into the analytic culture. When personal characteristics are embodied in compelling "war stories" told by mentors and peers, they can reinforce the cultural values of the agency, building corporate loyalty by reinforcing the sense of membership.



Characteristics of successful intelligence analysts.

Indoctrination into a particular analytic culture can also have negative implications. Although it may build loyalty, enhance behaviors, and inculcate values, it can also prevent objective analysis by reinforcing "group" thought patterns and analytic methodologies. The culture must allow for "a spirit of creativity to emerge and prosper."[36]

These personal characteristics of successful intelligence analysts are but one factor among many in influencing the success of intelligence process and product. Abilities and skills provide the tools for performing good intelligence analysis. Knowledge provides raw material for analysis as well as for an appreciation of the context and relevance of information.

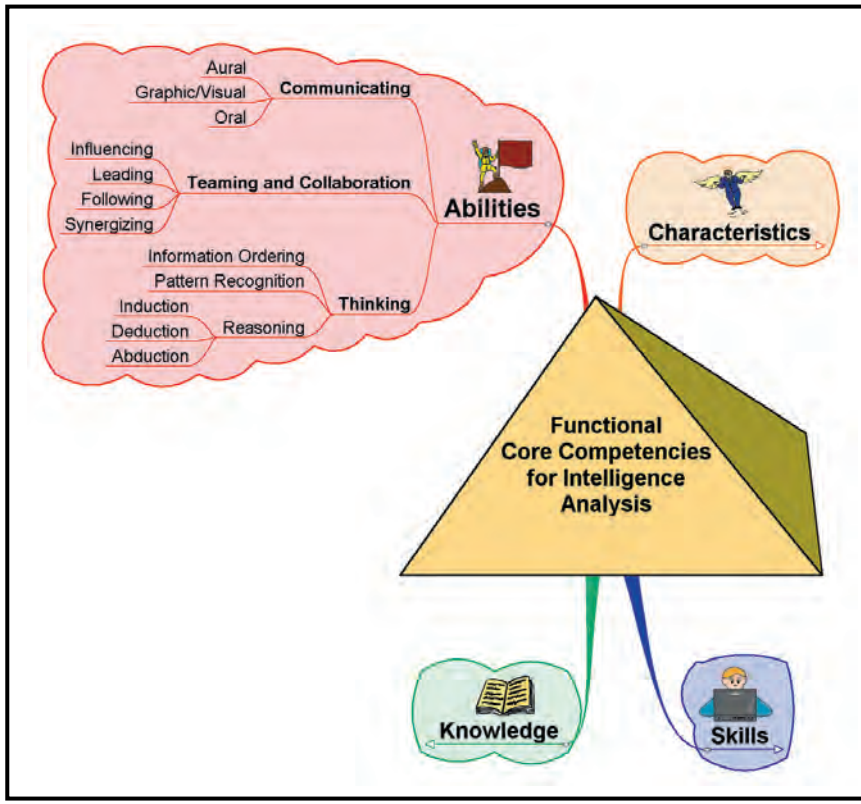
---

[36] Don McDowell, *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users* (Cooma, Australia: Istana Enterprises, Pty. Ltd., 1998), 216.

ABILITIES REQUIRED FOR INTELLIGENCE ANALYSIS

The competent intelligence analyst must have a unique combination of talents.
— Ronald D. Garst and Max L. Gross[37]

Abilities arise from aptitudes that can develop from an individual's innate, natural characteristics or talents. Although aptitudes may largely be determined by a person's genetic background, they may also be enhanced through training.[38] We find the abilities shown here to be necessary for intelligence analysis.



Abilities required for successful intelligence analysis.

[37] Garst and Gross, 47.

[38] Conversation with Dr. S. Alenka Brown-Vanhoozer, Director, Center for Cognitive Processing Technology, Advanced Computing Technologies, BWXT Y-12, Oak Ridge, TN, April 2001.

Communicating

Almost all animate life communicates, but humans are unique in possessing a brain structured to permit abstract, symbolic communication. Three communication abilities appear necessary for various aspects of intelligence analysis:[39]

- **Aural:** The ability to hear, listen to, and understand spoken words and sentences is one of the essential means humans employ to take in information. Aural ability can be improved through specific techniques of "active listening." This ability greatly enhances analysts' performance of certain technical tasks, and their interaction with consumers, peers and managers.
- **Graphic/Visual:** The ability to see, view, and understand graphic/visual symbols developed early in human history. Along with the ability to interpret symbols came the ability to present information in a graphic or visual manner so that others could understand. Even in speech, a majority of human communication remains non-verbal (that is, graphic or visual).[40] Developing this ability allows for effective graphical presentation of intelligence, which can dramatically heighten its impact.
- **Oral:** The ability to communicate via spoken words and sentences so that others will understand is unique to humans. While the physical capability has evolved over eons, key developmental milestones occur during the first years of life. The development of oral and aural abilities are closely linked. Effective oral communication directly affects the intelligence analyst's credibility.

Teaming and Collaboration

Humans are a social species, and associated abilities have evolved with human development. Teaming and collaborating were essential when proto-humans moved from the relative safety of the trees onto the more dangerous plains of Africa. Their collective lives depended on social abilities to solve problems and overcome threats. While today's threats have changed, humans retain these abilities in order to live and work together.

Teaming and collaboration abilities enhance intelligence analysis, since the analyst's relationship with consumers, peers, subordinates, and supervisors shapes the intelligence production process. Formalized means of enhancing all these abilities can lead intelligence professionals to considerably greater effectiveness as analysts and leaders of analysts. This is why the Director of Central Intelligence has indicated that collaboration is a cornerstone of strategic intelligence.[41] A collaborative environment also minimizes the likelihood of intelligence failures. For example, had imagery analysts communicated

[39] We do not suggest that individuals lacking one or more of these abilities due to physical impairment would be unable to perform intelligence analysis. However, we do suggest that in the absence of corrective technologies, an impaired person may not be able to perform certain functions of analysis or production that depend on the impaired ability.

[40] Conversation with Dr. S. Alenka Brown-Vanhoozer, April 2001.

[41] Director of Central Intelligence National Security Advisory Panel, accessed 1 June 2001.

effectively with their counterpart area analysts in 1999, the "Yugoslav War Office" bombed by U.S. forces that spring may have been identified as the Chinese Embassy in time to avoid the resultant tragedy.[42]

We identify four distinct teaming abilities, to show the complexity of the concept. Typically, formal training programs address leadership abilities only in the context of the management function; here, we focus on the analysis process itself.

- **Influencing:** Those with this ability effectively and positively influence superiors, peers, and subordinates in intelligence work. Analysts often need to persuade others that their methods and conclusions are valid, and they often need to leverage additional resources. The ability to influence determines the level of success they will have in these areas.
- **Leading:** Those who are more senior, more skilled, and more successful in intelligence analysis have an obligation to lead, that is, to direct others and serve as role models. The ability to lead involves working with and through others to produce desired business outcomes. Thus, developing leadership abilities enhances the field of intelligence analysis.
- **Following:** Almost every grouping of humans has a leader. Everyone else is a follower. Analysts must enhance their abilities to work within a team, taking direction, and acting on it.
- **Synergizing:** Drawing on the other three teaming abilities, players in the intelligence process cooperate to achieve a common goal, the value of which is greater than they could achieve when working alone.

Thinking

> As our species designation—*sapiens*—suggests, the defining attribute of human beings is an unparalleled cognitive ability. We think differently from all other creatures on earth, and we can share those thoughts with one another in ways that no other species even approaches.
>
> — *Terence W. Deacon, The Symbolic Species.*[43]

Intelligence analysis is primarily a thinking process; it depends upon cognitive functions that evolved in humans long before the appearance of language.[44] The personal characteristics of intelligence analysts are manifested in behaviors that reflect thinking and/or the inherent drive to think. Our national survival may depend on having better developed thinking abilities than our opponents. Three basic thinking abilities are

[42] Gregory Treverton, 10.

[43] Terence W. Deacon, *The Symbolic Species: The Co-Evolution of Language and the Brain* (London: W.W. Norton & Company, Ltd., 1997), 21.

[44] Keith Devlin, "The Role of Conceptual Structure in Human Evolution" in Bernhard Ganter and Guy W. Mineau, eds, *Conceptual Structures: Logical, Linguistic, and Computational Issues*, 8th International Conference on Conceptual Structures (Berlin: Springier Verlag, 2000), 1.

required for intelligence analysis. Given the limitations imposed by each one of them, only simultaneous application of all three may yield successful intelligence analysis.

- **Information Ordering:** This ability involves following previously defined rules or sets of rules to arrange data in a meaningful order. In the context of intelligence analysis, this ability allows people, often with the assistance of technology, to arrange information in ways that permit analysis, synthesis, and extraction of meaning. The arrangement of information according to certain learned rules leads the analyst to make conclusions and disseminate them as intelligence. A danger arises, however, in that such ordering is inherently limiting—the analyst may not look for alternative explanations because the known rules lead to a ready conclusion.
- **Pattern Recognition:** Humans detect patterns and impose patterns on apparently random entities and events in order to understand them, often doing this without being aware of it. Stellar constellations are examples of imposed patterns, while criminal behavior analysis is an example of pattern detection. Intelligence analysts impose or detect patterns to identify what targets are doing, and thereby to extrapolate what they will do in the future. Pattern recognition lets analysts separate "the important from the less important, even the trivial, and to conceptualize a degree of order out of apparent chaos."[45] However, imposing or seeking patterns can introduce bias. Analysts may impose culturally defined patterns on random aggregates rather than recognize inherent patterns, thereby misinterpreting the phenomena in question.
- **Reasoning:** The ability to reason is what permits humans to process information and formulate explanations, to assign meaning to observed phenomena. It is by reasoning that analysts transform information into intelligence, in these three ways:
  1. **Induction:** Inductive reasoning combines separate fragments of information, or specific answers to problems, to form general rules or conclusions. For example, using induction, a child learns to associate the color red with heat and heat with pain, and then to generalize these associations to new situations.[46] Rigorous induction depends upon demonstrating the validity of causal relationships between observed phenomena, not merely associating them with each other.

  2. **Deduction:** Deductive reasoning applies general rules to specific problems to arrive at conclusions. Analysts begin with a set of rules and use them as a basis for interpreting information. For example, an analyst who follows the nuclear weapons program of a country might notice that a characteristic series of events preceded the last nuclear weapons test. Upon seeing evidence that those same events are occurring again, the analyst might deduce that a second nuclear test is imminent.[47] However, this conclusion would be made cautiously, since deduction works best in

---

[45] Garst and Gross, 47.

[46] Jerome K. Clauser and Sandra M. Weir, *Intelligence Research Methodologies, An Introduction to Techniques and Procedures for Conducting Research in Defense Intelligence* (Washington DC: Defense Intelligence School, 1975), 81.

[47] Clauser and Weir, 81.

closed systems such as mathematics, making it of limited use in forecasting human behavior.

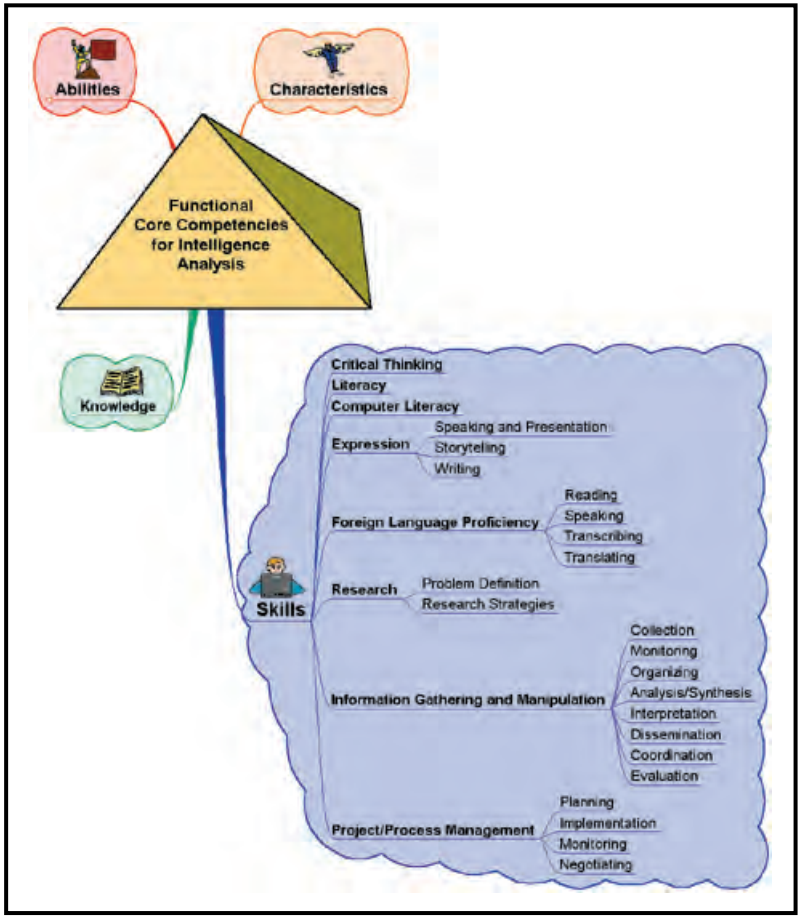
3. **Abduction:** Abductive reasoning describes the thought process that accompanies "insight" or intuition. When the information does not match that expected, the analyst asks "why?," thereby generating novel hypotheses to explain given evidence that does not readily suggest a familiar explanation. For example, given two shipping manifests, one showing oranges and lemons being shipped from Venezuela to Florida, and the other showing carnations being shipped from Delaware to Colombia, abductive reasoning is what enables the analyst to take an analytic leap and ask, "Why is citrus fruit being sent to the worldwide capital of citrus farming, while carnations are being sent to the world's primary exporter of that product? What is really going on here?" Thus, abduction relies on the analyst's preparation and experience to suggest possible explanations that must then be tested. Abduction generates new research questions rather than solutions.[48]

[48] Chong Ho Yu, "Abduction? Deduction? Induction? Is There a Logic of Exploratory Data Analysis," Paper presented at the annual meeting of the American Education Research Association, New Orleans, LA, April 1994, URL: *http://seamonkey.ed.asu.edu/~behrens/asu/reports/Peirce/Logic_of_EDA.html*, accessed 6 June 2001.

SKILLS REQUIRED FOR INTELLIGENCE ANALYSIS

Any institution that relies on professionals for success and seeks to maintain an authentic learning climate for individual growth must require its members to read (to gain knowledge and insight), research (to learn how to ask good questions and find defensible answers), discuss (to appreciate opposing views and subject their own to rigorous debate), and write (to structure arguments and articulate them clearly and coherently).

— Gregory D. Foster[49]



Skills required for successful intelligence analysis.

[49] Gregory D. Foster, "Research, Writing, and the Mind of the Strategist," *Joint Force Quarterly* 11 (Spring 1996): 74-79.

Whereas aptitudes and related abilities probably stem from an analyst's genetic makeup, a skill represents learned expertise or proficiency based on a particular ability or set of abilities. At least eight types of skills, shown here, are required for successful intelligence analysis.

Critical Thinking

It is by thinking that analysts transform information into intelligence. Critical thinking is the cognitive skill applied to make that transformation. Critical thinking can be defined as

> [An] intellectually disciplined process of actively and skillfully conceptualizing, applying, analyzing, synthesizing, and/or evaluating information gathered from, or generated by, observation, experience, reflection, reasoning, or communication, as a guide to belief and action....Thinking about [our] thinking while [we're] thinking in order to make [our] thinking better.[50]

> There is a clear need to educate and train intelligence analysts to use their minds...[Only] by raising their awareness can the intelligence unit be assured that the analysts will avoid the traps in being slave to conformist thought, precedent and imposed cultural values—all enemies of objective analysis.[51]

An ordered thinking process requires careful judgments or judicious evaluations leading to defensible conclusions that provide an audit trail. When the results of analysis are controversial, subject to alternate interpretations, or possibly wrong, this audit trail can prove essential in defending the process used to reach the conclusions.

Effective critical thinking also includes routine, systematic questioning of the premises upon which decisions are based. Without critical thinking, current beliefs and methods are not questioned, as long as they appear to produce results that can be reasonably explained. Yet they can prevent analysts from making alternative interpretations. Writing rhetorically, Gregory Treverton asks, "If intelligence doesn't challenge prevailing mind-sets, what good is it?"[52]

Intelligence failure can be the result when alternative premises are ignored, as happened from the mid-1970s to the mid-1990s in Sweden. During that time, the Swedish Navy expended considerable effort and ordnance attempting to "destroy" intruding Soviet submarines. Swedish naval analysts (and others) repeatedly acknowledged failure, rationalizing it as a "David versus Goliath" contest: Sweden's tiny navy was no match for the

---

[50] National Drug Intelligence Center, *Basic Intelligence Analysis Course*, # 9, PowerPoint Presentation, April 2001.

[51] McDowell, 216.

[52] Treverton, 5.

technologically advanced Soviet submarine fleet. It was not until 1995 that Swedish defense chief Owe Wiktorin revealed the truth; detected intruders previously believed to be submarines were in fact minks swimming in the waters off the Swedish coast. Blinded by the premise that the Soviets wanted to make war against Sweden, the navy had ignored this possible explanation for their failure to destroy "enemy" submarines, despite the fact that the alternative premise had been suggested as early as 1987.[53] An obvious conclusion from this story is that corporate mechanisms for questioning analytic premises could have resolved this intelligence question nearly a decade earlier. The lesson for present-day intelligence analysts is clear: corporate processes for intelligence analysis must allow for, and indeed, institutionalize, the questioning of premises.

Literacy

Intelligence analysis requires the reading and comprehension of written sentences and paragraphs, often in multiple languages, at many points in the intelligence process. Prospective intelligence analysts must be literate in order to perform their work at the most basic level, making this skill a prerequisite for employment. Literacy skills are crucial for understanding the target, the consumer and the intelligence process. Literacy is also necessary for conducting research.

Computer Literacy

It is a given that in the 21st Century, the computer is an essential tool for intelligence analysis. Today, analysts must be highly skilled in the use of computers themselves and in the use of software that will aid analysis. Word processing, spreadsheet, and presentation programs, as well as specific programs that assist at all stages of the analytic process, are the essential tools that can bolster success. However, tools themselves do not provide "truth" (if such can be said to exist in the intelligence analysis context). Rather, these tools for manipulation, correlation, and presentation of information are a means to an end: the production of intelligence. An analyst's skillful use of them hastens arrival at that end.

The fact that analysts are faced with massive volumes of data also makes use of selection and filtering tools essential. The analyst depends on these tools to make a "first cut" on the collected information. The tools are used to filter non-relevant information items and retain only those items that are pertinent to the issue being analyzed.

Expression

The results of analysis are useless if they are poorly presented. "The capable analyst must be competent and experienced in presenting analysis both orally and in writing."[54] Effective oral and written skills are therefore essential for the intelligence analyst. Fail-

[53] William H. Starbuck, "Unlearning Ineffective or Obsolete Technologies," *International Journal of Technology Management* 11, nos. 7/8 (Winter 1996): 725-726.

[54] Garst and Gross, 49.

ures of intelligence can indeed occur when the results of analysis are inadequately presented. For example, Berkowitz and Goodman note that lengthy daily or weekly briefings may be inadequate means for informing officials, regardless of their content. Warnings go "unheard because the officials [find] the hour-long briefings to be an inefficient use of their time and [stop] attending."[55] Similarly, they conclude that inadequate intelligence reporting of unrest in Iran in 1978 contributed to the U.S. Intelligence Community's failure to predict the fall of the Shah.[56] These examples also make it clear that whichever method of informing policymakers is selected, the resultant products must be concise, tailored ones that masterfully present the intelligence to the intended consumer or in the consumer's frame of reference.

- **Speaking and Presentation:** The oral presentation of information, particularly to senior officials, otherwise known as "briefing," and often accompanied by visual aids, allows an effective analyst to tailor both the content and delivery method to the consumer's abilities or predilections. The briefing's timing, level of detail, format and tone may all be matched to the consumer. In particular, key facts and conclusions come at the beginning of the exchange and determine its organization.[57] Effective briefing goes beyond these technical considerations. The heart of the intelligence briefing is the presenter's relationship with the consumer, thus, "the essence of briefing is not simply the projection of information, but rather the art of promoting understanding between individuals."[58] Through the briefing process, the presenter puts information into the consumer's frame of reference, making clear the possibilities for decision, action and consequences, thereby creating intelligence.
- **Storytelling:** While well-honed speaking and presentation skills allow effective intelligence dissemination, well developed storytelling skills ensure that intelligence is convincingly conveyed. Storytelling involves more than just creating the story. Its power lies in the way the story is told. In the words of transformational storytelling expert Stephen Denning, "[the] look of the eye, the intonation of the voice, the way the body is held, the import of a subtle pause, and [the storyteller's] own response to the audience's responses—all these aspects ... make an immense contribution to the meaning of the story for [the] audience."[59] Too often the consumer does not understand a poorly told but important story buried in a sophisticated presentation, making storytelling an essential skill for intelligence professionals.

---

[55] Bruce D. Berkowitz and Allan E. Goodman, *Strategic Intelligence for American National Security* (Princeton: Princeton University Press, 1989), 32.

[56] Berkowitz and Goodman, 202.

[57] Krizan, 40, 42-46.

[58] Benjamin T. Buring, LT, USN, *Function vs. Form: Successfully Briefing the Intelligence Story*, MSSI thesis (Washington, DC: JMIC, August 2001), 24.

[59] Stephen Denning, *The Springboard: How Storytelling Ignites Action in Knowledge-Era Organizations* (Boston, MA: Butterworth Heineman, 2001), xxii.

Storytelling in this context is not about fiction; it is not about "once upon a time." Rather, intelligence storytelling involves creating scenarios and alternative futures for consumers. Intelligence assessments that provide a variety of possible outcomes, recounted in considerable detail, can give the consumer clues to the most effective policies or strategies. An example of varying analytic outcomes expressed as scenarios can be found in the National Intelligence Council's *Global Trends 2015*. Four alternative futures for the next 15 years are outlined in addition to the principal scenario. These alternatives suggest a variety of possible outcomes based on population trends, resource availability, technological advances, economic conditions, ethnic identity and governance, and local and regional conflicts. The significance for the policymaker is that the future is fluid.[60] While all the alternatives are possible, certain political and strategic decisions could influence which outcome is most likely to occur. Being prepared for various outcomes enables the policymaker to be proactive and to respond appropriately as events unfold.

- **Writing:** The basic vehicle by which intelligence historically has been purveyed is the written report. At the beginning of the 21st Century this remains the case. Yet many contemporary intelligence analysts lack this basic skill, and improvement "of writing skills, basic though it may be, is often required as part of becoming a competent intelligence analyst."[61]

Foreign Language Proficiency

To be truly successful, analysts must be proficient in the language(s) employed by the subjects of their analysis. Without such proficiency they cannot completely comprehend target intentions and actions. When analysts misunderstand their targets, the intelligence they provide to consumers thus will be inaccurate or misleading.

Once upon a time, many intelligence analysts could rely upon the skills of professional linguists for translation of target information. Now this luxury has become unavailable to all but a few intelligence analysts working the largest, best-funded intelligence problems.[62] Foreign language proficiency has thus become a necessity for all who perform intelligence analysis.

If budget and personnel cuts are insufficient reason for analysts to have foreign language proficiency, changes in intelligence targets provide additional arguments for its necessity. Although targets of interest have traditionally used their native language(s) for internal communications, many employed non-native languages such as English for international communications and publications. This was especially true of the first decade of

[60] National Intelligence Council, 2000, 83-85.

[61] Berkowitz and Goodman, 54.

[62] For one view of the staffing cuts at the National Security Agency, see Mathew M. Aid, "The Time of Troubles: The US National Security Agency in the Twenty-First Century," *Intelligence and National Security* 15, no. 3, (Autumn 2000): 5-9.

the popular use of the Internet, when English was the *lingua franca* of that medium. However, this is changing. The use of native languages in international communications is growing both on and off the Internet. Thus, proficiency in non-English languages is necessary for analysis of information, approximately 80 percent of which "is *not* secret, is *not* online, is *not* in English, is *not* government associated, but is in the private sector, and is *not* available locally to the analyst."[63]

Furthermore, foreign language proficiency provides more than just a translation of non-English materials. The structure of a target's language and that target's culture are closely related. One well-known theory of this relationship, by Edward Sapir and Benjamin Whorf, posits that "language is a force in its own right and it affects how individuals in a society conceive and perceive reality."[64] Thus concepts essential to understanding the target are communicated in a context that goes beyond simplistic translation.

For example, the German terms *Gemeinschaft* and *Gesellschaft* both translate into English as "community." Yet this translation ignores the interpersonal nature of the relationship among the members of the first type of community, and the business context of the second. An analyst relying on translation by another might not be aware of the nature of the "community" in the material being analyzed.

In Somali there are two pronouns for the English "we." A speaker of Somali uses the pronoun *annagu* when referring to the speaker and someone other than the person being addressed. Conversely, the use of the pronoun *innagu* includes the person being addressed. So if someone says in English, "We are going to the movie," the question of "Who is 'we'?" must be asked. In Somali there is no doubt: If annagu are going to the movies, the person being addressed is not going; if innagu are going to the movies then the person being addressed is going. Again, an analyst depending on a translation into English must rely on the translator to convey that contextual information. This inclusion or exclusion from a group can be quite significant. There is a considerable difference between "annagu are going to blow up the embassy," and "innagu are going to blow up the embassy." This distinction is especially significant to the intelligence analyst in this case, even if the implications for the embassy remain the same.

Even the distinction between intelligence and information is language-derived. The Sinitic term *qingbao* refers to a concept that can be understood either as "information" or "intelligence."[65] This latter distinction is a "Western one not shared by East Asian languages or presumably their speakers," according to the Foreign Broadcast Information

[63] Robert David Steele, "The New Craft of Intelligence: an Alternative Approach Oriented to the Public," Conference on The Future of Intelligence in the 21st Century, Priverno, Italy, 14-16 February 2001. The quote is from Steele's remarks and is not in his published version of the paper. Clarification was made via personal email communication, 18 May 2001. Because the conference operated under the "Chatham House Rule," Mr. Steele is quoted with permission.

[64] Carol R. Ember and Melvin Ember, *Anthropology*, 9th ed. (Upper Saddle River: Prentice Hall, 1999), 225.

[65] *Concise English-Chinese/Chinese-English Dictionary*, 2nd ed. (Oxford: Oxford University Press, 1999), 363.

Service editor of the Chinese intelligence collection manual, *Guofang Keji Qingbaoyuan ji Houqu Jishu*.[66] Context must determine the translation, and an analyst lacking foreign language skills must trust the linguist to correctly understand that context. The expertise required for that understanding might render the linguist a better intelligence analyst than the original analyst. This begs the question: "Is such duplication of personnel affordable?"

We recognize that certain forms of technical analysis have previously not required foreign language proficiency. We suggest, however, that it is not truly known, nor can we know, whether foreign language proficiency would have enhanced that analysis. Some technical metadata analysis clearly does not require language proficiency. However, analysis of other types of metadata may indeed require foreign language proficiency and we caution against dismissing out of hand the need for it. Furthermore, staffing cuts require that analysts review both data and metadata. Even if the metadata do not require foreign language competency, the underlying data do require it. In addition, essential technical meaning is lost in the translation between linguist and technical analyst; technical analysts often need that original source and its context. This can be gained only from proficiency in the original language. Ultimately, foreign language proficiency enables the analyst to engage in a holistic, comprehensive analytic process.

We see a connection between the depth at which the analyst must work a target and the degree of required foreign language proficiency. If analysts work a great many targets at a superficial level, they need only have a casual acquaintance with their language(s). Similarly, when analysts are assigned to an *ad hoc* crisis cell working a specific target for a finite period, they may also need only superficial language skills. In this latter case, if the crisis is of sufficient importance, dedicated language assets will be assigned to compensate for their ignorance. However, should the crisis become long-term, it is reasonable to expect them to acquire more than a passing skill in the target's language(s).

Research

Research skills provide discipline and consistency for the creation of value-added intelligence. By providing methodologies for defining the requirement to be answered, as well as methodologies for answering that query, research skills ensure analytic consistency and enable thorough exploration of the issues. Necessary research skills include methods of problem definition that ensure that, in collaboration with the consumer, analysts correctly define or redefine the problem in terms of a "research question," so as to understand the consumer's and the analyst's own objectives.[67] Research strategies, when based on the issue to be answered, help identify required sources of information, the means of information collection, and the means of analyzing and synthesizing the data.

[66] FBIS Editor's comments on the English translation of Huo, Zhongwen and Wang, Zongxiao, Guofang Keji Qingbaoyuan ji Houqu Jishu (Sources and Techniques of Obtaining National Defense Science and Technology Intelligence) (Beijing: Kexue Jishu Wenxuan Publishing Co., 1991).

[67] Russell G. Swenson and others, "Research Design," in *Research: Design and Methods* (Washington DC: Joint Military Intelligence College, 2001), 19-20. This publication is an essential guide for Community analysts developing research and analytic strategies for long-term projects.

Information Gathering and Manipulation

Information is the grist for intelligence analysis, and to be successful, analysts must aggressively seek it out. Different information/data manipulation skills are required for the various stages of the intelligence process.

- **Collection:** This stage involves gathering information from all sources. The intelligence analyst directs the collection process, causing specific resources to be tasked. Related information manipulation skills include selecting and filtering in order to assess whether the information and its sources are of value.
- **Monitoring:.** Reliability of sources and the validity of the information are always in question. Monitoring skills focus on information review, and often may involve analysis of descriptors and summaries of that data.
- **Organizing:** Skillful arrangement, formatting, and maintenance of data for analysis and technical report generation ensure access to materials in a usable format.
- **Analysis/Synthesis:** Information manipulation skills can point to patterns, relationships, anomalies and trends.
- **Interpretation:** This is the stage in the process where information is transformed into intelligence by cognitive manipulation, that is, assigning meaning to analyzed and synthesized information using critical thinking. Computers aid in this step, however, a study of 12 major "analytic" software tools concludes "true analysis will remain a people function, assisted by computer technology."[68]
- **Dissemination:** Dissemination, except for some graphic products, is now of course mostly electronic. Information preparation and presentation skills allow its transformation and publication, so that the results of analysis appear in usable formats, which may be further tailored by users.
- **Coordination:** Coordination requires analysts as well as their managers to employ "collegial" skills in the bureaucratic environment; these skills are also needed to avoid diluting the intelligence message down to the "lowest common level of agreement."
- **Evaluation:** Internal and intra-community evaluation allows the intelligence to be discussed and placed in larger contexts than that viewed by a single agency. Such collaboration may also identify the additional intelligence required to clarify issues. Evaluation can become a continuous part of the production process.[69]

Project/Process Management

Few analysts enjoy the luxury of working full time on only one problem or on one aspect of a particular problem. We distinguish between projects and processes. The former tend to have finite scope and goals whereas the latter are open-ended. Both require planning, imple-

---

[68] Leonard Fuld, Fuld Associates, "Intelligence Software: Reality or Still Virtual Reality," *Competitive Intelligence Magazine* 4, no. 2 (March-April, 2001): 24-25.

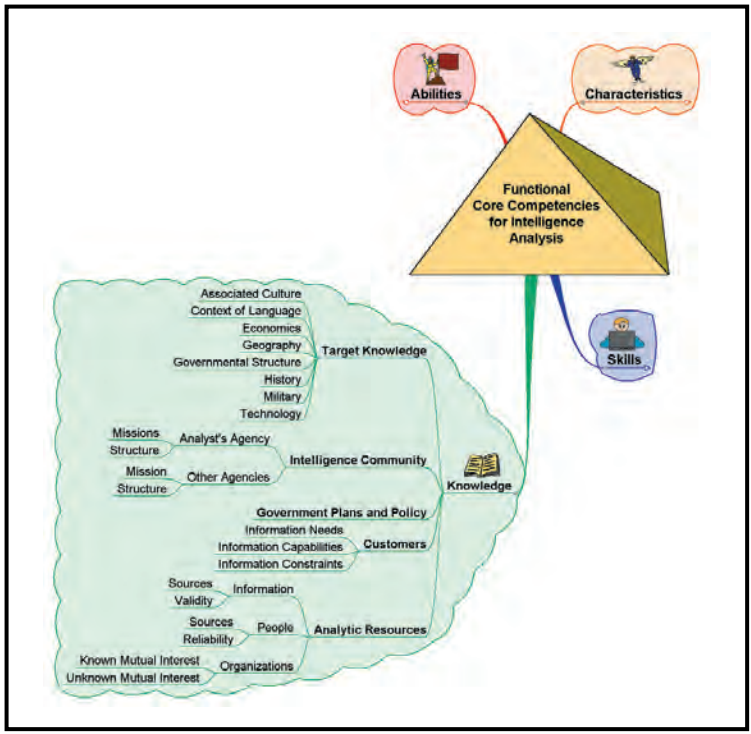
[69] See also Brei.

mentation, monitoring, and negotiating skills.[70] A project/process plan defines and clarifies what needs to be accomplished; identifies necessary resources; creates a timeline, including milestones; and makes the analyst accountable for successful completion.

KNOWLEDGE REQUIRED FOR INTELLIGENCE ANALYSIS

> Without a solid knowledge base concerning the region or issue to which the analyst is assigned, . . . the individual will not even know what questions to ask. That is, the person will not really be qualified to be called an "analyst."
>
> — *Ronald D. Garst and Max L. Gross*[71]

Knowledge consists of familiarities, awareness, or understanding gained through experience or study; it includes both empirical material and that derived by inference or interpretation.[72] Depending on the specific target, the knowledge required can vary widely. Our essential subset is shown in the figure and discussed below.



Knowledge required for successful intelligence analysis.

[70] Clifford C. Kalb, "Core Competencies: A Practitioner's View," document 207612, Merck & Co., Inc, n.d.

[71] Garst and Gross, 50.

Target Knowledge

Doing intelligence analysis in the information age is often like "being driven by someone with tunnel vision."[73] In the quest to answer a consumer's questions, the analyst often pushes aside "all the fuzzy stuff that lies around the edge—context, background, history, common knowledge, social resources."[74] Yet, to do so is perilous, for these provide balance and perspective. They offer breadth of vision and ultimately allow analysts to make sense of the information under study. By providing the context into which analysts place their work, fields of study such as anthropology, comparative religion, economics, geography, history, international relations, psychology, and sociology all interact to contribute vital knowledge about the target, which both analysts and consumers need to understand. Changes in the culture, religion, geography, or economic systems (among others) of a target may themselves be subjects of an intelligence requirement.

Gregory Treverton asserts that intelligence "is supposed to have the people who understand Bonn and Delhi better than they do Washington."[75] Without such understanding, intelligence and policy failures can occur. Treverton blames the failure of the U.S. Intelligence Community to predict India's 1998 nuclear test partially on a lack of understanding by U.S. analysts of "true" Indian motivations. He asserts that a questioning of premises coupled with greater knowledge of the reasons why India would want to conduct a nuclear test should have led U.S. analysts to different conclusions.[76]

The following selection of topics exemplifies some non-traditional but essential target knowledge areas required for thorough intelligence analysis.

- **Culture:** Culture can be defined as a group's values, standards, and beliefs. In turn, culture defines that group. The study of culture reveals the roles of individuals in the community, and how they relate to non-members of the culture. This provides insights into behaviors that are of value in predicting future behavior. This is true when the target is a people or a nation as well as when the target is a specific subgroup or individual member within a culture. Adda Bozeman points out that because political systems are grounded in cultures, "present day international relations are therefore by definition also intercultural relations ... [A]nalysts and policymakers in the West would be more successful in their respective callings if they would examine the cultural infrastructures of the nations and political systems they are dealing with."[77]
- **Message of Language:** The message of language is a part of culture, and while isolating it makes an artificial distinction, we do so to reiterate its importance for intelli-

[72] Knowledge," *The American Heritage Dictionary*, 2nd College Edition, 1976 Ed.

[73] John Seely Brown and Paul Duguid, *The Social Life of Information* (Boston: Harvard Business School Press, 2000), 1-2.

[74] Garst and Gross, 49.

[75] Treverton, 5.

[76] Treverton, 5.

[77] Adda Bozeman, *Politics and Culture in International History: From the Ancient Near East to the Opening of the Modern Age*, 2nd ed. (New Brunswick, NJ: Transaction Publishers, 1994), 5.

gence analysis. What languages are utilized, by whom, and in what context, is essential in understanding the target's culture. For example, much is revealed if members of an insurgent group primarily communicate using the language of the elite members of their culture. Additionally, what the language indicates about class and personal relationships may provide clues to behaviors.

- **Technology:** Technology itself can be the subject of study by the intelligence analyst. Someone developing a target may analyze specific technologies and their infrastructure as they pertain to that target. Further, the role of technology within a region, nation, or people is an indicator of behavior. The domains of communications, utilities, transportation, manufacturing, and others, as well as the attitudes of the people to them, are rich sources of study. Technology also can provide insights into sources of information that will be available to the intelligence analyst.

Professional Knowledge

In addition to understanding their targets, intelligence analysts need to know a great deal about the context and nature of the intelligence profession, and the resources available to help them do their job well. Understanding the plans and policies of their own government enables analysts to frame their work in terms of the nation's strategic and tactical objectives. Intelligence consumers are government officials. Their needs drive analytical process and priorities. Analysts base collection tasking on the imperative to match information sources to consumer needs. These information sources, such as human-source reporting, signals intercepts and documentary research, provide the analyst with raw materials for the creation of intelligence through analysis, synthesis and interpretation.

Determining what information must be analyzed is a precursor to the analytic process. Berkowitz and Goodman identify "four different types of 'information' [used by intelligence analysts] in preparing reports and estimates: known facts, secrets, disinformation, and mysteries."[78] Known facts and secrets must be placed in context or "revealed," disinformation must be discounted, and consumers must be informed that mysteries cannot be answered. For this to occur, the types of information available and their validity, as well as the sources of that information and their reliability, must be determined.

In addition, analysts need to know what specific sources of information relevant to a particular inquiry are available for exploitation. Knowing which expert sources and subject matter experts can guide the analytic process, or can offer different or additional perspectives, enhances intelligence work. The reliability of these sources is also critical. When different sources provide contradictory information, the reliability of one source versus another may provide insights into which information is accurate; the sources may be open or secret, technical or human.

Finally, others, known and unknown, may be examining similar information for the same or different consumers. Awareness that sources of information, possibly vital infor-

[78] Berkowitz and Goodman, 86.

mation, exist, even though they remain undiscovered or untapped, keeps the analyst constantly seeking out new connections.

IMPLICATIONS FOR THE INTELLIGENCE ANALYSIS WORKFORCE

Returning to our thesis, what makes an intelligence analyst successful? Given that the analyst's purpose is to create intelligence, success means following an effective process (rigorous analysis, sound management) and creating a quality product (that conveys intelligence and meets the consumer's needs). To do this requires appropriate abilities, knowledge and personal characteristics for rigorous intelligence analysis and production. Well-honed capabilities to communicate, cooperate and think, coupled with the skills that ensure technical competency, provide the means for intelligence work. Informed, deep knowledge of the issues and their background provides both content and context for analysis. Analysts who are motivated to succeed, to know targets, and to share that knowledge ensure that consumers receive intelligence of the highest caliber.

But do intelligence analysts today approach this ideal? And can we find or grow such talent to serve the Community's mission well into the 21st century?

> Of all the personnel problems the intelligence community will face in the coming years, the most difficult to solve is likely to be maintaining the base of talent the community requires to carry out its mission.... [Much] of the work of the intelligence community is highly specialized and requires exceptional creativity.... It is also safe to say that some of the most pressing analytic skills the community will require are precisely those we cannot even foresee at this time.
>
> *— Bruce D. Berkowitz and Allan E. Goodman*[79]

Berkowitz and Goodman's judgment from 1989 remains true in 2002. The Intelligence Community remains significantly challenged to maintain and enhance an analytic talent base against numerous rapidly changing threats to national security. Further, a possible uptick in hiring and rising rates of eligibility for retirement mean that, at the least, the savvy of the analytic population will continue to dwindle at the lower end and retire from the upper end.[80] Even an adequately sized analytic workforce, lacking adequate mentoring and training from senior, expert analysts, will leave the Intelligence Community unable to meet security challenges. For example, while NSA's technological capability remains widely recognized, former director General Kenneth A. Minihan noted, "If we

---

[79] Berkowitz and Goodman, 154.

[80] External Team Report: A management Review for the Director, NSA, 22 October 1999, URL: <http://www.nsa.gov/releases/nsa_external_team_report.pdf>, accessed 4 June 2001. For a different but related perspective see also the report of the "internal" New Enterprise Team, URL: *http://www.nsa.gov/releases/nsa_new_enterprise_team_recommendations.pdf*.

don't win the talent war, it doesn't matter if we invest in the infrastructure."[81] According to the Council on Foreign Relations' independent report on the future of intelligence, "less than a tenth of what the United States spends on intelligence is devoted to analysis; it is the least expensive dimension of intelligence....This country could surely afford to spend more in those areas of analysis where being wrong can have major adverse consequences."[82] Winning the talent war requires smart investment in the hiring, training, and deployment of analysts.

With simultaneous greening and greying of the analytic workforce, analysts as a group may lack many of the core competencies necessary for successful intelligence analysis. A strategic requirement exists to resolve this problem. However, the authors know of no stratagem under consideration other than their own focus on identifying core competencies for management attention. It may be feasible to conduct small-scale, *ad hoc* or more systematic experimentation with specific analytic techniques such as that pioneered by Folker, to determine which techniques may hold the most promise for improved rigor of analysis.[83] We suspect that some experienced analysts do already match the ideal described above, although others are still operating within the outdated Cold War paradigm. Further, many novice analysts also have the willingness and potential to develop toward the ideal. But they need tradecraft mentors and teachers. Presently, there are not enough expert analysts to do both the teaching and the performance of sophisticated intelligence production.

Therefore, the Intelligence Community needs ways to enable intelligence analysts now on the job to enhance their professional skills. One approach to this problem is to provide widespread, specialized training in analytic methods. In order, however, to ensure that subsequently produced intelligence is accurate and useful, such training must focus on rigorous analytic processes that minimize biases introduced by the analyst, the consumer, the sources of the information, or the information itself. Collaborative training efforts such as those proposed in the *Strategic Investment Plan for Intelligence Community Analysis* offer another way by which intelligence analysts can acquire the skills necessary to bring greater rigor to their analyses.[84]

One analytic method in particular, known as "Analysis of Competing Hypotheses," as presented by Central Intelligence Agency (CIA) analyst Richards J. Heuer, Jr., provides a readily applicable approach to rigorous intelligence analysis. In Heuer's methodology, as used at the CIA, the analyst begins with a full set of alternative possibilities rather than the apparent single most likely alternative. Then the analyst compares each piece of evidence against each hypothesis, and determines if that evidence supports or refutes it. Evi-

[81] Quoted in Robert K. Ackerman, "Security Agency Transitions from Backer to Participant," Signal 54, no. 2 (October 1999): 23.

[82] Council on Foreign Relations, 1996, 11-12.

[83] Folker, *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods*.

[84] Director of Central Intelligence National Security Advisory Panel, 29ff.

dence that has no diagnostic value is taken out of consideration. After noting the evidence chain attached to each hypothesis, the analyst selects as the most probable hypothesis the one with the least amount of evidence against it. This contrasts with conventional analysis, which generally entails looking for evidence to confirm a favored hypothesis. Following the scientific method, Analysis of Competing Hypotheses seeks to eliminate hypotheses, whereas conventional analysis seeks to prove them.[85] The end result of the former is an actionable intelligence product that adds value to the consumer's development and execution of policy or strategy.

Folker's recent experiments in Theater Joint Intelligence Centers provide enticing evidence that such rigorous methods do foster analytic excellence. In four experiments, Folker provided analysts with one hour of training in Analysis of Competing Hypotheses, and then presented them with two realistic scenarios requiring analytic judgments and conclusions. A significantly greater number of the newly trained analysts derived the correct answers to the scenarios than analysts in a control group that used their own *ad hoc* methods. These findings demonstrate that while "exploiting a structured methodology cannot guarantee a correct answer, using a structured methodology ensures that analysis is performed and not overlooked." [86]

Folker therefore recommends widespread teaching of these methodologies during "both initial and subsequent training."[87] However, training is of little value unless it can be immediately applied. Thus organizational structures, culture, and processes must be aligned to permit and to reward rigorous analysis. Unless analysts are recognized and appreciated for performing sophisticated analysis, they will not embrace change. Significant recognition for high-level analysis will inspire others to follow, creating a culture that fosters and sustains excellence in tailored intelligence production.

Even if the entire analytic workforce were to adopt rigorous analytic techniques, the Intelligence Community may still lack sufficient resources to meet consumer needs. It will still need to hire new analysts, either from outside the agency or from within. However, these new employees must be highly qualified. The government cannot afford remedial training for prospective new employees lacking the necessary abilities and skills for intelligence analysis. Similarly, employees transferring into the analytic disciplines from other fields must have the prerequisite abilities and skills for analysis before joining this discipline. The field of intelligence analysis cannot safely be a catchall for employees transferring from downsized career fields.

---

[85] For a discussion of the Analysis of Competing Hypotheses see Chapter 8 of Richards J. Heuer, Jr., *The Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999).

[86] Folker, 33.

[87] Folker, 33.

Some prospective new hires do come to the discipline with an academic background in intelligence, and many current employees pursue continuing studies related to intelligence. However, intelligence studies at the university level tend to focus on intelligence and policy, not on tradecraft. Further, it is questionable whether the fledgling field of intelligence studies by itself yet offers the wherewithal to support a claim of expertise by someone educated in that specialty, except in the narrow, self-assessed areas of intelligence process or organization. Only one non-governmental institution in the U.S. offers an undergraduate degree in intelligence research and analysis: Mercyhurst College in Pennsylvania; there, too, advanced studies are offered in conjunction with a law-enforcement related degree. Within several years, the University of New Mexico expects to offer undergraduate through doctoral degrees in intelligence; the stated goals of this program are to focus on the tradecraft of strategic intelligence.[88] Other institutions, such as Wright State University in Ohio, are beginning intelligence analysis programs. But these academic programs are too small and too limited to meet the needs of government intelligence agencies for qualified analysts.

Furthermore, general academic preparation is not enough. Training new and current intelligence analysts in professional tradecraft is a Community responsibility and obligation. Analysts need both specific job-related training and enculturation appropriate to their agencies' missions. With the investment of adequate resources, including the development of modern curricula in intelligence tradecraft, Community training programs can meet these specialized analytic training needs. This investment also can include partnering with academic institutions offering "distance learning" programs and other means of outsourcing instructional resources.

The Aspin-Brown Commission on the Roles and Capabilities of the United States Intelligence Community identified several additional actions to improve the quality of analysis. These include a minimal prerequisite to visit target countries as part of analytic orientation, rewards for acquiring and maintaining foreign language proficiency, encouragement to remain within substantive areas of expertise, and periodic rotational assignments to consumer agencies.[89] Enacted as part of employee training and orientation, these measures can substantially enhance analysts' target knowledge and skills.

In combination with the right knowledge, skills, abilities, characteristics, and methodologies, the organizational and structural changes under consideration offer a possibility to genuinely transform the analytic work force. Specific changes in analytic culture, processes, and techniques offer the Intelligence Community a unique opportunity to rebuild analysis to effectively cope with a changed world. The recognition that technol-

---

[88] James Hold en-Rhodes, personal communications, 11-14 June 2001.

[89] Aspin-Brown Commission, *Preparing for the 21st Century: An Appraisal of U.S. Intelligence* (Washington DC, GPO, 1 March 1996), 87.

ogy supports, and is not a replacement for, the mental processes of analysis, highlights this opportunity.

However, it remains to be seen whether the agencies and their personnel are willing and able to carry out this essential work. Organizational changes now underway may not go far enough. Agency structures remain large and centrally planned. More agile responses to intelligence challenges, as yet undefined, may be required to counter them.[90]

A Community strategy focusing both on what consumers require, and how a professional analytic workforce can be developed is a logical follow-on to the transformations the Intelligence Community already has begun. The results of implementing such a strategy will be profound, if the transformations remain grounded in mission and are sustained through changes in leadership. In this climate, talented and motivated analysts who are highly knowledgeable about their consumers and their targets will apply rigorous analytic techniques to create actionable intelligence for decisionmakers. Under expert management, analysts will apply critical thinking skills in evaluating their own work, ensuring that it is of the highest caliber. As these analysts collaborate extensively across the Intelligence Community, the example they set will inspire others to excellence. Making this vision a reality requires action. The ideas developed here can be used as a guide to action and an instrument of change.

BIBLIOGRAPHY

Ackerman, Robert K. "Information Age Poses New Challenges to Intelligence." *Signal* 53, no. 2 (October 1998): 23-25.

Aid, Mathew M. "The Time of Troubles: The US National Security Agency in the Twenty-First Century." *Intelligence and National Security* 15, no. 3 (Autumn 2000): 1-32.

The American Heritage Dictionary, 2nd College Edition, 1976.

Aspin-Brown Commission. *Preparing for the 21st Century*. U.S. Congress. Senate. 103rd Cong., 2d sess. 1 March 1996.

Berkowitz, Bruce D. and Allan E. Goodman. *Best Truth: Intelligence in the Information Age*. New Haven, CT: Yale University Press, 2000.

_____. *Strategic Intelligence for American National Security*. Princeton, NJ: Princeton University Press, 1989.

Bozeman, Adda. *Politics and Culture in International History: From the Ancient Near East to the Opening of the Modern Age*, 2nd Edition. New Brunswick, NJ: Transaction Publishers, 1994.

---

[90] For an examination of how intelligence analysis might be done in the 21st Century, see chapter 4 of Bruce D. Berkowitz and Allan E. Goodman, *Best Truth: Intelligence in the Information Age* (New Haven: Yale University Press, 2000).

_____. *Strategic Intelligence and Statecraft: Selected Essays*. McLean, VA: Brassey's, 1992.

Brei, William S., Captain, USAF. *Getting Intelligence Right: The Power of Logical Procedure*. Occasional Paper Number Two. Washington DC: Joint Military Intelligence College, 1996.

Brown, John Seely and Paul Duguid. *The Social Life of Information*. (Boston, MA: Harvard Business School Press, 2000.

Bush, George W. "National Security Presidential Directive 5." 9 May 2001.

Christopher, Warren. *In the Stream of History: Shaping Foreign Policy for a New Era*. Stanford, CA: Stanford University Press, 1998.

Clauser, Jerome K. and Sandra M. Weir. *Intelligence Research Methodologies, An Introduction to Techniques and Procedures for Conducting Research in Defense Intelligence*. Washington DC: Defense Intelligence School, 1975.

Council on Foreign Relations. *Making Intelligence Smarter: The Future of U.S. Intelligence: A Report of an Independent Task Force*, n.d., n.p. Available from the Federation of American Scientists, <http://www.fas.org/irp/efr.html>. Last accessed 4 June 2001.

Deacon Terence W. T*he Symbolic Species: The co-Evolution of Language and the Brain* London: W.W. Norton & Company, Ltd., 1997.

Denning, Stephen. *The Springboard: How Storytelling Ignites Action in Knowledge-Era Organizations*. Boston, MA: Butterworth Heineman, 2001.

Devlin, Keith. "The Role of Conceptual Structure in Human Evolution." In Bernhard Ganter and Guy W. Mineau, eds. *Conceptual Structures: Logical, Linguistic, and Computational Issues*, Proceedings of the 8th International Conference on Conceptual Structures. Berlin, Germany: Springier Verlag, 2000.

Director of Central Intelligence, National Security Advisory Panel. *Strategic Investment Plan for Intelligence Community Analysis*. Washington DC: Central Intelligence Agency, 2000. URL: <*www.cia.gov/cia/publications/unclass_sip/index.html*>. Last accessed 1 July 2001.

Ember, Carol R. and Melvin Ember. *Anthropology*, 9th Edition. Upper Saddle River, NJ: Prentice Hall, 1999.

Folker, Robert D. Jr., MSgt. USAF. *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods*. Occasional Paper Number Seven. Washington DC: Joint Military Intelligence College, 2000.

Foster, Gregory D. "Research, Writing, and the Mind of the Strategist." *Joint Force Quarterly*, 11 (Spring 1996): 74-79.

Fuld, Leonard. "Intelligence Software: Reality or Still Virtual Reality." *Competitive Intelligence Magazine* 4, no. 2 (March-April 2001): 24-25.

Garst, Ronald D. and Max L. Gross. "On Becoming an Intelligence Analyst. "*Defense Intelligence Journal* 6, no. 2 (Fall 1997): 47-60.

Haxton, Brooks, tr. *Fragments, the Collected Wisdom of Heraclitus*. New York: Penguin, 2001.

Herring, Jan P. *Measuring the Effectiveness of Competitive Intelligence: Assessing and Communicating CI's Value to Your Organization*. Alexandria, VA: Society of Competitive Intelligence Professionals, 1996.

Heuer, Richards. *The Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence, 1999.

Huo, Zhongwen and Zongxiao Wang. *Guofang Keji Qingbaoyuan ji Houqu Jishu*) Sources and Techniques of Obtaining National Defense Science and Technology Intelligence). Beijing: Kexue Jishu Wenxuan Publishing Co., 1991.

Johnson, Loch K. "Analysis for a New Age." *Intelligence and National Security* 11, no. 4 (October 1996): 657-671.

_____. *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security*. New York: New York University Press, 2000.

Juergensmeyer, Mark. *Terror in the Mind of God: the Global Rise of Religious Violence*. Berkeley: University of California Press, 2000.

Kalb, Clifford C. "Core Competencies: A Practitioner's View," document 207612, Merck & Co., Inc, n.d.

Kaplan, Robert D. *The Coming Anarchy: Shattering the Dreams of the Post-Cold War*. New York: Random House, 2000.

_____. *Eastward to Tartary: Travels in the Balkans, Middle East, and the Caucasus*. New York: Random House, 2000.

Kent, Sherman. "The Need for an Intelligence Literature," *Studies in Intelligence*, Spring, 1955. Reprinted in *Studies in Intelligence*, 45th Anniversary Special Edition, Washington DC: Government Printing Office, 2001, 1-11.

_____. *Strategic Intelligence for American World Policy*. Princeton, NJ: Princeton University Press, 1949.

Kovacs, Amos. "Using Intelligence." *Intelligence and National Security* 12, no. 4 (October 1997): 145-164.

Krizan, Lisa. *Intelligence Essentials for Everyone*. Occasional Paper Number 6. Washington DC: Joint Military Intelligence College, 1999.

Lorenz, Frederick M. and Edward J. Erickson. *The Euphrates Triangle: Security Implications of the Southeastern Anatolia Project*. Washington, DC: National Defense University Press, 1999.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. Washington, DC: CQ Press, 2000.

Mann, Steven R. "Chaos Theory and Strategic Thought." *Parameters* 22, no. 3 (Autumn 1992): 54-68.

McDowell, Don. *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users*. Cooma, Australia: Istana Enterprises, Pty. Ltd., 1998.

Mathams, R. H. "The Intelligence Analyst's Notebook," in *Strategic Intelligence: Theory and Application*, 2d. ed., Washington, DC: Joint Military Intelligence Training Center, 1995, 77-96.

National Drug Intelligence Center. *Basic Intelligence Analysis Course*, slide # 9. Power-Point Presentation, April 2001.

National Intelligence Council. *Global Trends 2015: A Dialogue About the Future with Nongovernment Experts*. Washington DC: National Foreign Intelligence Board, 2000.

National Security Agency External Team. *Report: A management Review for the Director, NSA*, 22 October 1999. URL: <*www.nsa.gov/releases/nsa_external_team_report.pdf*> Last accessed 4 June 2001.

Oxford Concise English-Chinese/Chinese-English Dictionary, 2nd ed. Oxford: Oxford U University Press, 1999.

Stack Kevin P. "Competitive Intelligence." *Intelligence and National Security* 13, no.4 (Winter 1998): 194-202.

Starbuck, William H. "Unlearning Ineffective or Obsolete Technologies." *International Journal of Technology Management* 11, nos. 7/8 (Winter 1996): 725-726.

Steele, Robert David. "The New Craft of Intelligence: an Alternative Approach Oriented to the Public," Paper presented at the 1st conference on the Future of Intelligence in the 21st Century, Priverno, Italy, 14-16 February 2001.

Steury, Donald P., ed. *Sherman Kent and the Board of National Estimates: Collected Essays*. Washington DC: Center for the Study of Intelligence, Central Intelligence Agency, 1994.

Swenson, Russell G., Francis J. Hughes, and others. "Research Design," in *Research: Design and Methods*. Ed. Russell G. Swenson. Washington DC: Joint Military Intelligence College, September 2000.

Treverton, Gregory. *Reshaping National Intelligence for an Age of Information*. Cambridge: Cambridge University Press, 2001.

Wheaton, Kristan J., *The Warning Solution: Intelligent Analysis in the Age of Information Overload***.** Fairfax, VA: AFCEA International Press, 2001.

Williams, Phil and Roy Godson. “Anticipating Organized and Transnational Crime.” Paper presented at the 1st conference on the Future of Intelligence in the 21st Century, Priverno, Italy, 14-16 February 2001.

Yu, Chong Ho. “Abduction? Deduction? Induction? Is there a Logic of Exploratory Data Analysis?” Paper presented at the annual meeting of the American Educational Research Association, New Orleans, LA, April 1994. URL: <http://seamonkey.ed.asu.edu/~behrens/asu/reports/Peirce/ Logic_of_EDA.html>. Last accessed 6 June 2001.

ABOUT THE AUTHOR

LT Michael Bennett enlisted in the Coast Guard in 1991. From 1991 to 1994 he was stationed at Marine Safety Office, Houston, Texas where he responded to oil and chemical spills and served as a member of a U.S. Customs Assist Team and Boarding Team Member enforcing federal laws and regulations in the Port of Houston/Upper Galveston Bay area. From 1994 to 1998, he was stationed at Marine Safety Office St. Louis, Missouri where he worked in the Port Operations Department responding to oil and chemical spills, enforcing federal environmental regulations and acting as the Safety and Occupational Health Coordinator for the Marine Safety Office and its two detachments located in Davenport, Iowa and St. Paul, Minnesota. In 1998, he received a Direct Commission as a Lieutenant Junior Grade and was assigned to the Office of Response at Coast Guard Headquarters where he assisted with the national and international coordination of the Coast Guard's Pollution Response Program and acted as the Coast Guard representative on the U.S. National Response Team, Response Sub-Committee. Prior to attending the Joint Military Intelligence College in 2002, LT Bennett was stationed at Marine Safety Office/Group Portland, Oregon where he was Assistant Chief of Contingency Preparedness and Planning, responsible for coordinating regional efforts relating to National Security, Port Security, Environmental Response, Anti-Terrorism and Force Protection, and response to Natural Disasters for the Pacific Northwest

THE U.S. COAST GUARD JOINS THE INTELLIGENCE COMMUNITY

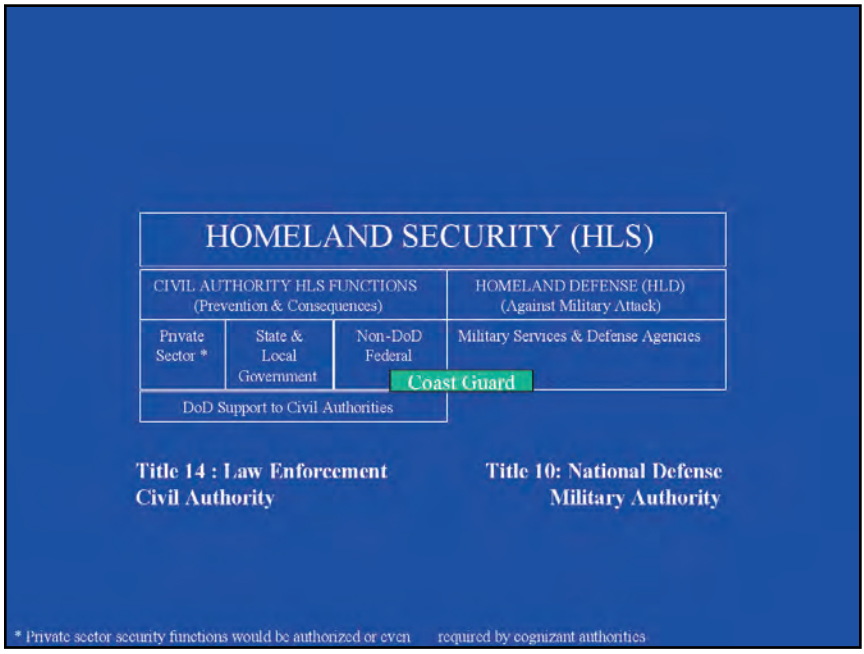
Michael E. Bennett, LT, USCG

The United States Coast Guard (USCG), like many other agencies, has experienced significant transformation since 11 September 2001. For example, the evolution of the intelligence function in the USCG was dramatically hastened, resulting in its gaining full membership in the Intelligence Community by year's end. The multiple responsibilities of this service are focused on National Defense, Environmental Protection, and Maritime Safety, Security, and Mobility in protecting the expansive U.S. Maritime Transportation System (MTS), which extends over 95,000 miles of coastline, 360 seaports, and 3.4 million square miles of Exclusive Economic Zone (EEZ)[1]

Source: Vice Admiral Allen, USCG, 7 October 2002.

[1] The EEZ consists of those areas adjoining the territorial sea of the U.S., the Commonwealth of Puerto Rico, the Commonwealth of the Northern Mariana Islands, and U.S. overseas territories and possessions. The EEZ extends up to 200 nautical miles from the U.S. coastline. The U.S. has sovereign rights over all living and non-living resources in the EEZ. Other nations may exercise freedom of vessel navigation and overflight within the EEZ. See *http://www.uscg.mil/hq/g-cp/comrel/factfile/Factcards/ Homeland.htm* for a description of the USCG Maritime Homeland Security Strategy.

Historically Coast Guard Intelligence has focused on the collection of information in support of law enforcement operations related to counter-drug and migrant interdiction. With the migration to the Department of Homeland Security (DHS) and membership in the IC, a less sharp line now exists between National Foreign Intelligence and Law Enforcement Intelligence collection because of the need for both to anticipate and prosecute illegal international migration, piracy, and other transnational threats. The USCG is the only organization simultaneously responsible for law enforcement, intelligence, and military activities. Title 14 of the U.S. Code provides the Coast Guard with its Law Enforcement and Civil authorities, and Title 10 provides this service with National Defense and Military authorities. The figure below depicts the law enforcement/military continuum for these authorities and demonstrates the placement of USCG intelligence as a bridge between the realms of law enforcement and national foreign intelligence.



Coast Guard Civil/Military Authorities Source: Vice Admiral Allen, USCG, 7 October 2002.

THE COAST GUARD ROLE IN INTELLIGENCE

The roots of the Coast Guard intelligence function trace back to the Rum War during the period of prohibition. From 1920 to 1933, the USCG provided operational

intelligence for law enforcement efforts.[2] After that era, although the Coast Guard continue intelligence support to its many law enforcement missions, not until 1984 did it establish the Intelligence Coordination Center (ICC), an information fusion activity that provides maritime intelligence support to the National Foreign Intelligence Community and Coast Guard commands at the strategic, operational and tactical level. In December 2001, through an amendment to the *National Security Act of 1947*, the USCG officially became a member of the Intelligence Community.[3] This development significantly expands the service's intelligence roles and responsibilities with respect to other members.

In a Congressional Research Service Report for Congress, a CIA official is cited as the source for the following observation comparing law enforcement and national security intelligence:

> Today there is no clear primacy for either the law enforcement or intelligence communities in the realms of international terrorism, narcotics, proliferation (as well as some areas of counterintelligence). Still, the law enforcement and intelligence communities remain designed to operate in fundamentally dissimilar manners, retaining different legal authorities, internal modes of organization and governing paradigms.[4]

As an organization straddling the boundaries between the law enforcement and intelligence communities, the USCG allows for collection of information domestically and abroad leading to detection, preemption and deterrence of threats, and when necessary, operations involving crisis and consequence management, and arrest and prosecution in the maritime environment.

ON BECOMING A COMMUNITY MEMBER

Community membership is a win-win for the Coast Guard and the Intelligence Community (IC). The IC gets a multi-mission agency with numerous regional, national, and international relationships, combined with extensive law enforcement and military authorities. The Coast Guard receives recognition for their existing efforts in support of national collection requirements, a clearly defined mission from the Director of Central Intelligence (DCI), and increased resources to support these new mission requirements.

---

[2] Robert E. Johnson, *Guardians of the Sea: History of the United States Coast Guard 1915 to the Present* (Annapolis, MD: Naval Institute Press, 1987), 89. Also see Eric S. Ensign, LT, USCG, *Intelligence in the Rum War at Sea*, 1920-1933 (Washington, DC: Joint Military Intelligence College, 2001).

[3] U.S. Congress, Senate, Intelligence Authorization Act for Fiscal Year 2002, 107th Cong, 1st sess., 2001, H. Res. 288.

[4] Richard A. Best, "Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.," *CRS Report for Congress* RL30252 (Washington, DC: Congressional Research Service, Library of Congress, 3 December 2001), 2.

But IC membership also involves congressional oversight, training and education, and the development of an infrastructure ready to accept these new duties. How is the Coast Guard handling this new responsibility?

An N2 for the Coast Guard

In October of 2002, the position of Assistant Commandant for Intelligence (G-C2) was created, elevating the office to a Directorate level within the Coast Guard organization. This position is held by Senior Executive Service Officer Mrs. Frances Fragos Townsend. Her position provides direct access to the Commandant of the Coast Guard, essentially filling both the N2 (Director of Intelligence) and Naval Security Group (NSG) roles for the Coast Guard. Additionally, Mrs. Townsend and the Commandant of the Coast Guard share the responsibility as the service's Senior Official of the Intelligence Community (SOIC), ensuring compliance with all community tasking and related oversight.

Mrs. Townsend, who came from the Justice Department's Office of Intelligence Policy Review, is responsible for a burgeoning Intelligence Directorate that could soon number more than 150 people at the headquarters level alone. This moves the Intelligence Directorate out of its longtime position under Coast Guard Operations, significantly expanding its responsibilities and expectations, one of them being the development of a career path to support the new mission.

Establishing a New Career Path

Prior to community membership, being a Coast Guard Intelligence Officer could have been detrimental to one's career. It was not that the job lacked excitement or qualified people; a recognized career path simply did not exist. An intelligence officer usually came from the operational (law enforcement) or marine safety (waterways management/environmental response) community, did one tour as an intelligence officer, and then went back to their specialty in order to improve chances for promotion. With the creation of G-C2, a formal career path now exists for enlisted and officers alike, supported by a rapidly developing training and education program.

A Direct Commission Program for Intelligence Officers seeks qualified enlisted or officer candidates from other services who are interested in a career with the Coast Guard, and who meet the prerequisites for commissioning (a Baccalaureate degree, combined with intelligence or law enforcement-related experience). Opportunities also exist for Officers to engage in post-graduate education at the Joint Military Intelligence College, where they can pursue an accredited Master of Science of Strategic Intelligence degree.

Bridging the Gap between Law Enforcement Information and National Foreign Intelligence Collection

Recent Coast Guard initiatives combined with current Coast Guard legal authorities have laid a foundation for the collection, fusion, and analysis of information in support of the IC and Department of Homeland Security. With IC membership comes an increase in responsibilities. The DCI will task the Coast Guard based on the new mission recently approved. Additionally, the USCG will continue to support other national collection requirements, but this will be done through its own Intelligence Coordination Center (ICC) and the development of newly created Maritime Intelligence Fusion Centers (MIFC) and Field Information Support Teams (FIST). The MIFC's are strategic fusion centers on the east and west coast that will collect, analyze and fuse information in support of national objectives, and the FIST will collect law enforcement intelligence at strategic economic and military ports throughout the country.

The USCG is also expanding its visibility in the Community through participation in numerous multi-agency operations. Although they have always participated in national and regional Joint Terrorism Task Force operations, recent initiatives also include additional participation with the Defense Intelligence Agency's Joint Intelligence Task Force-Combating Terrorism (JITF-CT), the U.S. Northern Command, and the Central Intelligence Agency's Crime and Narcotics Center (CNC) and Crime and Terrorism Center (CTC).

Dealing with Congressional Oversight

With Community membership comes Congressional oversight, and for the Coast Guard this means clearly defining the separation between law enforcement and Intelligence Community duties by establishing policies and procedures for collection and management of information within the service. In order to provide the necessary separation between these elements and yet maintain the continuity needed for detection, pre-emption and deterrence of threats, the Coast Guard has worked closely with the Community Management Staff and other intelligence organizations to capture best practices and lessons learned in order to avoid the information-sharing pitfalls experienced by other agencies. These lessons learned were then incorporated into the *Coast Guard Intelligence Capstone Document*[5] that delineates the role of the Coast Guard Intelligence Organization. The *Capstone Document* describes the Coast Guard Intelligence Program as a "binary organization consisting of two closely linked parts: the *National Intelligence Element* and the *Law Enforcement Intelligence Program*."

---

[5] United States Coast Guard, *Coast Guard Capstone Document*, *COMDTINST 3820.10*, 26 February 2003 (Washington D.C.). Cited hereafter as Capstone Document.

The *National Intelligence Element* conducts "intelligence activities," as described in Executive Order 12333 and the National Security Act of 1947, including the collection, retention, and dissemination, of *national intelligence (foreign intelligence and counter-intelligence*) under those authorities. The National Intelligence Element is part of the Intelligence Community and is governed by procedures approved by the Attorney General. The National Intelligence Element consists of only those personnel or components designated by the Assistant Commandant for Intelligence, with the approval of the Chief of Staff.

The *Law Enforcement Intelligence Program* describes the collection, retention, and dissemination of information pursuant to Coast Guard law enforcement and regulatory authority. Persons and components that collect, process and report law enforcement intelligence and other information, including those persons performing intelligence functions as a collateral duty, are conducting functions under the Law Enforcement Intelligence Program. These persons and components are not part of the National Intelligence Element.[6]

Additionally, under provisions of the USA PATRIOT ACT and *Homeland Security Act of 2002* (HLS), the Coast Guard (in addition to other agencies) is required to provide critical information or intelligence, "gathered in the course of operations to enforce criminal laws," to the DCI. Warning information on foreign or terrorist threats is also reported to the Undersecretary for Information Analysis and Infrastructure Protection in the Department of Homeland Security as required under the Homeland Security Act of 2002. Foreign Intelligence is defined in the *National Security Act of 1947* as "information related to the capabilities, intentions, or activities of foreign governments, foreign organizations, foreign persons, or international terrorist activities" related to threats against the United States."[7] These provisions are designed to eliminate obstacles for sharing law enforcement information with the DCI while enhancing the ability of DHS to "connect the dots between diffuse bits of information"[8] in order to detect and preempt terrorist activities. Prior to 11 September 2001 there was no one agency responsible for coordinating this task throughout the federal government. In the Coast Guard this responsibility for reporting rests with G-C2. By centralizing the reporting of this information within one directorate, the Coast Guard will be able to reduce circular and duplicate reporting and simultaneously measure the effectiveness of Coast Guard information sharing practices.[9]

---

[6] Capstone Document, Enclosure 1.

[7] United States Coast Guard, "Implementation of Mandatory Information Sharing Provisions Under the USA PATRIOT ACT and Homeland Security Act of 2002," *Memorandum*, (Washington D.C.): 23 January 2003. Cited hereafter as USCG Memorandum.

[8] Richard A. Best, "Homeland Security: Intelligence Support," *CRS Report for Congress* RS21283 (Washington, DC: Congressional Research Service, Library of Congress, 4 March 2003).

[9] USCG Memorandum.

By circumscribing the relationships between the *National Intelligence Element* and *Law Enforcement Intelligence Program*, as approved by the Attorney General, the Coast Guard remains the only federal agency that is simultaneously a law enforcement, military, and intelligence service. Having this capability within the newly created Department of Homeland Security, Secretary Ridge now has a powerful tool: the ability to collect, analyze, and fuse law enforcement intelligence with national foreign intelligence that can lead to the critical pre-emption of transnational or asymmetric threats to homeland security or to interests abroad. As noted by one senior Coast Guard Intelligence official: "The different designations of *Law Enforcement Intelligence* and *National Intelligence* defines how information is collected and not how it is used."[10]

Avoiding the Pitfalls

A CRS report for Congress has noted that several pitfalls appear "systemic" in the Intelligence Community: "lack of preparedness to deal with challenges of global terrorism, inefficiencies in budgetary planning, the lack of adequate numbers of linguists, a lack of human sources, and an unwillingness to share information among agencies."[11] Although new to the IC, the Coast Guard is not unversed in some or even all of these problems. One aspect where the Coast Guard has considerable experience is in sharing information with other agencies. As a small agency with limited resources and far-reaching responsibilities, the Coast Guard has developed extensive partnerships at the federal, state, and local level in order to accomplish its mission. Most, if not all Coast Guard operations involve multi-agency and interagency cooperation. However, one aspect needing further attention by the service is its lack of a formal language-training program. While the Coast Guard does have linguists, very few have attended a formal language school, and even fewer have the requisite skills necessary to meet the standards required of its Defense Department counterparts.

An October 1996 article presaged the difficulties facing a new intelligence organization. It notes that "launching and maintaining an intelligence system is a complex task. The hardest part is achieving the right level of balance among the key system elements, especially among published information, human collection, and analysis."[12] In other agencies, the organizational culture and information-sharing practices have often limited the flow and accuracy of information between the analyst and the decisionmaker. As Lowenthal observes, "a dialogue between producers and consumers should take place after the intelligence has been received. Policymakers should give the intelligence community some sense of how well their requirements are

[10] Senior Intelligence Official, at the U.S. Coast Guard Office of Intelligence, interviewed by the author, 12 March 2003.

[11] Richard A. Best, "Intelligence Issues for Congress," Issue Brief for Congress IB 10012 (Washington, DC: Congressional Research Service, Library of Congress, Updated 6 March 2003), 14.

[12] "Intelligence Pitfalls," *Management Review*, 85, no. 10 (October 1996): 51.

being met and discuss any adjustments needed" [13] Clearly defined requirements combined with doctrine, process, and training and education are the key, systematic elements that can provide the necessary balance the Coast Guard needs as a successful member of the IC.

As Amy Zegart concludes, "to do their jobs, national security officials must concern themselves with other agencies...their activities inherently overlap and intersect."[14] A noteworthy benefit of Coast Guard membership in the IC is that the service has no culture of "owning" information. On the contrary, the service has a reputation for sharing information (while maintaining the necessary safety protections) leading to relationship-building that can provide enhanced detection, pre-emption, and deterrence, while bringing together civilian, law enforcement, intelligence, and military agencies to combat threats to the homeland. These combined responsibilities to collect, analyze, and fuse law enforcement and national foreign intelligence information rest with an agency that has historically had a reputation for public trust and confidence.

[13] Mark M. Lowenthal, *Intelligence: From Secrets to Policy, 2d* rev ed. (Washington D.C.: CQ Press, 2003) 42.

[14] Amy B. Zegart, *Flawed by Design: The Evolution of the CIA, JCS and NSC* (California: Stanford University Press, 1999), 37.

INDEX

A

Academia 7-16
Blacklisting 10
Contributions 9, 13, 15-16
Distrust 8, 10, 14
Relations with Intelligence Community 7-16
Algeria 19-22, 24-25

C

Central Intelligence Agency (CIA) 1, 4, 7, 8, 11, 16, 41-56
Council of Intelligence Occupations (CIOC) 55-56
Counter Terrorism Center (CTC) 137
Cime and Narcotics Center (CNC) 137
Directorate of Intelligence (DI) 41, 43, 47-56
Institutional Obstacles 41, 47-56
Intelligence Production 41, 48-53, 56, 61-92, 102-104
Leadership Analysis Office (LDA) 53-55
Scholars-in-Residence Program 16
Chief of Naval Operations (CNO) 31
Coast Guard (USCG) 4, 133-139
Assistant Commandant for Intelligence (G-C2) 136, 138
Field Information Support Teams (FIST) 137
Maritime Intelligence Fusion Center (MIFC) 37
Missions 133-134
Congressional oversight 137
Colby, William 42
Cold War 10, 39
COLISEUM Database 77, 82
Current Intelligence 48-50

D

Databases 15, 80, 82
Defense Attaché (DATT) 28-39
Defense Intelligence Agency (DIA) 1, 11, 16, 61-82

Directorate for Intelligence (J2) 63-64, 76
Directorate for Intelligence Production (DI) 64
Joint Military Intelligence College (JMIC) 42, 64, 136
Office for Counterterrorism Analysis (TWC) 64
Operational Intelligence Coordination Center (OICC) 64
Operational Environment Analysis Division (OSJ-2) 64
Defense Intelligence Threat Data System (DITDS) 82
Department of Defense Intelligence Information System (DoDIIS) 82
Director of Naval Intelligence (DNI) 29-30

E

Exclusive Economic Zone (EEZ) 133
Executive Order 12333 137

F

Foreign Broadcast Information Service (FBIS) 3

H

Hitz, Fred 43

I

India 31-39, 43
Bangalore 35
Bhaba Atomic Research Laboratory 32, 34
Bombay 33
Hindustan Aeronautics Ltd. (HAL) 32, 35-36
Mazagon Dockyard 31-34
New Delhi 37
Nuclear Weapons Tests 43
Space Research Organization (ISRO) 32, 35
Intelligence Analysts
Abilities 107, 111
Characteristics 105, 106
Collaboration 85, 108
Competition 85, 86
Core Competencies 96

Evaluation 100-101
Failure 42-43
Knowledge Requirements 120-123
Pitfalls 139
International Studies Association 14
Internet 20, 23

J

Jeremiah, Admiral David 43
Jervis, Robert 41, 46
Johnson, Loch K. 44
Joint Analysis Center (JAC) 3, 18
Joint Terrorism Task Force 137
Joint Terrorism Task Force Combating Terrorism 137
Joint Worldwide Intelligence Communications System (JWICS) 82

K

Kent, Sherman 46, 97, 100

L

Law Enforcement Information 136, 137

M

Malcomb Baldridge National Quality Program 61, 64
Maritime Transportation System 133
McLaughlin, John 2, 46
Morocco 19, 20, 22-25

N

National Imagery and Mapping Agency (NIMA) 53
National Reconnaissance Office (NRO) 60
National Security Act of 1947 135
National Security Agency (NSA) 1, 95-127
North Africa 19-27
Northern Command (NORTHCOM) 137

O

Open Source Information System (OSIS) 82

P

Political Science Association 14

R

Requests for Information (RFI) 77
Rum War. 134

S

Senior Intelligence Officer (SIO) 62
Sherman Kent School. 46, 73
Secret Internet Protocol Router Network (SIPRNET) 82

T

Title 10 134
Title 14 134
Tunisia 19-20, 23-24

U

Union of Soviet Socialist Republics (USSR). 48

Other Books from the Joint Military Intelligence College

Pickert, Perry L. *Intelligence for Multilateral Decision and Action*, 1997.

Clift, A. Denis. *Clift Notes*. James S. Major, ed., 2000.

Ensign, Eric S., LT, USCG. *Intelligence in the Rum War at Sea*, 1920-1933, 2001.

Clift, A. Denis. *Clift Notes*, 2nd Ed. James S. Major, ed., 2002.

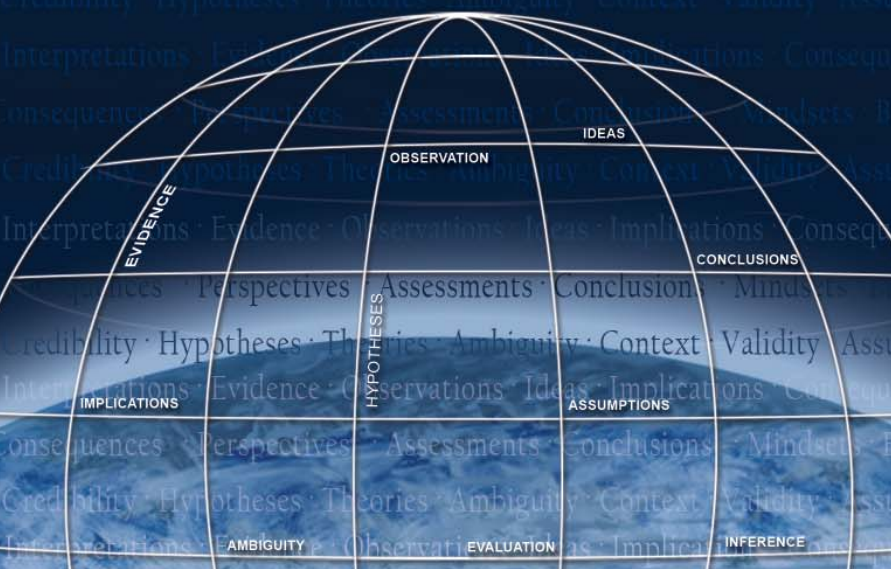
Grabo, Cynthia M. *Anticipating Surprise: Analysis for Strategic Warning*. Jan Goldman, ed., 2002.

Bringing Intelligence About: Practitioners Reflect on Best Practices. Russell G. Swenson, ed., 2003.

This Page Is Intentionally Left Blank

National Defense Intelligence College

Occasional Paper Number Fourteen



Critical Thinking and Intelligence Analysis

Consequences · Perspectives · Assessments · Conclusions · Mindsets · Bia
Credibility · Hypotheses · Theories · Ambiguity · Context · Validity · Assu
Interpretations · Evidence · Observations · Ideas · Implications · Consequ

David T. Moore

Interpretations · Evidence · Observations · Ideas · Implications · Consequen
Consequences · Perspectives · Assessments · Conclusions · Mindsets · Biase
Credibility · Hypotheses · Theories · Ambiguity · Context · Validity · Assu

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
MAR 2007		**00-00-2007 to 00-00-2007**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Critical Thinking and Intelligence Analysis	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense Intelligence College,Washington,DC,20340-5100**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**158**	

The National Defense Intelligence College supports and encourages research on intelligence issues that distills lessons and improves Intelligence Community capabilities for policy-level and operational consumers

Critical Thinking and Intelligence Analysis, Second Printing (with revisions)
David T. Moore

This series of Occasional Papers presents the work of faculty, students and others whose research on intelligence issues is supported or otherwise encouraged by the National Defense Intelligence College (NDIC) through its Center for Strategic Intelligence Research. Occasional Papers are distributed to Department of Defense schools and to the Intelligence Community, and unclassified papers are available to the public through the National Technical Information Service (www.ntis.gov). Selected papers are also available through the U.S. Government Printing Office (www.gpo.gov).

This work builds on earlier publications in this series, particularly Occasional Papers Two, Six, and Seven; *Getting Intelligence Right: The Power of Logical Procedure*, *Intelligence Essentials for Everyone*, and *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods*. The author's insights have been developed through years of creative interaction with the Community's leaders in analytic methododology, and tested for practicality by successive waves of students in training and education courses throughout the Community.

Proposed manuscripts for these papers are submitted for consideration to the NDIC Press Editorial Board. Papers undergo review by senior officials in Defense, Intelligence and civilian academic or business communities. Manuscripts or requests for additional copies of Occasional Papers should be addressed to Defense Intelligence Agency, National Defense Intelligence College, MC-X, Bolling AFB, Washington, DC 20340-5100.

This publication has been approved for unrestricted distribution by the Office of Security Review, Department of Defense.

Russell Swenson@dia.mil, Editor and Director
Center for Strategic Intelligence Research

Critical Thinking and Intelligence Analysis

Occasional Paper Number Fourteen

David T. Moore

National Defense Intelligence College
Washington, DC
March 2007

The opinions expressed in this paper are those of the author. They do not represent the official position of the National Security Agency, the Department of Defense, or any other agency of the U.S. Government.

Contents

Figures and Tables v

Preface vii

Foreword
Mark M. Lowenthal ix

Commentary
Jeffrey R. Cooper xiii
Francis J. Hughes xvi
Gregory F. Treverton xvii

Acknowledgments xix

Abstract 1

Definitions 2

Introduction: How Do People Reason? 3

What Is Critical Thinking? 8
Defining Critical Thinking 8
Standards for Critical Thinking 10
Skill-Based Definitions 13
A Disposition to Think Critically 15
The Role of Questions 17
Pseudo-Critical Thinking 18

What Can Be Learned from the Past?
Thinking Critically about Cuba 20
Deploying the Missiles 20
Assessing the Implications 24
Between Dogmatism and Refutation 26
Lacking: Disconfirmation 29
The Roles of Critical Thinking in the Cuban Crisis 33
Winners and Losers: The Crisis in Context 37
Ten Years Later, They Meet Again 45
Judgment: Critical Thinking Would
Have Made a Difference 46

How Can Intelligence Analysts Employ Critical Thinking? 48
The Poor Record 48
Assessing Evidence 51
Facilitating Evidentiary Assessment 56
Embracing a Methodology 57
Creating Better Inferences 58
Producing Intelligence 59

How can Analysts be Taught to Think Critically? 61
Critical Thinking Education
Outside the Intelligence Community 61
Critical Thinking Education
Inside the Intelligence Community 64
Implications of Teaching Critical Thinking 66
Evaluating Teaching Models 68
Encouraging Analysts to Think Critically 69
Persuading to Improve Analysis 70

How Does Critical Thinking Transform? 74
Transforming Intelligence Corporations 74
Learning from Early Adopters 75
The Costs and Benefits of Thinking Critically 76
Validation 84

What Other Points of View Exist? 86

What Does the Future Hold? 90

Conclusion 95

Appendix: NSA's Critical Thinking
and Structured Analysis Class Syllabus 97

Bibliography 117

About the Author 133

Colophon 134

Figures and Tables

Figure 1: A Comparison of Inductive, Deductive, and Abductive Reasoning 5

Figure 2: Elements of Thought..... 9

Figure 3: A Continuum of Intellectual Standards. 10

Figure 4: Levels of Questioning: Critical Thinking in a Social Setting. 17

Figure 5: Respective Ranges of Soviet SS-4 MRBM and SS-5 IRBM Missiles..... 22

Figure 6: A Place for Analysis between Dogmatism and Criticism 28

Figure 7: Detail of a U-2 Photograph of an SS-4 MRBM Launch Site, San Cristobal, Cuba, 14 October 1962 30

Figure 8: U-2 Tracks over Cuba, 4–14 October 1962 32

Table 1: A Comparison of Different Sets of Critical Thinker's Competencies 14

Table 2: Applying Paul and Elder's Critical Thinking Model to the Situation in Cuba, August–September 1962 27

Table 3: A Comparative Assessment of Rival Motivations 38

Table 4: Goals and Outcomes in the Cuban Missile Crisis..... 44

Table 5: How Analysts Decide 50

Table 6: Cooper's Analytic Pathologies..... 82

Table 7: Analysis: Past, Present and Future 92

Preface

The world in which intelligence analysts work has changed dramatically over the 67 years since the beginning of the Second World War. Adversaries have shifted from large armies arrayed on battlefields to individuals lurking in the shadows or in plain sight. Further, plagues and pandemics, as well as floods and famines, pose threats not only to national stability but even to human existence. To paraphrase a Chinese curse, we certainly live in interesting times.

Our times demand fresh, critical reasoning on the part of those tasked to assess and warn about threats *as well as those tasked to act on those threats*. Education in the bases and practices of intelligence foraging and sensemaking – often called intelligence collection and analysis – is a means by which this can be accomplished. Indeed, the Intelligence Reform and Terrorism Prevention Act of 2004 legislates improved education for intelligence analysis. But, that education is not specifically defined. This volume provides a framework for one area of the act's educational requirement: improving how analysts think – and by extension, how policymakers act. It asserts that people who are skilled critical thinkers are better able to cope with interesting times than those who are not.

The model for thinking developed here also provides specific tools for coping with accelerating disruptive technologies. Such technologies routinely appear in the hands of adversaries. They also offer intelligence professionals capabilities to counter adversaries in novel ways. The key is knowing which technologies are truly disruptive in advance, which pose threats, and which can be harnessed to mitigate threats. Critical thinking – as it is here defined and developed – provides part of the solution as it encourages careful consideration of the available evidence, close examination of presuppositions and assumptions, review of the alternate implications of decisions, and finally, discussion of alternative solutions and possibilities. In short, it equips intelligence professionals with an essential tool for their work.

Foreword

Mark M. Lowenthal
Former Assistant Director of Central Intelligence
for Analysis and Production
President, Intelligence & Security Academy, LLC

Some years ago, when I worked at the Congressional Research Service, my colleague next door had a sign in his office: "Thinking is hard work. That's why so few people do it." Indeed. As sentient beings we think all the time. Our waking, conscious hours are full of thoughts: what to wear; what to eat; how to respond to someone. These all take thought. One might venture to say that we think almost unconsciously through most of our day.

And then there is that *other* thinking: Thinking about the conundrums that we face, the alternatives and choices we have to make on larger issues, the dilemmas we wish to resolve. This *is* hard work. And if the work you do is largely intellectual in nature, then you are thinking that much more often about these more difficult problems. This is not to suggest that those who work with their hands or in crafts or industry do not think. Of course they do. But these people, in the end, have something physical to show for their thought and its execution. Intellectuals only have their thoughts to show, presumably expressed for others in some way.

Intelligence officers are engaged in an intellectual pursuit. They are trying to solve puzzles, resolve uncertainties, discover the nature and meaning of things that others would keep secret. They must have an entire intellectual apparatus to help them identify the problem, assess the parts they know and the parts they do not, come up with an explanation of what is going on and then express it in a way that others – including an audience not steeped in their own techniques – can understand.

As one would expect, the Intelligence Community has spent a fair amount of time thinking about how it does analysis. But most of this has been spent on techniques, presentation and outcomes; much less has been spent on what happens intellectually while you are thinking. That, indeed, is what critical thinking is about: the ability to step out of one's thoughts, if you will, to examine them and the process that brought them about even while you are thinking them. It does not require some higher level of cosmic consciousness or a split personality. It does require training and thought! So now we are thinking about our thinking while we are thinking – a mental triple play, if you will. This is no mean feat and it is a very crucial skill for intelligence analysts.

John McLaughlin, a former Deputy Director of Central Intelligence, has observed that one of the major perceptions that separates intelligence officers from the policy makers is that policy makers tend to be optimists, believing they can get things done, while intelligence officers tend to be skeptics, knowing that little is known with certainty. Like everyone else, however, intelligence analysts can be adamant about their conclusions, understanding the path they took to reach them, and well-satisfied that they have done the right work and come to the right end. That is where critical thinking comes in. The ability to examine how you came to your conclusion is an important adjunct to your other intellectual work. You may be certain or you may not – which is also acceptable. But you owe it to yourself and to your readers to have examined how you got there.

This is not as easy as it sounds for intelligence analysts for the simple reason that they are usually very pressed for time. There are not a lot of lulls in the analyst's work week, which makes it very difficult to be introspective. This means that critical thinking ought to be something that is ingrained in analysts as part of their training, so that it becomes reflexive. But to do that, one must first understand critical thinking – what it is, how to do it, how to teach or learn it. That is the outstanding value of this monograph by David Moore.

The Intelligence Community is filled with people happily working away under a cloak of anonymity, satisfied in making their contribution to part of a larger activity about which very few beyond their immediate circle of co-workers will know. David Moore has long been one of these contributors. In addition to his duties as an intelligence officer at the National Security Agency, David Moore has devoted many fruitful hours to the intellectual underpinnings of intelligence, especially to what makes analysts and what makes better analysts. His work on analytic core competencies, written with his colleague Lisa Krizan, is a fascinating dissection of the intellectual attributes that make up an intelligence analyst. It was also a very influential work, becoming a prime motivator in the creation of the Analytic Resources Catalog created under Director of Central Intelligence George Tenet and now much touted by Director of National Intelligence John Negroponte.

This new monograph on critical thinking will serve a similar purpose. Much has been written in the last five years about intelligence and about the errors that it can make. Some of this has been diagnostic; much of it has been blithely condemnatory. Prescriptions about connecting dots better (an absurd metaphor), about the need to share information better and alarms about groupthink do not get us closer to improvements in the art, craft and profession of intelligence. New ways of thinking about our profession, new ways of doing our work and new ways of assessing it will be useful. Critical thinking needs to be at the top of this list of desiderata.

I would like to believe that we are on the verge of a renaissance in intelligence studies, and more specifically in the intellectual basis of intelligence analysis. There are many straws in the wind: discussions about a national intelligence university and a lessons learned center, more schools offering serious courses about intelligence and books like this. Critical thinking is and should be critical for all analysts and they will profit from this book.

Commentary:

Jeffrey R. Cooper
SAIC Technical Fellow
Science Applications International Corporation

David Moore has written an elegant and largely persuasive argument for the Intelligence Community to move forthrightly and adopt critical thinking in order to improve the quality both of its analytic processes and its intelligence judgments. Since I have recently written about the need for the Community to identify and cure deep-seated and systemic "analytic pathologies," I am obviously sympathetic to the general case for incorporating more rigorous analytic processes—among which "critical thinking" is one attractive approach.[1] Along with Moore, I also believe strongly that the traits often associated with critical thinking need to become fundamental characteristics of every analyst and to be practiced consistently in their work habits. Moore discusses these aspects at some length and highlights their value to making sounder judgments.

In doing so, he makes a compelling case that critical thinking can help analysts reshape their methods in ways that help to avoid damaging errors and enhance judgment. He and I agree with Rieber and Thomason that we should validate the potential improvement before widespread deployment.[2] The need for validation raises some related points concerning the criteria for evaluation and measurement. As Philip Tetlock has noted, on the one hand, one can do evaluation by assessing whether a process (assumed to be good) has been followed; one the other hand, one can also assess

1 Jeffrey R. Cooper, "*Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*" (Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 2005). Cited hereafter as Cooper, *Pathologies*.

2 Steven Rieber and Neil Thomason, "Toward Improving Intelligence Analysis: Creation of a National Institute for Analytic Methods," *Studies in Intelligence* 49, no. 4 (Winter 2006), 71.

quality by looking at the products themselves.[3] However, following a good process does not guarantee good products, nor does a good judgment necessarily validate the quality of the analysis or the analyst. Both approaches have flaws as methods of validation.

I urge the leadership of the Intelligence Community to place far more emphasis on structured analytic methods. In my view, the transformation of the intelligence enterprise demands a more curious, more agile, and more deeply thoughtful cadre of intelligence analysts—but it should also require the same traits among its intelligence organizations and the intelligence enterprise as a whole. Moore notes that "Investment in critical thinking as part of the analysis process minimizes the likelihood of specific failures" (page 81). However, from my perspective, critical thinking (and other structured methods) are more important for changing the organization's overall approach to analysis, rather than in improving specific judgments or preventing particular failures.

I believe such methods are crucial in preventing systemic analytic pathologies from developing, exactly because the Community lacks many of the desirable self-corrective mechanisms found in science. Second, while Moore focuses on the role of critical thinking in improving an individual analyst's ability to make good judgments, my view emphasizes the importance of more rigorous processes for the organization as a whole if it is to improve its capacity to meet user needs. Indeed, given my emphasis on the systemic nature of the pathologies that afflict intelligence analysis, structured analytic methods become a first line of defense in preventing networks of errors—they are like "ripstops" that keep problems from propagating into wider "error-inducing systems," in Perrow's terms. The quality of "mindfulness" and a more self-reflective process are essential if the intelligence organizations are to acquire some of the desirable characteristics of high-reliability organizations. While critical thinking can clearly assist individual analysts, and these "memes" can be spread through viral dissemination, I would place far more emphasis on fomenting social and organizational changes as remedies.

---

3 Philip E. Tetlock, *Expert Political Judgment: How Good Is It? How Can We Know?* (Princeton, NJ: Princeton University Press, 2005).

Finally, exactly because Moore focuses so tightly on the value of critical thinking to improve how individual analysts reason, he largely ignores the important role such habits should, and could, play in the "social construction" of intelligence analysis *and its communication to users of that intelligence*. The use of more structured techniques "to present more effective assessments" should go beyond simply convincing policymakers "to question their own assumptions on the issues" (page 80). By restructuring both the analytic process and the modalities of interactions with policy users, critical thinking techniques can draw policy users into "co-creating" important judgments and, by doing so, get them to adopt some of the important attributes of critical thinking. This internalization would be more powerful than hoping the exquisite brilliance of the improved analytic judgments might make them more palatable.

These minor quibbles aside, David Moore has highlighted for the Intelligence Community and its users some tangible methods for improving intelligence analysis and addressing systemic analytic pathologies.

Commentary

Francis J. Hughes
Professor, National Defense Intelligence College

> The truly difficult problems of the information age are not technological; rather, they concern ourselves – what it is to think, to reason, and to engage in conversation [using] … new analytic techniques, new conceptual tools with which to analyze and understand the workings of the human mind.
>
> —Keith Devlin, *Goodbye Descartes: The End of Logic and the Search for a New Cosmology of the Mind*, 1997

David Moore has undertaken a valuable initiative on behalf of the Intelligence Community by producing this monograph on critical thinking. In doing so, he has addressed the concerns of Keith Devlin and many other scholarly writers on the subject of human reasoning. By contextualizing the concept and practices of critical thinking within intelligence analysis, he has set forth a much-needed cognitive linkage between intelligence analysis and the human thought process, which, as he states, remains otherwise "poorly understood."

Mr. Moore has developed a methods-of-thinking course, outlined in the Appendix to this paper, which should guide the collection of evidence, the reasoning from evidence to argument, and the application of objective decision-making judgment. Critical thinking in intelligence depends primarily on a conscious application of suitable habits of thought, and the course certainly promises to advance the education of intelligence professionals.

Commentary

Gregory F. Treverton
RAND Corporation
Former Assistant Director of Central Intelligence for
Analysis and Production
and Vice-Chairman, National Intelligence Council

David Moore has added his powerful voice to those calling for America's intelligence analysts to be more self-conscious about their methods and more venturesome in applying more formal methods. His starting point is critical thinking, but his strong case embraces a range of techniques from Paul and Elder's checklist, to analysis of competing hypotheses (ACH), to Factions analysis, which is really a way to be more systematic in aggregating subjective judgments, to techniques such as those developed by the Novel Intelligence from Massive Data (NIMD) project. These help analysts search for patterns and test hypotheses. Moore's discussion pays particular attention to critical thinking about *evidence* – that is perhaps natural given that the National Security Agency is his home agency, but it is also a welcome emphasis.

My own explorations of the analytic agencies over the last few years confirm my own experience managing the National Intelligence Council (NIC): In general, U.S. intelligence analysis has been neither very self-conscious about its methods, nor made much use of machines and formal analytic tools. That is Moore's point of departure, and it is a case made graphically by Rob Johnston, on whose work Moore draws. The state of affairs Moore and others describe is changing, and his work should contribute to accelerating that change, in a variety of experiments and pilot projects.

Moore's paper raises at least two intriguing questions at its edges. He rightly takes issue with Malcolm Gladwell's book about the power of unconscious thought or "deliberation without attention."

That said, clever defense lawyers often discredit ballistic experts by asking them to be explicit about how they reached their conclusions. Likewise, chess masters can be reduced to middle-weights by having to explain the logic of their moves. In both cases, the decisions result from patterns as much sensed as seen, the result of thousands of previous cases. I sometimes worried at the NIC that the more we required analysts to be explicit about their methods, the more we risked turning them into middle-weights.

Finding ways to incorporate not just expertise, but also hunch and sense into intelligence analysis is a challenge that lies ahead. The Defense Advanced Research Projects Agency's ill-fated experiment a few years ago seeking to establish a terrorism futures market was testimony to how hard the challenge will be. When the idea became public, every politician – right, left and center – quickly denounced it as borderline immoral. Over the ensuing days, however, a wide range of analysis commented on what a good idea it might have been when information is in short supply and there is a premium on sensing patterns before they become facts.

The second issue is consumers of intelligence, who figure only at the margins of Moore's discussion. We can only hope he is right that better analysis will find, and perhaps help create, a better audience. But the unboundedness of the terrorist threat we now face means that intelligence and policy no longer share a "story" comparable to that about state threats, like the Soviet Union. In principle, that would suggest that policy should accord more time and attention to intelligence, but that is not likely to happen in Washington's whirligig.

Thus, intelligence will need to be as creative in finding new ways to work and communicate with policy officials as it is in improving its analytic techniques. In the process, it will need to rethink what it regards as its *product.* I came to think at the NIC that our product was not really National Intelligence Estimates but, rather, National Intelligence *Officers* – people, not paper, and people in a position to come to know their policy counterparts and to make their expertise available informally, in meetings or at lunch.

Acknowledgments

The first notes for this paper were begun a year prior to the 11 September 2001 terrorist attacks in New York and Virginia as part of research conducted with a peer, Lisa Krizan, on a set of core competencies – knowledge, skills, abilities, and an associated set of personal characteristics – for successful intelligence analysis. At the time, the notion of critical thinking was at best vaguely understood by members of the Intelligence Community, and the National Security Agency (NSA) was no exception. Six years later critical thinking is a recognized key skill by which intelligence readiness is defined at NSA. Similar growth in its importance is recognized elsewhere in the Community. This recognition is due in part to the work of Dr. Linda Elder, Dr. Gerald Nosich and Dr. Richard Paul, all of the Foundation for Critical Thinking. They have created a practical model for critical thinking that is both effective and easy to teach.

That the Paul and Elder model is known within the Intelligence Community is due in no small part to Professor Francis J. Hughes of the National Defense Intelligence College (NDIC). It was he who introduced the author to the model and encouraged attendance at Paul and Elder's annual conference on critical thinking. He kindly also provided a commentary on the paper. Dax Norman, of the NSA Associate Directorate for Education and Training, a number of NSA colleagues, and approximately 250 participants in the NSA critical thinking and structured analysis course helped make that course a reality and additionally provided valuable insights into the nuances of critical thinking. Comments from LT Robert D. Folker, USAF, also provided insight into the teaching of critical thinking. LT Folker developed a similar course while a student at the NDIC that unfortunately did not remain in the curriculum.

As the paper progressed, a number of colleagues and peers provided feedback, comments, and challenges to the arguments presented. They include, in alphabetical order, Solveig Brownfeld, NDIC; James Bruce, SAIC; Jan Goldman, NDIC; Mary Rose Grossman, the John F. Kennedy Presidential Library and Museum; Alexandra Hamlet; Noel Hendrickson, James Madison University;

Robert Heibel, Mercyhurst College; Richards J. Heuer, Jr., Central Intelligence Agency (retired); Norval J. Hilmer, Defense Intelligence Agency; LTCOL James Holden-Rhodes, USMC (retired); Morgan D. Jones, Central Intelligence Agency (retired); Hugo Keesing, Defense Intelligence Agency (retired); Mark Marshall, NDIC; Stephen Marrin, University of Virginia; Montgomery McFate, Institute for Defense Analysis; William Reynolds, Least Squares Software; the staff of the Central Intelligence Agency's Sherman Kent Center; and the staff of the John F. Kennedy Presidential Library and Museum. Several other colleagues at the National Security Agency – who wish to remain anonymous – also offered valuable insight and suggestions.

Three colleagues, Mark Lowenthal, president of the Intelligence & Security Academy, LLC; Jeffrey Cooper, Science Applications International Corporation; and Gregory Treverton, Rand Corporation, also deserve mention. Mark kindly agreed to write the foreword and offered valuable suggestions. His quip about really good analysts set up much of the arguments presented herein. Both Jeff and Greg provided critical comments and suggestions late in the game. They also kindly agreed to write commentaries on the paper.

Russell Swenson, Director of NDIC's Center for Strategic Intelligence Research and NDIC Press editor, did what a really good editor is supposed to do: His input and recommendations ensured that the arguments that follow were focused and strong. The Center's William Spracher also provided valuable technical editing services. Colleague Lisa Krizan provided a final review of the text that proved extremely valuable. This paper would not have been published if not for their dedicated assistance to the author.

Acknowledgment is due to four other people. Peter and Mary Moore encouraged their son to be inquisitive and to always look beyond the obvious for answers. Anthropologist John McDaniel first introduced the author – then a student at Washington and Lee University – to an analogy for intelligence sensemaking: science-based field archaeology. Finally, Elizabeth Moore provided tremendous encouragement. She also graciously tolerated the many nights and weekends spent writing, listening to, and commenting on, ideas as

they occurred, sharpening the resulting arguments. It is to these people that this work is dedicated.

While the author was privileged to receive assistance of others, this remains his work and any errors are his. The author may be reached via electronic mail at dtmoore@nsa.gov.

CRITICAL THINKING AND INTELLIGENCE ANALYSIS

David T. Moore

Examples included in this paper were selected to illustrate points raised by the author. No interest by the National Security Agency, the Department of Defense, or any other agency of the U.S. Government should be inferred from their inclusion.

Abstract

Analysts and analysts alone create intelligence. Although technological marvels assist analysts by cataloguing and presenting data, information and evidence in new ways, they do not do analysis. To be most effective, analysts need an overarching, reflective framework to add structured reasoning to sound, intuitive thinking. "Critical thinking" provides such a framework and goes further, positively influencing the entire intelligence analysis process. Analysts who adopt critical thinking stand to improve their analyses. This paper defines critical thinking in the context of intelligence analysis, explains how it influences the entire intelligence process, explores how it toughens the art of intelligence analysis, suggests how it may be taught, and deduces how analysts can be persuaded to adopt this habit.

Definitions

Thinking – or reasoning – involves objectively connecting present beliefs with evidence in order to believe something else.

Critical Thinking is a deliberate meta-cognitive *(thinking about thinking)* and cognitive *(thinking)* act whereby a person reflects on the quality of the reasoning process simultaneously while reasoning to a conclusion. The thinker has two equally important goals: coming to a solution and improving the way she or he reasons.

Intelligence is a specialized form of knowledge, an activity, and an organization. As knowledge, intelligence informs leaders, uniquely aiding their judgment and decision-making. As an activity, it is the means by which data and information are collected, their relevance to an issue established, interpreted to determine likely outcomes, and disseminated to individuals and organizations who can make use of it, otherwise known as "consumers of intelligence." An intelligence organization directs and manages these activities to create such knowledge as effectively as possible.

CRITICAL THINKING AND INTELLIGENCE ANALYSIS

Introduction: How Do People Reason?

The best analytical tool remains a really good analyst.

—Mark Lowenthal, Former Assistant Director of Central Intelligence for Analysis and Production

To create intelligence requires transformations resulting from an intellectual endeavor that sorts the "significant from [the] insignificant, assessing them severally and jointly, and arriving at a conclusion by the exercise of judgment: part induction, part deduction," and part abduction.[4] That endeavor is known as *thinking*, or "that operation in which present facts suggest other facts (or truths)."[5] Thinking – or as it is sometimes known, reasoning – creates an "objective connection" between our present beliefs and "the ground, warrant, [or] evidence, for believing something else."[6]

These three reasoning processes trace the development of analytic beliefs along different paths. Whereas inductive reasoning reveals "that something is probably true," deductive reasoning demonstrates "that something is necessarily true."[7] However, both are limited:

4 William Millward, "Life in and out of Hut 3," in F. H. Hinsley and Alan Stripp, *Codebreakers: The Inside Story of Bletchley Park* (Oxford, UK: Oxford University Press, 1993), 17. The author adds "abduction" for reasons that will shortly become evident.

5 John Dewey, *How We Think: A Restatement of the Relation of Reflective Thinking to the Educative Process* (New York, NY: D.C. Heath and Company, 1910), 12. Cited hereafter as Dewey, *How We Think*.

6 Dewey, *How We Think*, 12.

7 David A. Schum, "Species of Abductive Reasoning in Fact Investigation in Law," *Cardozo Law Review* 22, nos. 5–6, July 2001, 1645, emphasis added. Cited

inductive reasoning leads to multiple, equally likely solutions and deductive reasoning is subject to deception. Therefore, a third aid to judgment, abductive reasoning, showing "that something is plausibly true," can offset the limitations of the others.[8] While analysts who employ all three guides to sound judgment stand to be the most persuasive, fallacious reasoning or mischaracterization of rules, cases, or results in any of the three can affect reasoning using the others.

Inductive reasoning, moving from the specific to the general, suggests many possible outcomes, or the range of what adversaries may do in the future. However, inductive reasoning lacks a means to distinguish among each outcome – all are possible. An analyst has no way of knowing whether a solution is correct.

Deductive reasoning on the other hand, moving from the general to the specific, addresses questions about adversarial behavior and intentions. Deductive reasoning becomes essential for warning. Based on past perceptions, certain facts indicate specific outcomes. If, for example, troops are deployed to the border, communications are increased, and leadership is in defensive bunkers, then war is imminent. However, if leadership remains in the public eye then these preparations indicate that an exercise is imminent.

Abductive reasoning reveals plausible outcomes to the intelligence analyst. When an adversary's actions defy accurate interpretation through existing paradigms, abductive reasoning generates novel means of explanation. In the case of intelligence warning, an abductive process presents policy–making intelligence consumers with an "assessment of probabilities." Although abduction provides no guarantee that the analyst has chosen the correct hypothesis, the probative force of the accompanying argument indicates that the most likely hypothesis is known and that elusive, actionable intelligence is on tap.

---

hereafter as Schum, "Species." American mathematician, logician, semiotician, and philosopher Charles Sanders Peirce (1839–1914) developed the concept of abductive reasoning. See Joseph Brent, *Charles Sanders Peirce: A Life* (Bloomington, IN: Indiana University Press, 1998).

8 Schum, "Species," 1645.

Figure 1 models analysts' thinking about HUMINT received during the summer of 1962 regarding reports of foreigners in Cuba. An initial (fallacious) conclusion derived from inductive reasoning apparently was reapplied through deductive reasoning as explained in the case study incorporated in this paper.[9] Something else was needed – but not considered – to challenge the initial conclusion that "All HUMINT from Cuba was false."

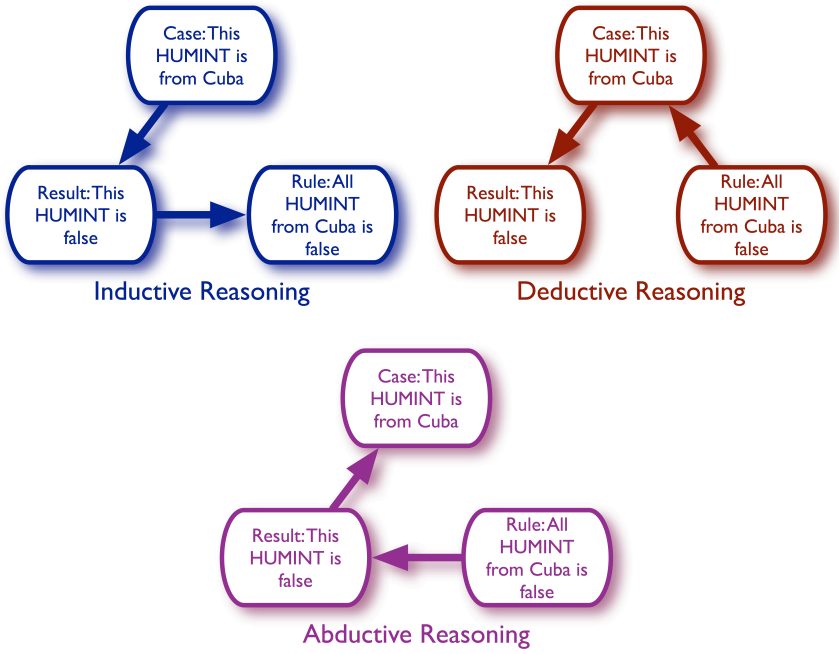


Figure 1: A Comparison of Inductive, Deductive, and Abductive Reasoning

Sources: Adapted from Thomas A. Sebeok, "One, Two, Three Spells UBERTY," in Umberto Eco and Thomas A. Sebeok, *The Sign of Three: Dupin, Holmes, Pierce* (Bloomington, IN: Indiana University Press, 1988), 8; and James H. Hansen, "Soviet Deception in the Cuban Missile Crisis," *Studies in Intelligence*, 46, no. 1 (2002), 56.

If analysts can model an adversary's intentions based on observable actions, adversaries also can deduce how those analysts will have

9 While there is no evidence it was applied in the Cuban case, abductive reasoning is included in the figure for purposes of illustration.

moved toward these conclusions. Under these circumstances, the adversary then can engage in deceptive practices that can lead an intelligence service to misinterpret that adversary's intentions.[10] For example, the Indian government deceived the U.S. Intelligence Community before the former's 1998 nuclear test. Through a 1995 demarche from the U.S. government, the Indian government knew what indicators the U.S. sought and was able to obscure them until after the test. Then, the Indian government boasted of its success.[11]

Abduction forces a close consideration of the evidence at hand. Given competing estimates – such as "war is imminent" or "an exercise will occur" – the body of facts and inferences must be examined to determine "whether there are facts which falsify one of the estimates."[12] Only then can an assessment of accuracy be determined. Even then, the selected estimate remains only the "most likely."[13]

Despite their individual limitations, induction, deduction, and abduction taken together offer a means of thoroughly examining evidence in order to arrive at accurate intelligence conclusions. However, as becomes obvious from studying figure 1, in order to be successful, intelligence analysis requires something more: an overarching framework is needed to ensure reasoning relies on valid assertions, is not fallacious, and is self–consciously objective. Critical thinking provides that framework by ensuring that each form of reasoning is appropriately used. Critical thinking extends to the entire intelligence analysis process. The claim here is that analysts who

---

10 Isaac Ben-Israel explores the duality of estimation in considerable detail. See "Philosophy and Methodology of Intelligence: The Logic of the Estimate Process, *Intelligence and National Security* 4, no. 4 (October 1989), 660–718. Cited hereafter as Ben-Israel, "Logic of the Estimate Process."

11 Paul J. Raasa, "The Denial and Deception Challenge to Intelligence," in Roy Godson and James J. Wirtz, *Strategic Denial and Deception* (New Brunswick, NJ: Transaction Publishers, 2002), 178, 223–224.

12 Ben-Israel, "Logic of the Estimate Process," 668.

13 Cynthia M. Grabo, *Anticipating Surprise: Analysis for Strategic Warning* (Washington, DC: National Defense Intelligence College, 2002), 13.

become better critical thinkers will improve their analyses, helping to lessen the likelihood of intelligence failures. In the example above, critically thinking analysts would have questioned the generalizing of their initial conclusion by asking, "Was all the HUMINT from Cuba *really* false?" To avoid the tautological problem of equating quality analysis with the concept of "critical thinking" requires a careful assessment of cognition in the intelligence environment. The underlying question is "How can the intelligence analysts to whom Lowenthal's epigraph refers be 'really good'?"

Defining Critical Thinking

Defining critical thinking is a first step to understanding how it contributes to intelligence analysis. Richard Paul and Linda Elder, of the Foundation for Critical Thinking, consider it to be

> that mode of thinking – about any subject, content, or problem – in which the [solitary] thinker improves the quality of his or her thinking by skillfully taking charge of the structures inherent in thinking and imposing intellectual standards upon them.[14]

In other words, critical thinking is both a deliberate meta-cognitive *(thinking about thinking)* and cognitive *(thinking)* act whereby a person reflects on the *quality* of the reasoning process simultaneously while reasoning to a conclusion. The thinker has two equally important goals: improving the way she or he reasons and coming to a correct solution.[15]

To accomplish these goals, the reasoner requires assisting structures. Paul and Elder define eight elements of reasoning, shown in figure 2. These elements lead thinkers to ask focused questions about the topic being considered and the thinking process itself. Paul and Elder assert that whenever people reason, they do so for a purpose. This reasoning exists within a point of view and is shaped by both conscious and unconscious assumptions. Reasoning involves the creation of inferences based on conceptual frameworks about reality. These inferences are generated as people consider evidence necessary to answer questions or solve problems. Further, reasoning leads to decision points with implications – things that might happen

14 Richard Paul and Linda Elder, *The Miniature Guide to Critical Thinking Concepts and Tools*, 4th Edition (Dillon Beach, CA: The Foundation for Critical Thinking, 2004), 1. Cited hereafter as Paul and Elder, *Concepts and Tools*.

15 Exactly what is the "correct solution" is issue and context dependent. What is important here is that the process of reasoning is enhanced.

– *and* consequences – things that do happen once the decision has been made. Finally, Paul and Elder insist that "learning to analyze thinking requires practice in identifying the structures in use."[16]

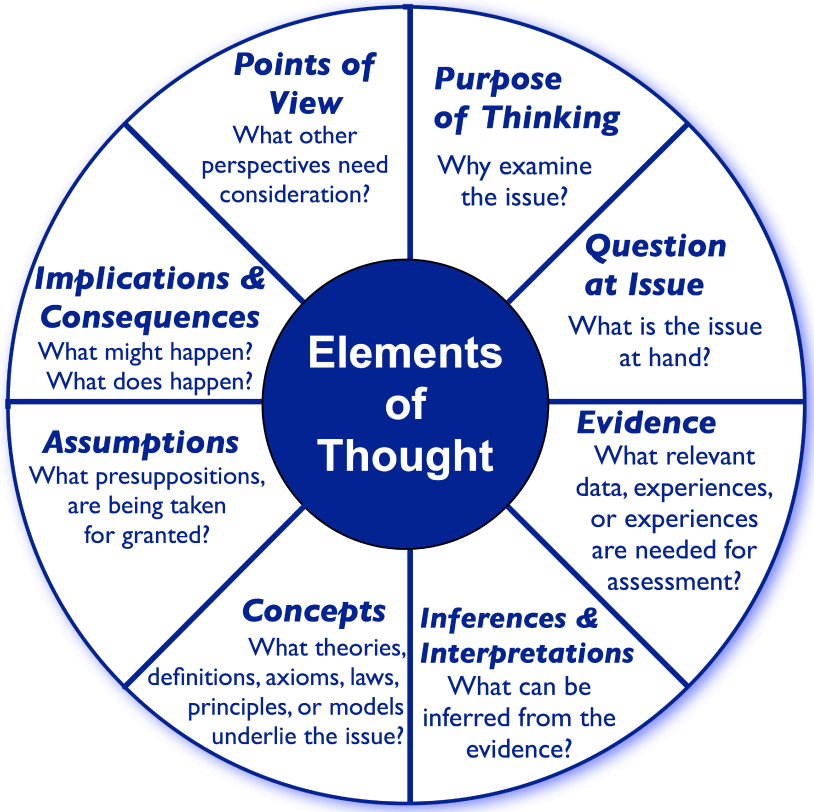


Figure 2: Elements of Thought

Source: Derived from Richard Paul and Linda Elder, *The Miniature Guide to Critical Thinking Concepts and Tools*, 4th Edition (Dillon Beach, CA: The Foundation for Critical Thinking, 2004), 2.

16 Linda Elder and Richard Paul, *The Foundations of Analytic Thinking: How to Take Thinking Apart and What to Look for When You Do* (Dillon Beach, CA: The Foundation for Critical Thinking, 2003), 5. Cited hereafter as Elder and Paul, *Analytic Thinking*. Paul and Elder, *Concepts and Tools*, 2.

Standards for Critical Thinking

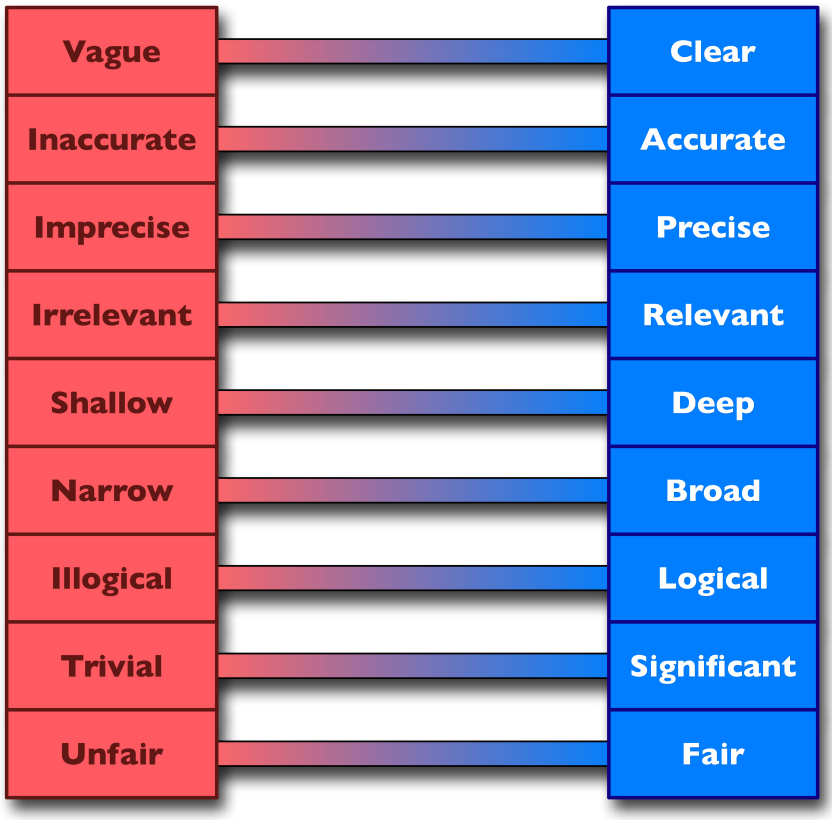


Figure 3: A Continuum of Intellectual Standards

Source: Derived from Paul and Elder, *Concepts and Tools*, 9.

Paul and Elder also establish a set of intellectual standards that offer criteria for assessing the level and quality of thinking. These form a continuum as shown in figure 3.[17] Active – or Socratic – questioning in a social setting becomes the means of critically exploring a topic or discipline as well as assessing the thinking on that topic. Questions assessing the issue delve into purpose, assumptions, inferences, as well as points of view on a topic.[18] Paul and Elder's

17 Elder and Paul, *Analytic Thinking*, 1–17.

18 Paul and Elder, *Concepts and Tools*, 2–9.

approach ensures that a topic or issue is thoroughly, logically, and objectively developed. Their continuum provides qualitative metrics to inform the thinker and others who may evaluate the object of the thinking along with the process employed. Each standard is related to but independent of the others. The object of consideration might be vaguely or clearly presented. But it also might be inaccurate. An example of this would be "the world is flat." This clear statement of reality is false.

The reasoning or its object might be clearly and accurately presented but remain imprecise, the level of detail required depending on the issue itself. Precision becomes important in assessing the location of an adversary or a threat as in "terrorists placed the improvised explosive device (IED) near the highway."

It is possible to create clear, accurate, and precise answers that are irrelevant. If one is considering the IED along the highway but the issue is how best to fly the troops in question from one location to another then the answer is irrelevant. Similarly, topics and their accompanying reasoning need to consider both the complexities involved (depth) and other points of view (breadth).[19] Such reasoning becomes essential when systems must be assessed because in systems "chains of consequences extend over time and many areas: The effects of action are always multiple."[20] Intelligence often must assess such systems – terrorist networks are but one example. Additionally, as sociologist Emile Durkheim observes, the combinations of elements related to an issue "combine and thereby produce, by the fact of their combination, new phenomena."[21]

When the correct phenomena or questions – and related alternative explanations – are not fully considered, intelligence failures occur. For instance, the Senate Select Committee on Intelligence

19 Elder and Paul, *Analytic Thinking,* 7.

20 Robert Jervis, *System Effects: Complexity in Political and Social Life* (Princeton, NJ: Princeton University Press, 1997), 10. Cited hereafter as Jervis, System Effects.

21 Emile Durkheim, *The Rules of Sociological Method* (Glencoe, IL: Free Press, 1938), xlvii.

found such reasoning to be among the causes of the Intelligence Community's failure to assess accurately Iraq's alleged programs to develop weapons of mass destruction (WMD). The senators noted that "Intelligence Community managers…did not encourage analysts to challenge their assumptions, fully consider alternative arguments, accurately characterize the intelligence reporting, or counsel analysts who lost their objectivity."[22]

Logic and significance also come into play. If the evidence presented does not imply the conclusions then the results are illogical. Focusing on appropriate evidence maintains significance. For example, evidence that terrorists who place an IED also have Stinger surface–to–air missiles bears on how troops can move across hostile territory.

Fairness deals with the agendas – hidden and expressed – of the thinker, her collaborative peers, and her customers. Knowing who has a stake in an issue as well as the stakes themselves helps ensure that issues are fairly reasoned and presented. Such considerations also reflect the analyst's own biases or opinions. In considering this point, Paul and Elder offer the evaluative question, "Am I misrepresenting a view with which I disagree?"[23]

Finally, while getting to the right-hand side of the spectrum on each of these standards in figure 3 is highly desirable, the standard of thinking on an issue will vary based on the skills of the thinkers and the issues under scrutiny. Assessing the resulting shortfalls in thinking reveals gaps that can be corrected. The continuum therefore provides a detailed assessment by which thinking on issues can be improved.

---

22 Senate Select Committee On Intelligence, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq,* United States Senate, 108th Congress, 7 July 2004, 23. Cited hereafter as SSCI, *Iraq.*

23 Elder and Paul, *Analytic Thinking,*, 7.

Skill-Based Definitions

Other approaches to defining critical thinking focus on the specific skills. For example, Diane Halpern considers that

> [critical] thinking is the use of those cognitive skills or strategies that increase the probability of a desirable outcome. It is… thinking that is purposeful, reasoned, and goal directed – the kind of thinking involved in solving problems, formulating inferences, calculating likelihoods, and making decisions, when the thinker is using skills that are thoughtful and effective to the particular context and type of thinking task.[24]

Additional advocates of skills-based critical thinking include Edward Glaser and Alec Fisher, and their sets of critical thinking skills include a number of elements common to those identified by Halpern. The overlapping competencies of critical thinkers as advanced by Paul and Elder and these three other proponents are summarized in table 1. The comparison reveals the completeness of the Paul and Elder model.

These competencies assist intelligence analysts who contribute to the solution of threats to national security by ensuring the formulation of sound inferences about adversarial capabilities and intentions. Resulting findings are disseminated in reports that are often referred to as "assessments." At their best, they offer choices to decision-making consumers, as well as a clear outline of the implications of those choices.[25]

---

24 Diane Halpern, *Thought and Knowledge: An Introduction to Critical Thinking*, 4th Edition (Mahwah, NJ: Lawrence Erlbaum Associates, Publishers, 2002), 37. Cited hereafter as Halpern, *Thought and Knowledge.*

25 The term "assessment" describes the result of an intelligence production process but is not universally used within the Intelligence Community. Assessments are created at the Central Intelligence Agency and at the Defense Intelligence Agency. Other names for the reports that analysts produce include "products" at the National Security Agency (NSA) and "estimates" at the National Intelligence Council (NIC). Regardless of how they are named, they record and disseminate the results of analysts' work.

Competencies of Critical Thinkers	Paul and Elder	Fisher	Glaser	Halpern
Recognize problems or questions and find effective means of solution	✓		✓	✓
Engage in meta-cognitive activities that identify assumptions, biases, and performance as solutions are developed	✓	✓	✓	✓
Interpret data, appraise evidence, and evaluate statements in order to recognize logical relationships between propositions	✓		✓	✓
Infer warranted conclusions and generalizations from evidence	✓	✓	✓	✓
Test generalizations and conclusions by seeking out contradictory evidence that enables them to judge the credibility of claims	✓	✓	✓	✓
Convey sound, well-reasoned arguments	✓	✓	✓	✓
Focus on the process of reasoning with the intention of improving the process	✓			

Table 1: A Comparison of Different Sets of Critical Thinker's Competencies

Sources: Compiled by author from Linda Elder and Richard Paul, *The Foundations of Analytic Thinking: How to Take Thinking Apart and What to Look for When You Do* (Dillon Beach, CA: The Foundation for Critical Thinking, 2003); Diane Halpern, *Thought and Knowledge: An Introduction to Critical Thinking,* 4th Edition (Mahwah, NJ: Lawrence Erlbaum Associates, Publishers, 2002), 37; Edward M. Glaser, *An Experiment in the Development of Critical Thinking* (New York, NY: AMS Press, 1941), 6; and Alec Fisher, *Critical Thinking: An Introduction* (Cambridge, UK: Cambridge University Press, 2001), 8.

A Disposition to Think Critically

It is not enough merely to know the skills needed for critical thinking. To be successful, analysts as critical thinkers also need "certain attitudes, dispositions, passions, [and] traits of mind."[26] Actively thinking critically hones the skills; practice yields proficiency. But in order to gain mastery, willingness to reason in this manner becomes essential. The importance of this disposition to critically think cannot be over-emphasized. According to Peter A. Facione, Noreen C. Facione, and Carol A. Giancarlo, "Empirical studies…at multiple sites indicate that for all practical purposes" both critical thinking skills and the disposition to critically think are essential.[27]

There are a number of characteristics associated with the disposition to think critically. The Faciones and Giancarlo identify "seven characterological attributes or habits of mind… truth-seeking, open-mindedness, analyticity, systematicity, critical thinking, self confidence, inquisitiveness, and maturity of judgment."[28] According to Richard Paul and Gerald Nosich, the characteristics of critical thinkers include

> thinking independently, exercising fair-mindedness, developing insight into egocentricity and sociocentricity, developing intellectual humility and suspending judgment, developing intellectual courage, developing intellectual good faith and integrity, developing intellectual perseverance,

---

26 Richard W. Paul and Gerald Nosich, *A Model for the National Assessment of Higher Order Thinking*, (Dillon Beach, CA: Foundation for Critical Thinking, n.d.), 20. Cited hereafter as Paul and Nosich, National Assessment.

27 Peter A. Facione, Noreen C. Facione, and Carol A. Giancarlo, "The Disposition Toward Critical Thinking: Its Character, Measurement, and Relationship to Critical Thinking Skill," *Informal Logic* 20, no. 1 (2000): 61–84. Reprinted by Insight Assessment, URL: <http://www.insightassessment.com/pdf_files/J_Infrml_Ppr%20_2000%20–%20Disp%20&%20Skls.PDF>, last accessed 31 March 2006. Cited hereafter as Facione, "Disposition."

28 Peter A. Facione, Noreen C. Facione, Carol A. F. Giancarlo, *Professional Judgment and the Disposition Toward Critical Thinking* (Milbrae, CA: California Academic Press, 2002), URL: < http://www.calpress.com/pdf_files/Prof_jmn.pdf>, last accessed 31 March 2006.

developing confidence in reason, exploring thoughts underlying feelings and feelings underlying thoughts, developing intellectual curiosity.[29]

Both sets closely match the characteristics of successful intelligence analysts identified by Lisa Krizan and the author in their work on intelligence analysts' core competencies. Krizan and the author observe that successful intelligence analysts are insatiably curious. Fascinated by puzzles, their high levels of self-motivation lead them to observe and read voraciously, and to take fair-minded and varied perspectives. This helps them to make the creative connections necessary for solving the hardest intelligence problems. Finally, the emotional tensions created by problems, and the cathartic release at their solution, powerfully motivate analysts.[30]

In addition, emotions play a significant part in the process of critical thinking. As adult learning expert Stephen Brookfield observes, "[emotive] aspects – feelings, emotional responses, intuitions, sensing – are central to critical thinking."[31] He argues that the consideration of alternatives "to one's current ways of thinking" characterizes the approach.[32] Indeed, the consideration of these alternatives requires creativity, which he considers a non–rational form of thought.[33] Creative reasoning generates hypotheses; it has contributed significantly to the development of intellectual, scientific, and technological knowledge.

---

29 Paul and Nosich, *National Assessment*.

30 David Moore and Lisa Krizan, "Intelligence Analysis: Does NSA Have What it Takes," reprint NSA Center for Cryptologic History, *Cryptologic Quarterly* 20, nos. 1/2 (Summer/Fall 2001), 8–11. Cited hereafter as Moore and Krizan, "NSA,"

31 Stephen D. Brookfield, *Developing Critical Thinkers: Challenging Adults to Explore Alternative Ways of Thinking and Acting* (San Francisco, CA: Jossey–Bass Publishers, 1987), 12. Cited hereafter as Brookfield, Developing Critical Thinkers.

32 Brookfield, *Developing Critical Thinkers,* 12.

33 Brookfield, *Developing Critical Thinkers,* 12.

The Role of Questions

Greg Treverton observes that in intelligence the right questions rarely get asked.[34] Yet, critical thinking offers a means by which at least *appropriate* questions may be raised. The combination of critical thinking skills and the disposition to think critically focuses and directs inductive, deductive, and abductive reasoning to solve problems. This is an interrogative paradigm. Critical thinking involves questioning that forces broader consideration of issues and problems as well as the various means of resolving or answering them. Such questioning happens at both the individual and collective levels as shown in figure 4.

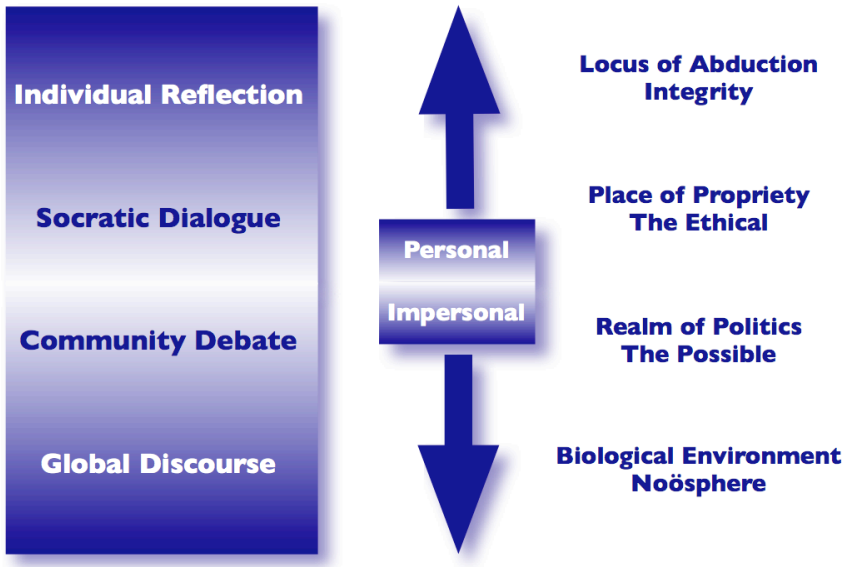


Figure 4: Levels of Questioning: Critical Thinking in a Social Setting

Source: Created by the author with contributions by Russell G. Swenson.

Questioning is either personal or impersonal and ranges from the musings of the individual critical thinker to that of a global discourse. As an individual ponders problems and issues, she abduces the most likely explanations. Moving up a level, questioning becomes a

34 Greg Treverton, conversation with the author, 18 April 2006.

hierarchical dialogue within dyads or larger assemblies. A critically thinking questioner ferrets out answers from others within the group. The process generates new questions that are answered in turn – and in turn, raise further questions. At the level of a community debate, critical thinkers explore what is possible politically and within the community's purview. Ideally, the relationship between thinkers is peer-to-peer. Finally, questions addressed within the context of a global discourse take into account the entire biological landscape (noösphere).[35]

Such questioning produces new and creative thinking, analogous to switching from Newtonian to quantum physics. In this analogy, an atomistic approach to analysis gives way to the associative impulse of synthesis as structured thoughts facilitate a leap to new questions, ideas, and possibilities. This overarching framework of structured reasoning frames questions to help analysts decide the best means or best combination of means that are suited to solving specific intelligence problems. The questions serve to alert an analyst to the notion that she might be deceived, or that she needs to employ some other means of reasoning to determine which of several alternative outcomes is most likely. These questions provide a formal means by which an analyst confronts her biases about likely outcomes. Therefore, in the context of intelligence analysis, critical thinking becomes one of the most – if not *the* most – important skills of the analyst. Facing symmetric and asymmetric threats, analysts have a potent and powerful tool to facilitate their asking the right questions in the process of improving their understanding of the problem at hand as well as their own reasoning about that problem.

Pseudo-Critical Thinking

It is important to understand what critical thinking is *not*. Critical thinking, as has been noted, focuses on both the process and the results of reasoning. However, the term is also used in reference to reasoning that is not reflective. The application of formal logic is sometimes (incorrectly) equated to critical thinking. So too are

35 Wikipedia defines the noösphere as the domain of human thought. Wikipedia, entry under "noösphere," accessed 27 February 2006.

problem solving and structured methods of analysis. Developers of school curricula and other exponents of "sound thinking" often lay claim to the mantel of critical thinking but are really leveraging their coverage of logic or problem solving to capitalize on an uncritical understanding of what critical thinking is. Problem solving, for example, focuses on answers and not on the process by which an answer is obtained. Additionally, logic or problem solving, being goal oriented, offer little means by which a person can improve the process of her thinking. The following problem is a typical example of pseudo–critical thinking:

> Two cyclists race along a straight course. The faster of the pair maintains an average speed of 30 mph. The slower cyclist averages 25 miles per hour. When the race ends, the judges announce that the faster cyclist crossed the finish line one hour before the slower racer. How many miles long was the racing course?[36]

This example (and others like it) focuses on the answer, provides no guidance on the process, and ignores any improvement in reasoning skills. Solvers either figure it out through trial and error or by following a rule-based strategy learned by rote. Therefore it fails to be critical thinking.

Unless the process, and the means, to improve a person's reasoning are emphasized, then at best such examples teach structured problem solving. At worst, they deal merely in criticism; they fail to assist people to learn to reason better. Central to critical thinking are the twin foci on the way in which a person is reasoning and the goal of improving that process. One could easily infer that misconceptions about critical thinking could be associated with what is taught as critical thinking in American educational institutions.[37]

---

36 Michael A. DiSpezio, *Classic Critical Thinking Puzzles* (New York, NY: Main Street, 2005), 85. The answer, by the way, is 150 miles (page 227).

37 Michael R. LeGault reaches this same conclusion in *Think: Why Crucial Decisions Can't Be Made in the Blink of an Eye* (New York, NY: Threshold Editions, 2006), 17. Cited hereafter as LeGault, *Think*.

What Can Be Learned from the Past? Thinking Critically about Cuba

Examining past intelligence successes and failures in light of new developments provides a means to reassess what happened and how outcomes could have been different. The case of the Soviet missiles in Cuba in the summer and fall of 1962 provides a means of examining how critical thinking and structured methodologies could have made a difference.

Deploying the Missiles

During the summer of 1962, CIA analysts received a spate of potentially alarming reports about Russians being seen in Cuba. The reports, however, were only part of a stream of similar, "farfetched tales of African troops with rings in their noses, lurking Mongolians, and even Chinese troops" on the island.[38] Most or all of these reports were discounted by analysts who were inured to spurious reports of Soviet equipment secreted away in caves.[39]

James Hansen – who worked in both the Central Intelligence Agency (CIA) and Defense Intelligence Agency (DIA) – posits that the U.S. Intelligence and Policy Communities were the victims of a concerted Soviet campaign of denial and deception that masked the deployment of Soviet forces and missiles into Cuba.[40] The deception campaign even included "accurate information about the deployment [leaked] so as to mask it."[41] As Raymond Garthoff relates, "there were literally thousands of reports of missiles in Cuba in the period *before* any missiles were actually brought there."[42]

---

38 James H. Hansen, "Soviet Deception in the Cuban Missile Crisis," *Studies in Intelligence* 46, no. 1 (2002), 56. Cited hereafter as Hansen, "Soviet Deception."

39 Hansen, "Soviet Deception," 56.

40 Hansen, "Soviet Deception," 49–58.

41 Domingo Amuchastegui, "Cuban Intelligence and the October Crisis," in James G. Blight and David A. Welch, Eds., *Intelligence and the Cuban Missile Crisis* (London, UK: Frank Cass, 1998), 101.

42 Raymond L. Garthoff, "US Intelligence in the Cuban Missile Crisis," in

In fact, the Soviets were able to deploy more than the offensive nuclear missiles that became the centerpiece of the subsequent crisis with the United States. While U.S. analysts and policymakers knew of the conventional weapons, they were blind to the presence of SS-4 Medium Range Ballistic Missiles (MRBM) and SS-5 Intermediate Range Ballistic Missiles prior to the U-2 overflights of 14 October. Additionally, it seems they never discovered the presence of approximately 100 tactical nuclear weapons deployed on the island.[43] There is debate whether U.S. Intelligence also *underestimated* the number of Soviet troops deployed to Cuba. Garthoff reports that one CIA unit concluded there were between 45,000 and 50,000 Soviet troops in Cuba (the actual number was about 42,000) but the official estimate was between 4,500 and 5,000 prior to the crisis.[44]

The Soviets employed an elaborate campaign of denial and deception that took advantage of American points of view about the likelihood of Soviet weapons being located in Cuba. As Robert Jervis makes clear,

> the U.S. did not expect the Russians to put missiles into Cuba or Japan to attack Pearl Harbor because American officials knew that the U.S. would thwart these measures if they were taken. These judgments were correct, but because other countries saw the world and the U.S. less accurately, the American predictions were inaccurate.[45]

It could have been worse. As Gil Merom writes, the Soviets might

---

James G. Blight and David A. Welch, Eds., *Intelligence and the Cuban Missile Crisis* (London, UK: Frank Cass, 1998), 22. Emphasis in original. Cited hereafter as Garthoff, "US Intelligence."

43 Garthoff, "US Intelligence," 29.

44 Garthoff, "US Intelligence," 28, 58. U.S. Intelligence never did reach a correct conclusion. The closest they got was an estimate of 22,000 troops in early 1963 (Garthoff, "U.S. Intelligence," 28).

45 Robert Jervis, *System Effects: Complexity in Political and Social Life* (Princeton, NJ: Princeton University Press, 1997), 45. Jervis draws on the work of Klaus Knorr. See Klaus Knorr, "Failures in National Intelligence Estimates: The Case of the Cuban Missiles," *World Politics* 16 (April 1964): 455–67.

have *completed* the bases and "threatened major U.S. cities with extinction."[46] The threat is brought home by figure 5.

What caused U.S. analysts to get it wrong? Apparently the U.S. analysts concluded that because some of the HUMINT evidence was ludicrous, all of it was. This inductive conclusion then led them to discount further evidence. For example, having concluded that all the previously considered Cuban HUMINT was false, each new piece, *since it came from Cuba,* also had to be false. Thus, a false inductive conclusion led subsequently to false deductive conclusions.[47] It does not appear that abductive reasoning strategies were ever employed.

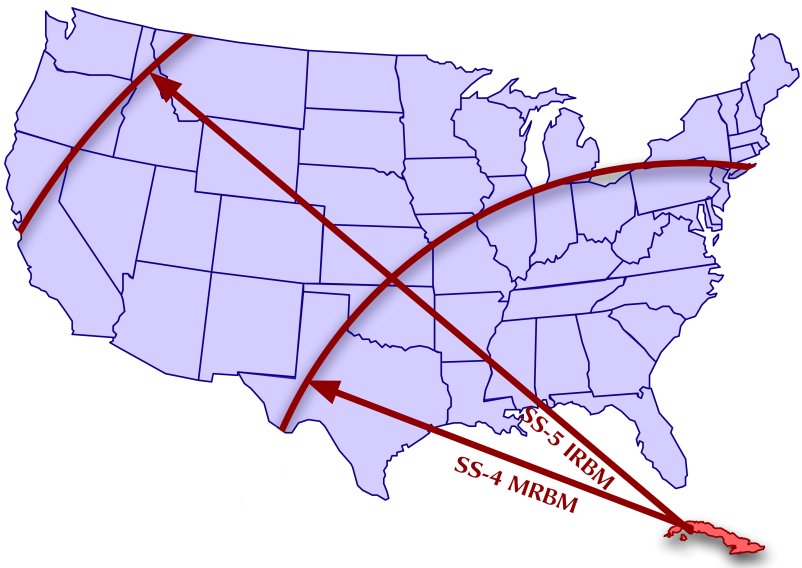


Figure 5: Respective Ranges of Soviet SS-4 MRBM and SS-5 IRBM Missiles

Source: Derived from Hansen, "Soviet Deception," 49.

46 Gil Merom, "The 1962 Cuban Intelligence Estimate: A Methodological Perspective," *Intelligence and National Security* 14, no. 3 (Autumn 1999), 49. Cited hereafter as Merom, "Estimate."

47 Inductive and deductive reasoning were illustrated in figure 1.

It should be noted that the U.S. Intelligence Community was not blind to the possibility that the Soviets might conduct a military buildup in Cuba. In fact, there were two theories being debated: One, that the Soviets would emplace *defensive* weapons, and the other that they would emplace *offensive* weapons. Senior analysts in the Intelligence Community held the former theory while John McCone, then Director of Central Intelligence, favored the latter.

Part of McCone's reasoning had to do with the cost and utility of the installation of SA-2 air defense missiles. McCone apparently reasoned that the purpose of installing such expensive missiles had to be greater than merely denying the United States overflight capabilities (the SA-2 could shoot down – as Francis Gary Powers discovered – a U-2).[48] This led McCone to come "up with an answer that no one wanted to hear: the SA-2s were on the island to deny the United States the capability to see the construction of offensive missile installations."[49]

Unfortunately, McCone was unable to dissuade the majority from their point of view. This may have stemmed, as James Blight and David Welch write, from the realization that while McCone's inference seemed reasonable when viewed in hindsight, in foresight it was faulty because it failed to sufficiently cover the alternatives.[50] Blight and Welch observe that

> the Soviets had also deployed SA-2 missiles to Egypt, Syria, and Indonesia, and in none of those cases had they also deployed strategic nuclear weapons. Indeed, the US intelligence community [sic] expected that the Soviet Union

48 Thomas R. Johnson and David A. Hatch, *NSA and the Cuban Missile Crisis* (Fort Meade, MD: National Security Agency Center for Cryptologic History, 1998), URL: <http://www.nsa.gov/publications/publi00033.cfm>, last accessed 18 April 2006. Cited hereafter as Johnson and Hatch, *NSA*.

49 Johnson and Hatch, *NSA*.

50 James G. Blight and David A. Welch, Eds., *Intelligence and the Cuban Missile Crisis* (London, UK: Frank Cass, 1998), 5. Cited hereafter as Blight and Welch, Intelligence and the Cuban Missile Crisis.

would deploy SA-2 missiles to Cuba, precisely because it had done so elsewhere.[51]

Even though history proved McCone to be correct (for the wrong reasons), the defensive weapons theory predominated.[52]

The Soviets took advantage of the American beliefs and faulty reasoning. Capitalizing on the idea that it is easier to lead a target astray than to try to change his mind, they successfully placed the nuclear missiles in Cuba.[53] Heuer observes that

> [deceptions] that follow this principle seldom fail, for the odds are then strongly in favor of the deceiver. The human capacity to rationalize contradictory evidence is easily sufficient to outweigh the pernicious effects of security leaks and uncontrolled channels of information that planners of deception…might compromise their efforts.[54]

Assessing the Implications

Exactly what happened in the Cuban case and does it apply to contemporary issues? Roberta Wohlstetter notes in retrospect, "We would like to know not only how we felt, but what we did and what we might have done, and in particular what we knew or what we could have known."[55] Wohlstetter's musings lead to two key questions for analysts: How could this successful deception campaign have been

51 Blight and Welch, *Intelligence and the Cuban Missile Crisis*, 5.

52 Merom, "Estimate," 58.

53 Richards J. Heuer, Jr., "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly* 25, no. 2 (June 1981), 200. Cited hereafter as Heuer, "Strategic Deception." It is interesting to speculate whether the Soviets had a feedback channel that informed them of the predominant theory.

54 Heuer, "Strategic Deception," 200.

55 Roberta Wohlstetter, "Cuba and Pearl Harbor: Hindsight and Foresight," *Foreign Affairs* 46, no. 3 (July 1965), 691. Cited hereafter as Wohlstetter, "Cuba."

thwarted? What can be learned to advise analysts about current adversarial denial and deception?

Simply looking at additional evidence is sometimes promoted as a means of detecting denial and deception by adversaries. In the Cuban case, however, analysts had already processed a superabundance of evidence. Wohlstetter suggests that such riches can be "embarrassing."[56] This is because even as "signals" point

> to the action or to an adversary's intention to undertake it, "noise" or a background of irrelevant or inconsistent signals, [and] signs pointing in the wrong directions…tend always to obscure the signs pointing the right way.[57]

HUMINT assets overwhelmed analysts' abilities to distinguish signals from noise. Heuer and Hansen agree that once "locked in," analysts resist changing their minds. More evidence alone fails to change an analyst's mind because "[new] information is assimilated to existing images."[58] Yet, analysts stand to benefit from changing their opinion in the face of disconfirming evidence.

The limitations of hindsight analysis notwithstanding, if analysts had employed critical reasoning in 1962 they could have detected the Soviet *maskirovka* in Cuba. For example, by applying Paul and Elder's model of critical thinking, analysts would have had a means to question their assumptions and points of view, and subsequently might have questioned the purpose of the apparent "noise" they were discounting as well as their assumptions about the prevalent point of view that the Soviets would not place missiles on the island because we would react. Gil Merom suggests that some appropriate questions would have included: "How aware were the analysts of their own assumptions? Were these assumptions sensible and was it sensible to adhere to them?"[59] Other considerations that critical

56 Wohlstetter, "Cuba," 691.

57 Wohlstetter, "Cuba," 691.

58 Heuer, *Psychology,* 10–11.

59 Merom, "Estimate," 57.

thinking about the crisis might have raised are included in table 2. Applying Paul and Elder's model reveals other considerations that conceivably would have led to an earlier detection of the likelihood of the deployed weapons being *offensive.*

Would this approach have allowed detection of what the Soviets were doing in Cuba before mid-October 1962? One could argue counterfactually that it might have enhanced analysis of collection from other sources.[60] SIGINT assets capable of collecting Russian communications were in place near the island.[61] Imagery assets might have been tasked differently prior to 14 October. Sources less subject to generating noise would have introduced inconsistencies to an analysis of competing hypotheses that was solely HUMINT-based.

Between Dogmatism and Refutation

A systematic approach to directed collection also would have moved analysts toward a disconfirmatory analytic approach. By contrast, a confirmatory approach, often characterized as confirmation bias, leads analysts to accept what they set out to confirm.[62] A disconfirmatory approach aims to refute alternative

---

60 Counterfactual reasoning explores differing outcomes arising from alternative causes. Counterfactuals are commonly used in whenever alternate hypotheses are explored. They are essential for both post-mortem reviews and futures scenario exercises. See Philip E. Tetlock, and Aaron Belkin, *Counterfactual Thought Experiments in World Politics: Logical, Methodological, and Psychological Perspectives* (Princeton, NJ: Princeton University Press, 1996), 1–38. In the same volume, Richard Ned Lebow and Janice Gross Stein conduct a counterfactual review of the Cuban missile crisis. See Richard Ned Lebow, and Janice Gross Stein, "Back to the Past: Counterfactuals and the Cuban Missile Crisis," in Philip E. Tetlock, and Aaron Belkin, *Counterfactual Thought Experiments in World Politics: Logical, Methodological, and Psychological Perspectives* (Princeton, NJ: Princeton University Press, 1996), 119–148.

61 Johnson and Hatch, *NSA*. According to the authors, SIGINT played a key role in determining the operational status of the SA-2 air defense missiles. However, SIGINT failed to detect the delivery and installation of the nuclear missiles.

62 Wikipedia defines confirmation bias as "a type of cognitive bias toward confirmation of the hypothesis under study." (Wikipedia, entry under "confirmation bias").

Purpose	· Determine what is going on in Cuba as a part of the U.S. "war" against Castro and the Cuban communists.
Key Questions	· If this really is a Soviet military buildup, what kinds of weapons are being deployed: offensive weapons or defensive weapons? · Why is an expensive missile system like the SA–2 being installed in Cuba? · What is the SA–2 really protecting? · Does a crisis exist?
Evidentiary Considerations	· If defensive weapons are being deployed, what evidence should be observed? · If offensive weapons are being deployed, what evidence should be observed? · What is not being seen?
Inferences	· What is inferred from the observed and collected evidence?
Assumptions	· What is being assumed about the evidence? · What is being assumed about the sources of the evidence? · What is being assumed about why the Soviets would deploy weapons to Cuba?
Concepts	· How does human perception affect the analysis? · How reliable are the sources of evidence? (Could also be an assumption.)
Implications and Consequences	· If conclusions are incorrect about the Soviet build up, what might occur next? · If conclusions are correct about the Soviet build up, what can be expected? · If conclusions are incorrect about offensive weapons being deployed, what happens next? · If conclusions are incorrect about defensive weapons being deployed, what happens next?
Points of View	· What other points of view about what is going on in Cuba exist?

Table 2: Applying Paul and Elder's Critical Thinking Model to the Situation in Cuba, August–September 1962.

Source: Developed by author.

hypotheses. Whatever was left at the end of the process would be the most likely explanation. Would this guarantee a correct "answer"? Ben-Israel concludes that although the answer has to be "no," the approach does allow for narrowing "the margin of error."[63] It does so by moving the analyst away from a "pole of dogmatic tenacity" toward a "pole of refutation" (summarized in figure 6).[64]

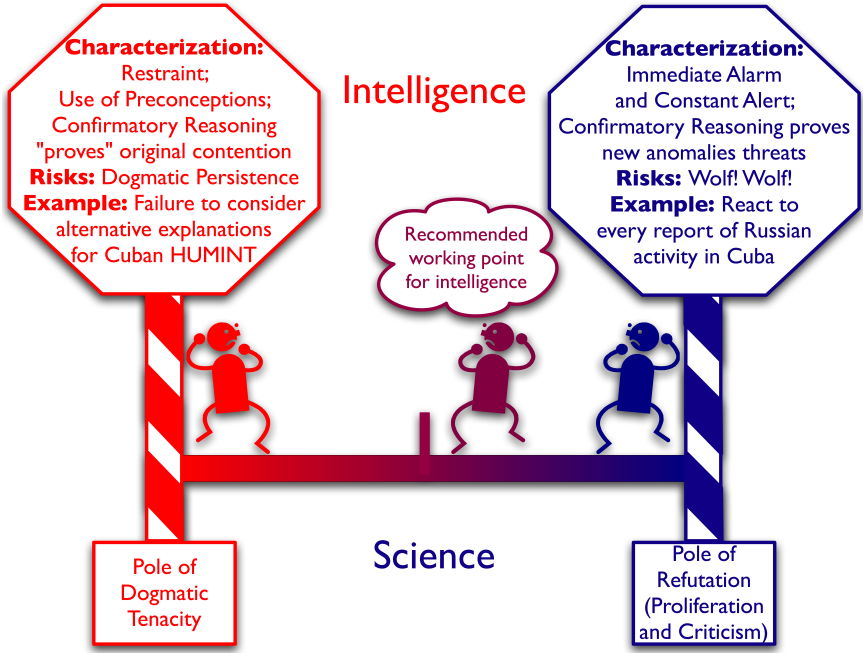


Figure 6: A Place for Analysis between Dogmatism and Criticism

Source: Derived from Ben-Israel, "Methodology of Intelligence," 679.

It should be noted that operating too closely to a pole of refutation can also create problems. For example, analysts might be unable to distinguish between real threats and false positives; they might react to each one regardless of its validity. In the Cuban case, this problem would have manifested itself in goading continual U.S. military reactions to every perceived Soviet and Cuban threat. Here again,

63 Ben-Israel, "Logic of the Estimate Process," 679

64 Ben-Israel, "Logic of the Estimate Process," 691.

critical thinking could moderate this Cassandrian approach.[65] The questioning of assumptions and points of view in critical thinking allows analysts to *discount* certain evidence. Based on his own Israeli intelligence analyst experiences, Ben-Israel asserts that anchoring oneself some distance from a pole of refutation, and not far from the center, is probably best.[66] In other words, enlightened skepticism probably works as a method for distinguishing between real and perceived threats. Critical thinking leads one to assess the processes one is using and the point on the continuum from which to work.

Lacking: Disconfirmation

Merom confirms that a disconfirmatory process did not occur on the Cuban missile problem: "Information that was inconsistent with the prevailing conservative theory was not considered as alarming and necessitating revision, but rather was 'rehabilitated' and rendered 'harmless' on the basis of *ad hoc* statements."[67] Instead, inductive reasoning generally led analysts to "prove" their theory and subsequently to adhere to it "*until it was proven wrong* by conclusive hard evidence" – the U–2 photos, to be exact (of which a detail is reproduced in figure 7).[68]

---

65 Cassandra was the daughter of Priam, King of Troy. She was blessed and cursed by the god Apollo to accurately predict the future yet never be believed. In intelligence, a Cassandrian approach is characterized as one that emphasizes dire outcomes and worst–case scenarios. Analysts who produce such assessments are often discounted and rarely thanked when they are correct. For a real account of how such warnings are perceived (at least at the time they are made), see Charles E. Allen, "Intelligence: Cult, Craft, or Business?" in *Seminar on Intelligence, Command, and Control, Guest Presentations,* Spring 2000 (Cambridge, MA: Harvard University Program on Information Resources Policy, I–01–1, April 2000), URL: <http://www.pirp.harvard.edu/pubs.html>, last accessed 11 January 2006.

66 Ben-Israel, "Logic of the Estimate Process," 679.

67 Merom, "Estimate," 69.

68 Merom, "Estimate," 69. Italics in original.

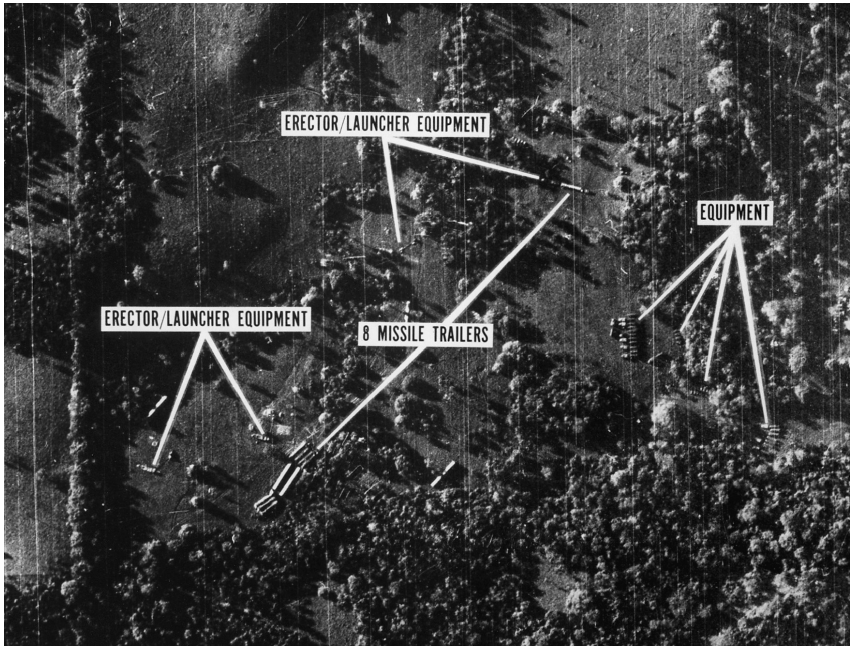


Figure 7: Detail of a U-2 Photograph of an SS-4 MRBM Launch Site, San Cristobal, Cuba, 14 October 1962. This evidence confirmed that Soviet missiles were being installed in Cuba.

Source: U.S. Department of Defense, photograph in the John Fitzgerald Kennedy Library, Boston, MA, PX 66–20:7 14 October 1962.

What tipped off the overhead surveillance were two HUMINT reports of "a Soviet truck convoy that appeared to be towing ballistic missiles toward the San Cristobal area."[69] That these reports were taken seriously is one of the curious serendipities that occur from time to time in intelligence analysis (and other research-based domains). What prompted the CIA and DIA analysts to take these reports seriously while earlier accounts had been dismissed remains a mystery. Garthoff asserts that it was new information taken in context with the observed "pattern of SA-2 surface-to-air missile sites in Western

69 Graham Allison and Philip Zelikow, *Essence of Decision: Explaining the Cuban Missile Crisis,* 2nd Edition (New York, NY: Longman, 1999), 220. Cited hereafter as Allison and Zelikow, *Essence of Decision.* Raymond Garthoff also notes this to be the case. See Garthoff, "US Intelligence," 23.

Cuba" that led to the tasking of the U-2 flight on 14 October (the track of which is shown in figure 8).[70]

Also contributing to the determination that the deployed missiles were SS-4 MRBMs was information transmitted to the British and American intelligence services by Oleg Penkovsky. While Penkovsky's espionage apparently did not warn the Americans that the Soviets were about to deploy offensive missiles in Cuba, he is credited with – among other things – providing technical information about the missiles.[71] Len Scott observes that Penkovsky provided the technical information that allowed the determination that the missiles were SS-4s instead of SS-3s, as well as information that allowed accurate assessment by the Americans of their readiness. Scott writes that this was important because

> the SS-3 had a range which US intelligence estimated at 630 nautical miles (nm), enabling coverage of seven Strategic Air Command (SAC) bomber/tanker bases; the 1020nm SS-4 could target 18 bomber/tanker bases (plus one ICBM complex), and some 58 cities with a population of over 100,000, including Washington, accounting for 92 million people.[72]

Shortly thereafter Penkovsky was detected, arrested, tried, and executed by the Soviets for his espionage.

---

70 Garthoff, "US Intelligence," 23.

71 Len Scott, "Espionage and the Cold War: Oleg Penkovsky and the Cuban Missile Crisis," *Intelligence and National Security* 14, no. 3 (Autumn 1999), 33. Cited hereafter as Scott, "Penkovsky."

72 Scott, "Penkovsky," 34. In making this assertion Scott draws on work previously published by Allison and Zelikow in *Essence of Decision* and by Mary S. McAuliffe, ed., *CIA Documents on the Cuban Missile Crisis, 1962* (Washington DC: Central Intelligence Agency, 1992).

Figure 8: U–2 Tracks over Cuba, 4–14 October 1962.

Sources: Map, Central Intelligence Agency. Tracks derived from a map in Mary S. McAuliffe, ed., *CIA Documents on the Cuban Missile Crisis, 1962* (Washington DC: Central Intelligence Agency, 1992), 3. Hereafter McAuliffe. Missile locations derived from Arthur C. Lundahl, "Additional Information – Mission 3102," Memorandum for Director of Central Intelligence and Director, Defense Intelligence Agency, 15 October 1962, in McAuliffe, 181–182; and Arthur C. Lundahl, "Additional Information – Mission 3107," Memorandum for Director of Central Intelligence and Director, Defense Intelligence Agency, 19 October 1962, in McAuliffe, 209. Track and missile locations are approximations. Lundahl was the Director, National Photographic Interpretation Center. The 19 October memo reports that a 5 September U–2 overflight did not detect the latter two missile sites. However, a review of the 5 September track (as presented in McAuliffe) shows the aircraft only came near the Sagua La Grande site. It should also be noted that the track of the U-2 – as flown on 14 October – deviated from the original planned route (which was farther to the west). The track as flown took the aircraft closer to the San Cristobal site. What might have happened had the original track been flown?

Despite their efforts at denial and deception, there was an evident lack of concealment of the missiles by the Soviets prior to their "discovery" on 14 October. General Anatoli Gribkov, a member of the Soviet General Staff in Cuba at the time relates,

> A missile–launching complex is not easily disguised…[Such] an installation…could be hidden from ground-level view. But from above, however, it could and did stick out like a sore thumb.[73]

Allison and Zelikow note that the Soviets only began to camouflage the sites *after* "the U.S. announced the discovery of the missiles and announced the blockade."[74] They conclude that the Soviet forces building the bases lacked personnel and resources to conceal them – a situation that apparently changed only after the missiles had been discovered.[75]

The Roles of Critical Thinking in the Cuban Crisis

Merom's critique of the Intelligence Community's estimate of Soviet intentions vis-à-vis Soviet weapons in Cuba reveals areas that would be well-served by critical thinking. First, when a critical thinking paradigm is in control, intelligence foraging and gathering are efficiently oriented. Questions are raised about the existing evidence – both anomalous and consistent – as well as where new disconfirming and confirming evidence might be discovered. Second, alternative – what in the context of Cuba, Merom calls *revolutionary* – theories are considered.[76] A structured process also speeds up the process of analytic sensemaking: estimates are crafted earlier.[77] Third, a methodological process opens analysis to "guiding principles of

---

73 Anatoli Gribkov, "The View from Moscow and Havana," in Anatoli Gribkov and William Y. Smith, *Operation ANADYR: U.S. and Soviet Generals Recount the Cuban Missile Crisis* (Chicago, IL: Edition Q, 1994), 39. Cited hereafter as Gribkov, "The View."

74 Allison and Zelikow, *Essence of Decision*, 208.

75 Allison and Zelikow, *Essence of Decision,* 214.

76 Merom, "Estimate," 71.

77 Structured processes provide a framework that reduces the flailing around as analysts seek to find a starting point for their analyses. Morgan Jones discusses this at some length. See Jones, *Thinker's Toolkit,* xi–xvi.

research," enriching both the process and the results.[78]

However, there are dangers to such a paradigm, especially as "science" commonly is understood. As Jeffrey Cooper notes, "a 'science of analysis' is a conceit, partly engendered by Sherman Kent's dominating view of intelligence as a counterpart of the scientific method."[79] Mark and Barbara Stefik argue that "the working methods of science and invention leaves [sic] out imagination. This makes it both boring and misleading."[80] Analysts must focus on both evidence and inferences; otherwise they can "get the details right at the cost of ignoring important inferential judgments that need to be conveyed in order to provide a true sense of the uncertainties of both evidence and judgment."[81] Here again, critical thinking, with its emphasis on creative questioning, moderates the process. Such questioning opens the way for imaginative thinking. "[Intuition], curiosity, and a thirst for discovery – all essential elements of good science" could have alerted analysts working in 1962 (or at any other time) to the possibility that they were being denied or deceived.[82]

An interesting intersection exists between critical thinking and analogy, or drawing comparisons to derive new patterns and explanations. This intersection lies at the heart of creativity.[83] According to Keith Holyoak and Paul Thagard, there are commonly four steps to analogical problem solving:

> Often a problem solver will select a source analog by retrieving information about it from memory (*selection*), map the source to the target and thereby generate inferences about the target

78 Merom, "Estimate," 57.

79 Cooper, Pathologies, 26..

80 Mark Stefik, and Barbara Stefik, *Breakthrough: Stories and Strategies of Radical Innovation* (Cambridge, MA: MIT Press, 2004), 110.

81 Cooper, *Pathologies,* 27.

82 Cooper, *Pathologies,* 31.

83 This statement illustrates just how pervasive and powerful the use of analogy is in human reasoning and discourse. Taken literally, creativity has no heart (nor any other organs) since it is a notion or a concept, not a living animal. Yet the analogy to a living being aids understanding.

(*mapping*), evaluate and adapt the inferences to take account of unique aspects of the target (*evaluation*), and finally learn something more general from the success or failure of the analogy (*learning*).[84]

Since analogy is such a powerful element in human reasoning, how can critical thinking outwit or control it? As developed in this paper, it does so by imposing a structure on the thinking. By examining inferences and implications as well as alternative points of view, critical thinking calls into question the appropriateness of the analogies in use. Recent work by Paul and Elder reveals how this works. They request, for example, that reasoners state and restate explanations, add examples, and then include an analogy.[85] While initial statements about a phenomenon *do not* imply understanding, restatement, examples, and analogies *do* and further, provide measures by which comprehension can be fixed and assessed; they make knowledge explicit – something that can be thought about.[86] When knowledge and reasoning are explicit, assumptions are revealed.

According to Richard Neustadt and Ernest May, it is known that analogy is a tool commonly invoked by policymakers.[87] Critically thinking analysts can add substantively to the policymakers' options by constructively challenging the tendency to rely upon analogy as a way of addressing situations. For example, Neustadt and May observe that in coping with the missile crisis in Cuba, President Kennedy and his advisers relied on – among other things – an analogy to Pearl Harbor to justify why a "surprise" bombing of the Soviet missile

84 Keith J. Holyoak and Paul Thagard, *Mental Leaps: Analogy in Creative Thought* (Cambridge, MA: The MIT Press, 1995), 15. Emphasis in original. Cited hereafter as Holyoak and Thagard, *Mental Leaps.*

85 Richard Paul and Linda Elder, "Instructions to Participants," 25th Annual Conference on Critical Thinking, Berkeley, California, 9 July 2005. The first three elements were developed previously; analogy was new in 2005.

86 Holyoak and Thagard, *Mental Leaps, 20–22.*

87 Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* (New York, NY: The Free Press, 1986). Cited hereafter as Neustadt and May, *Thinking in Time.*

bases was *not* a satisfactory option.[88] Kennedy's advisers, acting as analysts of the situation, critically evaluated the appropriateness of the analogy, pointing out its weaknesses and strengths. Kennedy concluded that sneak attacks were not a tactic lying within the U.S. tradition.[89]

In the Cuban case, getting analysts to restate their conclusions, provide examples, and make analogies would have revealed the strengths and weaknesses of their arguments about what they observed from the HUMINT sources. It would have shown their comprehension of what they wanted to conclude, revealed their assumptions and, in so doing, opened an avenue for "alternative" assessments of the issue. It would have done so by causing the analysts to question how it was that they failed to notice or ignore things.[90] The stage would have been set for an earlier, less risky, defusing of the impending crisis.

Another analogy employed in the Cuban missile crisis was the comparison to the Soviet position vis-à-vis the presence of *American* MRBMs in Turkey. A critical review reveals that the Soviet Union had tolerated the presence of these missiles – which had a longer range than those placed in Cuba – since 1957.[91] If the U.S. demanded the removal of the Soviet missiles from Cuba, was not a similar withdrawal of the American missiles from Turkey appropriate? Ultimately, this analogy provided a face-saving solution for the Soviet Union in the negotiations that followed. As a "secret" part of the agreement, the American Jupiter MRBMs were removed from Turkey five months after the Soviet Union removed its missiles from Cuba.[92]

---

88 Neustadt and May, *Thinking in Time,* 6.

89 Neustadt and May, *Thinking in Time,* 7.

90 Margaret A. Boden, *The Creative Mind: Myths and Mechanisms* (New York, NY: Basic Books, 1990), *25.*

91 Neustadt and May, *Thinking in Time,* 9.

92 Neustadt and May, *Thinking in Time,* 15.

Winners and Losers: The Crisis in Context

A Critical Assessment of the Leaders. In any confrontation there are winners and there are losers. Thinking critically about the confrontation over the Soviet missiles also involves determining who actually won as well as what the other outcomes might have been. Each of the three actors, Castro, Khrushchev, and Kennedy, had a number of interests at stake. In a number of circumstances each stood to gain at the expense of the others. What solutions were the most advantageous to each of the three actors? What were the motivating factors? A speculative – and admittedly simplified – critical comparison, again using Paul and Elder's model (summarized in table 3) illustrates how critical thinking also reveals much about who stood to gain and who stood to lose in the crisis.

Castro. Castro found his country under attack from the United States – both directly through economic sanctions and indirectly by Batista loyalists living in Florida.[93] The previous year the United States had launched an invasion attempt at the Bay of Pigs – which was repulsed. However the attempts by the United States to destabilize or overthrow the Cuban government did not end with their defeat. As Raymond Garthoff observes, "by the spring of 1962 the United States had embarked on a concerted campaign of overt and covert political, economic, psychological, and clandestine operations to weaken the Castro regime…including attempts to assassinate Castro."[94] In short, the United States was doing everything *except* conventional warfare to destroy Castro and his regime.

Castro's point of view was that the United States was a real enemy. He could reasonably assume that in light of its other activities and having attempted an invasion once, the United States would repeat its actions and this time *might* succeed (an implication). Another possible outcome that probably was considered was that war, conventional or nuclear, was likely. Castro must have possessed evidence of the military capabilities of the United States and probably inferred that

93 Raymond L. Garthoff, *Reflections on the Cuban Missile Crisis* (Washington, DC: The Brookings Institution, 1989), 7. Cited hereafter as Garthoff, *Reflections.*

94 Garthoff, *Reflections,* 9.

Element of Thinking	Considerations as seen from Castro's Point of View
Purpose	· Preserve Regime
Point of View	· United States threatens regime
Assumptions	· A second invasion will be attempted
Implications	· Invasion might succeed · War: conventional or nuclear
Evidence	· U.S. armed forces formidable
Inferences	· U.S. can overcome unaided Cuban forces.
Concepts	· Military strategy and doctrine, communist and capitalist theories
Key Questions	· How to deter United States from invading island

Table 3: A Comparative Assessment of Rival Motivations

Source: Developed by author.

Considerations	
as seen from Khrushchev's Point of View	as seen from Kennedy's Point of View
· Protect Cuba from United States · Force concessions from United States · Remove U.S. and NATO from Berlin · Spread Communism · Preserve Regime	· Get the missiles out of Cuba · Defend U.S. and allies against Communism · Preserve Regime
· United States a threat to Communism · Cuba threatened with invasion	· Communism threatens United States · Missiles are a threat
· Missiles in Cuba bargaining points · Missiles in Cuba protect Castro · Effort will be successful.	· Small Soviet Force · Strategy of removal is possible
· U.S. concessions ·War: conventional or nuclear	· Successful removal · Escalation of measures ·War: conventional or nuclear
· U.S. armed forces formidable	·Administration politically vulnerable over crisis · Khrushchev is a formidable adversary · Khrushchev is bluffing
· U.S. can overcome unaided Cuban forces. · Missiles provide necessary aid · United States will concede.	· Khrushchev will back down · Military option not required
· Military strategy and doctrine, communist and capitalist theories	· Military strategy and doctrine, communist and capitalist theories · Monroe Doctrine
· How to deter United States from invading Cuba · How to dominate the United States	· How to get the Soviets and their missiles off of Cuba

unaided, his own forces were no match for the U.S. forces. Underlying Castro's considerations were a number of ideas about military strategy and doctrine, as well as communist and capitalist theories. A corollary consideration commonly believed by many Americans (at the time and still today) might have been how Communism could have been spread across the Western Hemisphere, especially the United States. Castro's key question was, "How can I prevent the United States from invading again?"

Khrushchev. What motivated Khrushchev remains controversial. His motives certainly were more complex, as various explanatory hypotheses reflect. First, there is the argument that Khrushchev had an ally "in the faith" to protect. He too believed that the United States would invade Cuba a second time.[95] However, as Allison and Zelikow counsel, the troop buildup itself and *not* the nuclear missiles was what Khrushchev did to offset the perceived threat to Cuba from the United States.[96] The deployment of the nuclear missiles was related to some other issue.

Next, the situation posed an opportunity to force concessions from the United States – perhaps about Berlin, or the United States' own offensive missiles located in Europe and Turkey. Allison and Zelikow find sufficient evidence to lead them to believe that removing the U.S. and NATO troops from Berlin was a key factor motivating Khrushchev to deploy the missiles to Cuba.[97] Securing his borders from the American's Jupiter missiles may have been an additional motivating factor.

Additionally, there was Khrushchev's avowed purpose of spreading Communism across the globe. In this context the deployment of weapons lies within the context of "a great power rivalry… between the U.S. and the values and interests it represented…and

95 James J. Wirtz, "Organizing for Crisis Intelligence: Lessons form the Cuban Missile Crisis," in Blight and Welch, *Intelligence and the Cuban Missile Crisis,* 130. Cited hereafter as Wirtz, "Organizing."

96 Allison and Zelikow, *Essence of Decision*, 87.

97 Allison and Zelikow, *Essence of Decision*, 99–109.

the Soviet Union's communist agenda."[98] At a reception for foreign ambassadors in Moscow in 1956, Khrushchev threatened, "Whether you like it or not, history is on our side. We [the communists] will bury you!"[99] This remark (among others) also reveals an additional purpose: Khrushchev, like all dictators, had to appear stronger than his adversaries – his political survival depended on it.

Khrushchev's point of view was that the United States (and its allies) were a threat to Communism everywhere and needed to be contained. He was presented with a confluence of opportunities and responded with the military buildup in Cuba and the deployment of the missiles. He apparently assumed that if he could get nuclear missiles into Cuba he'd have bargaining points useful in such a containment strategy. Later, Khrushchev believed he could effect a change in the balance of power between the two nations.[100] Possible outcomes included the prospect of further U.S. concessions, protection of Cuba from invasion, and either conventional or nuclear war.

Khrushchev had direct evidence drawn from the Korean War and possibly other evidence from spies operating in the United States about the capability of the U.S. military. Given the nuclear missiles he actually deployed as well as his assignment (temporary) of operational control of those missiles to the Soviet Group of Forces commander, General Issa Pliyev, Khrushchev seems to have inferred the U.S. forces were formidable.[101] He also apparently concluded that the missiles – and the other forces – would be adequate to the task of successfully satisfying his purposes; the United States, faced with

98 Allison and Zelikow, *Essence of Decision*, 88.

99 Nikita Khrushchev, "Speech to Ambassadors at Reception, 17 November 1956," in James Beasley Simpson, compiler, *Simpson's Contemporary Quotations: The most Notable Quotes since 1950* (Boston, MA: Houghton Mifflin Company, 1988), online edition, URL: <http://www.bartleby.com/63/83/183.html>, last accessed 20 April 2006. Ironically, Khrushchev was wrong. History sided with his adversaries.

100 Cited in Garthoff, *Reflections,* 23.

100 Gribkov, "The View," 4. Control reverted back to Moscow in September.

operational missiles in Cuba, would concede.[102] The concepts on which Khrushchev relied probably were the same as those on which Castro relied: military strategy and doctrine as well as communist and capitalist theories. Again, Khrushchev's key question mirrored that of Castro: How to keep the Americans from invading Cuba. Additionally, there could have been a second question on how to dominate, or at least gain concessions from, the United States.

Kennedy. Finally, there was Kennedy. While Kennedy's exact purpose vis-à-vis Cuba *prior* to the discovery of the missiles also remains unclear, it is known that he did not plan to invade the island during the summer and fall of 1962.[103] However, 1962 was an election year and the Kennedy administration was vulnerable with respect to Cuba.[104] Kennedy could not afford to appear soft on Communism. Kennedy also had an interest in keeping the U.S. and NATO forces in Berlin.

All this changed once the missiles were discovered. Kennedy's deliberations revolved around removing the missiles as expeditiously as possible. He no doubt realized that if his administration bungled the crisis they might lose at the polls in November.[105] Therefore, it is reasonable to conclude that Kennedy's goals included retaining control of Congress – he too had a regime to preserve. Kennedy's point of view was clear: the deployed Soviet strategic nuclear missiles were a threat to the United States and must be removed. He assumed that such a strategy could be developed. He apparently also assumed that the Soviets had placed a *small* force on the island. Possible outcomes included successful removal of the missiles and their

---

102 Wirtz, "Organizing," 128. Wirtz argues that the Soviets were not only wrong about the U.S. reaction, they were *surprised!*

103 Wirtz, "Organizing," 130.

104 Fen Osler Hampson, "The Divided Decision-Maker: American Domestic Politics and the Cuban Crises," *International Security* 9, no 3 (Winter 1984/85), 136. Cited hereafter as Hampson, "Divided."

105 Hampson, "Divided," 143.

supporting forces, an escalation of measures to prompt that removal, and the possibility of conventional or nuclear war.[106]

Kennedy had evidence of his political vulnerability He also had evidence – Khrushchev's own actions included – that the Soviet leader was a formidable adversary. But based on Penkovsky's evidence he inferred that Khrushchev might be persuaded to back down. As Scott concludes, "various writers contend that Penkovsky's intelligence…[guided] Kennedy's handling of the crisis from a position of strength."[107] This occurred in part because "the KGB's discovery of Penkovsky's espionage alerted Khrushchev to the fact that Kennedy now knew he was bluffing."[108] As has been noted, Kennedy lacked accurate evidence about what was really on the island. Nevertheless as has been noted, he inferred that military strikes were not – at least at that time – an option. Kennedy probably relied on the same concepts on which Castro and Khrushchev relied. In addition, the concepts embodied in the Monroe Doctrine were also probably a factor. Kennedy's key question was, "How to get the Soviets and their missiles out of Cuba?"

Foresight. Viewed with foresight, there were a number of possible outcomes to the crisis based on the inferrable goals that could be associated with any of the three leaders. A win for one of the leaders was not necessarily a loss for the others as table 4 shows. In some cases, achieving one's goal was a win for the leader, but a failure to achieve it was *not* necessarily a loss. "Winning" the crisis should have involved attaining all or most of one's goals. However, since not all goals were of equal importance, failing to achieve one could mean that one lost in the larger crisis. Similarly, achieving one's goals did not guarantee winning the larger crisis. This becomes evident as the actual winners and losers are considered.

---

106 Neustadt and May, *Thinking in Time*, 6-15. Given the presence of the Soviet tactical nuclear weapons on Cuba it is probable that *any* invasion that began with conventional forces would have escalated to nuclear scenarios.

107 Scott, "Penkovsky," 31.

108 Scott, "Penkovsky," 32.

And the Winner is? Who actually won the Missile Crisis? Critical assessments of the three leaders involved and the attainment of their goals reveals the answers. First, Castro certainly got what he wanted: The United States never again invaded Cuba.

What did Khrushchev get out of the resolution of the crisis? From the standpoint of his first goal, to protect Cuba from the United States, he was successful. The subsequent removal of the Jupiter

Goal	Outcome	Leader		
		Castro	Khrushchev	Kennedy
Prevent U.S. Invasion of Cuba	Achieve	Win	Win	Neutral
	Fail	Lose	Lose	Win
Get the Missiles out of Cuba	Achieve	Neutral	Lose	Win
	Fail	Win	Win	Lose
Spread Communism	Achieve	Win	Win	Lose
	Fail	Neutral	Lose	Win
Get U.S. and Allies out of Berlin	Achieve	Neutral	Win	Lose
	Fail	Neutral	Lose	Win
Force Concessions from United States	Achieve	Win	Win	Lose
	Fail	Lose	Lose	Win
Force Concessions from Soviet Union	Achieve	Neutral	Lose	Win
	Fail	Neutral	Win	Lose
Force Concessions from Cuba	Achieve	Lose	Neutral	Win
	Fail	Win	Win	Neutral
Preserve Regime	Achieve	Win	Win	Win
	Fail	Lose	Lose	Lose

Table 4: Goals and Outcomes in the Cuban Missile Crisis

Source: Developed by author.

missiles in Turkey appeared to increase the security of his borders – an apparent concession from the United States.[109] However, Khrushchev failed to spread Communism further. And Berlin remained partially

109 The issue of the Jupiter missiles is complex. They were not included in the formal agreement but were offered up in a secret unilateral assurance from Kennedy (Garthoff, *Reflections,* 132).

in the hands of the West. If, as Allison and Zelikow postulate, this was the real motivation behind the nuclear deployment then Khrushchev's failure was highly significant. Additionally, his regime was embarrassed by the revelation in the United Nations of the presence of the missiles. Ultimately, he was removed from power two years later and placed under house arrest until his death in 1971. So, Khrushchev, while he won a number of his goals, wound up the overall loser.

Kennedy is the other winner in the crisis. He gets the Soviets missiles removed from Cuba while avoiding war. He is later able to retire an obsolete missile system (the Jupiters). He prevents the Soviet Union from seizing control of Berlin. Finally, his popularity increases and the Democrats retained power in the 1962 elections.

Ten Years Later, They Meet Again

It is worth noting that Soviet denial and deception in support of military deployments and operations in Cuba did not end in the early winter of 1962. In 1970 Henry Kissinger stormed into the office of H. R. Haldeman and demanded to see President Nixon. Aerial reconnaissance had brought news. "The Cubans are building soccer fields," Kissinger said. "Cubans play *baseball*. *Russians* play soccer."[110] The Soviets it seems had been discovered building a submarine base at Cienfuegos. Prior to a particular overflight, that fact had been denied to the United States. The soccer fields were for the recreation of Soviet troops.

---

110 H.R. Haldeman, with Joseph DiMona, *The Ends of Power* (New York, NY: Times Books, 1978), 85–86, in Patrick J. Haney, "Soccer Fields and Submarines in Cuba: The Politics of Problem Definition," *Naval War College Review* L, no 4, sequence 360 (Autumn 1997), URL: <http://www.nwc.navy.mil/press/Review/1997/autumn/art5–a97.htm>, last accessed 6 April 2006. Emphasis in original.

Judgment: Critical Thinking Would Have Made a Difference

As this case study makes clear, there are a number of junctures where critical thinking or structured analytic methods could have made a difference in analyzing the Soviet missile deployment to Cuba. While it is true that Sherman Kent argued for a scientific approach to analysis, it does not seem to have been widely practiced at the time.[111] As of 1962, most studies that we now have in hand on human reasoning in intelligence had not been completed. The champions of structured intelligence analysis methods had not yet developed their techniques.

Nevertheless, a study of the crisis is germane because the same kinds of errors *repeat themselves again and again.* The errors seen in the Cuban case – failure to question assumptions, to take seriously the evidence and the patterns they imply, to counterfactually examine analytic implication and consequences, in short to make reflective judgments – also were cited by the Senate in its critique of the 2002 Iraqi WMD estimate.[112] In both cases, deceptions confounded analysts, leading them to wrong conclusions.[113] In the Cuban case the analysts eventually figured it out. This did not occur in the

---

111 Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, PA: Princeton University Press, 1949), 151–208.

112 In the Cuban situation, the debate between McCone and analysts over the nature of the weapons the Soviets might emplace came close to overcoming these errors. Regarding the Iraqi WMD estimate, the debate between the CIA and the Department of Energy over the use of the aluminum tubes also came close. Unfortunately, the incipient debate focused on the results, not the process. In both cases, the side that was eventually proved right failed to make the now-accepted case.

113 Sherman Kent challenged this assertion in his defense of the original estimate and the process by which it was created. He believed that an earlier revelation of the Soviet actions would have led to an intractable situation. However, an earlier revelation – say in August – would have offered President Kennedy and his advisers more options, particularly more *diplomatic* options. Kent also failed to observe that denial and deception occurred – at least for the record. See Sherman Kent, "A Crucial Estimate Relived," Reprint, *Studies in Intelligence* 36, no. 5 (1992): 111–119.

most recent failure. Critical thinking skills went unused among both generations of analysts.

How Can Intelligence Analysts Employ Critical Thinking?

The Poor Record

Critical thinking is what consumers of intelligence appear to expect when they task producers to examine issues. Corporate consumers require analysts creating intelligence to "[evaluate] a situation, problem, or argument and [choose] a path of investigation that leads to finding the best possible answers."[114] In the national security field, strategic intelligence pioneer Washington Platt notes that "[intelligence] is a meaningful statement derived from information which has been selected, evaluated, interpreted, and finally expressed so that its significance to a current national policy problem is clear."[115] Derived from strategic intelligence, "best answers" should clearly express what is significant to national policy problems. They may also support warfighters with essential operational and tactical intelligence. Critical thinking leads to the best answers for the specific context at hand.

Unfortunately, analysts' biases and mindsets repeatedly obscure best questions and answers. From well before the Japanese surprise attack on Pearl Harbor to the 2002 estimate on Iraqi weapons of mass destruction, a failure to think critically about potential crises contributed to repeated intelligence failures.[116] "Expert analysis"

---

114 Daniel Feldman, *Critical Thinking: Strategies for Decision Making* (Menlo Park, CA: Crisp Publications, Inc, 2002), 4.

115 Washington Platt, *Strategic Intelligence Production: Basic Principles* (New York, NY: Frederick A. Praeger, 1957), 8.

116 George S. Pettee, *The Future of American Secret Intelligence* (Washington, DC: Infantry Journal Press, 1946). Chapter 1 provides a summary of U.S. intelligence failures during the first half of the 20th Century. While hindsight is an imperfect mirror for reviewing the past, one conclusion to be drawn from a review of the evidence is that critical thinking could have minimized many of the ensuing crises.

was not enough.[117] Biases and mindsets too often converted subject-matter confidence into arrogance; false assumptions blinded analysts to their target's true intentions. For example, at least one CIA Iraq analyst acknowledged that the 1990 invasion of Kuwait,

> was an intelligence failure…We were guilty of a kind of mindset…The idea that a country [Iraq] would march up to the border, put 100,000 troops there, go in and do what they've done; I don't think anybody thought they'd do it.[118]

In 2002, Intelligence Community analysts failed to definitively assess whether the Iraqi government still possessed weapons of mass destruction. The Senate noted in its review of the failure that

> [rather] than thinking imaginatively, and considering seemingly unlikely and unpopular possibilities, the Intelligence Community instead found itself wedded to a set of assumptions about Iraq, focusing on intelligence reporting that appeared to confirm those assumptions.[119]

The mistakes of 2002 also occurred in 1990 – and for that matter in 1941. Analysts failed to question assumptions widely held at the time. Instead they chose the first answer that satisfied the situation, a phenomenon known as "satisficing."[120] Other means by which intelligence analysts and policymaking customers reasoned poorly are listed in table 5. According to Ephraim Kam, the problem is so great that the intelligence analysis process is "consistently biased, and…bias

---

117 Anthropologist Rob Johnston explores this paradox. See Dr. Rob Johnston, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study* (Washington, DC: Center for the Study of Intelligence, 2005), 64–66. Cited hereafter as Johnston, *Analytic Culture.*

118 Anonymous CIA Analyst, 1990, in Don Oberdorfer, "Missed Signals in the Middle East," *Washington Post Magazine*, 17 March 1991, 40.

119 The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *Report to the President of the United States,* March 31, 2005, URL: <http://www.wmd.gov/report/ index.html>, last accessed 28 July 2005, 155. Cited hereafter as WMD Commission, *Report.*

120 Morgan D. Jones, conversation with the author, 15 December 2003.

is the cornerstone of intelligence failures."[121] Paul and Elder claim that much thinking is "biased, distorted, partial, uninformed, or down-right [sic] prejudiced."[122] There are repeated failures to think critically; but could critical thinking about these situations prevent the failures?

Means by Which Decisions are Made
Select first answer that appears "good enough."
Focus on narrow range of alternatives, ignoring need for dramatic change from existing position.
Opt for answer that elicits the greatest agreement and support.
Choose the answer that appears most likely to avoid some previous error or duplicate a previous success.
Rely on a set of principles that distinguish "good" alternatives from "bad" alternatives.

Table 5: How Analysts Decide

Source: Excerpted from Alexander George, *Presidential Decisionmaking in Foreign Policy: The Effective Use of Information and Advice* (Boulder, CO: Westview Press, 1980), Chapter 2.

Critical thinking helps mitigate the effects of mindsets and biases by invoking skillful examination of evidence both for and against an issue, as well as consideration of obvious and less obvious alternative explanations. In the 1990 example, thinking critically would have raised other possible explanations for why Hussein's troops were on the Kuwaiti border and what he intended for them to do.[123] That the Iraqi troops were trained by the former Soviet Union and followed its tactics might have been an indicator of future intentions. In the case of the weapons of mass destruction (WMD), analysts might have

121 Ephraim Kam, Surprise Attack: The Victim's Perspective (Cambridge, MA: Harvard University Press, 1990), 85.

122 Paul and Elder, *Concepts and Tools,* 1.

123 A consideration of who trained Hussein's troops – in this case, the Soviet Union – might have led to an examination of military doctrine. Thus, it quickly would have become clear that troops mobilized on a border were going to cross that border. Analysts would then have known that an invasion of Kuwait was imminent.

asked, as they realized they had no new evidence of the weapons, "How can we prove that the weapons of mass destruction definitely are not there?" or "What would we expect to see if Saddam Hussein had gotten rid of his weapons of mass destruction?"[124]

We must assume that analysts can be encouraged to think in this manner. Modern strategic intelligence pioneer Sherman Kent believed this to be the case when he wrote nearly 60 years ago that intelligence analysts "are supposed to have had more training in the techniques of guarding against their own intellectual frailties" than the larger populace.[125]

Assessing Evidence[126]

Understanding how evidence is assessed is a necessary first step in understanding how analysts can better reason with and about it. The incomplete and ambiguous information and data with which intelligence professionals work compounds their reasoning process.[127] Sources are unreliable and contradictory; adversarial denial and deception increase doubt. When information and data are questionable, derived evidence is even more uncertain, and inferences arising from that evidence may be highly suspect. One way that analysts can reduce this uncertainty is by building defensible inferences

---

124 These analyses are those of the author. The last question was jointly arrived at in a conversation between the author and Mark Lowenthal, 26 July 2005.

125 Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton, NJ: Princeton University Press, 1949), 199.

126 This section is based (with additions) on materials developed by Francis J. Hughes and the author for a structured analytic methods course taught at the National Defense Intelligence College. For a deeper examination of evidence assessment see Francis J. Hughes and David A. Schum, *Credibility Assessment: A First Step in Intelligence Analysis,* unpublished tutorial, National Defense Intelligence College, April 2003.

127 Information, data, and evidence are different kinds of knowledge. Pieces of information comprise data, which in turn comprise evidence. Evidence is further distinguished from data by the fact that it contributes to discrimination among alternative end states. Data, while relevant, do not necessarily allow discrimination.

TESTIMONIAL: APPLYING CRITICAL THINKING

This is a true story. All the characters are real and really naive.

As a fresh graduate of NSA's critical thinking and structured analysis class, I attended an Intelligence Community class on counterintelligence. My fellow students included folks from all over the community, including CIA and FBI case officers. During the class, the instructor put forth a case study for students to think about and decide how best to "analyze and investigate" to find the mole. Differing opinions surfaced, but a common thread appeared among the case officers: follow your "gut" feeling and collect evidence to support that assumption, no matter how long it took.

The instructor, enjoying the collective mindset and the opportunity to shatter paradigms, concentrated on how information was collected and analyzed. Again, the case officers agreed the best solution was to continue gathering information until you "proved your case." I, the lone NSA token student, raised my objection, "How long is long enough? Until you've ruined the career of innocent, hardworking persons in the IC, or until you find another answer you like?" Although it did not earn me friends, it did open up a window to inform these case officers and other attendees about the intricacies of analysis.

Critical thinking is not just about putting information together, finding a pattern, then choosing an answer, it is about reducing bias, considering all options available, and presenting options to a decision–maker. And critical thinking is about paying attention to what and how you are doing it. I reasoned that, since the investigators in the case study concentrated on only one

Source: A mid–level intelligence professional at the National Security Agency

from the evidence. At their most basic level, these inferences depend on credibility (can it be believed), relevance (does the evidence bear on the issue), and inferential or probative force (how compelling is it in answering the questions raised by the issue). Unfortunately, no mass or body of evidence – in intelligence or anywhere else – comes with these three properties already established. Establishment of these properties to abet uncertainty reduction through inference occurs only through a process of argument, creative hypothesis generation, and the development of chains of reasoning.

Authenticity, accuracy, and reliability represent criteria for establishing the credibility of tangible evidence.[128] An analyst striving

128 "Tangible evidence" is a technical term describing *things* that bear relevance to an issue under scrutiny. It is contrasted with "testimonial evidence"

person, the analysis was faulty because somewhere along the line they limited their suspects (introduced bias) regardless of reason (access, family connections, angel–like qualities, etc.). Although it would take time, the investigators should conduct quantitative and qualitative analysis, make a decision tree (options open to a mole in a heavy security environment), and then play Devil's Advocate. In addition, analysis never reveals one "solution" or "smoking gun"; it leads to two or three "options" which can be investigated in detail.

The instructor, pleased that someone in the class knew what the "Analysis of Competing Hypotheses" was, revealed the answers of the real–life case study: after three years of investigating, the case officers had the wrong person due to incorrect information in old reports and limiting their suspect list. Instead of going back to the original source information, the officers read old reports that were unfortunately biased by Agency politics and external societal events (1950–60s). The real mole was discovered over a decade later; he was the son of a former Agency chief, well educated and well liked, but did not have access to the information. The individual "borrowed" interesting reports from friends who had access, covered his tracks, and continued spying against the U.S. for several years. Just as the authorities were about to arrest him, he was found dead in a hotel room from a reported suicide, but the cops could not figure out how he had two bullets in his chest and one in the back of his head. Miracle suicide.

What is the moral of the story? Conduct a thorough analysis right the first time and you can catch a mole anytime. I only hope the attending case officers got the message, especially from a non–gun toting NSA analyst.

who wishes to remain anonymous, email to the author, 9 March 2006.

to determine authenticity may ask, "Is the evidence what it seems to be?" In determining accuracy, the key question is whether the piece of evidence or the system that produced it has the resolution to reveal what the analyst believes the event or record should reveal. Assessing reliability involves determining whether different means of collection produce the same results.

If, on the other hand, the evidence is testimonial, different criteria apply. The first thing to be established is whether the source is being truthful. Truthfulness is not absolute. Rather, it is time- and context-dependent. A source may believe he is being truthful about an issue or may have legitimate reasons to be untruthful about that issue. In

– what people say about the issue.

another time and about another issue, these impediments to veracity may not exist for that source. Therefore, establishing the truthfulness of a source can pose a significant challenge to the analyst.

In an ideal situation, a review of evidentiary relevance causes an analyst to examine the likelihood of any potential answer to the problem or question – a hypothesis – with an eye to the modification of existing hypotheses or even the invention of new ones. In other words, an analyst might theorize that a certain bit of evidence will indicate that an individual or a group of individuals will engage in nefarious activity. Yet, if none of the evidence at hand bears on the issue, then the analyst may need to reconsider – or even reject – this evidence based on its lack of relevance. The analyst also should consider that the individual *may not* engage in the activity.

What is true about the future is also true about the present and the past. A lack of evidence relevant to an issue should prompt analysts to reassess their theories about the issue at hand. For example, an unnamed FBI investigator in the 2001 anthrax case noted, "[Reasoning] says that if you think a person is your guy, but you can't find anything to put him in the game, you've got to keep looking at others."[129] The failure of the FBI to implicate its principal suspect forced it to consider other explanations as to who sent the anthrax-laden letters in September 2001 to political leaders and media figures.

The analyst also is concerned with how strongly the evidence

129 Allan Lengel and Guy Gugliotta, "Md. Pond Produces No Anthrax Microbes: FBI Sought Clues In Deadly Attacks," *Washington Post*, 1 August 2003, A03. Cited hereafter as *Washington Post,* "No Anthrax." While this is a law-enforcement example, it illustrates good critical questioning about an apparent lack of evidence. Criminal investigation and intelligence analysis similarly assess events and evidence with the goal of description, explanation, and interpretation. The principal difference is that intelligence analysis endeavors to do so *before* the event occurs – in other words, *to estimate.* It is worth noting that over two years after the pond was drained the case remains unsolved; the individual under suspicion at the time was never charged with the crime. The FBI was unable to link the evidence to the individual. See for example, Allan Lengel, "Little Progress In FBI Probe of Anthrax Attacks: Internal Report Compiled As Agents Hope for a Break," *Washington Post,* 16 September 2005, A01.

undermines or supports the particular hypotheses under examination – the probative force of the evidence. Certain evidence, coming from certain kinds of sources, persuades more strongly than does other evidence drawn from other sources. Tangible evidence might have greater probative force than testimonial evidence. Consider, for example, a hypothetical biological weapons issue. Traces of certain toxic substances found near an alleged biological weapons lab carry greater probative force than the testimonial denials of the government of the country in which the lab and the samples were found.

The "ideal" analyst also assesses the objectivity, observational sensitivity, and competence of sources. One question suitable for this assessment is how biases may have corrupted a source's objectivity. Did the source see or hear the evidence directly, and under what conditions did this occur? A reality check also is made at this point. Does it makes sense that a particular source claims to have been in a position to make the observation or have access to the source of information?

Another consideration involves denial and deception. In assessing the evidence, the analyst should ask, "What is the likelihood that I am being deceived? This question is surprisingly difficult to answer accurately. Given that anchoring biases and confirmation heuristics cause analysts to find what they seek to find, a denial and deception hypothesis is often easily proved.[130] Critical thinking challenges this by forcing an examination of alternative points of view. For intelligence analysts, proactive, focused and surreptitious collection of information about the often minimal disconfirming evidence pays rich dividends.[131] In this case, the question becomes, "What is the likelihood that I am *not* being deceived?" Thus engaged, really good intelligence analysts create valuable knowledge.

---

130 Author's notes, National Defense Intelligence College, Denial and Deception Advanced Studies Program, Spring 2005. The author is a National Intelligence Council-sponsored participant in the Foreign Denial and Deception Committee's Denial and Deception Advanced Study Program at the NDIC.

131 Ben-Israel, "Logic of the Estimate Process," 708–709.

Facilitating Evidentiary Assessment

The questions that need to be asked about each piece of evidence are the same as those employed in critical thinking. In making her evaluation of what constitutes evidence, the analyst repeatedly asks "why": "Why do I believe this information is relevant to the question at hand (either against or for) and therefore exists as evidence?" "Why do I believe the source to be credible?" Additional questions about the analyst's own thinking processes might arise, such as: "What are my biases and why do they lead me to think this way?"

For example, in assessing the intentions of former Iraqi dictator Saddam Hussein in light of the U.S. destruction of his intelligence headquarters in 1993, an analyst might ask whether Hussein's declarations not to retaliate against the United States were credible. A corollary question might be, "What does Saddam Hussein gain by denial and deception?" Based on Hussein's statement, a determination that additional evidence was needed would stimulate collection of similar statements from other episodes. By analyzing what Hussein did in those instances, the analyst might determine that he was usually untruthful. Therefore, this piece of evidence would be deemed to be of low credibility despite its probative force, and relevance to the determination whether Hussein would or would not retaliate.[132] In other words, Hussein's statement might reflect an ongoing deception campaign. To explore this hypothesis further, the analyst might seek to determine whether increases in Iraqi agent communications were relevant to the issue and whether additional collection of such broadcasts was warranted.[133]

In practice, these and similar questions can be answered quickly. Analysts often answer some of them unconsciously as they struggle

132 Heuer develops this scenario and evidence in an example of the analysis of competing hypotheses. See Heuer, *Psychology*, 101–102.

133 Heuer, *Psychology,* 101–102. For a recent detailed look at Saddam Hussein and deception see Kevin Woods, James Lacey, and Williamson Murray, "Saddam's Delusions: The View from the Inside," *Foreign Affairs* 85, no. 3 (May/June 2006). URL: <http://www.foreignaffairs.org/20060501faessay85301/kevin-woods-james-lacey-williamson-murray/sadda-s-delusions-the-view-from-the-inside.html>, last accessed 31 March 2006.

to meet short deadlines. However, as a function of not employing scientific methods or other structured and critical thinking techniques, their thinking is largely intuitive. Analysts choose to ignore how mindsets and assumptions impede their judgments. Conversely, critical thinking ensures that the reasoning process is a self-conscious one. By making the unconscious conscious, analysts reveal where they may be biased, helping ensure that questions they address are thoroughly and fairly considered.

Each method of analysis uniquely interacts with the intelligence question; therefore, the method (or methods) selected can produce profoundly different results – affecting the analyst's arrival at the most accurate answer.

An analyst committed to critical thinking continually asks questions while developing the mass of evidence needed to assess an issue. Evidence arises from questions answered satisfactorily. Information for which the questions cannot satisfactorily be answered is excluded – but only after the analyst reflects on the process of evidence development. Consideration is owed to the question of how biases, and possibly active denial and deception by an adversary, have influenced the selection of both questions and answers. One way of revealing bias is by asking questions such as, "If the opposite outcome is actually true, what other evidence would I expect to see?"

The marshaling of evidence refers to a questioning process by which data and information are assessed and evidence is created. It may be done in solitary fashion, Socratically with a teammate, or collegially among Intelligence Community focus groups. It is a vital ingredient of productively imaginative intelligence analysis. Each question an analyst asks not only becomes a device for attracting existing evidence, but also generates new evidence not yet visible. Identifying new evidence increases the thoroughness by which the issue is evaluated and increases the probability that the correct solution has been discovered.

Embracing a Methodology

Once a relevant mass of evidence is established, the analyst evaluates which method or methods of analysis may best develop

a solution to the issue. Differences among various analytic methodologies, techniques, and tools are not trivial.

In fact, comparing the results of different analysis methods can be a valid means of establishing the accuracy of the answer. If various means of analysis yield multiple results, a review by different analysts makes for the ideal environment for critical thinking to discuss and debate those results.[134]

Therefore, assessment of the available evidence includes redirecting thinking, soliciting feedback from other sources, appraising the quality of possible answers, and comparing initial goals with results. In so doing an analyst employs interpretive and evaluative skills to select the best mass of evidence to analyze.

Creating Better Inferences

Critical thinking aims to ensure that inferences are reasonable and evidence-based. Inference creation begins at the same time that analysis starts. As each piece, or the whole mass of evidence, is considered, inferences are made.[135] Resulting "chains" of inferences linking the evidence to the hypotheses under consideration are known as arguments. Chains of inferences converge – strengthening the argument – or diverge – weakening it. The self-reflective nature of critical thinking places a check on these inferences. The analyst asks, "Do my inferences flow from the evidence?" and, "Are my inferences logical given the evidence and other inferences I have made?"

Inferences lead to a search for additional evidence. In other words, based on inferences drawn from the evidence at hand, an analyst may infer that there are other sources of evidence to consider. For example, such reasoning was cited in the explanation of why

134 For a more detailed discussion of this and other means of countering biases, see Heuer, *Psychology*, 170–184; Irving Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*, 2nd Edition (Boston, MA: Houghton Mifflin Company, 1982); and Scott Plous, *The Psychology of Judgment and Decision-making* (New York, NY: McGraw Hill, Inc., 1993).

135 Indeed, the analyst's acceptance – or rejection – of this evidence is a result of inferences: either the evidence is valid, credible, and relevant, or it is not.

the FBI investigated a pond in western Maryland during June 2003, searching for the source of the 2001 anthrax attacks. At the time, the FBI believed their primary suspect lived near the pond in question. In their search for additional evidence, they reasoned that the pond might be something in which evidence had been hidden. Thus, inference led the FBI to drain the pond to search for that evidence.[136]

The analyst self-consciously evaluates the thinking process and the biases that have affected it to reduce unproductive thinking and to consciously develop new ways of understanding the evidence at hand. This self-regulation also plays a role as the available evidence is considered. A means of accomplishing this within a collaborative setting is to seek the assistance of colleagues of diverse backgrounds. The underlying premise is that their biases differ sufficiently to enable productive and thorough analysis to occur.[137]

Producing Intelligence

Analysts who produce intelligence assessments and judgments have the opportunity to employ what Peter Facione considers the core cognitive skills of critical thinking: interpretation, analysis, evaluation, inference, explanation, and self-regulation.[138] Each of these competencies contributes to the integration of available evidence through a clear line of reasoning to the most probable answer.

Facione asserts that good critical thinkers can explain "what they think and how they arrived at that judgment."[139] By documenting the

---

136 *Washington Post,* "No Anthrax."

137 See Robert Callum, "The Case for Cultural Diversity in the Intelligence Community," *International Journal of Intelligence and Counter Intelligence* 14, no. 1, Spring 2001: 25–48.

138 Peter A. Facione, Critical Thinking: What It Is and Why It Counts (Milbrae, CA: California Academic Press, 1998, updated 2004), URL<http://www.insightassessment.com/>, last accessed 22 July 2005, 4. Cited hereafter as Facione, Critical Thinking.

139 Facione, *Critical Thinking,* 5.

reasoning process used to arrive at an answer, analysts move beyond merely "stating results [to] justifying procedures, and presenting arguments."[140] Questioning biases and mindsets encourages consideration of alternative possibilities that overcome what Josh Kerbel refers to as "single–outcome [analytic] trajectories."[141] Most importantly, analysts demonstrate a critical spirit – a reflection of character.[142]

Thus, critical thinking contributes to short-term analysis and assumes an essential role in longer-term analysis. Indeed, building a comprehensive picture of an issue or target requires critical thinking to determine which previous reports are included or excluded. "How do the parts contribute to the whole?" is one question the analyst asks. Another is, "How is the whole greater than the sum of its parts?" When previously published intelligence reports diverge, the critical thinking process helps the analyst ensure that the divergence is considered fairly and that the resulting intelligence does not merely satisfice.

---

140 Facione, *Critical Thinking*, 6.

141 Josh Kerbel, "Thinking Straight: Cognitive Bias in the US Debate about China," *Studies in Intelligence* 48 no. 3 (2004), URL: <http://cia.gov/csi/studies/vol48no3/index.html>, last accessed 22 February 2006.

142 Facione, *Critical Thinking*, 7. See also Moore and Krizan, "Intelligence Analysis," 9–11.

How can Analysts be Taught to Think Critically?

Many people would rather die than think – in fact, they do.

—Bertrand Russell

Critical Thinking Education Outside the Intelligence Community

Critical thinking offers a framework for structured problem solving. Yet, despite a corpus of associated literature, critical thinking remains in its infancy as a discipline. It is still "largely misunderstood…existing more in stereotype than in substance, more in image than in reality."[143] As Bertrand Russell's humorous quip reminds us, critical thinking is not a habit acquired by just being alive.

Ideally, valuable skills and dispositions should be developed among prospective analysts before they join intelligence-producing corporations. Yet, observations by the author of newly hired intelligence analysts suggest this happens rarely if at all. This raises two questions, "What are the opportunities for prospective analysts to become critical thinkers before they are hired?" and often "Why do these opportunities not exist?"

Despite its importance, critical thinking is not widely taught in schools and universities. A mid-1990s California study on the role of critical thinking in the curricula of 38 public and 28 private universities concluded that the skill is "clearly an honorific phrase in the minds of most educators."[144] The study concluded that university

143 Richard W. Paul, "A Draft Statement of Principles," The National Council for Excellence in Critical Thinking, URL: <www.criticalthinking.org/ncect.html>, last accessed March 18, 2003. The reasons why critical thinking remains an undeveloped discipline while important, go beyond the scope of this essay and are not addressed.

144 Richard W. Paul, Linda Elder, and Ted Bartell, "Executive Summary,

faculty members "feel obliged to claim both familiarity with it and commitment to it in their teaching, despite the fact that…most have only a vague understanding of what it is and what is involved in bringing it successfully into instruction."[145] Indeed, the authors of the study found that while 89% of the faculty they interviewed "claimed critical thinking was the primary objective of their instruction," only 19% could define the term and only 9% were evidently using it on a daily basis in their instruction.[146] If the results of the California study are representative of the nation at large, they explain why prospective new hires – themselves college graduates – generally fail to exhibit skill in critical thinking at any level of proficiency.[147]

Informal conversations with recent hires at NSA support this premise. Although slightly fewer than half of these individuals indicate they have been exposed to critical thinking skills in college, most have been exposed only in one class and then only as an approach to learning the materials covered in that class. While not discouraged, respondents apparently were not encouraged to apply the skills to other subjects. Thus, a disposition to think critically is rarely fostered. Further, when asked to define critical thinking, most

Study of 38 Public Universities and 28 Private Universities To Determine Faculty Emphasis on Critical Thinking In Instruction," *California Teacher Preparation for Instruction in Critical Thinking: Research Findings and Policy Recommendations,* California Commission on Teacher Credentialing, Sacramento California, 1997 (Dillon, CA: Foundation for Critical Thinking, 1997), URL: <criticalthinking.org/schoolstudy.htm>, last accessed March 18, 2003. Cited hereafter as Paul, Elder, and Bartell, *Executive Summary.*

145 Paul, Elder, and Bartell, *Executive Summary.*

146 Richard W. Paul, Linda Elder, and Ted Bartell, *California Teacher Preparation for Instruction in Critical Thinking: Research Findings and Policy Recommendations California Commission on Teacher Credentialing,* Sacramento California, 1997 (Dillon, CA: Foundation for Critical Thinking, 1997), 18.

147 A recent but unscientific survey of several major eastern American universities' online catalogs shows the term "critical thinking" to be used widely in course descriptions. Further examination of some of those courses suggests that East Coast academics may share a similar lack of understanding about critical thinking. Although beyond the purview of this paper, it appears that there is sufficient evidence to warrant repeating the California survey on a national basis.

young analysts were unable to do so in any comprehensive fashion.[148] Finally, few employ any form of critical thinking in their analytic (or other) reasoning unless they have been trained to do so.

In fairness, it should be noted that critical thinking awareness, attitude, and skills varies from one academic discipline to another. For example, students of the physical sciences who employ the scientific method in a community setting probably have a greater inclination toward a basic form of critical thinking if only through osmosis.[149]

There are also some primary, secondary, and university education programs that have adopted a meta-cognitive critical thinking paradigm. Although the results of the impact of such programs are largely anecdotal, at least one study, conducted by Jennifer Reed as part of her dissertation found that students' critical thinking skills improved *after just one course.*[150] Faculty and administrators of these programs routinely attend the annual critical thinking conference sponsored by the Center for Critical Thinking where their results are shared. However, the approximately 500 people who attend this international event represent a small fraction of the educators in the United States.

The elements of scientific method – the formulation of hypotheses, collection of relevant data, testing and evaluation of hypotheses, and the logical derivation of conclusions – are matched step-by-step by

148 These conversations occur routinely as part of a training course the author teaches to newly hired intelligence and language analysts at NSA. When asked to complete the following statement, "In my opinion, critical thinking involves…" typical answers center on "thinking outside the box."

149 Francis J. Hughes, conversation with the author, Washington, DC: National Defense Intelligence College, 8 May 2003. Mr. Hughes is one of the few proponents and teachers of evidence-based inferential intelligence analysis, a means of analysis requiring critical thinking at every stage in the process.

150 Jennifer H. Reed, *Effect of a Model For Critical Thinking on Student Achievement In Primary Source Document Analysis And Interpretation, Argumentative Reasoning, Critical Thinking Dispositions, And History Content in a Community College History Course,* PhD Dissertation, College of Education, University of South Florida, December 1998, vii. URL: <http://www.criticalthinking.org/resources/JReed-Dissertation.pdf>, last accessed 6 May 2006.

critical thinking.[151] Given that most newly hired intelligence analysts – at least at NSA – are drawn from fields other than the physical sciences, one can expect that new hires lack adequate critical thinking skills. If NSA's newly hired intelligence analysts are representative of those being hired across the Intelligence Community then it is probable that few of the thousands of new hires arrive with adequate critical thinking skills.

Critical Thinking Education Inside the Intelligence Community

That analysts need to develop critical thinking skills is recognized within the Intelligence Community. Heuer wrote in 1999, "[Traditionally], analysts at all levels devote little attention to improving how they think."[152] As a direct response to Heuer's criticism, the CIA's Sherman Kent School includes critical thinking as part of the curricula for training new analysts, and recently initiated a class in critical thinking.[153] New employees are encouraged to develop a disposition to think critically as they are taught the skills of intelligence analysis.

A similar approach is employed in courses on structured analysis methods at the National Defense Intelligence College (NDIC). Critical thinking is claimed as a feature of many NDIC courses. However, the emphasis in most courses is on topical or issue-related material, and only incidentally on the process of thinking. At present, the skill itself is largely not taught. Instead, students are expected to figure

151 Steven D. Schafersman, "An Introduction to Critical Thinking," January 1991, URL: <www.freeinquiry.com/critical-thinking.html>, last accessed 9 March 2006.

152 Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: CIA Center for the Study of Intelligence, 1999), 173. Cited hereafter as Heuer, *Psychology*.

153 For a detailed account of how the faculty of the CIA's Sherman Kent School are working to improve their analysts' knowledge, skills, and abilities, see Stephen D. Marrin, "CIA's Kent School: Improving Training for New Analysts," *International Journal of Intelligence and Counter Intelligence* 16, no. 4 (Winter 2003–2004): 609–637.

it out on their own, encouraged by the thesis writing process. The college is aware of the importance of critical thinking and new core courses may include formal critical thinking instruction.

New NSA analysts are provided with an introduction to the solitary part of the skill (as discussed in figure 4) as part of their orientation. The agency's 40-hour follow-on program is the first Intelligence Community course to focus primarily on enhancing analysts' solitary and communal critical thinking skills. In addition to critical thinking skills, participants learn and apply, and then assess, the appropriateness of fourteen structured methods of analysis. The course has been taught to both U.S. and Allied personnel drawn from intelligence, counterintelligence, information assurance, and law enforcement communities.[154]

Training in critical thinking is offered to Defense Intelligence Agency (DIA) analysts using a variation of the NSA-developed course. Also, in 2005, DIA tested the "critical thinking skills" of a sample of its employees using the *Watson-Glaser Critical Thinking Appraisal*. The instrument claims to "measure abilities involved in critical thinking, including the abilities to define problems, select important information for the solution to problems, recognize stated and unstated assumption, formulate and select relevant and promising hypotheses, [and] draw valid conclusions and judge the validity of inferences."[155] The appraisal appears to confuse abilities with skills, although both do belong within the domain of analysis.[156] Finally, it appears that the test does not evaluate an individual's meta-cognitive skills in assessing and correcting the *process* of reasoning.

The increasing opportunities for enhancing critical thinking skills and dispositions reflect a recognition of the importance of critical

---

154 The syllabus from the course is in the Appendix.

155 Harcourt Assessment, Inc., *Local Norms Report, Watson-Glaser Critical Thinking Assessment*, Report prepared for the Defense Intelligence Agency, 2005, 2. Cited hereafter as Harcourt, *Watson–Glaser.*

156 Abilities and skills are easily differentiated. Individuals are born with certain abilities (and can improve them through training) but they *must* learn a skill. See for example, Moore and Krizan, "NSA."

thinking in intelligence analysis.[157] Evidence becomes intelligence through an "ordered thinking process [involving] careful judgments or judicious evaluations leading to defensible conclusions" – through critical thinking.[158] Former CIA analyst Morgan Jones asserts that methods for critical thinking and problem solving, if applied, can improve the quality of analysis and decisionmaking.[159]

Implications of Teaching Critical Thinking

Although Sherman Kent, Richards J. Heuer, Jr., and others have over the years addressed intelligence analysis and its relationship with critical thinking, recent presidential executive orders and legislative mandates are bringing a new emphasis to how the Intelligence Community can change analytic practices to achieve improved outcomes. Teaching analysts to be better critical thinkers may be seen as an easy way to satisfy these requirements. However, linkages between intelligence analysis and critical thinking remain poorly understood. Considerable confusion remains about what constitutes critical thinking and how it supports intelligence analysis.

A common excuse among analysts to defend their "non-use of such self-conscious processes is a lack of time."[160] Teaching critical thinking skills is of little value if analysts are not inclined to use them.[161] For those who are willing to think critically, various

157 The Director of National Intelligence, John D. Negroponte, in the Foreword of the initial *National Intelligence Strategy of the United States of America* (Washington, DC: Office of the DNI, October 2005), wrote that one of the three principal tasks for the reformed Intelligence Community is to "bring more depth and accuracy to intelligence analysis." See http://www.dni.gov/NISOctober2005.pdf.

158 Moore and Krizan, "Intelligence Analysis," 14.

159 Morgan D. Jones, *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving* (New York, NY: Random House, Inc, 1995), xi. Cited hereafter as Jones, *Thinker's Toolkit.*

160 Stephen Marrin, email to the author, December 8, 2003. The author has heard similar complaints from analysts at NSA and DIA.

161 Linda Elder, Alec Fisher, Diane Halpern, Gerald Nosich, Richard Paul, and others develop and publish the materials for – as well as teach – such courses.

instructional models offer complementary means of expanding and enhancing analysts' skills. For example, in an area studies class on Russia, students might be asked to evaluate and comment in depth on what different sources say about the influence of organized crime on the national government. Alternatively, critical thinking can be injected into the course as part of a problem-solving curriculum. Here students focus on *how* they think as they apply different strategies to each assignment, and then, ideally, transfer those enhanced skills to their day-to-day analysis. The use of realistic case studies makes classroom-acquired knowledge actionable. Self-reflective and group-reflective analyses of the process of reasoning keep the classes focused toward the working environment of analysts.

Such transformations involve behavior modification and as such take time. Participants engaged in such instruction cannot be expected to become critical thinkers in a one-day or even a week-long course. The instructors of the NSA course attempt over a period of 10 weeks to transform their students into critical thinkers. Some other Community efforts also provide instruction over an extended period. Even so, students leaving the course are still novices in this practice and can slip back to their old methods of reasoning. Becoming critical thinkers requires a change in behavior that extends long past the end of the formal instruction. There is no substitute for continued practice.

Finally, it serves critically thinking analysts poorly if their management and corporations are indisposed toward the application of the skills. It is well known that "engendering the desire to use [critical thinking] as a favored means of problem solving and decision making prepares the ground for teaching and learning the [critical thinking] skills."[162] Such encouragement can occur in the classroom but its effectiveness is limited unless the corporation encourages and welcomes strategies to employ critical thinking in the workplace.

However, there are few metrics for determining the effectiveness of these materials and courses and so their value remains undetermined. The fact that the books developed for, and used in, such courses remain in print (in successive editions) is an indicator that at least this approach is popular, if not effective.

162 Facione, "Disposition."

The best place for such encouragement is from senior and midlevel management. In order for this to occur, they too must be educated in the methods of, and reasons for, critical thinking.

Evaluating Teaching Models

Removing analysts from their work for education and training disrupts their primary mission of intelligence production. Spreading instruction over time provides a reasonable answer to this dilemma. Since improving critical thinking requires a high level of experiential, hands-on practice, an extended course offers students time to practice and apply what they are learning. This is the model used for the NSA course on critical thinking. Feedback from students indicates that once-a-week instruction works best. Mission is minimally disrupted and there is time to study and practice what is being taught. However, the long duration limits students' work-related travel and leave.

Experiential learning also requires that such classes be relatively small and that instructors be proficient. Without a large teaching staff, training a large workforce takes years. Since senior managers – and their strategic visions – change often, a long-term corporate commitment is crucial to success.[163]

Such a long-term commitment exists at the Sherman Kent School for Intelligence Analysis. The school itself grew out of a month-long course on analytic tradecraft developed by former Deputy Director for Intelligence Douglas J. MacEachin.[164] Beginning in 1996, the course was delivered to the entire analytic workforce. The school itself was established in 2000 and continues to evolve as both a training center and a center of best analytic practices.[165]

---

163 Alternately, a large staff can be created, trained, and assigned to teach an entire workforce. This was accomplished in a knowledge domain at NSA in the 1990s. If inducements and cultural change accompanied such a program, this approach might present certain advantages even if its costs are high. An analytic workforce could be transformed rapidly through such a "boot camp" approach.

164 Marrin, "Kent School," 615.

165 Marrin, "Kent School," 609.

Another means of critical thinking instruction is to create an interactive, computer-based or web-based course. This has the benefit of allowing as many analysts to attend as wish to do so. One or two instructors working full-time can answer students' questions. Exercises allow student self-assessment. However, this is presently an unsatisfactory model for critical thinking instruction. Learning to think critically requires Socratic interaction and the impersonal nature of web-based instruction discourages the practice even for the population of dedicated solitary learners. In the future, multi-player simulations and other games could be used to reinforce the lessons learned. However, these are not yet available.

Although computer- and web-based instruction can be accomplished at the analyst's desk, there are other reasons why this may not be a good idea. Analysts who remain in their offices are subject to interruptions. Further, course work is often relegated to the end of the workday, when analysts are tired and learning is impaired. Little learning occurs when taking a class is a chore. The current limitations of both classroom and computer- or web-based education suggest that experimentation with new means of instruction for critical thinking is needed.

Encouraging Analysts to Think Critically

Incorporating critical thinking into both orientation and basic analyst education and training is one way to help newly hired analysts develop their skills. Subsequently placing those analysts in offices where critical thinking is practiced is another way to encourage an analytic culture that fosters thinking critically. Through direct exposure to successful, experienced analysts, junior analysts' doubts about the employment of critical thinking techniques can be overcome.

"Skills pay" can be an inducement for analysts to learn and then employ critical thinking. Rewarding the acquisition, maintenance, and use of other special skills is common in government and industry. For example, linguists at NSA earn significant bonuses for achieving specific levels of foreign-language proficiency – an effective way

to maintain critical language competencies within one intelligence agency's workforce. Given the high-level concern for the health of the intelligence analysis process, direct monetary incentives should be available for analysts to master new tools and demonstrate constructive analytical behaviors.

On the other hand, if an intelligence enterprise fails to recognize and reward the acquisition and application of analytic skills such as critical thinking, it sends a very clear message: the enterprise does not value those skills. Faced with such a message and a lack of inducements to excel, the best and brightest analysts may leave, especially from the more junior ranks – and midlevel employees with families and mortgages may "retire in place." Either outcome hurts mission-critical functions, and can be avoided. As a previous Director of NSA, Air Force Lieutenant General Kenneth A. Minihan, noted, "If we don't win the talent war, it doesn't matter what we invest in the infrastructure."[166] Recognizing and rewarding critical thinkers is one way to win that talent war – with the assumption that really good analysts are more likely to remain active within their intelligence agency workforces.

If an analyst adopts a congeries of skills that contributes to the mastery of critical thinking, and is compensated monetarily, that mastery needs to be certified. If a curriculum that drives the acquisition of those skills is in place, then an assessment of those skills can be administered in-house. Specific tests exist for the assessment of critical thinking, such as the "Thinking Skills Assessment Test."[167]

Persuading to Improve Analysis

Teaching critical thinking is but a first step toward improving analysis. Because analysts and managers have different needs and

166 LtGen Kenneth A. Minihan, USAF, Director, NSA, in Robert K. Ackerman, "Security Agency Transitions from Backer to Participant," *Signal* 53, no. 2 (October 1998), 23.

167 For more information, see http://tsa.ucles.org.uk/index.html, last accessed 15 March 2006.

time constraints, multiple versions of a course are needed to meet the needs of each group. Analysts and first-line supervisors may take an entire course, midlevel managers an abbreviated course, and senior managers an overview. This strategy already is employed at the CIA's Sherman Kent School where new employees spend 13 weeks learning analysis skills, techniques, and methods while supervisors, depending on their seniority, spend three days or one day becoming familiar with these same skills and methods. The analysts also have opportunities to apply new skills immediately as they perform four-week "internships" in various CIA offices.

Other CIA analysts, already in place, do not have the same opportunities to receive this training. Thus a two-tiered analyst population with more skilled junior analysts and more knowledgeable senior analysts is being created. Ideally, each will transfer skills and knowledge to the others. However, an alternate possibility is that it will generate distrust and animosity between the two groups. Older, more experienced analysts may resent the opportunities given to their newer counterparts. This issue is not trivial. Offering the wrong curriculum to the wrong groups of analysts and managers can destroy its effectiveness. Managers in the CIA and elsewhere can influence how the new analytic methods being taught will be adopted, as agencies respond to new legislative and executive mandates.

Will analysts embrace critical thinking as a means to improve their analysis? There are numerous observations of analysts' reluctance to adopt new paradigms.[168] This is true even when analysts are confronted with the fact that their conclusions were wrong. In referring to her work on the issue of Iraqi WMD, one CIA analyst told Senate investigators, "their 'bottom line' judgments would have remained the same."[169] Rob Johnston also found a similar reluctance to change opinions among the analysts he studied. He noted that

168 Stephen Marrin, "Homeland Security and the Analysis of Foreign Intelligence," Markle Foundation Task Force on National Security in the Information Age, 15 July 2002, URL: <www.markletaskforce.org /documents/ marrin_071502.pdf>, last accessed December 9, 2003, 9. Cited hereafter as Marrin, "Homeland Security."

169 SSCI, *Iraq,* 299.

although "analysts can change an opinion based on new information or by revisiting old information with a new hypothesis," they perceive a loss of trust and respect and a subsequent loss of "social capital, or power, within [their] group."[170]

Yet, a case can be made that analysts, and especially experienced analysts, will benefit the most from enhanced critical thinking skills training. These are the analysts who are in positions of technical leadership, who work the most difficult aspects of complex targets. There may be significant consequences if they fail to notice and make sense of an issue. On the other hand, the fact that many of these senior personnel will soon be eligible for retirement raises an important question: Does the corporation get added value from teaching analysts who will soon retire to think more critically in their analysis if they are predisposed not to do so? Maybe so. Heuer, while the head of CIA's Methods and Forecasting Division found that analysts, once persuaded to use new analytic methods, found them "interesting and well worth doing."[171]

Other intelligence analysts have adopted new analytic methods that add value to their analyses. In one example, NSA personnel involved in research and development adopted a means of matching target characteristics and their vulnerabilities with exploitation capabilities and their costs.[172] Such analyses helped ensure that appropriate resources were dedicated to collection and that such collection was better tailored to production analysts' needs. However, some research analysts initially refused to employ the model, claiming it took too much time even as it reduced the volumes of information

---

170 Johnston, *Analytic Culture,* 22.

171 Richards J. Heuer, Jr., *Adapting Academic Methods and Models to Governmental Needs: The CIA Experience* (Carlisle, PA: Strategic Studies Institute, U.S. Army War College, 31 July 1978), 5. Referenced in Marrin, "Homeland Security," 9.

172 In this context, a "target" refers to an entity – geographical, individual, or topical – in which the Intelligence Community has an interest.

they were required to examine.[173] Adoption of the analytic paradigm required appropriate persuasion.

One interesting means of self-persuasion may be analysts' frustration with the really hard problem. This frustration may lead analysts to try something new.[174] Such frustration occurs more often among experienced analysts. Years of attempting to make sense of overwhelming masses of information with inadequate analytic paradigms and technologies leaves some experienced analysts willing to grasp at anything that will improve how they work. On the other hand, newly hired analysts who have not yet experienced the frustration of inadequate paradigms for analysis may be resistant to adopting rigorous analytic paradigms such as that afforded by critical thinking.[175]

173 Multiple midlevel NSA analysts, interviews with the author, 1998–2005.

174 LT Robert D. Folker, USAF, email to the author, 9 December 2003. Cited hereafter as Folker, email, 9 December 2003.

175 Folker, email, 9 December 2003.

Transforming Intelligence Corporations

In order for an institution to change, all affected personnel, from the lowest to the highest, must first recognize that change is needed and is advantageous – both corporately and personally. As retired World Bank executive Stephen Denning argues, this is difficult to accomplish. Logically sound arguments do not sway employees. Instead, employees remain convinced that what they are doing is satisfactory.[176] Further, outsiders who attempt to induce change face opposition because employees presume that external consultants are arrogant in suggesting that things are not right, and that change is needed.

One way to effect change is through a "springboard story." This approach contrasts with past conventional – and largely unsuccessful – transformation efforts that relied on fixing the systems involved and were characterized by an overabundance of buzzwords:

> Enhance quality. Streamline procedures. Reform and flatten the organizational structure. Analyze things in terms of grids and charts. Develop plans in which individuals are programmed to operate like so many obedient computers. Hone our interpersonal mechanics and build skill inventories. Bring to our difficulties a fix-it attitude, as though our past errors can be easily corrected with straightforward explanations.[177]

---

176 For a discussion of Denning's philosophy about change, see Jeff de Cagna, "Making Change Happen: Steve Denning Tells the Story of Storytelling," Information Outlook, January 2001, 28–35, and Stephen Denning, *The Springboard: How Storytelling Ignites Action in Knowledge-Era Organizations* (Boston, MA: Butterworth-Heinemann, 2001). Cited hereafter as Denning, Springboard.

177 Denning, *Springboard,* xvii. In 23 years of Intelligence Community work, the author heard all of these phrases as slogans for various programs designed to "fix" analysis or the corporations involved. These associated corporate efforts to bring these goals about often had the opposite effect. In the process of "flattening

As Denning points out, these strategies fail to account for the messy and chaotic reality in which real organizations live and work, especially intelligence agencies which have the charter to engage honestly with "the other," or mission-related targets, outside of the bureaucracy in which they serve.[178]

The springboard story helps employees at all levels envision what is needed for the proposed transformation. Denning asserts that it "invites them to see analogies from their own backgrounds, their own contexts, their own fields of expertise."[179] He cautions that transformational stories are not a panacea – there are situations and circumstances in which they are not effective, such as when the change being proposed is a bad idea.[180] The key is finding the appropriate stories within the corporate culture.

One way to find these stories is to examine the best practices of intelligence analysis successes where critical thinking played a role. Just recounting a success is not enough. Listeners need to be able to identify and empathize with the scenario and its actors. The effective story is "about people who have lived [a] knowledge-sharing idea and how things happen in a real-life situation."[181] For example, conducting a trial or experiment on critical thinking within the intelligence analysis process, if it leads to certifiable, actionable success, *does* effectively persuade.

Learning from Early Adopters

Once a sustained number of early adopters openly apply systematic, critical thinking to hard analytic problems, the stage is set for a "tipping point" in the spread of structured methods across

---

the organization" at one intelligence agency, more hierarchical managerial layers were actually created!

178 Denning, *Springboard,* xvii.

179 Denning, *Springboard,* xix.

180 Denning, *Springboard,* xxi.

181 Denning, *Springboard,* 51.

analytic populations.[182] Stanley Feder recounts how a tipping point began to apply to a political analysis method at the CIA in the 1970s and 1980s. The method involved two estimative tools known as Factions and Policon that were used by the "Intelligence Directorate and the National Intelligence Council's Analysis Group to analyze scores of policy and instability issues in over 30 countries."[183] The reasons for the adoption of these tools remain the same: "Forecasts and analyses…have proved to be significantly more precise and detailed than traditional analyses."[184] Writing about the method in 1987, Feder predicted that its use would continue to expand.[185] The method is still in use 19 years after Feder's article was published. However, expanded use failed – perhaps because the tool was on a computer platform that ceased to be supported by the Agency. The recent transfer of the tool to a new suite of programs corresponds with observations that its use is once again expanding.[186]

Non-intelligence-related transformational stories can be applied in the Intelligence Community to facilitate the spread of new ways

182 Malcolm Gladwell, *The Tipping Point: How Little Things Can Make a Big Difference* (Boston, MA: Little Brown and Company, 2000), 15–29. Gladwell shows how "social epidemics" can infect a variety of domains.

183 Stanley Feder, "Factions and Policon: New Ways to Analyze Politics," in H. Bradford Westerfield, ed., *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955–1992* (New Haven, CT: Yale University Press, 1995), 275. Cited hereafter as Feder, "Factions and Policon."

184 Feder, "Factions and Policon," 292.

185 Feder, "Factions and Policon," 292. Feder was wrong about its sustained popular growth.

186 This story is not an isolated instance. In the author's experience, initial implementation and popularization are often followed by a gradually reduced user-base. Certain organizations find the tools useful and they tend to continue to use them even though any underlying technology may be obsolete. In the case of Factions and Policon, the tools were maintained on an aged Macintosh computer. They were updated in 2006 as part of the work of an intelligence research firm in New Mexico. The Factions tool was rewritten and included in Landscape Decision®, a suite of modeling and simulation tools developed under a research contract with the Department of Defense's Advanced Research and Development Activity (ARDA). The updated technology was reinserted into the tasking organization. Other technology transfers are pending.

of thinking. For example, two video commercial advertisements from the Electronic Data System (EDS) company resonate with the challenge of rebuilding intelligence analysis in the face of skeptics, and what it takes to be an intelligence analyst.[187] The two related commercials depict farcical situations based on two well-known clichés: "You've got to build it before you can fly it!" and "It's like herding cats; it can't be done!" In the former, a group of mechanics is building an airplane in mid-flight; while in the other, a group of cowboys has accomplished the impossible – they are herding cats across the Great Plains. EDS' depiction of its revolutionary design capabilities bears a message about corporate rebuilding and individual transformation. The message encourages managers and analysts to compare themselves and their situation to the people tasked with building an airplane at "60,000 feet," or with herding cats across a river.

Intelligence analysts and managers who have seen the videos have had little trouble drawing analogies with the corporate and personal transformations needed in the Intelligence Community. That the situations are humorous only adds to a viewer's buy-in – they are "hooked" before they realize it. Developing other stories that specifically apply to corporate transformation within the Intelligence Community and its various elements is a logical next step in encouraging analysts and managers to use and support critical thinking in analysis. If these stories can be drawn from recent analytic successes, their value can only increase.

The Costs and Benefits of Thinking Critically

Are intelligence failures inevitable if analysts lack critical thinking skills? Yes. However, critical thinking is not a panacea. Intelligence failures still can be expected. If no measure "will guarantee that accurate conclusions will be drawn from the incomplete and ambiguous information that intelligence analysts

187 See *Building Airplanes in Flight*, television advertisement produced for EDS by Fallon-McElligott, November 2000, videocassette; and *Herding Cats,* television advertisement produced for EDS by Fallon-McElligott, January 2000, videocassette.

typically work with…[and] occasional failures must be expected," why should the Intelligence Community invest in teaching its analytic workforce to think critically?[188] A brief review of the causes of failure clarifies the need for such an investment.

Intelligence failures occur in both systematic and functional domains. Systematic intelligence failures occur when producers fail to notice phenomena and the consumers of intelligence fail to heed warnings or even to notice that they are being warned. It may be that both consumers and producers are focused on other issues at the time. Alternatively, intelligence-based warning is not taken seriously at high official levels. In cases where collaboration among intelligence agencies might be critical, key evidence may not be recognized and shared.

All of these failings are illustrated in the "intelligence failure" to warn of the attacks of 11 September 2001 on the World Trade Center in New York and the Pentagon near Washington, DC. In the first place, the policy issue that was at the forefront – according to press at the time – was a national missile defense system, not the likelihood of a terrorist attack on the United States. Richard Clarke, the Clinton and then Bush administrations' terrorism "czar" observes that Bush administration officials were slow to recognize or consider the threats posed by Osama bin Laden.[189] Evidence passed by an FBI field agent about students learning to fly large aircraft with little regard for landing or takeoffs was not taken seriously at higher levels within the Bureau.[190] The Joint Congressional investigation into the attacks noted in its report that collaboration was lacking between agencies, especially between the law enforcement and strategic

188 Heuer, *Psychology,* 184.

189 "Clarke: Bush Didn't see Terrorism as 'Urgent,'" *CNN.com,* 19 May 2004, URL: <http://www.cnn.com /2004/ALLPOLITICS/03/24/911.commission/index.htm>, last accessed 9 March 2006.

190 Michael Elliott, "How the U.S. Missed the Clues," *CNN.com,* 20 May 2002, URL: < http://archives.cnn.com/2002/ALLPOLITICS/05/20/time.clues/index.html>, last accessed 9 March 2006.

intelligence agencies.[191] This was both a cultural and a physical phenomenon. Airport security breaches during the summer of 2001 may have been related, but based on assessments of the catastrophe, were not connected to the events.[192]

The same kinds of failings were identified by the Senate Select Committee on Intelligence in its assessment of the National Intelligence Estimate on Iraqi WMD. As has already been observed, analysts and their managers were focused on the results and not the process.[193]

Critical thinking can mitigate some common causes of failure and provide means by which they can be avoided in the future. Specifically, an intelligence process based on critical thinking offsets the following failures:

Analysts are Wrong. It is unrealistic to expect that analysts can always be correct. Regardless of the processes they employ, analysts make errors and fail. Anthropologist Rob Johnston defines *errors* as "factual inaccuracies in analysis resulting from poor or missing data." Conversely, intelligence *failures* are "systemic organizational surprise resulting from incorrect, missing, discarded, or inadequate hypotheses."[194] Critical thinking mitigates these by providing means to assess errors in reasoning as they occur and before they become

191 U.S. Congress, *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001,* Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee On Intelligence, Together with Additional Views, Senate Report No. 107–351/House Report. No. 107–792, 107th Congress, 2nd Session, December 2002, xvi.

192 The author recalls that media reports of persons hopping over or otherwise improperly passing airport security checkpoints in and around Boston, New York, and Washington seemed to be higher than usual during the summer of 2001.

193 DNI Negroponte, in the *National Intelligence Strategy of the United States* (October 2005, 2) highlights the notion that the Community appropriately undertakes study of its internal processes, as well as of the quality of its products, by addressing both "enterprise" objectives as well as "mission" objectives.

194 Johnston, *Analytic Culture,* 6.

systemic failures. Such a meta-cognitive approach to the analytic process helps keep it under active review at the highest levels.

Policymakers Ignore Intelligence.[195] A critically thinking analytic population cannot directly affect what a policymaker can or will do – neither in fact, can a *non-critically thinking* analytic population. What critically thinking analysts can do, however, is present more effective assessments, perhaps leading policymakers to question their own assumptions on the issues. Additionally, thinking critically about how analysts interact with policymakers can identify ways to restructure the analysis dissemination process to involve policymakers more effectively. Such a process might also encourage them to adopt some of the attributes of critical thinking leading to (it may be presumed) more effective policy.[196]

Adversary Denies and Deceives. Critical thinking reduces the effects of adversarial denial and deception by leading analysts to consider alternative possibilities, to question biases and assumptions, to examine systematically the validity of evidence being considered, and to take seriously anomalies in the evidence.

Adversary is More Capable. In any adversarial system, there are winners and there are losers. While analysts can do everything possible to ensure their work is correct, they rarely work with all the evidence, and indeed may still be deceived. In such cases, they may come to wrong conclusions. Critical

---

195 There is a "classic" argument as to whether this is or is not an "intelligence" failure. In summary, the two sides condense as follows: On the one hand, intelligence should have been so persuasively presented as to compel the policymaker to pay attention. On the other hand, intelligence should not be telling the policymaker what to do. The argument goes all the way to the roots of the post-World War II strategic intelligence system currently in place. Former CIA analyst Jack Davis summarizes the issue in "The Kent-Kendall Debate of 1949," *Studies in Intelligence* 35, no. 2 (Summer 1991): 37–50.

196 Cooper, email to the author, 31 March 2006. Cited hereafter as Cooper, email, 31 March 2006.

> thinking, however, by providing structure and oversight to their reasoning, provides an audit trail. In this case, the means by which the analytic conclusions were reached can be subsequently reviewed, errors and deceptions revealed, and steps taken to improve the process so that the failure is not repeated**.** Indeed, because of its focus on the process, critical thinking becomes a powerful tool for evaluating and enhancing analytical reasoning.

Investment in critical thinking as part of the analysis process minimizes the likelihood of specific failures. With critical thinking essential to so many parts of the intelligence production process, enhancing it increases the likelihood of intelligence success.[197] With the cost of failure catastrophically high, the Intelligence Community is well advised to improve the likelihood of intelligence success, including improving critical thinking. As diplomat Richard Holbrooke opined in 2003, "intelligence is…indispensable. And its greatest successes are preventative."[198]

There are other reasons why systemic intelligence failures occur. Jeffrey Cooper considers ten pathologies, summarized in table 6, that impede successful analysis at both the individual and corporate levels. Cooper specifically believes that given the

> [emphasis] on the systemic nature of the pathologies that afflict intelligence analysis, structured analytic methods

---

197 One metric for intelligence is decreasing intelligence failures. In this case, fewer failures could be considered as "improving intelligence." But the reasons for the prevention of the failures need to be considered. The reduced number of failures could be due to a critically thinking workforce. Or it could be due to coincidences. Although a pointed discussion of metrics for intelligence is beyond the scope of this paper, recent articles explore the issue of intelligence metrics. See, for example, David T. Moore, Lisa Krizan, and Elizabeth J. Moore, "Evaluating Intelligence: A Competency-Based Model," *International Journal of Intelligence and Counterintelligence* 18, no. 2 (Summer 2005): 204–220.

198 Richard Holbrooke, in Judith Miller, "A Battle of Words Over War Intelligence," *New York Times,* online edition, 22 November 2003, URL: <www.nytimes.com/2003/11/22/arts/22INTE.html>, last accessed November 28, 2003.

Cooper's Analytic Pathology	Description
Inefficient "Account" Structure	Work is subdivided into accounts with ownership; provides basis for accountability; ownership inhibits sharing, cooperation, and collaboration; encourages "stovepiping" in collection disciplines.
Evidence-Based Scientism	Descriptive and explanatory intelligence support current policy and military operations; less support for anticipatory intelligence; analysis needs to be "augmented and leavened with intuition, curiosity, and a thirst for discovery – all essential elements of good science."
Tyranny of Current Intelligence	Response to customers' current concerns; support to current, ongoing military operations; little long-term research.
Over-Emphasis on Production	Databases need filling; scheduled reports and assessments must be produced on time; metrics for success measure data collected and processed; number of reports issued used to determine and justify resources allocated.
Over-Reliance on Previous Judgments	Previous reports presumed to be authoritative; previous reports combined to form new judgments; agreed-upon positions retained despite newer contradictory evidence.

Table 6: Cooper's Analytic Pathologies

Source: Summarized from Cooper, *Pathologies*, 30–39.

> become a first line of defense in preventing the networks of errors from developing – they are like "ripstops" that keep problems from propagating into wider "error-inducing systems," in [Charles] Perrow's terms.[199]

199 Jeffrey Cooper, email to the author, 31 March 2006. Cooper refers to Charles Perrow, *Normal Accidents: Living with High-Risk Technologies* (Princeton, NJ: Princeton University Press, 1999).

Cooper's Analytic Pathology	Description
Neglect of Research	Short–term taskings prevent longer–term research; reward structure favors current reporting, not longer term work; stunts development of deep target expertise.
Neglect of Anticipatory Intelligence	"Information Revolution" leaves intelligence competing with journalism and Internet for policymakers' attention; lack of predictive intelligence against new emerging threats ensures continuing failures to warn.
Loss of "Keystone Species" and "Intellectual Middleware"	Periodic reductions in force skew analyst demographics; "Keystone Species" (journeymen analysts) lacking; journeymen do bulk of professional maintenance; essential for knowledge retention and transfer to apprentices; maintain "intellectual Middleware" or deep understanding of analytic domains and processes.
Lack of Analytic Tools and Methods of Validation	Available and proposed tools not formally validated for accuracy and usefulness; focus on results, not processes, to determine success.
Hindrances of Security Mindset	Security procedures impede multi–source analysis; protection of sources and methods more important than "effective exploitation and cross–fertilization;" artificial and outdated mission distinctions prevent collaboration.

Critical thinking combats this by enhancing the processes by which decisions are made and by which such processes are reviewed. This paper focuses primarily on *individual experience*, and of course, intelligence corporations are made up of individuals. If a sufficient number of intelligence professionals are thinking critically, it is likely they will transform their corporations, if only through the sheer attrition of non-critically thinking managers and leaders who are

retiring from the work force. It should be observed that an Intelligence Community enterprise-wide emphasis on developing critical thinking skills at all levels would speed the process.

Validation

A critically thinking Intelligence Community remains essential for effective intelligence reform. Steven Rieber and Neil Thomason advance this argument in their recent article. The authors assert that "the opinions of experts regarding which methods [of analysis] work may be misleading or seriously wrong."[200] Unfortunately, as the authors show, past (and present) efforts at intelligence reform rely on expert intuitive judgments. However, "[examples] from a wide range of fields show that expert opinion about which methods work are often [not only] dead wrong…but also are generally not self-correcting."[201] Further support of Rieber's thesis is seen in devil's advocacy – not as theoretically applicable but as practiced. They cite Irving Janis who, quoting a Stanford political scientist, notes that "instead of stirring up much-needed turbulence among the members of a policymaking group, [devil's advocacy] may create 'the comforting feeling that they have considered all sides of the issue.'"[202]

To mitigate this and similar analysis-improvement fallacies, Rieber and Thomason argue that improvements in analysis and any proposed methods of judgment and decision-making require validation through scientific study. They note, for example, that research reveals "[a] certain cognitive style, marked by an open-mindedness and skepticism toward grand theories, is associated with

---

200 Rieber and Thomason, "Creation of a National Institute for Analytic Methods," 71.

201 Rieber and Thomason, "Creation of a National Institute for Analytic Methods," 72.

202 Irving L. Janis, *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*, 2nd edition. (Boston, MA: Houghton Mifflin and Company, 1982), 268. Referenced in Rieber and Thomason, "Creation of a National Institute for Analytic Methods," 73.

substantially better judgments about international affairs."[203] As the present paper has argued, such attitudes are found in critical thinkers. Scientific study of this and other methods will determine when and how they are appropriate. Critical thinking also supports Rieber and Thomason's call for a "National Institute for Analytic Methods" by providing an overarching structure to champion open-mindedness and skepticism in the study of which methods are appropriate for intelligence analysis. Only then, they argue, will real intelligence reform and improvement occur.

Rieber and Thomason's proposed institute could determine which strategies are most effective at disposing analysts and their corporations to employ critical thinking. Research evidence indicates that simply teaching critical thinking (or for that matter, structured analytic) skills is insufficient. People will not adopt the strategies unless motivated to do so. As noted here, springboard stories are one means of implanting a positive disposition toward critical thinking. Other means certainly also exist. A desirable objective of research in the proposed National Institute for Analytic Methods would be to discover and assess what might motivate analysts most effectively toward thinking critically.

203 Rieber and Thomason, "Creation of a National Institute for Analytic Methods," 74.

What Other Points of View Exist?

A recent best-selling book advances the comfortable idea that conscious reasoning may not confer advantage to the reasoner.[204] Recent research suggests that whereas simple choices may benefit from conscious thought, complex issues are best left to unconscious thought, or "deliberation-without-attention."[205] The explanation of this finding is that in conscious thinking, people face a severe limit on the number of factors that they can effectively consider simultaneously and, second, that in conscious thought people "inflate the importance of some attributes at the expense of others."[206] The authors base this finding on four experiments with subjects who were asked to indicate their preference for various consumer items. The experiments involved differing levels of complexity in terms of factors to be taken into consideration. They ultimately suggest that:

> [there] is no *a priori* reason to assume that the deliberation-without-attention effect does not generalize to other types of choices – political, managerial or otherwise. In such cases, it should benefit the individual to think consciously about simple matters and to delegate thinking about more complex matters to the unconscious.[207]

It appears true that the human capacity to weigh evidence *consciously* is limited to approximately seven factors.[208] But this seven-

---

204 Malcolm Gladwell, *Blink: The Power of Thinking Without Thinking* (New York, NY: Little Brown and Company, 2005). Gladwell argues that thinking does not require detailed assessment of information. Instead, rapid cognitive responses are adequate for decisionmaking.

205 Ap Dijksterhuis, Martin W. Bos, Loran F. Nordgren, and Rick B. von Baren, "On Making the Right Choice: The Deliberation-Without-Attention Effect," *Science* 311, no. 5763 (17 February 2006), 1005. Cited hereafter as Dijksterhuis, "Deliberation-Without-Attention."

206 Dijksterhuis, "Deliberation-Without-Attention," 1005.

207 Dijksterhuis, "Deliberation-Without-Attention," 1005.

208 George A. Miller. "The Magical Number Seven, Plus or Minus Two," *The Psychological Review* 63 (1956), 87. The paper is available online: URL: < http://psychclassics.yorku.ca/Miller/>, last accessed 14 March 2006.

item limit is easily extended: people can hierarchically consider multiple sets of seven items.[209] Employing structured methods of reasoning also extends this capacity. In this context, critical thinking is at once both a structuring method and a means of assessing and monitoring the processes of selecting and using other structured methods. Additionally, "deliberation-without-attention" as applied to consumer choices in the study noted above was measuring *preferences.* Preferences change from person to person – different people conclude differently about oven mitts and cars – as the variety of these products on the market, in kitchens, or on the roads makes clear.[210]

Intelligence analysis is not about preferences; it is about best answers in ambiguous situations with high-stakes implications and consequences. As recent intelligence failures make clear, without forced consideration of alternatives, results are biased. Structured reasoning methods such as Analysis of Competing Hypotheses (ACH) develop these alternatives, allow for multiple factors to be considered fairly, and extend analyst capacities to assess complex situations as accurately as possible.

Intuition is what both Dijksterhuis and Gladwell consider in their respective works. However, exactly *what is intuition?* Rather than just appearing from nowhere, intuition is "almost always informed by experience and hard knowledge won by reasoning things out."[211] As Michael LeGault notes,

> good decisions [are] a nuanced and interwoven mental process involving bits of emotion, observation, intuition, and critical thinking....The essential background to all this is a solid base of knowledge...The broader the base, the more likely all the parts will fit together.[212]

---

209 William Reynolds, conversation with the author, 14 March 2006.

210 Oven mitts and cars are two of the categories for which Dijksterhuis and his colleagues tested.

211 LeGault, *Think*, 12.

212 LeGault, *Think*, 12.

Uninformed "intuitive thinking" contributes to intelligence failures because it fails to reflect on presuppositions. Such unexamined biases and mindsets contributed to the Cuban missile intelligence failure described above. Heuer's outline of the specific biases and mindsets that impede effective analysis is reinforced by the findings of others.[213] For example, Merom, writing about the Cuban crisis, concludes that intelligence failures occur due to a "lack of commitment to fundamental principles of investigation and analysis."[214] Although intuition or "thin slicing" may be appropriate in some domains, in intelligence analysis it appears to be associated with cognitive impediments that cause costly intelligence failures.[215]

However, as Rieber and Thomason note, testing needs to be conducted to determine which methods do work best in which situations in intelligence analysis.[216] Their work ought to go further, developing and modifying methods to overcome the very limitations they identify. For example, investigators have found that ACH suffers from confirmation bias.[217] The present author notes that this may be because non-confirmatory reasoning is so difficult for people to do.[218]

---

213 See for example, Scott Plous, *The Psychology of Judgment and Decision-making* (New York, NY: McGraw Hill, Inc., 1993); Thomas Gilovich, Dale Griffin, and Daniel Kahneman, Eds. *Heuristics and Biases: The Psychology of Intuitive Judgment* (Cambridge, UK: Cambridge University Press, 2002); and Daniel Kahneman, Paul Slovic, and Amos Tversky, eds. *Judgment under Uncertainty: Heuristics and Biases* (Cambridge, UK: Cambridge University Press, 1982).

214 Merom, "Estimate," 49.

215 Gladwell introduces the notion of "thin slicing" as a reasoning strategy in *Blink*.

216 Rieber and Thomason, "Creation of a National Institute for Analytic Methods," 76.

217 Brant A. Cheikes, Mark J. Brown, Paul E. Lehner, and Leonard Adelman, *Confirmation Bias in Complex Analyses,* Mitre Technical Report MTR 04B0000017 (Bedford, MA: Center for Integrated Intelligence Systems, October 2004).

218 The author teaches Analysis of Competing Hypotheses to both new and experienced analysts at the National Security Agency. He notes that holding a non-confirmatory attitude – which ACH, as developed by Heuer, requires – is

Finally, it may be a fallacy that conscious and unconscious reasoning are truly separate. Instead, Morgan Jones (citing work by Richard Restak) asserts that "the unconscious has a governing role in much that we consciously think and do."[219] This means that analysts commit a variety of "analytic sins," including focusing on the initially favored solution – which is also often the first satisfactory solution considered.[220] Part of the problem seems to arise from confusion about "'discussing/thinking hard' about a problem and 'analyzing' it, when the two activities are not at all the same."[221] Ultimately, the unconscious or instinctive approach to reasoning seems to "remain closed to alternatives."[222] This is an unsatisfactory model for intelligence analysis where alternatives *must* be considered.

---

extremely difficult for people to do. Since the method has value, a means of mitigating this difficulty is worth developing.

219 Jones, *Thinker's Toolkit*, 10. Jones bases his assertions and argument on the work of Richard Restak, *The Brain has a Mind of Its Own* (New York, NY: Harmony Books, 1991).

220 Jones, *Thinker's Toolkit*, 11.

221 Jones, *Thinker's Toolkit*, 11.

222 Jones, *Thinker's Toolkit*, 12.

What Does the Future Hold?

Looking ahead, new paradigms for analysis become necessary in light of the many changes occurring across the globe. Rapidly emerging twenty-first century issues and challenges stress both infrastructures and sensemaking enterprises. The changes needed to maintain an edge against adversaries becomes clear as one considers what it is that analysts do, and how and when, as table 7 illustrates.

Gregory Treverton's observations about the evolution of intelligence sensemaking and the organizations that comprise the national intelligence enterprise suggest that current "reform" efforts are merely the first steps in a much lager – and fundamental – transformation. A careful, considered examination of what intelligence must accomplish and how this can be best achieved may ensure that the goals Treverton identifies as necessary for the future are met – and met sooner rather than later. Here again critical thinking has much to offer. By encouraging discussion of the alternatives and their advantages and disadvantages, and by examining analogous cases, critical thinkers aid the transformation. Questioning of assumptions about the roles of intelligence, its activity, and organization will reveal which long-held beliefs need retirement.

Further, technology efforts in support of analysis, such as those being developed through the efforts of the ARDA – and other – advanced technology efforts presume that analysts think critically. For instance, by focusing "analytic attention on the most critical information found within massive data,"[223] some research projects seek to uncover otherwise unknown information that indicates the potential for strategic surprise.[224] These projects seek to build

223 Critical information is that which is *essential* for analysts to make sense of what their targets are going to do. Often it is buried in massive amounts of "noise."

224 Advanced Research and Development Activity, *Broad Agency Announcement for the Novel Intelligence from Massive Data (NIMD) R&D Program,* NMA401–02–BAA–0004, 7 JUNE 2002, 1.

partnerships between analysts and technology applications.[225] In one case, a research firm has developed technology that enables analysts to generate and validate novel hypotheses, distill complex systems into digestible elements, create effective narratives, and inspire creative thinking.[226] Other examples are illustrated in the adjacent text box. Follow-on research efforts such as the Collaboration and Analyst/System Effectiveness (CASE) effort will develop these efforts further.[227] The intelligence workforce these ARDA-supported efforts presuppose is being hired and trained now.

The future also holds opportunities for further developing models of reasoning in intelligence. Exactly how analogy and critical thinking interact, the roles of creative thinking, the roles of intuition, and specific strategies for bias mitigation are all areas warranting further research. Formal validation of how critical thinking improves intelligence reasoning is another research topic. Rieber and Thomason's proposed National Institute of Analytic Methods is an obvious venue for such research. Additionally, the ARDA advanced questioning and answering research program, AQUAINT, as well as other ARDA programs dealing with predictive analysis, prior and tacit knowledge, and hypothesis generation offer other domains in which such research could occur.[228] Such research is of both intrinsic value and necessary for developing new means

225 The five areas on which the NIMD effort focused were modeling analysts and how they work; analysts' prior and tacit knowledge; creating, representing, and tracking multiple scenarios, hypotheses, and/or strategies; massive data management and analysis; and the means by which analysts interact with technology. The author represented his agency in evaluating and mentoring the efforts of the researchers.

226 The author is a technical mentor of this firm's work.

227 For more information, see "Collaboration and Analyst/System Effectiveness (CASE)," AFRL Directorate: IFED BAA 06–02–IFKA, 28 October 2005, URL: <http://www.rl.af.mil/div/IFK/baa/>, last accessed 11 March 2006.

228 Advanced Research and Development Activity (ARDA), "Preliminary Solicitation Information for Advanced QUestion & Answering for INTelligence (AQUAINT)," URL: <http://www.digitalgovernment.org /library/library/pdf/preliminary_information.pdf>, last accessed 26 March 2006.

Issue	1970s and 1980s
Focus of Analysis	Continuing large, well-defined issues and adversaries
	Space for longer-term thinking
Organization and Workflow	Large, centrally organized and managed
	Hierarchical
	Institutional and operational memory mostly in analysts heads
	Time pressure persistent but low intensity (mostly)
Sources and Methods	Dominated by secret sources
	Analysts are separated from collectors
	Analysts mostly passive recipients of information
	Analysis focuses on previous patterns
	Analysts operate on basis of own experience and biases
Analysts' Characteristics	Many analysts are deep specialists
	Analysts mostly work alone or in small groups
	Key analytic choices with analysts

Table 7: Analysis: Past, Present and Future

Source: Developed by Gregory F. Treverton with input from the author.

1990s and 2000s	Future
Emergence of complex, rapidly shifting issues and adversaries	Complex, rapidly shifting issues and adversaries and large, well-defined issues and adversaries
Bias toward current intelligence	Both immediate question–answering and deeper analysis
Large, centrally organized and managed	Tailored to rapidly adapt to shifting foci
Still hierarchical, though problem-oriented "centers" added	Flat, problem-centric networks
Institutional and operational memory mostly in analysts heads	Technology helps to notice what analysts are watching and asking
Time pressure drives toward premature closure	Technology allows memory even of hypotheses, data rejected by analysts
Broader range of sources, but secrets still primary	Draws on a wide variety of sources, open and secret
Analysts are also their own collectors	Analysts are their own collectors
Limited searching of available data	Much more aggressive searching and reaching for data…both classified and unclassified
Same, though growing interest in new methods and tools for shaping, remembering, and examining hypotheses	Formative pattern recognition and data mining capabilities searches for out of the ordinary
Limited use of formal method and technology	Wide use of method and technology – from aggregating expert views to searching, data mining, pattern recognition
Many, perhaps most, analysts are generalists	Mix of generalists and deep specialists, both technical and political
Analysts mostly work alone or in small groups	Analysts work in larger virtual networks
Key analytic choices with analysts	Key analytic choices with analysts

Email exchanges 17–18 May 2006.

of improving intelligence analysis. Knowing the details of how analysts reason and how they might reason more effectively guides managers to understand where educational and training efforts can be most valuable.

TECHNOLOGICAL ADVANCES IN CRITICAL THINKING

One ARDA research team has created a technological system employing an automated critical thinking-based model that provides an overarching control structure for analytic reasoning. It includes both model generation (for counter–examples) and more traditional argument building. The system's creators assert – based on preliminary testing – that analysts employing the system are faster and more accurate problem solvers.

Suppose an analyst develops an argument in the course of using this system, that confirms that Saddam Hussein has WMD and an argument that confirms that Saddam does not have WMD. Working both sides of this issue, this analyst will make inferences from evidence and link them with other evidence-derived inferences. She will not imagine a situation in which all her evidence is true, but her hypothesis is not. For example, the evidence might include communications from which she infers that those communicating – including Saddam's scientists – believe they have WMD. Using the system, she also would be led to consider that the scientists might have wanted to deceive Saddam into believing that they were further along than they were. The generation of this alternative model can only arise through a mechanism that conducts the analyst away from the comfortable, inductive, confirmation path associated with the initial hypothesis.

Conclusion

> Never before in our peacetime history have the stakes of foreign policy been higher.
>
> —Sherman Kent, 1949

This paper posed the intriguing question: "How can intelligence analysts be 'really good'"? Critical thinking, if conceived and employed by intelligence analysts as suggested here, appears capable of leading analysts to adopt personal habits of thought appropriate to the resolution of hard intelligence problems. The idea that intelligence analysts are expected to bring to the table a capability to draw reasoned and actionable conclusions from scant and conflicting information distinguishes their charge from that of their academic brethren. Thus, intelligence analysts in government or other applied work environments may deserve the lavish budgets and technological capabilities they often enjoy.

To earn their high level of resource support, analysts can take advantage of a capability to redirect unique intelligence collection capabilities. In doing so, they are perfectly positioned to apply critical thinking methods to the hard problems. They can, for example, order up special collection against targets that exhibit even fleeting evidence that convincingly disconfirms one or more alternative hypotheses about an impending threat. This is the nub of Ben-Israel's argument for a "logical" approach to intelligence analysis for national security, and is an approach no doubt under-used by those who do not systematically think about threats in the manner developed in this paper.

Although most of the specific threats have changed since Sherman Kent first wrote in 1949, his epigraph remains as true today as it was then: the survival and prosperity of the United States remain at stake; they depend on effective, informed foreign policy.[229] Critical thinking brings with it an indispensable capability to inform a rational

229 Kent, *Strategic Intelligence,* ix.

foreign policy. "Really good analysts" are those who think critically about the issues they work and the problems they solve; they bring structured thought to the foreign policy realm.

Appendix

NSA's Critical Thinking and Structured Analysis Class Syllabus[230]

Background

Twenty-first Century intelligence issues involve uncertainty, mysteries, and risk. This differs from the 20th Century paradigms of security, secrets, and prevention. Analysis of current complex issues requires of its practitioners novel approaches including a productively imaginative process of inquiry. Questions an analyst asks not only serve as devices for attracting existing evidence, but also as devices for generating new evidence not presently considered. In this way, analysts more thoroughly examine complex issues and, aided by technology, are more likely to create novel intelligence and prevent strategic surprise.

However, such reasoning is at odds with how people – all people, including intelligence analysts – naturally think. Instead, people seek to confirm the first answer to a problem they discover, selectively using evidence to support that position *even when there is compelling evidence that an alternative hypothesis may actually be the correct one.* That people routinely fall prey to such poor thinking is well documented. Indeed, most commercial advertisers strive to take advantage of this. So do adversaries. One element of most intelligence failures includes poor thinking on the part of analysts—poor thinking of which adversaries have taken advantage. So how can analysts avoid such thinking?

One solution is to teach intelligence analysts to think critically.

230 This syllabus has been developed and refined by the author through several years of teaching critical thinking at the National Security Agency's National Cryptologic School. An early version of the course bore similarity to one developed by (then) MSGT Robert D. Folker, while a student at the (now) National Defense Intelligence College. Folker's course focused on the methods of analysis, not on the overarching critical thinking. His course (as written) is not taught at the college.

Critical thinking provides structure to the reasoning process that identifies for analysts where they are likely to go astray. It offers a means for self-reflective reasoning that leads to improved thinking. If such thinking is aided by structured analytic techniques, then analysts will (and do) improve how they resolve issues with which they are confronted. The quality of their work improves.

This critical thinking and analytic problem-solving course offers participants a chance to learn a paradigm for critical thinking and critically explore 14 different structured methods of analysis. Texts by critical thinking experts Richard Paul and Linda Elder, and structured analysis experts Morgan Jones and Richards Heuer, as well as materials developed by the instructor, teach the concepts and techniques. Classroom problems as well as operational examples (introduced and developed by the students from their own work) reinforce and help transfer what is learned into the operational environment. A final project developed by student teams completes the formal requirements.

Learning to think critically and to solve problems in a structured manner requires active participation. The class requires 40 hours of classroom time, consisting of ten sessions of four hours each. The method of instruction is Socratic, demanding active classroom participation. Participants also can expect homework, requiring both office and non-office time. Participants will prepare reading summaries for each class session, and develop one (or more) operational examples of at least one structured analytic method. Finally, participants work together on teams to complete classroom assignments and a final project dealing with an operational issue (employing at least five structured analytic methods).

Administration:

Enrollment: Up to 21 Students.
Class Date/Time/Duration: One 4-hour class per day for 10 weeks.
Class Location: _____.
Homework: Yes, but hopefully not too odious. Operational examples are required. A team project is due at the end of the course.

Texts:

Elder, Linda, and Richard Paul. *The Foundations of Analytic Thinking: How to Take Thinking Apart and What to Look for When You Do* (Dillon Beach, CA: Foundation for Critical Thinking, 2003).

Heuer, Richards J., Jr. *The Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999), URL: <http://cia.gov/csi/books/19104/index.html>, last accessed 15 March 2006.

Jones, Morgan D. *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions* in B*usiness and in Life* (New York, NY: Crown Publishing Group, 1997).

Several handouts (TBD)

Objectives:

The overall objective of the class is to enable you to critically think about analysis and what analysts are tasked to analyze. A second objective is to provide you with a set of analytic tools that are useful to your analysis. At the end of the class you will be equipped with a set of analytic skills and will have honed your critical thinking skills, allowing you to better function in the workplace. Specifically, the course objectives are as follows:

Upon completion of this course you will be able to:

- Use critical thinking techniques to provide structure to your analytic reasoning.
- Identify, describe, and employ 14 methods for structured reasoning.
- Demonstrate critical thinking proficiency through lecture, classroom participation, and weekly homework assignments.
- Complete a final class assignment using a minimum of five structured analytic methods presented in this course.
- Apply knowledge of critical thinking by using a set of analytic tools designed to hone your skills as an analyst.

In other words, at the end of this 10-week-long class, you will have

- Learned to critically analyze intelligence-associated data, information, and evidence.
- Honed your critical thinking skills.
- Built a "toolbox" of analytic and problem-solving methods.
- Become better analysts.

For example, when you approach a problem you will be able to

- Discover the true problem by restating and considering alternative outcomes.
- Have a variety of methods by which you can organize and make sense of the relevant evidence.

Formal Requirements:

Written summaries of readings. (No more than one page per chapter assigned.) The summaries should answer ***exactly*** the questions on page five of the syllabus. The summaries should also include answers to the exercises in Morgan Jones' book. The summaries will be typed unless prior arrangements have been made with the instructor. In-class discussions will draw heavily on the readings.

Problems from the work environment (Operational Exemplars). As we study the elements of reasoning and the methods of problem solving, we need operational examples

against which to apply/illustrate what we are learning. You will be responsible for providing at least one of those examples for the class to be presented during the week we discuss the method. The best exemplars may be saved for use in subsequent classes.

Final project. Working in teams of three or four, and using any Problem Restatement and Divergent and Convergent Thinking plus at least three other methods developed in the course – for a total of of at least five methods – you will develop an operational project to be presented at the last class. You will apply the elements of critical thinking to the method chosen as well as the specific problem, apply the appropriate methods to solve of problem, report the results, and evaluate the process. The project will be presented during a 15–20 minute briefing. A list of the specific elements that must be included and the format by which the project is graded is on the last page of this syllabus.

Grading:

- **Written Summaries (25%).** Due weekly. The first summary will be graded. Subsequently, a random number generator will be used to select three (3) additional summaries for grading. Grading will be based on the "Universal Intellectual Standards" in *The Foundations of Analytic Thinking* and on whether instructions are followed. For example, if you are asked to identify what key questions an author is attempting to answer, *it is expected that you will provide those questions in the reading summary.*
- **Class Participation (25%).** Since this is a discussion course, you are expected to engage in the process.
- **Operational Exemplars (25%).** Assigned the first week. No longer than 5 minutes each.
- **Final Project (25%).**

Class Descriptions and Weekly Assignments (complete prior to each class):

Class 1 – How We Don't Think and How We Might

Reading Assignment: *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life*, Chapters 1–2 (Part One).
Psychology of Intelligence Analysis, 1–30.
Critical Thinking: Concepts and Tools, entire work.

Written Assignment: *Reading summaries for chapters from Jones and Heuer. Exercises in text.*

Class Objectives: *At the end of Class 1 you will be able to:*

- Define a bias and discuss the implications of biases in our decisions.
- Identify sources of cognitive biases.
- Describe the inherent dangers/benefits of biases and the difficulty of compensating for perceptual biases.
- Describe the characteristics and three principles of perception.
- Describe how analysts fall prey to absence-of-evidence biases.
- Describe how anchoring impacts analytical decision-making.
- Describe how a target can use assimilation biases to deceive.
- Acknowledge how analysts unwittingly use confirmation bias to support early assessments.
- Discuss how hindsight and reliability biases play a part in intelligence failures.
- Describe how oversensitivity to consistency bias can lead to undesirable results.
- Discuss how expert biases and the Pollyanna and Cassandra complexes distort our thinking.
- Describe how cultural, personal, and organizational

mindsets impact analysis.

- Define mindsets, discuss how they are derived, and describe how they influence predictions.
- Identify how we think.
- Describe critical thinking and the standards used for evaluating our thinking.
- Identify the elemental structures of thought.
- Describe the differences between inferences and assumptions in intelligence analysis.

Class 2 – Critical Problem Restatement and Alternative Thinking

Reading Assignment: *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life,* Chapters 3, 5.

Written Assignment*: Reading summaries for each chapter. Exercises in text.*

Class Objectives: *At the end of Class 2 you will be able to:*

- Demonstrate knowledge of the critical thinking process by providing an example that meets the universal intellectual standards.
- Describe the role of questioning in critical thinking.
- Identify the three types of questions used in critical thinking.
- Determine the sample domains involved in complex questions.
- Define problem restatement and apply its use through a practical example.
- Discuss the role that our biases play in problem restatement.
- Demonstrate knowledge of the critical thinking process by providing an example that meets the universal intellectual standards.
- Define divergent thinking and its benefits when performing a problem restatement.
- Discuss the pitfall involved in problem definition and how it relates to problem restatement.
- Describe some effective techniques for problem restatement.
- Identify the types of problems that benefit from problem restatement.
- Discuss how points of view influence the critical thinking process.
- Discuss the logic, benefits, risks, and elements of divergent thinking.
- Identify the four main ideas of divergent thinking.

- Describe what is needed to move from divergence to convergence.
- Identify the types of problems that benefit from divergent thinking.

Class 3 – Pollyanna, Cassandra, and Marshaling

Reading Assignment: *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life*, Chapters 4, 6.

Written Assignment*: Reading summaries for each chapter. Exercises in text.*

Class Objectives: *At the end of Class 3 you will be able to:*

- Discuss the pros-cons-fixes approach to critical thinking and the six-step method employed by successful analysts.
- Identify the logic behind the pros-cons-fixes approach and discuss those critical thinking problems best suited to this method.
- Apply the techniques of sorting, chronologies, and timelines to critical thinking and identify those critical thinking problems best suited for this approach.
- Identify the two-step technique used for sorted lists, chronologies, and timelines.

Class 4 – Causes, Squares, and Shrubs

Reading Assignment: *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life*, Chapters 7, 8, 9.

Written Assignment: *Reading summaries for each chapter. Exercises in text.*

Class Objectives: *At the end of Class 4 you will be able to:*

- Discuss the purpose, logic, underlying question, evidence, concepts, and types of problems best suited for causal flow diagramming.
- Identify the major factors and cause-and-effect relationships influencing causal flow diagramming.
- Characterize the differences between direct and inverse relationships and their impact on causal flow diagramming.
- Define a feedback loop and discuss what makes it stable or unstable.
- Apply your knowledge of causal diagramming by participating in a classroom exercise.
- Discuss the purpose, logic, underlying question, evidence, concepts, and types of problems best suited for scenario matrices and trees.
- Define and discuss the characteristics and differences between matrices and scenario trees.
- Apply your knowledge of scenario matrices by participating in a classroom exercise.
- Apply your knowledge of scenario trees by participating in a classroom exercise.

Class 5 – Weighing the Likelihood

Reading Assignment: *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life*, Chapters 10, 13.

Written Assignment: *Reading summaries for each chapter. Exercises in text.*

Class Objectives: *At the end of Class 5 you will be able to:*

- Discuss how individuals view issues.
- Discuss the purpose, logic, underlying question, evidence, concepts, and types of problems best suited for weighted ranking.
- List the 9-step process involved in weighted ranking.
- Demonstrate knowledge of weighted ranking through class and small group exercises.
- Discuss the purpose, logic, underlying question, evidence, concepts, and types of problems best suited for probability.
- Define and describe how and why we characterize and assign events, and how this influences intelligence analysis.
- Discuss and explain the differences between mutually exclusive and conditionally dependent events relative to probability.
- Identify the seven steps in creating a probability tree.
- Apply your knowledge of probability by participating in a classroom exercise.

Class 6 – Testing the Devil's and Other's Advocacy

Reading Assignment: *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life,* Chapters 11–12.
The Psychology of Intelligence Analysis, Chapter 8.

Written Assignment: *Reading summaries for each chapter. Exercises in text.*

Class Objectives: *At the end of Class 6 you will be able to:*

- Define intelligence.
- Discuss the purpose, logic, underlying question, evidence, concepts, and types of problems best suited for devil's advocacy.
- Define, describe, and characterize situations appropriate to employ methods of devil's advocacy in intelligence analysis
- Demonstrate prowess in devil's advocacy through participation in a practical case study.
- Discuss the purpose, logic, underlying question, evidence, concepts, and types of problems best suited for hypothesis testing.
- Discuss the benefits of hypothesis testing.
- Identify the 8-step process of hypothesis testing.
- Demonstrate prowess in hypothesis testing through participation in a practical case study.

Class 7 – Analyzing Apples and Toyotas

Reading Assignment*: The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life*, Chapters 14, 15, 16.

Written Assignment: *Reading summaries for each chapter. Exercises in text.*

Class Objectives: *At the end of Class 7 you will be able to:*

- Describe how individual viewpoints influence utility analysis.
- Define utility analysis and discuss the type of problems best suited for this method.
- Identify the logic of utility analysis.
- Employ utility analysis to arrive at the most cost-effective solutions.
- List the steps involved in creating a utility tree and apply this knowledge by participating in classroom exercises.
- List the steps involved in creating a utility matrix and apply this knowledge by participating in classroom exercises.
- Examine the benefits of structuring as it applies to utility and probability analysis.
- Describe the differences between utility and probability analysis.
- Examine multi-perspective utility analysis and its use by participating in classroom exercises.
- List the 13 steps of multi-perspective utility analysis.
- Apply your knowledge of multi-perspective utility analysis by participating in a classroom exercise.

Class 8 – And Now for Something Completely Different

Reading Assignment: *Review all assigned readings.*

Written Assignment: *None.*

Class Objectives: *At the end of Class 8 you will be able to:*

- Describe which structured analysis methods work best in particular situations.
- Demonstrate knowledge of critical thinking and structured analysis through a practicum.
- Demonstrate your knowledge of critical thinking and structured analysis through a small group exercise.

Class 9 – Final Project Preparation

Reading Assignment: *Review all assigned readings.*

Written Assignment: *None.*

Class Objectives: *During Class 9 you will:*

- Learn through experience the pros and cons of research, analysis and reporting in small teams.

Class 10 – Final Project Presentation and Wrap-up

Reading Assignment: *Review all assigned readings.*

Written Assignment: *None.*

Class Objectives: *During Class 10:*

- Your small group will make a multi-media presentation on the analytic problem you chose.

Methods:

- A sample of the problem statement and restatement process.
- A sample of the convergent and divergent thinking applied to the problem.
- Concise demonstrations of the three structured analytic methods used to answer the analytic problem.

Assessment:

- **You are evaluated on how clearly the group presents its project, and on whether the project requirements listed above are met as shown on the last page of the syllabus.**

Reading Summary Questions:[231]

For each chapter/work, answer the following questions (in writing) about the reading.

1. What is the author's purpose? If there is more than one main point, what is the overarching purpose?

2. What are the key questions the author raises/addresses?

3. What evidence does the author provide to support his argument?

4. What inferences does the author make from the evidence?

5. On what underlying concepts does the author rely?

6. What does the author take for granted? What assumptions does the author make?

7. What are the implications of the author's point of view? What are the implications if we adopt/do not adopt what the author recommends?

8. What is the author's point of view? What other points of view are there?

231 Paul and Elder, *Concepts and Tools*, 13.

Final Project Evaluation Worksheet[232]

	Clarity	Accuracy	Precision	Relevance	Depth	Breadth	Logic	Significance	Fairness
Purpose									
Key Questions									
Assumptions									
Evidence									
A: Methods									
B: Analysis									
Concepts									
Inferences									
Implications									
Other Points of View									
Lessons Learned									
Comments									

232 Derived by author from Paul and Elder, *Concepts and Tools, 2–9.*

Bibliography

Ackerman, Robert K. "Information Age Poses New Challenges to Intelligence." *Signal* 53, no. 2 (October 1998): 23–25.

Advanced Research and Development Activity. *Broad Agency Announcement for the Novel Intelligence from Massive Data (NIMD) R&D Program.* NMA-401-02-BAA-0004, 7 June 2002, 1.

_____. "Preliminary Solicitation Information for Advanced QUestion & Answering for INTelligence (AQUAINT)." URL: <http://www.digitalgovernment.org/library/library/pdf/preliminary_information.pdf>. Last accessed 26 March 2006.

Air Force Research Laboratory (AFRL). IFED Directorate. "Collaboration and Analyst/System Effectiveness (CASE)." BAA 06-02-IFKA, 28 October 2005. URL: <http://www.rl.af.mil/div/IFK/baa/>. Last accessed 11 March 2006.

Allen, Charles E. "Intelligence: Cult, Craft, or Business?" In *Seminar on Intelligence, Command, and Control, Guest Presentations, Spring 2000.* Cambridge, MA: Harvard University Program on Information Resources Policy, I-01-1, April 2000. URL: <http://www.pirp.harvard.edu/pubs.html>. Last accessed 11 January 2006.

Allison, Graham, and Philip Zelikow. *Essence of Decision: Explaining the Cuban Missile Crisis,* 2nd Edition. New York, NY: Longman, 1999.

Amuchastegui, Domingo "Cuban Intelligence and the October Crisis." In James G. Blight and David A. Welch, Eds. *Intelligence and the Cuban Missile Crisis.* London, UK: Frank Cass, 1998: 88–119.

Anderson, Terence J., and William Twining. *Analysis of Evidence: How to Do Things with Facts Based on Wigmore's Science of Judicial Proof.* Chicago, IL: Northwestern University Press, 1991.

Anderson, Terence J., David A. Schum, and William Twining. *Analysis of Evidence.* Cambridge, UK: Cambridge University Press, 2005.

Bathurst, Robert B. *Intelligence and the Mirror: On Creating an Enemy.* Oslo, Norway: International Peace Research Institute, 1993.

Ben-Israel, Isaac. "Philosophy and Methodology of Intelligence: The Logic of the Estimate Process. *Intelligence and National Security* 4, no. 4 (October 1989): 660–718.

Blight, James G., and David A. Welch, Eds. *Intelligence and the Cuban Missile Crisis.* London, UK: Frank Cass, 1998.

Boden, Margaret A. *The Creative Mind: Myths and Mechanisms.* New York, NY: Basic Books, 1990.

Brei, William S., CAPT, USAF. *Getting Intelligence Right: The Power of Logical Procedure.* Occasional Paper Number Two. Washington, DC: Joint Military Intelligence College, January 1996.

Brent, Joseph. *Charles Sanders Peirce: A Life.* Bloomington, IN: Indiana University Press, 1998.

Brookfield, Stephen D. *Developing Critical Thinkers: Challenging Adults to Explore Alternative Ways of Thinking and Acting.* San Francisco, CA: Jossey-Bass Publishers, 1987.

Callum, Robert. "The Case for Cultural Diversity in the Intelligence Community." *International Journal of Intelligence and CounterIntelligence* 14, no. 1, Spring 2001: 25–48.

Cheikes, Brant A., Mark J. Brown, Paul E. Lehner, and Leonard Adelman. *Confirmation Bias in Complex Analyses,* Mitre Technical Report MTR 04B0000017. Bedford, MA: Center for Integrated Intelligence Systems, October 2004.

Christensen, Clayton M. *The Innovator's Dilemma: When New Technologies Cause Great Firms to Fail.* Boston, MA: Harvard Business School Press, 1997.

Christensen, Clayton M., and Michael E. Raynor. *The Innovator's Solution: Creating and Sustaining Successful Growth.* Boston, MA: Harvard Business School Press, 2003.

Christensen, Clayton M., Scott D. Anthony, and Erik A. Roth. *Seeing What's Next: Using the Theories of Innovation to Predict Industry Change.* Boston, MA: Harvard Business School Press, 2004.

"Clarke: Bush Didn't See Terrorism as 'Urgent'." *CNN.com, 19* May 2004. URL: <http://www.cnn.com/2004/ALLPOLITICS/03/24/911.commission/index.htm>. Last accessed 9 March 2006.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States.* Washington DC: Government Printing Office, March 31, 2005. URL: <http://www.wmd.gov/report/ index.html>, last accessed 28 July 2005.

Cooper, Jeffrey R. *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis.* Washington, DC: Center for the Study of Intelligence, 2005.

_____. Email to the author. 31 March 2006.

Davis, Jack. "The Kent-Kendall Debate of 1949." *Studies in Intelligence* 35, no. 2 (Summer 1991): 37–50.

De Bono, Edward. *de Bono's Thinking Course.* New York, NY: Facts on File Publications, 1982.

De Cagna, Jeff. "Making Change Happen: Steve Denning Tells the Story of Storytelling." *Information Outlook*, January 2001: 28–35.

De Rivera, Joseph. *The Psychological Dimension of Foreign Policy.* Columbus, OH: Charles E. Merrill Publishing Company, 1968.

Denning, Stephen. *The Springboard: How Storytelling Ignites Action in Knowledge-Era Organizations.* Boston, MA: Butterworth-Heinemann, 2001.

Devlin, Keith. *Goodbye Descartes: The End of Logic and the Search for a New Cosmology of the Mind.* New York, NY: John Wiley & Sons, Inc., 1997.

Dewey, John. *How We Think: A Restatement of the Relation of Reflective Thinking to the Educative Process.* New York, NY: D.C. Heath and Company, 1910.

Dijksterhuis, Ap, Martin W. Bos, Loran F. Nordgren, and Rick B. von Baren. "On Making the Right Choice: The Deliberation-Without-Attention Effect." *Science*, 311, no. 5763 (17 February 2006): 1005–1007.

DiSpezio, Michael A. *Classic Critical Thinking Puzzles.* New York, NY: Main Street, 2005.

Durkheim, Emile. *The Rules of Sociological Method.* Glencoe, IL: Free Press, 1938.

Eco, Umberto, and Thomas A. Sebeok. *The Sign of Three: Dupin, Holmes, Pierce.* Bloomington, IN: Indiana University Press, 1988

EDS. *Herding Cats*. Television advertisement produced for EDS by Fallon-McElligott. Videocassette, January 2000.

_____. *Building Airplanes in Flight.* Television advertisement produced for EDS by Fallon-McElligott. Videocassette, November 2000.

Elder, Linda, and Richard Paul. *The Foundations of Analytic Thinking: How to Take Thinking Apart and What to Look for When You Do.* Dillon Beach, CA: The Foundation for Critical Thinking, 2003.

Elliott, Michael. "How the U.S. Missed the Clues." *CNN.com*, 20 May 2002. URL: < http://archives.cnn.com/2002/ALLPOLITICS/05/20/time.clues/index.html>. Last accessed 9 March 2006.

Facione, Peter A. *Critical Thinking: What It Is and Why It Counts*. Milbrae, CA: California Academic Press, 1998, updated 2004. URL<http://www.insightassessment.com/>. Last accessed 22 July 2005.

Facione, Peter A., Noreen C. Facione, and Carol A. Giancarlo. "The Disposition Towards Critical Thinking: Its Character, Measurement, and Relationship to Critical Thinking Skill," *Informal Logic* 20, no. 1 (2000): 61–84.

_____. *Professional Judgment and the Disposition Toward Critical Thinking* (Milbrae, CA: California Academic Press, 2002). URL: < http://www.calpress.com/ pdf_files/Prof_jmn.pdf>. Last accessed 31 March 2006.

Feder, Stanley. "Factions and Policon: New Ways to Analyze Politics." In Westerfield, H. Bradford, ed. *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955–1992.* New Haven, CT: Yale University Press, 1995.

Feldman, Daniel. *Critical Thinking: Strategies for Decision Making.* Menlo Park, CA: Crisp Publications, Inc, 2002.

Fisher, Alec. *Critical Thinking: An Introduction.* Cambridge, UK: Cambridge University Press, 2001.

Folker, Robert D., MSGT, USAF. *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods.* Occasional Paper Number Seven. Washington, DC: Joint Military Intelligence College, January 2000.

Folker, Robert D., LT, USAF. Email to the author. 9 December 2003.

Fursenko, Aleksandr and Timothy Naftali. *"One Hell of a Gamble:" Khrushchev, Castro, and Kennedy, 1958–1964.* New York, NY: W. W. Norton & Company, 1997.

Garthoff, Raymond L. "US Intelligence in the Cuban Missile Crisis." In James G. Blight and David A. Welch, Eds. *Intelligence and the Cuban Missile Crisis.* London, UK: Frank Cass, 1998: 18–63.

George, Alexander. *Presidential Decisionmaking in Foreign Policy: The Effective Use of Information and Advice.* Boulder, CO: Westview Press, 1980.

Gilovich, Thomas. *How We Know What Isn't So: The Fallibility of Human Reason in Everyday Life.* New York, NY: The Free Press, 1991.

Gilovich, Thomas, Dale Griffin, and Daniel Kahneman, Eds. *Heuristics and Biases: The Psychology of Intuitive Judgment.* Cambridge, UK: Cambridge University Press, 2002.

Gladwell, Malcolm. *The Tipping Point: How Little Things Can Make a Big Difference*. Boston, MA: Little Brown and Company, 2000.

_____. *Blink: The Power of Thinking without Thinking.* Boston, MA: Little Brown and Company, 2005.

Glaser, Edward M. *An Experiment in the Development of Critical Thinking.* New York, NY: AMS Press, 1941.

Grabo, Cynthia M. *Anticipating Surprise: Analysis for Strategic Warning.* Washington DC: Joint Military Intelligence College, 2002.

Gribkov, Anatoli. "The View from Moscow and Havana." In Gribkov, Anatoli, and William Y. Smith. *Operation ANADYR: U.S. and Soviet Generals Recount the Cuban Missile Crisis.* Chicago, IL: Edition q, 1994: 3–76.

Gribkov, Anatoli, and William Y. Smith. *Operation ANADYR: U.S. and Soviet Generals Recount the Cuban Missile Crisis.* Chicago, IL: Edition q, 1994.

Halpern, Diane. *Thought and Knowledge: An Introduction to Critical Thinking,* 4th Edition. Mahwah, NJ: Lawrence Erlbaum Associates, Publishers, 2002.

Hampson, Fen Osler. "The Divided Decision-Maker: American Domestic Politics and the Cuban Crises." *International Security,* 9, no 3 (Winter 1984/85): 130-165.

Harcourt Assessment, Inc. *Local Norms Report, Watson-Glaser Critical Thinking Assessment.* Report prepared for the Defense Intelligence Agency, 2005.

Heuer, Richards J., Jr. "Strategic Deception and Counterdeception: A Cognitive Process Approach." *International Studies Quarterly* 25, no. 2 (June 1981): 294–327.

_____. *Adapting Academic Methods and Models to Governmental Needs: The CIA Experience.* Strategic Studies Institute. U.S. Army War College. July 31, 1978.

_____. *Psychology of Intelligence Analysis.* Washington, DC: CIA Center for the Study of Intelligence, 1999.

Hinsley, F. H., and Alan Stripp, Eds. *Codebreakers: The Inside Story of Bletchley Park*. Oxford, UK: Oxford University Press, 1993.

Holyoak, Keith J., and Paul Thagard. *Mental Leaps: Analogy in Creative Thought.* Cambridge, MA: The MIT Press, 1995.

Hughes, Francis J. Conversation with the author. Washington, DC: Joint Military Intelligence College. 8 May 2003.

Hughes, Francis J., and David A. Schum. *Credibility Assessment: A First Step in Intelligence Analysis.* Unpublished tutorial. Joint Military Intelligence College, April 2003.

Janis, Irving. *Groupthink: Psychological Studies of Policy Decisions and Fiascoes,* 2nd Edition. Boston, MA: Houghton Mifflin Company, 1982.

Jervis, Robert. *System Effects: Complexity in Political and Social Life.* Princeton, NJ: Princeton University Press, 1997.

Johnson Thomas R., and David A. Hatch. *NSA and the Cuban Missile Crisis.* Fort Meade, MD: National Security Agency Center for Cryptologic History, 1998. URL: <http://www.nsa.gov/publications/publi00033.cfm>. Accessed 18 April 2006

Johnston, Rob. *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study.* Washington, DC: Center for the Study of Intelligence, 2005.

Jones, Morgan D. *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving.* New York, NY: Random House, Inc, 1995.

_____. Conversation with the author. 15 December 2003.

Kahneman, Daniel, Paul Slovic, and Amos Tversky, eds. *Judgment under Uncertainty: Heuristics and Biases.* Cambridge, UK: Cambridge University Press, 1982.

Kam, Ephraim. *Surprise Attack: The Victim's Perspective*. Cambridge, MA: Harvard University Press, 1990.

Kent, Sherman. *Strategic Intelligence for American World Policy.* Princeton, NJ: Princeton University Press, 1949.

_____. "A Crucial Estimate Relived." *Studies in Intelligence* 36, no. 5 (1992): 111–119.

Kerbel, Josh. "Thinking Straight: Cognitive Bias in the US Debate about China." *Studies in Intelligence* 48, no. 3 (2004), URL: <http://cia.gov/csi/studies/vol48no3/index.html>. Last accessed 22 February 2006.

Klein, Gary. *Intuition at Work: Why Developing Your Gut Instincts Will Make You Better at What You Do.* New York, NY: Doubleday, 2003.

Krizan, Lisa. *Intelligence Essentials for Everyone.* Occasional Paper Number Six. Washington, DC: Joint Military Intelligence College, 1999.

Lebow, Richard Ned, and Janice Gross Stein. "Back to the Past: Counterfactuals and the Cuban Missile Crisis." In Philip E. Tetlock, and Aaron Belkin *Counterfactual Thought Experiments in World Politics: Logical, Methodological, and Psychological Perspectives*. Princeton, NJ: Princeton University Press, 1996: 119–148.

LeGault, Michael R. *Think: Why Crucial Decisions Can't Be Made in the Blink of an Eye.* New York, NY: Threshold Editions, 2006.

Lengel, Allan. "Little Progress in FBI Probe of Anthrax Attacks: Internal Report Compiled As Agents Hope for a Break." *Washington Post.* 16 September 2005. A01.

Lengel, Allan, and Guy Gugliotta. "Md. Pond Produces No Anthrax Microbes: FBI Sought Clues In Deadly Attacks." *Washington Post.* 1 August 2003. A03.

Lipman, Matthew. *Thinking in Education,* 2nd Edition. Cambridge, UK: Cambridge University Press, 2003.

Lundahl, Arthur C. "Additional Information—Mission 3102." Memorandum for Director of Central Intelligence and Director, Defense Intelligence Agency, 15 October 1962. In Mary S. McAuliffe, ed., *CIA Documents on the Cuban Missile Crisis, 1962.* Washington DC: Central Intelligence Agency, 1992: 181–182.

_____. "Additional Information—Mission 3107." Memorandum for Director of Central Intelligence and Director, Defense Intelligence Agency, 19 October 1962. In Mary S. McAuliffe, ed., *CIA Documents on the Cuban Missile Crisis, 1962*. Washington DC: Central Intelligence Agency, 1992: 209.

McAuliffe, Mary S., ed. *CIA Documents on the Cuban Missile Crisis, 1962* Washington DC: Central Intelligence Agency, 1992.

Marrin, Stephen. "Homeland Security and the Analysis of Foreign Intelligence," Markle Foundation Task Force on National Security in the Information Age, 15 July 2002, URL: <www.markletaskforce.org/documents/marrin_071502.pdf>. Last accessed December 9, 2003.

_____. Email to the author, 8 December 2003.

_____. "CIA's Kent School: Improving Training for New Analysts." *International Journal of Intelligence and CounterIntelligence* 16, no. 4 (Winter 2003–2004): 609–637.

May, Ernest R. *Lessons of the Past: The Use and Misuse of History in American Foreign Policy.* Oxford, UK: Oxford University Press, 1973.

Merom, Gil. "The 1962 Cuban Intelligence Estimate: A Methodological Perspective." *Intelligence and National Security*, 14, no. 3 (Autumn 1999): 48–80.

Mid-Level Intelligence Professional. National Security Agency. Email to the author, 9 March 2006.

Miller, George A. "The Magical Number Seven, Plus or Minus Two." *The Psychological Review* 63 (1956): 81–97.

Miller, Judith. "A Battle of Words over War Intelligence." *New York Times.* Online edition, 22 November 2003. URL: <www.nytimes.com/2003/11/22/arts/22INTE.html>. Last accessed November 28, 2003.

Millward, William. "Life in and out of Hut 3." In Hinsley, F. H., and Alan Stripp, Eds. *Codebreakers: The Inside Story of Bletchley Park.* Oxford, UK: Oxford University Press, 1993: 17–29.

Moore, David T. *Creating Intelligence: Evidence and Inference in the Analysis Process.* MSSI Thesis. Washington, DC: Joint Military Intelligence College, July 2002.

_____. "Species of Competencies for Intelligence Analysis." *Defense Intelligence Journal* 11, no. 2 (Summer 2002): 97–119.

_____. Personal Notes. Joint Military Intelligence College, Denial and Deception Advanced Studies Program, Spring 2005.

Moore David T., and Lisa Krizan. "Intelligence Analysis: Does NSA Have What it Takes." Reprint: NSA Center for Cryptologic History. *Cryptologic Quarterly,* 20, nos 1/2 (Summer/Fall 2001): 1–33.

_____. "Core Competencies for Intelligence Analysis at the National Security Agency." In Swenson, Russell G., ed. *Bringing Intelligence About: Practitioners Reflect on Best Practices.* Washington DC: Joint Intelligence Military College, 2003: 95–132.

Moore, David T., Lisa Krizan, and Elizabeth J. Moore. "Evaluating Intelligence: A Competency-Based Model." *International Journal of Intelligence and Counterintelligence* 18, no. 2 (Summer 2005): 204–220.

Myers, David G. *Intuition: Its Powers and Perils.* New Haven, CT: Yale University Press, 2002.

Negroponte, John D., Director of National Intelligence. *National Intelligence Strategy of the United States of America.* Washington, DC: Office of the Director of National Intelligence, October 2005. URL: <http://www.dni.gov/NISOctober2005.pdf>. Last accessed 12 March 2006.

Neustadt, Richard E., and Ernest R. May. *Thinking in Time: The Uses of History for Decision Makers.* New York, NY: The Free Press, 1986.

Oberdorfer, Don. "Missed Signals in the Middle East." *Washington Post Magazine*, 17 March 1991.

Paul, Richard W. "A Draft Statement of Principles." The National Council for Excellence in Critical Thinking. URL: <www.criticalthinking.org/ncect.html>. Last accessed March 18, 2003.

Paul, Richard W., and Linda Elder. *The Miniature Guide to Critical Thinking Concepts and Tools*, 4th Edition. Dillon Beach, CA: The Foundation for Critical Thinking, 2004.

Paul, Richard W., and Gerald Nosich. *A Model for the National Assessment of Higher Order Thinking.* Dillon Beach, CA: Foundation for Critical Thinking, n.d.

Paul, Richard W., Linda Elder, and Ted Bartell. "Executive Summary, Study of 38 Public Universities and 28 Private Universities To Determine Faculty Emphasis on Critical Thinking In Instruction." *California Teacher Preparation for Instruction in Critical Thinking: Research Findings and Policy Recommendations.* California Commission on Teacher Credentialing, Sacramento, California, 1997. Dillon, CA: Foundation for Critical Thinking, 1997. URL: <criticalthinking.org/schoolstudy.htm>. Last accessed March 18, 2003.

Paul, Richard W., Linda Elder, and Ted Bartell. *California Teacher Preparation for Instruction in Critical Thinking: Research Findings and Policy Recommendations.* California Commission on Teacher Credentialing, Sacramento California, 1997. Dillon, CA: Foundation for Critical Thinking, 1997.

Perrow, Charles. *Normal Accidents: Living with High-Risk Technologies.* Princeton, NJ: Princeton University Press, 1999.

Pettee, George S. *The Future of American Secret Intelligence.* Washington, DC: Infantry Journal Press, 1946.

Platt, Washington. *Strategic Intelligence Production: Basic Principles.* New York, NY: Frederick A. Praeger, 1957.

Plous, Scott. *The Psychology of Judgment and Decision-Making.* New York, NY: McGraw Hill, Inc., 1993.

Raasa, Paul J. "The Denial and Deception Challenge to Intelligence." In Godson, Roy, and James J. Wirtz, *Strategic Denial and Deception.* New Brunswick, NJ: Transaction Publishers, 2002: 223–228.

Reed, Jennifer H. *Effect of a Model For Critical Thinking on Student Achievement In Primary Source Document Analysis And Interpretation, Argumentative Reasoning, Critical Thinking Dispositions, and History Content in a Community College History Course.* PhD Dissertation. College of Education, University of South Florida, December 1998. URL: <http://www.criticalthinking.org/resources/JReed-Dissertation.pdf>. Last accessed 6 May 2006.

Restak, Richard, M.D. *The Brain Has a Mind of Its Own: Insights from a Practicing Neurologist.* New York, NY: Harmony Books, 1991.

Reynolds, William. Conversation with the author, 14 March 2006.

Rieber, Steven, and Neil Thomason. "Toward Improving Intelligence Analysis: Creation of a National Institute for Analytic Methods." *Studies in Intelligence* 49, no. 4 (Winter 2006): 71–80.

Schafersman, Steven D. "An Introduction to Critical Thinking," January 1991. URL: <www.freeinquiry.com/critical-thinking.html>. Last accessed 9 March 2006.

Schecter Jerrold L., and Peter S. Deriabin. *The Spy Who Saved the World.* New York, NY: Scribner's, 1992.

Schum, David A. *Evidence and Inference for the Intelligence Analyst,* 2 volumes. Lanham, MD: University Press of America, 1987.

_____. *Evidential Foundations of Probabilistic Reasoning.* New York, NY: John Wiley & Sons, Inc., 1994.

_____. "Species of Abductive Reasoning in Fact Investigation in Law" *Cardozo Law Review* 22, nos. 5/6 (July 2001): 1645–1681.

_____. "Evidence Marshaling for Imaginative Fact Investigation." *Artificial Intelligence and Law* 9 (2001): 165–188.

Sebeok, Thomas A. "One, Two, Three Spells UBERTY." In Umberto Eco and Thomas A. Sebeok. *The Sign of Three: Dupin, Holmes, Pierce.* Bloomington, IN: Indiana University Press, 1988: 1–10.

Senate Select Committee On Intelligence. *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq.* United States Senate. 108th Congress, 7 July 2004.

Simon, Herbert A. "Invariants of Human Behavior." *Annual Review of Psychology* 41 (1990):1–19.

Stefik, Mark, and Barbara Stefik. *Breakthrough: Stories and Strategies of Radical Innovation.* Cambridge, MA: MIT Press, 2004.

Swenson, Russell G., ed. *Research: Design and Methods.* Washington, DC: Joint Intelligence Military College, 2000.

_____. *Bringing Intelligence About: Practitioners Reflect on Best Practices.* Washington, DC: Joint Intelligence Military College, 2003.

Tetlock, Philip E. *Expert Political Judgment: How Good Is It? How Can We Know?* Princeton, NJ: Princeton University Press, 2005.

Tetlock, Philip E. and Aaron Belkin. *Counterfactual Thought Experiments in World Politics: Logical, Methodological, and Psychological Perspectives.* Princeton, NJ: Princeton University Press, 1996.

Thagard, Paul. *Coherence in Thought and Action.* Cambridge, MA: The MIT Press, 2000.

Treverton, Gregory F. Conversation with the author, 18 May 2006.

_____. Email exchanges with the author, 17–18 May 2006.

U.S. Congress. *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001.* Report of the U.S. Senate Select Committee on Intelligence and U.S. House Permanent Select Committee on Intelligence, Together with Additional Views. Senate Report No. 107-351/House Report. No. 107-792. 107th Congress, 2nd Session. December 2002.

U.S. Department of Defense. Photograph in the John Fitzgerald Kennedy Library. Boston, MA. PX 66-20:7 14 October 1962.

White, Mark J. *Missiles in Cuba: Kennedy, Khrushchev, Castro, and the 1962 Crisis.* Chicago, IL: Ivan R. Dee, 1997.

Wikipedia. "The Free Encyclopedia." URL: <www.wkikpedia.org>. Last accessed 12 March 2006.

Wirtz, James J. "Organizing for Crisis Intelligence: Lessons form the Cuban Missile Crisis." In James G. Blight and David A. Welch, Eds. *Intelligence and the Cuban Missile Crisis.* London, UK: Frank Cass, 1998: 120–149.

Wohlstetter, Roberta. "Cuba and Pearl Harbor: Hindsight and Foresight." *Foreign Affairs* 46, no. 3 (July 1965): 691–707.

Woods, Kevin, James Lacey, and Williamson Murray. "Saddam's Delusions: The View from the Inside," *Foreign Affairs*, 85, no. 3 (May/June 2006). URL: <http://www.foreignaffairs.org/20060501faessay85301/kevin-woods-james-lacey-williamson-murray/saddam-s-delusions-the-view-from-the-inside.html>. Accessed 31 March 2006.

Woods, Kevin M., Michael R. Pease, Mark E. Stout, Williamson Murray, and James G. Lacey, *Iraqi Perspectives Project: A View of Operation Iraqi Freedom from Saddam's Senior Leadership*. Norfolk, VA: Joint Center for Operational Analysis, 2006. URL: <http://www.foreignaffairs.org/special/iraq/ipp.pdf>. Last accessed 31 March 2006.

Zlotnick, Jack. "Bayes' Theorem for Intelligence Analysis." *Studies in Intelligence* 11, no. 4 (Spring 1972): 1–12. URL: <http://cia.gov/csi/kent_csi/pdf/v08i4a11p.pdf#page=1>. Last accessed 7 April 2006.

About the Author

David T. Moore is a career senior intelligence analyst and technical director at the National Security Agency where he is an advocate for, and mentor of best practices in intelligence analysis. He is an adjunct faculty member of the National Cryptologic School; has taught at the National Defense Intelligence College, Washington, DC; and at Trinity University, Washington, DC. Mr. Moore holds a B.A. in sociology from Washington and Lee University and a Master of Science of Strategic Intelligence from the National Defense Intelligence College (formerly the Joint Military Intelligence College).

Mr. Moore's other publications include:

- "Species of Competencies for Intelligence Analysis," *Defense Intelligence Journal,* 11, no. 2 (Summer 2002): 97-119.
- "Species of Competencies for Intelligence Analysis," *American Intelligence Journal*, 23 (2005): 29–43 (an expanded version of the original article).
- With coauthor Lisa Krizan:
    - "Intelligence Analysis, Does NSA Have What it Takes," *Cryptologic Quarterly,* 20, nos. 1/2 (Summer/Fall 2001): 1-32.
    - "Core Competencies for Intelligence Analysis at the National Security Agency," in *Bringing Intelligence About: Practitioners Reflect on Best Practices,* Russell Swenson, ed. (2004): 95-131.
- With coauthors Lisa Krizan and Elizabeth J. Moore
    - "Evaluating Intelligence: A Competency-Based Approach," in the *International Journal of Intelligence and CounterIntelligence*, 18, no. 2 (Summer 2005): 204-220.
- With coauthor William N. Reynolds:
    - "So Many Ways To Lie: The Complexity of Denial and Deception," *Defense Intelligence Journal,* 15, no. 2 (Fall 2006): 95-116.

Colophon

A colophon records the details of the layout and design of a publication. It acknowledges the craftsmanship and art required in creating a printed work. Whereas the acknowledgements record the textual assistance an author receives, a colophon records the equally important technical assistance received.

This Occasional Paper was set in Baskerville, a transitional typeface created by Birmingham printer John Baskerville around 1752. George Jones redesigned it in 1930 for Linotype-Hell; the International Typeface Corporation licensed it in 1982. The long, elegant serifs and the subtle transfer of stroke weight from thick to very thin give it a delicacy and grace that makes it an excellent text typeface. Titling and primary headings were set in Castellar, a Monotype typeface created by John Peters in 1957. Named after a town in the Alps, Castellar also was designed for refined display work. Tables were set in Gill Sans, designed by artist and type designer Eric Gill in 1931 for Monotype. Unlike many sans serif typefaces it is highly legible and readable in text. The cover was set in Californian, a typeface originally designed by Frederic Goudy in 1938 and adapted by various designers for the Font Bureau.

This publication was composed on an Apple iMac and a Macbook Pro using Adobe Systems InDesign. Masters were created in Adobe Acrobat. Illustrations were prepared in Omni Systems Omni Graffle and Adobe Photoshop.

Baskerville, Californian, Castellar, Gill Sans, iMac, Macbook Pro, Acrobat, InDesign, Omni Graffle, and Photoshop are registered trademarks of their respective companies.

Desktop composition by the author.

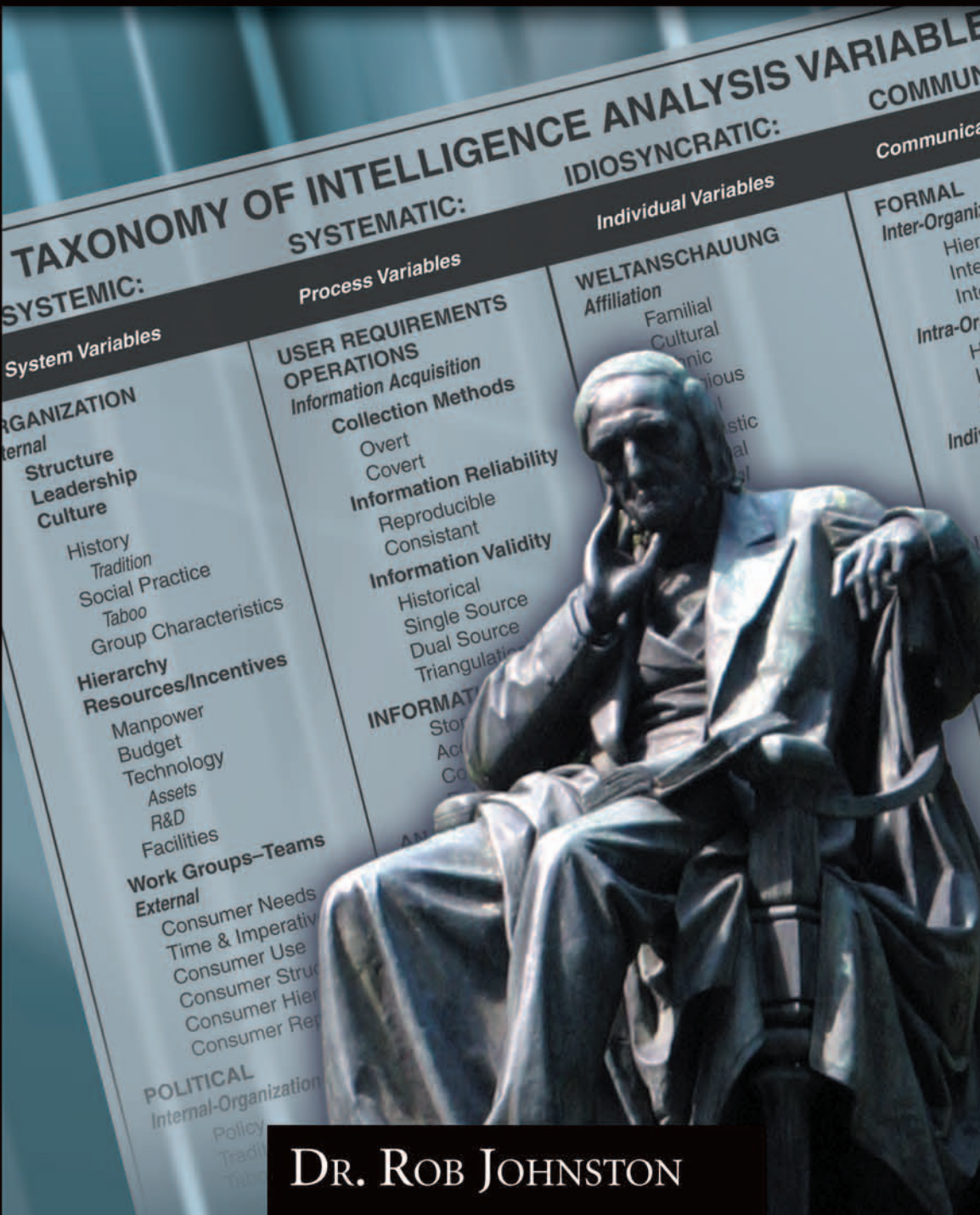
The cover was designed by Bridgette White.

Published by the National Defense Intelligence College Press, May 2006; and by the National Defense Intelligence College Foundation, March 2007. Printed at the Defense Intelligence Agency, Washington DC.

This Page Is Intentionally Left Blank

Analytic Culture in the U.S. Intelligence Community

An Ethnographic Study



Dr. Rob Johnston

All statements of fact, opinion, or analysis expressed in this book are those of the authors. They do not necessarily reflect official positions of the Central Intelligence Agency or any other US government entity, past or present. Nothing in the contents should be construed as asserting or implying US government endorsement of the authors' factual statements and interpretations.

The Center for the Study of Intelligence

The Center for the Study of Intelligence (CSI) was founded in 1974 in response to Director of Central Intelligence James Schlesinger's desire to create within CIA an organization that could "think through the functions of intelligence and bring the best intellects available to bear on intelligence problems." The Center, comprising professional historians and experienced practitioners, attempts to document lessons learned from past operations, explore the needs and expectations of intelligence consumers, and stimulate serious debate on current and future intelligence challenges.

To support these activities, CSI publishes *Studies in Intelligence* and books and monographs addressing historical, operational, doctrinal, and theoretical aspects of the intelligence profession. It also administers the CIA Museum and maintains the Agency's Historical Intelligence Collection.

Comments and questions may be addressed to:

Center for the Study of Intelligence
Central Intelligence Agency
Washington, DC 20505

Printed copies of this book are available to requesters outside the US government from:

Government Printing Office (GPO)
Superintendent of Documents
P.O. Box 391954
Pittsburgh, PA 15250-7954
Phone: (202) 512-1800
E-mail: orders@gpo.gov

ISBN: 1-929667-13-2

Analytic Culture in the US Intelligence Community

The Center *for the* Study *of* Intelligence

Central Intelligence Agency

Washington, DC 20505

Library of Congress Cataloguing-in-Publication data

Johnston, Rob

Analytic Culture in the US Intelligence Community: An Ethnographic Study/
Dr. Rob Johnston

Includes bibliographic references.

ISBN 1-929667-13-2 (pbk.:alk paper)

1. Intelligence—United States. 2. Intelligence analysis.
3. Intelligence policy. 4. Intelligence training.

Typeset in Times and Ariel.

Printed by Imaging and Publication Support, CIA.

Cover design: Imaging and Publication Support, CIA.

The pensive subject of the statue is Karl Ernst von Baer (1792–1876), the Prussian-Estonian pioneer of embryology, geography, ethnology, and physical anthropology (Jane M. Oppenheimer, Encyclopedia Brittanica*).*

ANALYTIC CULTURE IN THE US INTELLIGENCE COMMUNITY

AN ETHNOGRAPHIC STUDY

DR. ROB JOHNSTON

Center *for the* Study *of* Intelligence

Central Intelligence Agency

Washington, DC

2005

ACKNOWLEDGEMENTS

There are literally slightly more than 1,000 people to thank for their help in developing this work. Most of them I cannot name, for one reason or another, but my thanks go out to all of those who took the time to participate in this research project. Thank you for your trust. Particular thanks are due the other researchers who coauthored chapters: Judith Meister Johnston, J. Dexter Fletcher, and Stephen Konya.

There is a long list of individuals and institutions deserving of my gratitude, but, at the outset, for making this study possible, I would like to express my appreciation to Paul Johnson and Woody Kuhns, the chief and deputy chief of the Central Intelligence Agency's Center for the Study of Intelligence, and their staff for their support and to John Phillips and Tom Kennedy of the Intelligence Technology Innovation Center who, along with their staff, administer the Director of Central Intelligence Postdoctoral Fellowship Program.

I would like to thank Greg Treverton and Joe Hayes for their help throughout this project and for their willingness to give of their time. Dr. Forrest Frank, Charles Perrow, and Matthew Johnson deserve recognition for the material they contributed. Although it was not possible to cite them as references for those contributions, these are indicated in the footnotes, and I give them full credit for their work and efforts.

I would also like to thank Bruce Berkowitz, Mike Warner, Fritz Ermarth, Gordon Oehler, Jeffrey Cooper, Dave Kaplan, John Morrison, James Wirtz, Robyn Dawes, Chris Johnson, Marilyn Peterson, Drew Cukor, Dennis McBride, Paul Chatelier, Stephen Marrin, Randy Good, Brian Hearing, Phil Williams, Jonathan Clemente, Jim Wilson, Dennis, Kowal, Randy Murch, Gordie Boezer, Steve Holder, Joel Resnick, Mark Stout, Mike Vlahos, Mike Rigdon, Jim Silk, Karl Lowe, Kevin O'Connell, Dennis Gormley, Randy Pherson, Chris Andrew, Daniel Serfaty, Tom Armour, Gary Klein, Brian Moon, Richard Hackman, Charlie Kisner, Matt McKnight, Joe Rosen, Mike Yared, Jen Lucas, Dick Heuer, Robert Jervis, Pam Harbourne, Katie Dorr,

Dori Akerman, and, most particularly, my editors: Mike Schneider, Andy Vaart, and Barbara Pace. Special thanks are also due Adm. Dennis Blair, USN (Ret.), and Gen. Larry Welch, USAF (Ret.), and their staff.

There were 50 peer reviewers who made sure I did not go too far afield in my research and analysis. Again, there are mitigating reasons why I cannot thank them by name. Suffice it to say, their work and their time were invaluable, and I appreciate their efforts.

Because I cannot name specific individuals, I would like to thank the organizations of the Intelligence Community that gave me access to perform this research and made available research participants: Air Force Intelligence; Army Intelligence; Central Intelligence Agency; Defense Intelligence Agency; Department of Energy; Department of Homeland Security; Bureau of Intelligence and Research, Department of State; Department of the Treasury; Federal Bureau of Investigation; Marine Corps Intelligence; National Geospatial Intelligence Agency; National Reconnaissance Office; National Security Agency; Navy Intelligence.

Thanks are also due the following: Institute for Defense Analyses; the Sherman Kent Center and the Global Futures Partnership at the CIA University; the CIA's Publications Review Board; Office of Public Affairs, National Archives; Joint Military Intelligence College; Advanced Research and Development Activity, Defense Advanced Research Projects Agency (DARPA); International Association of Law Enforcement Intelligence Analysts; Drug Enforcement Administration and the DEA Academy; FBI Academy; National Military Intelligence Association; Association of Former Intelligence Officers; MITRE; RAND; Analytic Services, Inc. (ANSER); Potomac Institute; Center for Strategic and International Studies; Woodrow Wilson International Center; Booz Allen Hamilton; Naval Postgraduate School; Columbia University; Dartmouth College; University of Pittsburgh; Georgetown University; Carnegie Mellon University; Cambridge University; Johns Hopkins University and the Advanced Physics Laboratory; George Mason University; Harvard University; Yale University; American Anthropological Association; Society for the Anthropology of Work; Society for Applied Anthropology; National Association for the Practice of Anthropology; Inter-University Seminar on Armed Forces and Society; Royal Anthropological Institute, and the national laboratories.

I express my sincere apologies if I have failed to include any individuals or organizations to which thanks are due. Moreover, any errors of commission or omission are my own. God knows, with this much help, there is no one to blame but myself. Mostly, though, I would like to thank my long-suffering wife, to whom this book is dedicated. Thanks, Jude.

CONTENTS

Foreword by Gregory F. Treverton xi

Introduction xiii

Background xiv
Scope xvii
A Work in Progress xix

Part I: Research Findings

Chapter One: Definitions 3

Chapter Two: Findings 9

The Problem of Bias 10
Finding: Secrecy Versus Efficacy 11
Finding: Time Constraints 13
Finding: Focus on Current Production 15
Finding: Rewards and Incentives 16
Finding: "Tradecraft" Versus Scientific Methodology 17
Finding: Confirmation Bias, Norms, and Taboos 21
Finding: Analytic Identity 25
Finding: Analytic Training 28

Part II: Ethnography of Analysis

Chapter Three: A Taxonomy of Intelligence Variables 33

Intelligence Analysis 34
Developing the Taxonomy 37
Systemic Variables 39
Systematic Variables 40
Idiosyncratic Variables 41
Communicative Variables 42
Conclusion 43

Chapter Four: Testing the Intelligence Cycle Through Systems Modeling and Simulation 45

The Traditional Intelligence Cycle 45
Systematic Analysis 47
Findings Based on Systematic Analysis 47
Systemic Analysis 50

Findings Based on Systems Analysis 54
Recommendations 55

Part III: Potential Areas for Improvement

Chapter Five: Integrating Methodologists into Teams of Experts 61

Becoming an Expert 61
The Power of Expertise 63
The Paradox of Expertise 64
The Burden on Intelligence Analysts 66
The Pros and Cons of Teams 68
Can Technology Help? 71
Analytic Methodologists 72
Conclusion 72

Chapter Six: The Question of Foreign Cultures:
Combating Ethnocentrism in Intelligence Analysis 75

Case Study One: Tiananmen Square 76
Case Study Two: The Red Team 81
Conclusion and Recommendations 84

Chapter Seven: Instructional Technology:
Effectiveness and Implications for the Intelligence Community 87

Background 88
Meta-analysis Demonstrates the Effectiveness of
Instructional Technology 90
Current Research on Higher Cognitive Abilities 92
Discussion 94
Conclusion 96

Chapter Eight: Organizational Culture:
Anticipatory Socialization and Intelligence Analysts 97

Organizational Socialization 98
Anticipatory Socialization 99
Consequences of Culture Mismatch 101
Anticipatory Socialization in the Intelligence Community 102
Conclusion and Recommendations 104

Chapter Nine: Recommendations 107

The First Step: Recognizing A Fundamental Problem 107
Performance Improvement Infrastructure 108
Infrastructure Requirements 108
Research Programs 111
The Importance of Access 115

Part IV: Notes on Methodology

Chapter Ten: Survey Methodology 119

Methodology 120
Demographics 124

Chapter Eleven: Q-Sort Methodology 127

Chapter Twelve: The "File-Drawer" Problem and
Calculation of Effect Size 129

Appendix: Selected Literature 133

Intelligence Tools and Techniques 133
Cognitive Processes and Intelligence 134
Tools and Techniques as Cognitive Processes 134
Intelligence Analysis as Individual Cognitive Process 135
Error 135
Language and Cognition 136

Bibliography..... 139

Published Sources 139
Web resources 157

Afterword by Joseph Hayes 159

The Author 161

FOREWORD

Gregory F. Treverton

It is a rare season when the intelligence story in the news concerns intelligence analysis, not secret operations abroad. The United States is having such a season as it debates whether intelligence failed in the run-up to both September 11 and the second Iraq war, and so Rob Johnston's wonderful book is perfectly timed to provide the back-story to those headlines. The CIA's Center for the Study of Intelligence is to be commended for having the good sense to find Johnston and the courage to support his work, even though his conclusions are not what many in the world of intelligence analysis would like to hear.

He reaches those conclusions through the careful procedures of an anthropologist—conducting literally hundreds of interviews and observing and participating in dozens of work groups in intelligence analysis—and so they cannot easily be dismissed as mere opinion, still less as the bitter mutterings of those who have lost out in the bureaucratic wars. His findings constitute not just a strong indictment of the way American intelligence performs analysis, but also, and happily, a guide for how to do better.

Johnston finds no baseline standard analytic method. Instead, the most common practice is to conduct limited brainstorming on the basis of previous analysis, thus producing a bias toward confirming earlier views. The validating of data is questionable—for instance, the Directorate of Operation's (DO) "cleaning" of spy reports doesn't permit testing of their validity—reinforcing the tendency to look for data that confirms, not refutes, prevailing hypotheses. The process is risk averse, with considerable managerial conservatism. There is much more emphasis on avoiding error than on imagining surprises. The analytic process is driven by current intelligence, especially the CIA's crown jewel analytic product, the *President's Daily Brief* (PDB), which might be caricatured

as "CNN plus secrets." Johnston doesn't put it quite that way, but the Intelligence Community does more reporting than in-depth analysis.

None of the analytic agencies knows much about the analytic techniques of the others. In all, there tends to be much more emphasis on writing and communication skills than on analytic methods. Training is driven more by the druthers of individual analysts than by any strategic view of the agencies and what they need. Most training is on-the-job.

Johnston identifies the needs for analysis of at least three different types of consumers—cops, spies, and soldiers. The needs of those consumers produce at least three distinct types of intelligence—investigative or operational, strategic, and tactical.

The research suggests the need for serious study of analytic methods across all three, guided by professional methodologists. Analysts should have many more opportunities to do fieldwork abroad. They should also move much more often across the agency "stovepipes" they now inhabit. These movements would give them a richer sense for how other agencies do analysis.

Together, the analytic agencies should aim to create "communities of practice," with mentoring, analytic practice groups, and various kinds of on-line resources, including forums on methods and problem solving. These communities would be linked to a central repository of lessons learned, based on after-action post-mortems and more formal reviews of strategic intelligence products. These reviews should derive lessons for individuals and for teams and should look at roots of errors and failures. Oral and written histories would serve as other sources of wherewithal for lessons. These communities could also begin to reshape organizations, by rethinking organizational designs, developing more formal socialization programs, testing group configurations for effectiveness, and doing the same for management and leadership practices.

The agenda Johnston suggests is a daunting one, but it finds echoes in the work of small, innovative groups across the Intelligence Community—groups more tolerated than sponsored by agency leaders. With the challenge workforce demographics poses for the Community—the "gray-green" age distribution, which means that large numbers of new analysts will lack mentors as old hands retire—also comes the opportunity to refashion methods and organizations for doing intelligence analysis. When the finger-pointing in Washington subsides, and the time for serious change arrives, there will be no better place to start than with Rob Johnston's fine book.

INTRODUCTION

In August 2001, I accepted a Director of Central Intelligence postdoctoral research fellowship with the Center for the Study of Intelligence (CSI) at the Central Intelligence Agency. The purpose of the fellowship, which was to begin in September and last for two years, was to identify and describe conditions and variables that negatively affect intelligence analysis. During that time, I was to investigate analytic culture, methodology, error, and failure within the Intelligence Community using an applied anthropological methodology that would include interviews (thus far, there have been 489), direct and participant observation, and focus groups.

I began work on this project four days after the attack of 11 September, and its profound effect on the professionals in the Intelligence Community was clearly apparent. As a whole, the people I interviewed and observed were patriotic without pageantry or fanfare, intelligent, hard working, proud of their profession, and angry. They were angry about the attack and that the militant Islamic insurgency about which they had been warning policymakers for years had murdered close to 3,000 people in the United States itself. There was also a sense of guilt that the attack had happened on their watch and that they had not been able to stop it.

Having occurred under the dark shadow of that attack, this study has no comparable baseline against which its results could be tested, and it is difficult to identify biases that might exist in these data as a result of 11 September. In some ways, post-9/11 data may be questionable. For example, angry people may have an ax to grind or an agenda to push and may not give the most reliable interviews. Yet, in other ways, post-9/11 data may be more accurate. When people become angry enough, they tend to blurt out the truth—or, at least, their perception of the truth. The people I encountered were, in my judg-

ment, very open and honest; and this, too, may be attributable to 9/11. In any case, that event is now part of the culture of the Intelligence Community, and that includes whatever consequences or biases resulted from it.

Background

The opportunity to do this research presented itself, at least in part, as a result of my participation in a multiyear research program on medical error and failure for the Defense Advanced Research Projects Agency (DARPA).[1] The DARPA research focused on team and individual error in minimally invasive or laparoscopic surgical procedures. This research revealed that individual errors were cognitive rather than purely psychomotor or skill-based. For example, some surgeons had trouble navigating three-dimensional anatomical space using the existing laparoscopic technology, with the result that these surgeons would identify anatomical structures incorrectly and perform a surgical procedure on the wrong body part.

Other individual errors were discovered during the DARPA studies, but, for the most part, these were spatial navigation and recognition problems for which there were technological solutions. Team errors, unlike individual errors, proved to be more challenging. The formal and informal hierarchical structures of operating rooms did not lend themselves to certain performance interventions. Generally, junior surgical staff and support personnel were not willing to confront a senior staff member who was committing, or was about to commit, an error.

The culture of the operating room, coupled with the social and career structure of the surgical profession, created barriers to certain kinds of communication. For a surgical resident to inform a senior surgeon in front of the entire operating room staff that he was about to cut the wrong organ could result in career "suicide." Such a confrontation could have been perceived by the senior surgeon as a form of mutiny against his authority and expertise and a challenge to the social order of the operating room. Although not universal, this taboo is much more common than surgeons would care to admit. Unlike individual errors, purely technological solutions were of little value in trying to solve team errors in a surgical environment.

The DARPA surgical research was followed up by a multiyear study of individual and team performance of astronauts at the National Aeronautics and Space Administration's (NASA) Johnson Space Center. Results of the NASA study, also sponsored by DARPA, were similar to the surgical study

[1] Rob Johnston, J. Dexter Fletcher and Sunil Bhoyrul, *The Use of Virtual Reality to Measure Surgical Skill Levels*.

with regard to team interactions. Although, on the face of it, teams of astronauts were composed of peers, a social distinction nevertheless existed between commander, pilots, and mission specialists.

As with surgery, there was a disincentive for one team member to confront or criticize another, even in the face of an impending error. Eighty percent of the current astronauts come from the military, which has very specific rules regarding confrontations, dissent, and criticism.[2] In addition to the similarities in behavior arising from their common backgrounds, the "criticism" taboo was continually reinforced throughout the astronaut's career. Virtually any negative comment on an astronaut's record was sufficient for him or her to be assigned to another crew, "washed out" of an upcoming mission and recycled through the training program, or, worse still, released from the space program altogether.

Taboos are social markers that prohibit specific behaviors in order to maintain and propagate an existing social structure. Generally, they are unwritten rules not available to outside observers. Insiders, however, almost always perceive them simply as the way things are done, the natural social order of the organization. To confront taboos is to confront the social structure of a culture or organization.

I mention the surgical and astronautical studies for a number of reasons. Each serves as background for the study of intelligence analysts. Astronauts and surgeons have very high performance standards and low error rates.[3] Both studies highlight other complex domains that are interested in improving their own professional performance. Both studies reveal the need to employ a variety of research methods to deal with complicated issues, and they suggest that there are lessons to be learned from other domains. Perhaps the most telling connection is that, because lives are at stake, surgeons and astronauts experience tremendous internal and external social pressure to avoid failure. The same often holds for intelligence analysts.

In addition, surgery and astronautics are highly selective and private disciplines. Although their work is not secret, both groups tend to be shielded from the outside world: surgeons for reasons of professional selection, training, and the fiscal realities of malpractice liability; astronauts because their community

---

[2] National Aeronautics and Space Administration, *Astronaut Fact Book*.

[3] NASA has launched missions with the shuttle fleet 113 times since 1981 and has experienced two catastrophic failures. It is probable that both of those were mechanical/engineering failures and not the result of astronaut error. Surgical reporting methods vary from hospital to hospital, and it is often difficult to determine the specific causes of morbidity and mortality. One longitudinal study of all surgical procedures in one medical center puts the surgical error rates at that center between 2.7 percent and 7.5 percent. See Hunter McGuire, Shelton Horsley, David Salter, et al., "Measuring and Managing Quality of Surgery: Statistical vs. Incidental Approaches."

is so small and the selection and training processes are so demanding.[4] Intelligence analysts share many of these organizational and professional circumstances.

The Intelligence Community is relatively small, highly selective, and largely shielded from public view. For its practitioners, intelligence work is a cognitively-demanding and high-risk profession that can lead to public policy that strengthens the nation or puts it at greater risk. Because the consequences of failure are so great, intelligence professionals continually feel significant internal and external pressure to avoid it. One consequence of this pressure is that there has been a long-standing bureaucratic resistance to putting in place a systematic program for improving analytical performance. According to 71 percent of the people I interviewed, however, that resistance has diminished significantly since September 2001.

It is not difficult to understand the historical resistance to implementing such a performance improvement program. Simply put, a program explicitly designed to improve human performance implies that human performance needs improving, an allegation that risks considerable political and institutional resistance. Not only does performance improvement imply that the system is not optimal, the necessary scrutiny of practice and performance would require examining sources and methods in detail throughout the Intelligence Community. Although this scrutiny would be wholly internal to the community, the concept runs counter to a culture of secrecy and compartmentalization.

The conflict between secrecy, a necessary condition for intelligence, and openness, a necessary condition for performance improvement, was a recurring theme I observed during this research. Any organization that requires secrecy to perform its duties will struggle with and often reject openness, even at the expense of efficacy. Despite this, and to their credit, a number of small groups within the Intelligence Community have tasked themselves with creating formal and informal ties with the nation's academic, non-profit, and industrial communities. In addition, there has been an appreciable increase in the use of alternative analyses and open-source materials.

These efforts alone may not be sufficient to alter the historical culture of secrecy, but they do reinforce the idea that the Intelligence Community itself has a responsibility to reconsider the relationship between secrecy, openness, and efficacy. This is especially true as it relates to the community's performance and the occurrence of errors and failure. External oversight and public debate will not solve these issues; the desire to improve the Intelligence Com-

[4] There are currently 109 active US astronauts and 36 management astronauts. See National Aeronautics and Space Administration-Johnson Space Center career astronaut biographies.

munity's performance needs to come from within. Once the determination has been found and the necessary policy guidelines put in place, it is incumbent upon the Intelligence Community to find and utilize the internal and external resources necessary to create a performance improvement infrastructure.

Scope

This project was designed explicitly as an applied research program. In many respects, it resembles an assessment of organizational needs and a gap analysis, in that it was intended to identify and describe conditions and variables that affect intelligence analysis and then to identify needs, specifications, and requirements for the development of tools, techniques, and procedures to reduce analytic error. Based on these findings, I was to make recommendations to improve analytic performance.

In previous human performance-related research conducted in the military, medical, and astronautic fields, I have found in place—especially in the military—a large social science literature, an elaborate training doctrine, and well-developed quantitative and qualitative research programs. In addition to research literature and programs, these three disciplines have substantial performance improvement programs. This was not the case with the Intelligence Community.

This is not to say that an intelligence literature does not exist but rather that the literature that does exist has been focused to a greater extent on case studies than on the actual process of intelligence analysis.[5] The vast majority of the available literature is about history, international relations, and political science. Texts that address analytic methodology do exist, and it is worth noting that there are quantitative studies, such as that by Robert Folker, that compare the effectiveness of different analytic methods for solving a given analytic problem. Folker's study demonstrates that objective, quantitative, and controlled research to determine the effectiveness of analytic methods is possible.[6]

The literature that deals with the process of intelligence analysis tends to be personal and idiosyncratic, reflecting an individualistic approach to problem solving. This is not surprising. The Intelligence Community is made up of a variety of disciplines, each with its own analytic methodology. The organizational assumption has been that, in a multidisciplinary environment, intelli-

[5] There are exceptions. See the appendix.

[6] MSgt. Robert D. Folker, *Intelligence Analysis in Theater Joint Intelligence Centers*. Folker's study contains a methodological flaw in that it does not describe one of the independent variables (intuitive method), leaving the dependent variable (test scores) in doubt.

gence analysts would use analytic methods and tools from their own domain in order to analyze and solve intelligence problems. When interdisciplinary problems have arisen, the organizational assumption has been that a variety of analytic methods would be employed, resulting in a "best fit" synthesis.

This individualistic approach to analysis has resulted in a great variety of analytic methods—I identified at least 160 in my research for this paper—but it has not led to the development of a standardized analytic doctrine. That is, there is no body of research across the Intelligence Community asserting that method X is the most effective method for solving case one and that method Y is the most effective method for solving case two.[7]

The utility of a standardized analytic doctrine is that it enables an organization to determine performance requirements, a standard level of institutional expertise, and individual performance metrics for the evaluation and development of new analytic methodologies.[8] Ultimately, without such an analytic baseline, one cannot assess the effectiveness of any new or proposed analytic method, tool, technology, reorganization, or intervention. Without standardized analytic doctrine, analysts are left to the rather slow and tedious process of trial and error throughout their careers.

Generally, in research literature, one finds a taxonomy, or matrix, of the variables that affect the object under study. Taxonomies help to standardize definitions and inform future research by establishing a research "road map." They point out areas of interest and research priorities and help researchers place their own research programs in context. In my search of the intelligence literature, I found no taxonomy of the variables that affect intelligence analysis.

Following the literature review, I undertook to develop working definitions and a taxonomy in order to systematize the research process. Readers will find the working definitions in the first chapter. The second chapter highlights the the broader findings and implications of this ethnographic study. Because the first two chapters contain many quotes from my interviews and workshops, they illustrate the tone and nature of the post-9/11 environment in which I worked.

The taxonomy that grew out of this work was first described in an article for the CSI journal, *Studies in Intelligence,* and is presented here as Chapter

---

[7] There is no single Intelligence Community basic analytic training program. There is, however, community use of advanced analytic courses at both the CIA University and the Joint Military Intelligence College. The Generic Intelligence Training Initiative is a recent attempt to standardize certain law enforcement intelligence analysis training programs through a basic law enforcement analyst training curriculum. The program has been developed by the Training Advisory Council, under the Counterdrug Intelligence Coordinating Group and the Justice Training Center.

[8] See the appendix.

Three. In addition to the normal journal review process, I circulated a draft of the taxonomy among 55 academics and intelligence professionals and incorporated their suggestions in a revised version that went to press. This is not to assert that the taxonomy is final; the utility of any taxonomy is that it can be revised and expanded as new research findings become available. The chapter by Dr. Judith Meister Johnston that follows offers an alternative model—more complex and possibly more accurate than the traditional intelligence cycle—for looking at the dynamics of the intelligence process, in effect the interrelationships of many elements of the taxonomy

The following chapters, prepared by me and other able colleagues, were developed around other variables in the taxonomy and offer suggestions for improvement in those specific areas. One of them—Chapter Five, on integrating methodologists and substantive experts in research teams—also appeared in *Studies in Intelligence*. Chapter Nine contains several broad recommendations, including suggestions for further research.

To the extent possible, I tried to avoid using professional jargon. Even so, the reader will still find a number of specific technical terms, and, in those cases, I have included their disciplinary definitions as footnotes.

A Work in Progress

In some respects, it may seem strange or unusual to have an anthropologist perform this type of work rather than an industrial/organizational psychologist or some other specialist in professional performance improvement or business processes. The common perception of cultural anthropology is one of fieldwork among indigenous peoples. Much has changed during the past 40 years, however. Today, there are many practitioners and professional associations devoted to the application of anthropology and its field methods to practical problem-solving in modern or postindustrial society.[9]

It is difficult for any modern anthropological study to escape the legacy of Margaret Mead. She looms as large over 20th century anthropology as does Sherman Kent over the intelligence profession. Although Franz Boas is arguably the father of American anthropology and was Margaret Mead's mentor, hers is the name everyone recognizes and connects to ethnography.[10] Chances are, if one has read anthropological texts, one has read Mead.

---

[9] The Society for Applied Anthropology and the National Association for the Practice of Anthropology section of the American Anthropological Association are the two principal anthropological groups. Another group is the Inter-University Seminar on Armed Forces and Society, a professional organization representing 700 social science fellows, including practicing anthropologists, applying their research methods to issues in the military.

I mention Mead not only because my work draws heavily on hers, but also because of her impact on the discipline and its direction. She moved from traditional cultural anthropological fieldwork in the South Pacific to problem-oriented applied anthropology during World War II. She was the founder of the Institute for Intercultural Studies and a major contributor to the Cold War RAND series that attempted to describe the Soviet character. She also pioneered many of the research methods that are used in applied anthropology today. I mention her work also as an illustrative point. After two years of field research in the South Pacific, she wrote at least five books and could possibly have written more.

As I look over the stacks of documentation for this study, it occurs to me that, given the various constraints of the fellowship, there is more material here than I will be able to address in any one text. There are the notes from 489 interviews, direct observations, participant observations, and focus groups; there are personal letters, e-mail exchanges, and archival material; and there are my own notes tracking the progress of the work. Moreover, the fieldwork continues. As I write this, I am scheduling more interviews, more observations, and yet more fieldwork.

This text, then, is more a progress report than a final report in any traditional sense. It reflects findings and recommendations to date and is in no way comprehensive. Finally, based as it is on my own research interests and research opportunities, it is but one piece of a much larger puzzle.

[10] Boas (1858–1942) developed the linguistic and cultural components of ethnology. His most notable work was *Race, Language, and Culture* (1940).

PART I

Research Findings

eth•nog•ra•phy\n **[F** *ethnographie*, fr. *ethno-* + *-graphie* -graphy**]** (1834) : the study and systematic recording of human cultures: *also*: a descriptive work produced from such research. (*Merriam Webster's Collegiate Dictionary, Eleventh Edition*)

CHAPTER ONE

Definitions

Because I conducted human performance–related fieldwork before I came to this project, I carried into it a certain amount of experiential bias, or "cognitive baggage." The research findings from those other studies could bias my perspective and research approach within the Intelligence Community. For example, surgeons and astronauts do not need to deal with intentionally deceptive data. Patients are not trying to "hide" their illnesses from surgeons, and spacecraft are not thinking adversaries intent on denying astronauts critical pieces of information. This one difference may mean that intelligence analysis is much more cognitively challenging than the other two cases and that the requisite psychomotor skills are significantly less important. In an effort to counteract the biases of experience, I will attempt to be explicit about my own definitions in this work.

Working Definitions

The three main definitions used in this work do not necessarily represent definitions derived from the whole of the intelligence literature. Although some of the definitions used in this work are based on the Q-sort survey of the intelligence literature described later, some are based on the 489 interviews, focus groups, and two years of direct and participant observations collected during this project.

Definition 1: Intelligence is secret state or group activity to understand or influence foreign or domestic entities.

The above definition of *intelligence*, as used in this text, is a slightly modified version of the one that appeared in Michael Warner's work in a recent article in *Studies In Intelligence*.[1] Warner reviews and synthesizes a number of previous attempts to define the discipline of intelligence and comes to the conclusion that "*Intelligence is secret state activity to understand or influence foreign entities*."

Warner's synthesis seems to focus on strategic intelligence, but it is also logically similar to actionable intelligence (both tactical and operational) designed to influence the cognition or behavior of an adversary.[2] This synthesis captures most of the elements of actionable intelligence without being too restrictive or too open-ended, and those I asked to define the word found its elements, in one form or another, to be generally acceptable. The modified version proposed here is based on Warner's definition and the interview and observation data collected among the law enforcement elements of the intelligence agencies. These elements confront adversaries who are not nation states or who may not be foreign entities. With this in mind, I chose to define intelligence somewhat more broadly, to include nonstate actors and domestic intelligence activities performed within the United States.

Definition 2: Intelligence analysis is the application of individual and collective cognitive methods to weigh data and test hypotheses within a secret socio-cultural context.

This meaning of *intelligence analysis* was harder to establish, and readers will find a more comprehensive review in the following chapter on developing an intelligence taxonomy. In short, the literature tends to divide intelligence analysis into "how-to" tools and techniques or cognitive processes. This is not to say that these items are mutually exclusive; many authors see the tools and techniques of analysis as cognitive processes in themselves and are reluctant to place them in different categories. Some authors tend to perceive intelligence analysis as essentially an individual cognitive process or processes.[3]

My work during this study convinced me of the importance of making explicit something that is not well described in the literature, namely, the very

---

[1] Michael Warner, "Wanted: A Definition of 'Intelligence'," *Studies in Intelligence* 46, no. 3 (2002): 15–22.

[2] US Joint Forces Command, *Department of Defense Dictionary of Military and Associated Terms*.

[3] The appendix lists literature devoted to each of these areas.

interactive, dynamic, and social nature of intelligence analysis. The interview participants were not asked to define intelligence analysis as such; rather, they were asked to describe and explain the process they used to perform analysis. The interview data were then triangulated with the direct and participant observation data collected during this study.[4]

Despite the seemingly private and psychological nature of analysis as defined in the literature, what I found was a great deal of informal, yet purposeful collaboration during which individuals began to make sense of raw data by negotiating meaning among the historical record, their peers, and their supervisors. Here, from the interviews, is a typical description of the analytic process:

> *When a request comes in from a consumer to answer some question, the first thing I do is to read up on the analytic line. [I] check the previous publications and the data. Then, I read through the question again and find where there are links to previous products. When I think I have an answer, I get together with my group and ask them what they think. We talk about it for a while and come to some consensus on its meaning and the best way to answer the consumer's question. I write it up, pass it around here, and send it out for review.*[5]

The cognitive element of this basic description, "when I think I have an answer," is a vague impression of the psychological processes that occur during analysis. The elements that are not vague are the historical, organizational, and social elements of analysis. The analyst checks the previous written products that have been given to consumers in the past. That is, the analyst looks for the accepted organizational response before generating analytic hypotheses.

The organizational-historical context is critical to understanding the meaning, context, and process of intelligence analysis. There are real organizational and political consequences associated with changing official analytic findings and releasing them to consumers. The organizational consequences are associated with challenging other domain experts (including peers and supervisors). The potential political consequences arise when consumers begin to question the veracity and consistency of current or previous intelligence reporting. Accurate or not, there is a general impression within the analytic community

---

[4] In research, triangulation refers to the application of a combination of two or more theories, data sources, methods, or investigators to develop a single construct in a study of a single phenomenon.

[5] Intelligence analyst's comment during an ethnographic interview. Such quotes are indented and italicized in this way throughout the text and will not be further identified; quotes attributable to others will be identified as such.

that consumers of intelligence products require a static "final say" on a given topic in order to generate policy. This sort of organizational-historical context, coupled with the impression that consumers must have a final verdict, tends to create and reinforce a risk-averse culture.

Once the organizational context for answering any given question is understood, the analyst begins to consider raw data specific to answering the new question. In so doing, the analyst runs the risk of confirmation biases. That is, instead of generating new hypotheses based solely on raw data and then weighing the evidence to confirm or refute those hypotheses, the analyst begins looking for evidence to confirm the existing hypothesis, which came from previous intelligence products or was inferred during interactions with colleagues. The process is reinforced socially as the analyst discusses a new finding with group members and superiors, often the very people who collaborated in producing the previous intelligence products. Similarly, those who review the product may have been the reviewers who passed on the analyst's previous efforts.

This is not to say that the existing intelligence products are necessarily inaccurate. In fact, they are very often accurate. This is merely meant to point out that risk aversion, organizational-historical context, and socialization are all part of the analytic process. One cannot separate the cognitive aspects of intelligence analysis from its cultural context.

Definition 3: Intelligence errors are factual inaccuracies in analysis resulting from poor or missing data; intelligence failure is systemic organizational surprise resulting from incorrect, missing, discarded, or inadequate hypotheses.

During interviews, participants were asked to explain their understanding of the terms *intelligence error* and *intelligence failure*. There was little consensus regarding the definitions of error and failure within the Intelligence Community or within the larger interview sample. Here are some sample responses:

I don't know what they mean.

There are no such things. There's only policy failure.

You report what you know, and, if you don't know something, then it isn't error or failure. It's just missing information.

Failure is forecasting the wrong thing.

Failure is reporting the wrong thing.

Error is forecasting the wrong thing.

Error is reporting the wrong thing.

A failure is something catastrophic, and an error is just a mistake.

Error is about facts; failure is about surprise.

Error is when nobody notices, and failure is when everybody notices.

Some responses disavowed the existence of intelligence error and failure; some placed the terms in the broader context of policy and decisionmaking; some interchanged the two terms at random; some defined the terms according to their outcomes or consequences. Despite the variability of the responses, two trends emerged: novice analysts tended to worry about being factually inaccurate; senior analysts, managers, and consumers, tended to worry about being surprised. Often, participants' responses were not definitions at all but statements meant to represent familiar historical examples:

The attack on Pearl Harbor.

The Chinese sending combat troops into Korea.

The Tet Offensive.

The Soviet invasion of Afghanistan.

The collapse of the Soviet Union.

The Indian nuclear test.

September Eleventh.

The danger of defining by example is that each case is contextually unique and can be argued ad infinitum. What is important about these examples as a whole is that they all indicate one central and recurring theme. Specifically, all these examples signify surprise—in some cases, intelligence surprise; in other cases, military, civil, and political surprise. Even if the Intelligence Community itself was not surprised by one of these events, it was unable to convince the military, civil, and political consumers of intelligence that these events might occur; in which case, the failure was one of communication and persuasion.

When I began this study, my own definition of error and failure derived from the psychological and cognitive disciplines. Specifically, I took it that human error and failure are related to measures of cognitive and psychomotor accuracy, commission of error being at one end of the accuracy scale and omission or not performing the correct action being at the other.[6]

[6] See Appendix A for a list of literature on error.

During the interviews for this study, I soon found that the psychological definition was insufficient. The psychological definition took into account the cognitive and psychomotor components of task-structure, time-to-task, and accuracy-of-task as measures of errors and error rates, but it did not fully take into account the notion of surprise.[7] Surprise is the occurrence of something unexpected or unanticipated. It is not precisely commission or omission; it indicates, rather, the absence of contravening cognitive processes. Measures of accuracy may account for factual errors in the intelligence domain, but measures of accuracy are insufficient to account for surprise events and intelligence failure.

To put this in context, an analyst, while accounting successfully for an adversary's capability, may misjudge that adversary's intention, not because of what is cognitively available, but because of what is cognitively absent. The failure to determine an adversary's intention may simply be the result of missing information or, just as likely, it may be the result of missing hypotheses or mental models about an adversary's potential behavior.

[7] Sociological definitions are more akin to the definitions proposed in this study. Failure can occur due to system complexity and missing data as well as through the accumulation of error. See Charles Perrow, *Normal Accidents. Living with High Risk Technologies*. I'd like to thank Dr. Perrow for his assistance with this work.

CHAPTER TWO

Findings

Scientific knowledge, like language, is intrinsically the common property of a group or else nothing at all. To understand it we shall need to know the special characteristics of the groups that create and use it.

Thomas Kuhn[1]

The more we learn about the world, and the deeper our learning, the more conscious, specific, and articulate will be our knowledge of what we do not know.

Karl Popper[2]

The purpose of this research was to identify and describe conditions and variables that negatively affect intelligence analysis, to develop relevant and testable theory based on these findings, and to identify areas in which strategies to improve performance may be effective. Although there has recently been a great deal of concern that intelligence error and failure rates are inordinately high, in all likelihood, these rates are similar to those of other complex socio-cognitive domains, such as analysis of financial markets. The significant differences are that other complex domains employ systematic performance

[1] Philosopher of science Thomas Kuhn described the now-common concept of paradigm shifts in scientific revolutions. He posited that paradigm shifts are tied to cultural and social constructionist models, such as Vygotsky's (See footnote 22 in Chapter Three). Thomas Kuhn, *The Structure of Scientific Revolutions*.

[2] Karl Popper was one of the 20th century's pre-eminent philosophers of science. Karl Popper, *Conjectures and Refutations: The Growth of Scientific Knowledge*.

improvement infrastructures and that the consequences of intelligence error and failure are disproportionately high in comparison with other domains.

It is evident from the literature that intelligence organizations recognize the need to improve their performance and that it is possible to make the domain of intelligence analysis into a coherent scientific discipline. The first step in this transition is to identify and describe performance gaps.[3] Once gaps have been identified, it will be possible to introduce performance improvement methods systematically and to measure the effectiveness of the results. This work is intended to further research toward creating intelligence organizations that are more effective.

The Problem of Bias

Although a researcher might pretend to be neutral and unbiased in presenting his findings and conclusions, personal biases can creep into a finished product. The methods ethnographers employ to collect raw data and the use of interpretational analysis to extract meaning and generate theory virtually guarantee it. In my view, one should be candid about this possibility. I noted in Chapter One that ethnographers bring a certain amount of experiential baggage to their work, myself included. At this point, before discussing analytical difficulties and problems I identified during my research, I want to make the readers aware of an additional personal bias that has developed from observing the Intelligence Community.

During my research, I developed a great deal of empathy for individual analysts and the problems they face in trying to perform their jobs. The reason for this is straightforward and something every anthropologist recognizes. It is part of the process that anthropologists reach a point where they can modify their own identity in order to gain insight into a different culture. The risk is that empathy and identity modification will induce the researcher to "go native" and produce bias in his findings.

Although I may empathize with analysts personally, it is critical for theory development to avoid parroting the views, kudos, or complaints of individual analysts, who may or may not be dissatisfied with their unique professional experience. In order to counteract the empathy bias, I employed multiple data collection techniques and then used those data to refute or confirm each categorical finding. Triangulation is not an infallible system, however, and the reader is advised to approach these findings with both a critical eye and the

[3] Performance gaps are the difference or distance between ideal (perfect) organizational performance and actual organizational performance. In this case, ideal performance includes complete data sets, reportorial accuracy, and the ability to avoid strategic, operational, and tactical surprise.

foreknowledge that this researcher has a number of personal and professional biases.[4]

Finding: Secrecy Versus Efficacy

Secrecy and efficacy conflict. Secrecy interferes with analytic effectiveness by limiting access to information and sources that may be necessary for accurate or predictive analysis. In turn, openness interferes with security by degrading the value of information resources and by revealing specific sources and methods.

Perfect secrecy would ultimately be unproductive, because it would restrict information to one mind or to a very small group of minds. Limiting available resources in this way would produce organizational failure in competition with resources available to a large and diverse group of adversaries. Perfect openness would also lead to organizational failure, because, with full access to all information, there would never be an instance of advantage for any one group over any other group. In addition, perfect openness would result in adversaries being aware they are under observation and could lead them to alter their behavior to deceive the observer if they so desired.[5]

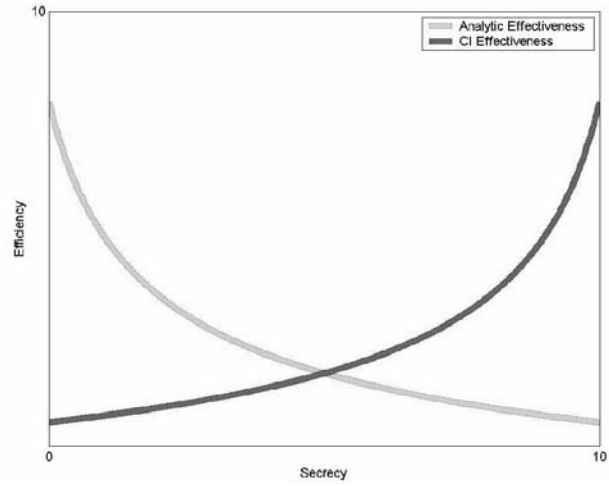
Between these two extremes, there is some notional point where secrecy and openness converge to create an optimal performance tradeoff. My perception is that, within the Intelligence Community, more organizational emphasis is placed on secrecy than on effectiveness. It is important, in my view, that there be a voice in favor of openness to counterbalance the many voices whose sole or primary responsibility is the advocacy and maintenance of

---

[4] Throughout the project, my data collection method consisted of written field notes. Anthropologists traditionally include specific detail from participant input or direct observation. Usually, this is in the form of precise descriptions of the actual behavior of participants and transcripts of their verbal interactions. It is also standard practice in field work to capture these data, and the data from the interviews and focus groups, on audio- or videotape. These practices were not followed in this particular case for two reasons: first, the nature of my work was not to document actual practices and procedures; rather, it was to derive categories of variables and individual variables in order to create a taxonomy, and to use the prototype taxonomy to structure the interactions; second, the nature of intelligence work and the environment in which it occurs, as well as its professional practitioners, require that certain data be restricted.

[5] This has been demonstrated in the psychological literature and is referred to as the Hawthorne Effect. Derived from research that began with an experimental program at Western Electric's Hawthorne Works conducted between 1927 and 1930, the Hawthorne Theory, broadly interpreted, states that the behavior of subjects changes when they are aware of being observed. See Fritz J. Roethlisberger and William J. Dickson, *Management and the worker*; Elton Mayo, *The Human Problems of an Industrial Civilization*.

Secrecy vs. Efficacy



secrecy. I believe this secrecy-efficacy conflict can be stated as a theory, along the following lines.[6]

The more open the system (where zero is perfect information access and sharing on the X axis secrecy scale [as shown on the above graph]), the more access an analyst has to all sources of information within the Intelligence Community regarding an adversary. In addition, this openness encourages interorganizational communication, interaction, and sharing of information among analysts and increases the likelihood that an analyst will be more efficient (in this case the Y axis efficiency scale) and therefore effective or accurate in his or her assessment of a situation.

Conversely, counter-intelligence is negatively affected by zero-level secrecy and perfect openness. The less open or more compartmentalized the system, the more efficient and effective are counterintelligence activities. Notionally, the two curves would meet somewhere in the tradeoff between efficiency and secrecy. Where they meet would depend on program goals and a clear definition of starting points and end-states.

The notional set of curves above illustrates the tradeoff between system efficiency and system secrecy and the effect that the tradeoff has on performance effectiveness, both positive and negative. In this case, the starting and ending points of effectiveness for analysis and for counterintelligence are arbitrary and could be positioned anywhere along a continuum between zero

[6] I would like to credit and thank Matthew Johnson at the Institute for Defense Analyses for his help in formulating this theory.

and ten. In this theory, analytic efficiency and effectiveness are purely functions of system openness and do not take into account analytic methods or personnel.

This theory will require additional refinement, and it may or may not be represented by a tradeoff curve like the one proposed here. The theory will also require numerous controlled quantitative experiments to test its explanatory power.

Finding: Time Constraints

> *The work itself is a 24-hour-a-day job, but it never seems like I have any time to actually analyze anything when I'm at my desk. I spend most of my time reading daily traffic, answering e-mail, coordinating papers with everybody, and writing. Mostly I read and write, but when the workday is over, I go home and think. It isn't like I can turn off my brain. So, I guess I do most of my real analysis on my own time.*

The majority of the analysts interviewed indicated that time was one of their greatest constraints at work. This comment triangulated with the findings from direct and participant observation. In addition, analysts indicated that there has been a communitywide shift toward focusing on short-term issues or problem solving, thereby addressing the immediate needs of intelligence consumers. This shift in product focus, coupled with a growth in available all-source raw intelligence, has resulted in a change in the pace of analytic production. In order to generate the daily products, analysts have had to change the way they go about doing their work.

> *I haven't been doing this very long, but I wish I had been a journalism major instead of poli-sci. The pace is excruciating.*
>
> *I don't get much sleep. It's like cramming for finals, except we do it every day.*
>
> *Everything I do is reactive. I don't have time to work my subject. We're not pro-active here.*
>
> *I'm so busy putting out today's fires, I don't have any time to think about what kind of catastrophe is in store for me a month from now.*
>
> *About 15 years ago, I used to have 60 percent of my time available for long-term products. Now, it's between 20 and 25 percent.*
>
> *I probably have about 30 percent of my time for self-initiated products.*

You know, someday somebody is bound to notice that velocity isn't a substitute for quality. We've gotten rid of the real analytic products that we use to make, and now we just report on current events.

Not all analysts indicated that time constraints and information load had a negative effect on their performance. A minority indicated that there was sufficient time to perform analytic duties and prepare analytic products.

This is a tactical shop. It's all we do. Current reporting is our job.

I work a slow desk. I have plenty of time for self-initiated products—maybe 60 percent or more.

I multitask pretty well. I don't really experience a time-crunch.

Maybe I just process better than other people, but I don't really feel pressed for time. Besides, I'd rather be at a hot desk than at a cold desk.

Analytic supervisors were more evenly mixed in their opinions about time constraints. A slight majority of the managers interviewed said time constraints had negative effects on the work environment, work processes, and the morale of their staff. A majority of them also put analytic time constraints in a larger context of policy making. They indicated that the decision-cycle of policymakers was 24 hours a day and that their responsibility was to support that decision cycle with current intelligence.

In discussing their perceptions of consumer demand, the managers' views of the nature of those demands were mixed.

I want my analysts to produce long-term products. I want them thinking through their subjects. The decision makers want well-thought-out products, not just daily briefs.

Our customers want current production. They never complain about the daily products and, frankly, I doubt they have time to read the longer stuff.

My consumers like the bigger pieces. They like having the context and broader picture. They don't want to be spoon fed.

I've never had a customer tell me they want more to read.

Our customers want to avoid surprise. As long as we keep them from being surprised, I don't care if we do daily or long-term production. I don't think they care either.

Finding: Focus on Current Production

The present daily production cycle and the focus on current intelligence also affect group interactions and the analytic process.

Group Interactions:

It doesn't matter if I'm writing a piece myself or if I'm coordinating a piece with some group. We don't sit around and test hypotheses, because we're too busy writing. We've got serious deadlines here.

If, by group analysis, you mean the senior expert in the room tells everybody what he thinks, and then we generally agree so that we can get back to our own deadlines, then, sure, there's a group process.

We used to have groups that did current reporting and different groups that did longer term products. We still have some of that, but it is very limited. I couldn't say what happened exactly, but we're all doing current production now.

The Analytic Process:

People seem to have confused writing with analyzing. They figure that if you just go through the mechanics of writing something, then you must have analyzed it. I don't know about everybody else, but it doesn't work that way for me. I need time to think through the problem.

Our products have become so specific, so tactical even, that our thinking has become tactical. We're losing our strategic edge, because we're so focused on today's issues.

Alternative analysis is a nice concept, but I don't have the time to do it. I've got to keep up with the daily traffic.

I use several analytic techniques that are relatively fast. Scenario development, red teams, competing hypotheses, they're all too time consuming.

We've got Bayesian tools, simulations, all kinds of advanced methods, but when am I supposed to do any of that? It takes all my time to keep up with the daily reporting as it is.

I don't have time to worry about formal analytic methods. I've got my own system. It's more intuitive and a lot faster.

Finding: Rewards and Incentives

The shift in the analytic production cycle is not only reflected in the products and processes but also in the way analysts perceive the system by which intelligence organizations reward and promote employees. Employees see their opportunities for promotion as being tied directly to the number of daily products they generate and the amount of social capital or direct consumer influence they amass, most often when their work is recognized by senior policymakers.[7]

> *In any given week, I could devote about 20 percent of my time to longer think pieces, but why should I? You can write all the think pieces you want, but, if you don't write for the daily briefs, you aren't going to move into management. These days the only thing that matters is getting to the customers.*
>
> *If I write a 12-page self-directed piece that goes out as a community product, and somebody else writes one paragraph with two bullet points that goes into a daily brief, the guy who got in the daily brief is going to get the recognition. Why waste my time with the big products?*
>
> *It isn't really official policy, but the reality is that sheer production equals promotion. People talk about quality, but, in the end, the only measurable thing is quantity.*
>
> *Our group has a "team award" of 5,000 bucks. Last year, they gave it to the one guy who published the most. I'm not sure how that one guy won a "team award," but there you go.*
>
> *Technically, I have four bosses. The only thing that seems to keep them all happy is volume. It's like piece work.*
>
> *Quality? How do you measure quality? Quantity—now that's something you can count.*
>
> *Promotion is based on production—pure and simple.*

In sum, aside from specific tactical groups, staff positions that generate limited social capital, and individual cognitive differences, there is a majority sentiment among the analysts interviewed that the combination of a shorter

---

[7] Social capital refers to the set of norms, social networks, and organizations through which people gain access to power, resources, and reciprocity and through which decisionmaking and policy creation occur. In other words, whom you know is just as important as what you know. Pierre Bourdieu, "The Forms of Capital"; Robert Putnam, "The Prosperous Community" and *Bowling Alone*. See also the empirical work on social capital summarized in Tine Feldman and Susan Assaf, *Social Capital: Conceptual Frameworks and Empirical Evidence.*

production cycle, information load, a shift in product focus, and organizational norms regarding promotion have had an impact on analytic work and intelligence analysis itself.

Finding: "Tradecraft" Versus Scientific Methodology

> *Human beings do not live in the objective world alone, nor alone in the world of social activity as ordinarily understood, but are very much at the mercy of the particular language which has become the medium of expression for their society…The fact of the matter is that the "real world" is to a large extent unconsciously built upon the language habits of the group…We see and hear and otherwise experience very largely as we do because the language habits of our community predispose certain choices of interpretation.*
>
> Edward Sapir[8]

The Intelligence Community, in its culture and mythos and in its literature, tends to focus on intelligence *operations* rather than on intelligence *analysis*. Open literature about the community certainly does so. Along with time constraints and the analytic production cycle, the private and public focus on operations has had an effect on intelligence analysts and analytic methodology. The principal effect is the spread of the concept of **"**tradecraft**"** within the analytic community.

Community members quite often used the word "tradecraft" to describe intelligence analysis during the interviews, observations, training programs, workshops, and actual analytic tasks that I performed for this study. Analysts, managers, instructors, and academic researchers employed the word "tradecraft" as a catchall for the often-idiosyncratic methods and techniques required to perform analysis. Although the intelligence literature often refers to tradecraft, the works tend to be a collection of suggestions and tips for writing and communicating with co-workers, supervisors, and consumers instead of focusing on a thorough examination of the analytic process and techniques.

The notion that intelligence operations involve tradecraft, which I define as *practiced skill in a trade or art*, may be appropriate, but the analytic community's adoption of the concept to describe analysis and analytic methods is not. The obvious logical flaw with adopting the idea of tradecraft as a standard of practice for analytic methodology is that, ultimately, analysis is neither craft nor art. Analysis**,** I contend**,** is part of a *scientific* process. This is an important

[8] Edward Sapir is best known for the Sapir-Whorf hypothesis, which asserts linguistic/cognitive relativity (language and thought are inseparable; therefore, different languages mean different ways of thinking). Edward Sapir, *Language*.

distinction, for language is a key variable in anthropology and often reveals a great deal about the cognition and culture of a community of interest.[9]

The adoption by members of the analytic community of an inappropriate term for the processes and methods employed in their professional lives obfuscates and complicates the reality of their work. The adoption of the word "tradecraft" demonstrates the analytic community's need to create a professional identity separate and unique from other disciplines but tied directly to the perceived prestige and cachet of intelligence operations. Adopting "tradecraft" as a term of reference for explaining work practices and as a professional identity marker may seem trivial. Yet the term, and its effect on the community, has unanticipated consequences.

Tradecraft purposefully implies a mysterious process learned only by the initiated and acquired only through the elaborate rituals of professional indoctrination. It also implies that the methods and techniques of analysis are informal, idiosyncratic, unverifiable, and perhaps even unexplainable. "Good" methods are simply those that survive, and then are passed on by "good" analysts to novice analysts. Unfortunately, "good" in both instances is not an objective measure. That is, there is no formal system for measuring and tracking the validity or reliability of analytic methods, because they are both perceived and employed within the context of idiosyncratic tradecraft. When asked to describe the analytic process, analysts responded in a variety of ways.

> *First, I figure out what I know and what I don't know about some situation. Then, I look for information to fill the gap.*
>
> *I have a model of the situation in my head. Whenever something new comes in, I see if it fits with the model. If it does, I add it to the model; if it doesn't, I try to figure out why.*
>
> *I've found a system that lets me keep up. I just look for anomalies. When I see any novel data, then I worry.*
>
> *I'm always looking for anything strange or out of place. Then, I source it to see if it is meaningful.*
>
> *The current data ought to fit a certain pattern. If it doesn't, I know something is wrong.*
>
> *First, I print the daily traffic I'm concerned with; then I lay out all of the relevant stuff in front of me on my desk or the floor; then I start looking for threads.*

[9] The literature on this subject is extensive. For a representative list, see the appendix.

I'm looking for links and patterns. Once I figure out the pattern, I can figure out where to look next.

I use patterns. If things start happening, out of the ordinary things, I pay attention to them.

I try to build patterns out of the data. It helps me predict what will happen next.

I come up with a few scenarios and see what the evidence supports.

I look for data that are diagnostic: some piece of evidence that rules out certain possibilities.

I try to weigh the evidence to see which scenario it supports.

Although anomaly-detection, pattern-recognition, and weighing data may appear to be idiosyncratic tradecraft based on individual expertise and cognitive skills, these methods can be formalized and replicated if the operating parameters, variables, and rules of evidence are made explicit.[10] This is to say that intelligence analysis can be reconstructed in the context of a scientific method, which is merely an articulated, formal process by which scientists, collectively and over time, endeavor to put together a reliable, consistent, and nonarbitrary representation of some phenomena. Broadly, the steps include:

- observation and description of phenomena;
- formulation of hypotheses to explain phenomena;
- testing of hypotheses by independent experts;
- refutation or confirmation of hypotheses.

These steps do not suggest that any specific scientific methodology results in what is ultimately the truth, rather that scientific methods are merely formal processes used to describe phenomena, make predictions, and determine which hypothesis best explains those phenomena. The principal value of any type of methodological formalism is that it allows other researchers to test the validity and reliability of the findings of any other researcher by making explicit, and therefore replicable, the means by which anyone reaches a specific conclusion.[11]

The idea that intelligence analysis is a collection of scientific methods encounters some resistance in the Intelligence Community. The interview data analyzed in this study highlight many subtle—and not so subtle—prejudices

[10] A corollary to these methods can be found in the practice of radiologists. See Chapter Five for more on expertise.

that analysis is not a science. That is, it is an art or craft in which one can attain skill but not a formal discipline with tested and validated methodology.

> *What we do is more art and experience than anything else.*
>
> *Science is too formal. We can't actually run experiments here.*
>
> *How would you actually test a hypothesis in intelligence?*
>
> *Science is what you do in a lab.*
>
> *We're not scientists; we're analysts. We don't generate the data.*
>
> *We don't worry too much about theory; we worry about the facts.*
>
> *In my discipline, I might be a scientist, but, in intelligence, I am a practitioner.*
>
> *I use science for my area, but I don't think intelligence analysis is science.*

As long as intelligence analysis continues to be tradecraft, it will remain a mystery. The quality of any tradecraft depends on the innate cognitive capabilities of the individual and the good fortune one has in finding a mentor who has discovered, through many years of trial and error, unique methods that seem to be effective. This process of trial and error is, in general, similar to any scientific process, except that the lessons learned in tradecraft, unlike those of other disciplines, often occur without being captured, tested, or validated.

In an oral tradition, individual tradecraft methods are passed on by means of apprenticeship. The consequence for any culture tied to an oral tradition is the loss of important knowledge that occurs with the loss of practitioners. In organizations, the retirement of experts and innovators leads to the loss of that expertise and innovation, unless there is some formal written and educational system to keep that knowledge alive.[12]

The data collected through both interviews and observation indicated that there were, in fact, general methods that could be formalized and that this process would then lead to the development of intelligence analysis as a scientific discipline. The principal difficulty lies not in developing the methods them-

---

[11] Rather than engage in the longstanding and ongoing debate in the academic community about what is and what is not science or a scientific method, suffice it to say that any scientific method needs to be explicit, replicable, and refutable. The literature surrounding this debate is voluminous. The philosophy of science, logic, language, and epistemology has taken this debate in a number of directions. There is, however, a general theme that replication is a key ingredient to any scientific method.

[12] See section on Endangered Languages in Barbara Grimes, ed., *Ethnologue*. 14th ed.

selves, but in articulating those methods for the purpose of testing and validating them and then testing their effectiveness throughout the community. In the long view, developing the science of intelligence analysis is easy; what is difficult is changing the perception of the analytic practitioners and managers and, in turn, modifying the culture of tradecraft.

Finding: Confirmation Bias, Norms, and Taboos

> *Organization is key, because it sets up relationships among people through allocation and control of resources and rewards. It draws on tactical power to monopolize or parcel out liens and claims, to channel action into certain pathways while interdicting the flow of action into others. Some things become possible and likely; others are rendered unlikely.*
>
> Eric Wolf[13]

Time constraints affect both the general analytic production cycle and analytic methodology by contributing to and exacerbating cognitive biases. Although there are any number of cognitive biases to which the human mind is susceptible, one in particular became evident during the triangulation phase and interpretive analysis of the interview and observation data of this study. The cognitive bias identified most often was confirmation bias, which is the tendency of individuals to select evidence that supports rather than refutes a given hypothesis.[14]

Although the psychological mechanism by which confirmation bias occurs is in debate, confirmatory behavior is a consistent finding throughout the experimental psychology and cognitive science literature. Rather than focus on the mechanism and nomenclature, the term "confirmation bias" is used in this work as a description of confirmatory behavior. This behavior was

---

[13] Eric Wolf was an anthropologist who focused on power, social structures, and the third world. His work on power and the lives of peasants is considered a modern anthropological classic. Eric Wolf, *Pathways of Power.*

[14] There is a fair amount of disagreement in the psychological literature regarding the mechanism by which an individual displays confirmatory behavior. Some researchers attribute it to motivational factors, for example, a desire to maintain respect within a group. Other researchers attribute it to selectivity factors, an unconscious cognitive selection of data that confirms the current status quo. Some researchers attribute it to social factors, a subspecies of groupthink (see Irving Janis, *Groupthink*). Still others ascribe it to a misapplication of heuristics, whereby an individual learns a set of rules that solves one problem and then begins using that same set of rules to try to solve other types of problems. Although the literature is extensive, Karl Popper's *The Logic of Scientific Discovery* provides a foundation for understanding the issue. Jonathan Evans' *Bias in Human Reasoning: Causes and Consequences* is still a useful and concise summary of the research related to confirmation bias.

described by participants during the interviews and observed during direct and participant observations throughout the fieldwork.

Analysts were asked to describe the work processes they employed to answer questions, solve problems, describe and explain phenomena, make forecasts, and develop intelligence products. The process they described began with an examination of previous analytic products developed by their organization in order to establish a baseline from which they could build their own analysis.

> *When a request comes in from a consumer to answer some question, the first thing I do is to read up on the analytic line.*
>
> *The first thing I do is check the pervious publications, and then I sort through the current traffic.*
>
> *I've looked at our previous products, and I've got a good idea of the pattern; so, when I sort through the traffic, I know what I'm trying to find.*
>
> *I try to keep up with all the products that come out of our area, so I know where to start my piece.*

A literature search is often the first step in any research endeavor. The utility of this practice is not merely to define and understand the current state of research in the field but also to determine major controversies and divergences of opinion. Trying to discern controversies and divergence in intelligence products is often difficult, because some of them—national intelligence estimates (NIE), in particular—are specifically designed to produce a corporate consensus for an audience of high-level policymakers.

These products can and do include divergent opinions, in the form of footnotes, but these tend to indicate inter-, rather than intra-, organizational differences. Dissenting footnotes are products of the coordination process, the result of an inability on the part of one or several community organizations to convince the others of a particular point of view. Not surprisingly, the least probable opinion is often the hardest to defend, whereas the most probable opinion is the easiest to support.

The literature search approach may promote a logical consistency among analytic products, but it has the unintended consequence of imposing on the analyst using it a preexisting mental model of the phenomena in question. The existing analytic products describe, implicitly or explicitly, a set of working hypotheses that an analyst may wish to reflect in his or her own work. Of course, these existing hypotheses are rarely tested each time they are incorporated into new products. What tends to occur is that the analyst looks for current data that confirms the existing organizational opinion or the opinion that

seems most probable and, consequently, is easiest to support. As this strategy is also the most time-efficient technique, it reduces the time constraints associated with the daily production cycle.

This tendency to search for confirmatory data is not necessarily a conscious choice; rather, it is the result of accepting an existing set of hypotheses, developing a mental model based on previous corporate products, and then trying to augment that model with current data in order to support the existing hypotheses. Although motivational and heuristic factors and a tendency toward "groupthink" might contribute to confirmatory behavior in intelligence analysis, my observations and interviews during this study suggest that the predominant influence is selectivity bias in order to maintain a corporate judgment.

The maintenance of a corporate judgment is a pervasive and often-unstated norm in the Intelligence Community, and the taboo against changing the corporate product line contributes to confirmation biases. Once any intelligence agency has given its official opinion to policymakers, there exists a taboo about reversing or significantly changing the official or corporate position to avoid the loss of status, trust, or respect. Often, policymakers perceive a change in judgment as though the original opinion was wrong, and, although unstated, there are significant internal and external social pressures and consequences associated with being perceived as incorrect.

An analyst can change an opinion based on new information or by revisiting old information with a new hypothesis; in so doing, however, he or she perceives a loss of trust and respect among those with whom the original judgment was shared. Along with this perceived loss of trust, the analyst senses a loss of social capital, or power, within his or her group.[15]

It is even more difficult for an intelligence agency to change its official position once it has made its judgments known to those outside of the organization. There is a sense that changing the official product line will be seen outside of its context—the acquisition of new information, for instance—and that it will be perceived by the policymakers as an example of incompetence or, at least, of poor performance on the part of the intelligence agency.

This perception then carries with it the threat of a loss in status, funding, and access to policymakers, all of which would have a detrimental effect on the ability of the intelligence agency to perform its functions. In short, it serves the interest of the intelligence agency to be perceived as decisive

[15] Reciprocity in this case has to do with information, judgment, and trust. The classic anthropological text on social reciprocity and trust within and between groups is Marcel Mauss's *The Gift*. Originally published in 1950 and based in part on the work of his uncle and mentor, Emile Durkheim, Mauss's work (*Essai sur le Don* in its French version) lays the foundation for his contention that reciprocity is the key to understanding the modern concept of social capital.

instead of academic and contradictory, and that message is transmitted to the analysts. In response to the organizational norm, the analyst is inclined to work the product line rather than change it.

> *Our products are company products, not individual products. When you publish something here, it's the official voice. It's important for us to speak with one voice.*
>
> *It doesn't do us any good if people think we can't make up our mind.*
>
> *Access matters; if people think you don't know what you're talking about, then they stop seeing you.*
>
> *We already briefed one thing. I can't go in there and change it now. We'll look like idiots.*
>
> *When I was new, I wrote a piece that disagreed with our line. Let's just say, I'm more careful about that now.*

Another organizational norm that contributes to confirmation bias in the Intelligence Community is the selection and weighing of data according to classification. Secrets carry the imprimatur of the organization and, in turn, have more face validity than information collected through open sources.[16]

Most analysts indicated that they considered "secret" data collected by covert means to be more important or meaningful than "open" or unclassified data. Analysts said that they rely on open sources to help fill in missing pieces of their mental models but that they test the model's validity with secret information. Choosing to rely on classified data as more meaningful to problem solving and as a tool for testing the validity of their hypotheses serves to exacerbate the confirmation bias.

> *I'm an all-source analyst, so I use whatever I can get my hands on; but, if the traffic comes from operations, I tend to pay more attention to it than to information in the open literature.*
>
> *There is something special about the word "secret" in my business. It says that it must be important because people had to go and get it rather than its just showing up in the news. We tend to weigh classified material as more important than other sources.*

---

[16] In research methodology, face validity is the concept that a measurement instrument *appears* or *seems* to measure what it is actually intended to measure and requires no theoretical supporting material. In contrast, content validity depends on the content of the domain and established theories to determine its measures of validity. See David Brinberg and Joseph McGrath, *Validity and the Research Process*; Edward Carmines and Richard Zeller, *Reliability and Validity Assessment*; Jerome Kirk and Marc Miller, *Reliability and Validity in Qualitative Research*; Mark Litwin, "How to measure survey reliability and validity"; William Trochim, *The Research Methods Knowledge Base*.

We get all kinds of sourced material, but I think I trust technical collection more than the other INTs.

I try to use everything we get, but, if we are jammed, I rely on sources we collect.

Our value-added is classified sourcing. Everybody has access to the Web and CNN.

All our customers are analysts these days. What we bring to the party is information no one else has.

We're in the business of secrets. If you see that stamped on something, it must be there for a reason.

The over reliance on classified information for hypothesis testing creates a situation in which the data are screened and sorted by the organization before they are selected and tested by the analysts. Classified information comes from very specific types of technical and human sources, and it is filtered through very specific reporting channels. It also has a tendency to become homogeneous because of the source types and reporting mechanisms. Because it is generated and packaged in specific formats using specific processes, classified information lacks the diversity that is inherent in open information, and this contributes to confirmation bias.

In sum, operating under difficult time constraints, trying to make new work accord with previous products, trying to maintain the prestige and power of the organization, and assigning greater weight to secret information than to open information have a cumulative effect, and the analyst often finds himself or herself trying to produce daily products using the most time-efficient strategies available instead of generating or testing hypotheses by way of refutation.

The persistence of the notion of tradecraft, coupled with organizational norms, promotes the use of disjointed analytic strategies by separating intelligence analysts from other scientific disciplines. These conditions have had an effect on the self-concept of analysts and have molded the way analysts perceive their own identity.

Finding: Analytic Identity

The self is something which has a development; it is not initially there, at birth, but arises in the process of social experience and activity, that is, develops in the given individual as a result of his relations to that process as a whole and to other individuals within that process.

George Mead.[17]

Asked to define their profession, the majority of analysts described the process of analysis rather than the actual profession. The question, "What is an intelligence analyst?" resulted most often in a description of the work day and of the production cycle of analytic products and very seldom in an explanation of analytic methodology or a definition of an analyst outside of some specific context. With very few exceptions, analysts did not describe intelligence analysis as its own discipline with its own identity, epistemology, and research tradition.

This is not necessarily uncommon. When physicians are asked to describe their profession, they tend to respond with a specific subdiscipline: "I'm a cardio-thoracic surgeon," for example. When asked for a more general description, however, they tend to respond, "I'm a doctor" or "I'm a physician." That is, in selective, insular professional cultures, practitioners are able to define their role in both a specific and general fashion. Intelligence analysts had difficulty defining their professional identity in a general way and often relied on specific context to explain what it is that they do and, by extension, who they are.

The perception of individual analysts regarding their professional identity was associated most often with their organization's function or with their own educational background and not with intelligence analysis as its own unique discipline.

I work counternarcotics.

I work counterterrorism.

I'm a military analyst.

I'm a leadership analyst.

I'm an economist.

I'm a political scientist.

In addition to these categories, many analysts described their professional identity in terms of intelligence collection methods or categories.

I do all-source analysis.

I'm a SIGINT analyst.

I'm an IMINT analyst.

I'm a technical analyst.

---

[17] George Mead was an American pragmatist philosopher and social psychologist, who, with John Dewey, made the University of Chicago the home of pragmatist philosophy and the "Chicago School" of sociology at the end of the 19th century. George Mead, *Mind, Self, and Society.*

The shift in focus to daily analytic products, the changes in the production cycle, and a heterogeneously defined professional discipline have had an additional effect on the professional identity of analysts within the Intelligence Community. Analysts often commented that they perceived their job and their daily work routine as more akin to reporting than to analysis.

> *Basically, on a day-to-day basis, it's like working at CNN, only we're CNN with secrets. Actually, it's more like CNN's* Headline News.

> *Imagine* USA Today *with spies—bullet points, short paragraphs, the occasional picture. You know, short and simple.*

> *I think of myself as a writer for the most important newspaper in the world.*

Many analysts expressed dissatisfaction with the shift in work processes from long-term forecasts and toward current reporting and the subsequent shift in their own professional identity within the Intelligence Community. The current sentiment about identity was often contrasted against an idealized past that was described as being freer of current production practices and products.

> *About 15 years ago, I would have described myself as a scholar. Now, I'm a reporter. I've got 15 people trying to change my work into bullet points. Presumably, nobody has time to read anymore.*

> *When I joined, it seemed that the word "analyst" was shorthand for "problem solver." Now, it's shorthand for "reporter."*

> *I'm proud of where I work. I'm proud of the job that we do. But, it is hard to take pride in one paragraph. I have to look at the big picture, or I would get discouraged.*

> *I spend most of my waking hours doing this, but I still can't really say what an analyst is.*

> *I'm not a reporter, and I'm not an academic. I'm somewhere in between.*

The heterogeneous descriptions and definitions of intelligence analysis as a professional discipline were consistent findings during this study, indicating that there needs to be a clear articulation and dissemination of the identity and epistemology of intelligence analysis. A clearly defined professional identity would help to promote group cohesion, establish interagency ties and relationships, and reduce intra- and interagency communication barriers by establishing a professional class throughout the Intelligence Community. At an individual level, a clearly defined professional identity helps to reduce job dis-

satisfaction and anxiety by giving larger meaning to an individual's daily actions.[18]

Finding: Analytic Training

> *When I started, there wasn't much training available. There were a few advanced courses, but, for the most part, it was on the job.*

A professional identity is generally a disciplinary norm, and it regularly occurs in other domains that are as cognitively demanding as intelligence analysis, such as medicine, aeronautics, and jurisprudence. These other domains practice a general system of professional enculturation that progresses from a basic education program to specialized training.[19] These training programs help to differentiate communities of practitioners from the general public, create specific and unique professional identities, and develop basic communication and task-specific skills. They also help the profession to continue to advance through formal research efforts.

This is not the case within the Intelligence Community as a whole. Generally, the intelligence agencies that do provide basic and advanced training do so independently of other intelligence organizations.[20] A number of intelligence agencies do not provide basic analytic training at all or have only recently begun to do so, relying instead on on-the-job experiences and informal mentoring.

> *We haven't had a culture of training analysts here in the past. It's only in the last year or so that we've started to change that.*

> *When I started here, analysts were considered administrative personnel. We didn't have a training program. I think they just started one this year.*

> *My background was technical analysis, and we had a lot of operational training where I used to work. But now that I'm doing more strategic analysis, I've had to make it up as I go along.*

---

[18] Philip Cushman, *Constructing the Self, Constructing America*; Anthony Giddens, *Modernity and Self-Identity*; John P. Hewitt, *Self and Society*; Lewis P. Hinchman and Sandra K. Hinchman, *Memory, Identity, Community*; Carl Jung, *The Undiscovered Self*; George Levine, ed., *Constructions of the Self*.

[19] Enculturation is the process or mechanism by which a culture is instilled in a human being from birth until death. In this instance, professional enculturation refers to the acquisition of a professional identity through specific cultural rituals and practices, as displayed, for example, by practitioners who have graduated from medical school, law school, and basic military training.

[20] See footnote 7 in the Introduction for several recent cross-agency training initiatives.

We have a basic training program, but it is different from the other agencies. Our mission is different. The problem is that we talk past each other all the time.

When I got hired, I had an advanced degree. People assumed that, if I had a Masters, I could just figure out what I was supposed to do.

The focus of training within the community varies widely and is shaped by the mission of the agency, such as technical, tactical, and operational. Many spend a considerable amount of time teaching new analysts how to prepare briefings, write papers, and perform administrative functions unique to their agency. This is logical from the perspective of agency managers, who naturally believe that investments made in personnel, training, and readiness ought to be tailored specifically for their own organizations.

The problem with an agency-centric view is that, without a general communitywide training program for intelligence analysts, agencies and their analysts have difficulty finding, communicating, and interacting with one another.[21] Analysts often said they were disinclined to draw on resources outside of their own agency, indicating that either they do not know whom to contact or their experience in the past has been influenced by a strict organizational focus.

The media keep talking about intelligence failures and communication breakdowns in the Intelligence Community. What do they expect? We don't even speak the same language.

It's taken me 15 years to build my own network. If I didn't have my own contacts, I wouldn't know who to call.

I don't bother going outside. Our focus is different here.

We have official channels, but it only really works if you trust the person on the other end of the phone. That's hard to do if you don't know them.

Without an inclusive communitywide basic training program, differentiation between the intelligence analysis discipline, as a whole, and other fields of study is unlikely. A community of practitioners will have difficulty interacting with one another, communicating between and within organizations, and establishing a professional identity, which is a key ingredient in the development of a professional discipline.

---

[21] Stephen Marrin, *CIA's Kent School: A Step in the Right Direction* and "Improving CIA Analysis by Overcoming Institutional Obstacles."

PART II

Ethnography of Analysis

Taxonomy of Intelligence Analysis Variables

Systemic Variables
- Organization
  - Internal
    - Structure
    - Leadership
    - Culture
      - History
    - Traditions
      - Social Practice
      - Taboo
      - Group Characteristics
    - Hierarchy
    - Resources & Incentives
      - Manpower
      - Budget
      - Technology
      - Assets
      - R&D
      - Facilities
    - Work Groups-Teams
- External
  - Consumer Needs
  - Time and Imperatives
  - Consumer Use
  - Consumer Structure
  - Consumer Hierarchy
  - Conumer Reporting
- Politics
  - Internal-Organization
    - Policy
    - Tradition
    - Taboo
    - Security/Access
  - External-National
    - Law
    - Policy
  - External-International
    - Security
      - Denial
      - Deception
    - Policy

Systematic Variables
- User Requirements
- Operations
  - Information Acquisition
    - Collection Methods
      - Overt
      - Covert
        - Information Reliability
        - Reproducible
        - Consistent
        - Information Validity
        - Historical
        - Single Source
        - Dual Source
        - Triangulation
- Information Archive
  - Storage
  - Access
  - Correlation
  - Retrieval
- Analytical Methodology
  - Approach
    - Intuitive
    - Structured
    - Semi-structured
  - Information Processing
    - Historical Information
    - Current Information
  - Decision Strategies
    - Estimative
    - Predictive
- Reporting
  - Verbal Methods
  - Written Methods

Idiosyncratic Variables
- Weltanschauung
- (worldview)
  - Affiliation
    - Familial
    - Cultural
    - Ethnic
    - Religious
    - Social
    - Linguistic
    - Political
  - Psychology
    - Bias
    - Personality Profile
    - Security Trust
    - Cognitive Processing
      - Learning Style
      - Information Acquisition
      - Information Processing
      - Expertise
      - Problem-solving
      - Decisionmaking
      - Cognitive Load
      - Speed/Accuracy
    - Stress Effects
  - Education
    - Domain
    - Location
    - Mentor
  - Training
    - Organizational
    - Domain
    - Procedural
  - Readiness
    - Resources
    - Facilities

Communicative Variables
- Formal
  - Inter-organization
    - Hierarchical
    - Inter-division
    - Inter-group
  - Intra-organization
    - Hierarchical
    - Intra-division
    - Intra-group
  - Individual
    - Hierarchical
    - Inter-division
    - Intra-group
- Informal
  - Inter-organization
    - Hierarchical
    - Inter-division
    - Inter-group
  - Intra-organization
    - Hierarchical
    - Intra-division
    - Intra-group
  - Individual
    - Hierarchical
    - Inter-group
    - Intra-group
  - Technology
    - Networked Analysis
    - Collaboration

CHAPTER THREE

A Taxonomy of Intelligence Variables[1]

Science is organized knowledge.

Herbert Spencer[2]

Aristotle may be the father of scientific classification, but it was biologist Carolus Linnaeus who introduced the first formal taxonomy—kingdom, class, order, genera, and species—in his *Systema Naturae* in 1735. By codifying the naming conventions in biology, Linnaeus's work provided a reference point for future discoveries. Darwin's development of an evolutionary theory, for example, benefited greatly from Linnaeus's creation of a hierarchical grouping of related organisms. The *Systema Naturae* taxonomy was not a fixed product but rather a living document. Linnaeus himself revised it through 10 editions, and later biologists have continued to modify it.[3]

In response to new discoveries and the development of new research methods in other domains, taxonomies were created to help organize those disciplines and to assist researchers in identifying variables that required additional study. The development of specific taxonomies—from highly structured systems, such as the periodic table of chemical elements, to less structured approaches, such as Bloom's Taxonomy[4]—is a key step in organizing knowl-

[1] A version of this chapter, "Developing a Taxonomy of Intelligence Analysis Variables," originally appeared in *Studies in Intelligence* 47, no. 3 (2003): 61–71.

[2] Herbert Spencer's *The Study of Sociology*, published in 1874, set the stage for the emergence of sociology as a discipline.

[3] Ernst Haeckel introduced *phylum* to include related classes and *family* to include related genera in 1866. The Linnaeus taxonomy is currently being revised to accommodate genomic mapping data.

edge and furthering the growth of individual disciplines. A taxonomy differentiates domains by specifying the scope of inquiry, codifying naming conventions, identifying areas of interest, helping to set research priorities, and often leading to new theories. Taxonomies are signposts, indicating what is known and what has yet to be discovered.

This chapter, to which more than 100 individuals contributed their time and advice, proposes a taxonomy for the field of intelligence. It is my hope that the resulting organized listing of variables will help practitioners strengthen their understanding of the analytic process and point them in directions that need additional attention.

Intelligence Analysis

> *We could have talked about the science of intelligence, but . . . the science of intelligence is yet to be invented.*
>
> Charles Allen[5]

Developing an intelligence taxonomy is complicated by the fact that the literature in the field is episodic and reflects specialized areas of concern. Perhaps it is best to begin with what appears to be a key distinction between general analysis and intelligence analysis, that of solving a problem in the public domain, and solving a problem in a private or secret domain.

Ronald Garst articulates two arguments that are used to support this distinction: intelligence analysis is more time sensitive than analysis in other domains and it deals with information that intentionally may be deceptive.[6] The notion that intelligence is uniquely time sensitive is questionable, however. Intelligence is not the only domain where time constraints can force decisions to be made before data are complete. Time is always a key variable, whether one is in an operating room or in a cockpit. To be sure, intelligence is a life and death profession, but so are medicine and mass transportation. In each instance, failure can mean casualties.

Garst's point about intentional deception is more germane. With the possible exception of business and financial markets, analysts in other fields seldom deal with intentional deception. As discussed in Chapter One, Michael Warner makes a good case for secrecy being the primary variable distinguish-

---

[4] See Benjamin S. Bloom, *Taxonomy of Educational Objectives*. Bloom's taxonomy is a classification of levels of intellectual behavior in learning, including knowledge, comprehension, application, analysis, synthesis, and evaluation.

[5] Comment made by the Associate Director of Central Intelligence for Collection at a public seminar on intelligence at Harvard University, spring 2000.

[6] Ronald Garst, *A Handbook of Intelligence Analysis.*

ing intelligence from other such activities.[7] He argues that the behavior of the subject of intelligence changes if the subject is aware of being observed or analyzed. As discussed earlier, Warner's argument is supported by a long history of psychological research, beginning with an experimental program between 1927 and 1930 at Western Electric's Hawthorne Works in Chicago.[8]

Intentional deception can occur outside intelligence—in connection with certain law enforcement functions, for example—but most of the professional literature treats this as the exception rather than the rule. In the case of intelligence analysis, deception *is* the rule; the validity of the data is always in doubt. Moreover, intelligence analysts are specifically trained to take deception into account as part of the analytic process—to look for anomalies and outliers instead of focusing on the central tendencies of distribution.

The taxonomy being developed here requires a definition of intelligence analysis that is specific to the field. Intelligence pioneer Sherman Kent, who saw intelligence as a "special category of knowledge," laid the foundation for understanding the activities inherent in intelligence analysis by demonstrating that the analytic process itself was subject to being analyzed.[9] Kent's approach to analysis was to reduce the process to smaller functional components for individual study.[10] For example, he described intelligence analysis as having a basic descriptive element, a current reporting element, and an estimative element.

Following suit, other authors focused attention on the process or methodological elements of intelligence analysis. In *Intelligence Research Methodology*, Jerome Clauser and Sandra Weir followed Kent's three functional areas and went on to describe basic research foundations and the inductive and deductive models for performing intelligence analysis.[11] Garst's *Handbook of Intelligence Analysis* contains less background in basic research methods than Clauser and Weir's book, but it is more focused on the intelligence cycle.[12]

Bruce Berkowitz and Allan Goodman highlight the process of strategic intelligence and define intelligence analysis as: "[T]he process of evaluating and transforming raw data into descriptions, explanations, and conclusions for intelligence consumers."[13] Lisa Krizan, too, focuses on process. She writes

---

[7] Michael Warner.

[8] The Hawthorne Effect. See footnote 5 in Chapter Two.

[9] Sherman Kent, *Strategic Intelligence for American World Policy.*

[10] See Chapter Seven for a fuller discussion of this approach, now usually referred to as meta-analysis.

[11] Jerome K. Clauser and Sandra M. Weir, *Intelligence Research Methodology.*

[12] See also: Morgan Jones, *The Thinker's Toolkit*. Jones's book is a popular version of the work of Garst and Clauser and Weir in that it describes a collection of analytic methods and techniques for problem-solving; however, the methods are not necessarily specific to intelligence.

that, "At the very least, analysis should fully describe the phenomenon under study, accounting for as many relevant variables as possible. At the next higher level of analysis, a thorough explanation of the phenomenon is obtained, through interpretation of the significance and effects of its elements on the whole."[14] In addition, several authors have written about individual analytic approaches.[15]

Although the referenced works focus on methods and techniques, they do not suggest that analysis is limited to these devices. The view that analysis is both a process and a collection of specific techniques is explicit in the above definitions. Analysis is seen as an action that incorporates a variety of tools to solve a problem. Different analytic methods have something to offer different analytic tasks.

Although largely implicit in the above definitions, analysis is also seen as a product of cognition, and some authors directly link the two. Robert Mathams defines analysis as: "[T]he breaking down of a large problem into a number of smaller problems and performing mental operations on the data in order to arrive at a conclusion or generalization."[16] Avi Shlaim writes: "Since the facts do not speak for themselves but need to be interpreted, it is inevitable that the individual human propensities of an intelligence officer will enter into the process of evaluation."[17] Yet others describe analysis as a process whereby: "[I]nformation is compared and collated with other data, and conclusions that also incorporate the memory and judgment of the intelligence analyst are derived from it."[18]

Several authors make the case that analysis is not just a product of cognition but is itself a cognitive process. J. R. Thompson and colleagues write that "[I]ntelligence analysis is an internal, concept-driven activity rather than an external data-driven activity."[19] In his *Psychology of Intelligence Analysis*, Heuer observes: "Intelligence analysis is fundamentally a mental process, but understanding this process is hindered by the lack of conscious awareness of the workings of our own minds."[20] Ephraim Kam comments: "The process of intelligence analysis and assessment is a very personal one. There is no agreed-upon analytical schema, and the analyst must primarily use his belief

---

[13] Bruce D. Berkowitz and Allan E. Goodman, *Strategic Intelligence for American National Security*, 85. See Chapter Four for more on the intelligence cycle.
[14] Lisa Krizan, *Intelligence Essentials for Everyone*.
[15] See the apprendix for a listing of the literature.
[16] Robert Mathams, "The Intelligence Analyst's Notebook."
[17] Avi Shlaim, "Failures in National Intelligence Estimates: The Case of the Yom Kippur War."
[18] John Quirk et al., *The Central Intelligence Agency: A Photographic History.*
[19] J. R. Thompson, R. Hopf-Weichel, and R. Geiselman, *The Cognitive Bases of Intelligence Analysis*.
[20] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis.*

system to make assumptions and interpret information. His assumptions are usually implicit rather than explicit and may not be apparent even to him."[21]

These definitions reflect the other end of the spectrum from those concerned with tools and techniques. They suggest that the analytic process is a construction of the human mind and is significantly different from individual to individual or group to group. Certainly, Kam goes farthest along this path, but even he does not suggest that one forgo tools; rather, he says that the process of choosing the tool is governed by cognition as well.

Recognizing that the scope of intelligence analysis is so broad that it includes not only methods but also the cognitive process is a significant step. Viewing analysis as a cognitive process opens the door to a complex array of variables. The psychology of the individual analyst must be considered, along with individual analytic tools. In the broadest sense, this means not merely understanding the individual psyche but also understanding the variables that interact with that psyche. In other words, *intelligence analysis is the socio-cognitive process,*[22] *occurring within a secret domain, by which a collection of methods is used to reduce a complex issue to a set of simpler issues.*

Developing the Taxonomy

> *The first step of science is to know one thing from another. This knowledge consists in their specific distinctions; but in order that it may be fixed and permanent distinct names must be given to different things, and those names must be recorded and remembered.*
>
> Carolus Linnaeus

My research was designed to isolate variables that affect the analytic process. The resulting taxonomy is meant to establish parameters and to stimulate dialogue in order to develop refinements. Although a hierarchic list is artificial and rigid, it is a first step in clarifying areas for future research. The actual variables are considerably more fluid and interconnected than such a structure suggests. Once the individual elements are refined through challenges in the literature, they might be better represented by a link or web diagram.[23]

To create this intelligence analysis taxonomy, I used Alexander Ervin's applied anthropological approach, which employs multiple data collection methods to triangulate results.[24] I also drew on Robert White's mental work-

---

[21] Ephraim Kam, *Surprise Attack. The Victim's Perspective*, 120

[22] That is, analysis does not occur in a vacuum. It is socially constructed. See Lev Vygotsky, *Mind and Society.*

[23] See Chapter Four for Judith Meister Johnston's systems analysis approach to describing the fluidity of the intelligence process.

load model, David Meister's behavioral model, and the cognitive process model of Gary Klein and his colleagues.[25] Each model focuses on a different aspect of human performance: White's examines the actual task and task requirements; Meister's looks at the behavior of individuals performing a task; and Klein's uses verbal protocols to identify the cognitive processes of individuals performing a task.

Surveying the literature. My research began with a review of the literature, both for background information and for the identification of variables. The intelligence literature produced by academics and practitioners tends to be episodic, or case-based. This is not unique to the field of intelligence. A number of disciplines—medicine, business, and law, for example—are also case-based. Many of the texts were general or theoretical rather than episodic. Again, this is not an uncommon phenomenon. The review yielded 2,432 case studies, journal articles, technical reports, transcripts of public speeches, and books related to the topic. I then narrowed the list to 374 pertinent texts on which a taxonomy of intelligence analysis could be built, and I analyzed them to identify individual variables and categories of variables that affect intelligence analysis.[26]

Using a methodology known as "Q-Sort," by which variables are sorted and categorized according to type, I read each text and recorded the variables that each author identified.[27] These variables were then sorted by similarity into groups. Four broad categories of analytic variables emerged from this process.[28]

Refining the prototype. Next, I used the preliminary taxonomy derived from my reading of the literature to structure interviews with 51 substantive experts and 39 intelligence novices. In tandem, I conducted two focus group sessions, with five individuals in each group. As a result of the interviews and focus group discussions, I added some variables to each category, moved some to different categories, and removed some that appeared redundant.

Testing in a controlled setting. Finally, to compare the taxonomy with specific analytic behaviors, I watched participants in a controlled intelligence analysis–training environment. Trainees were given information on specific

---

[24] Alexander Ervin, *Applied Anthropology.* See Chapter One, note 4 for a definition of triangulation.

[25] Robert White, *Task Analysis Methods*; David Meister, *Behavioral Analysis and Measurement Methods*; G. Klein, R. Calderwood, and A. Clinton-Cirocco, *Rapid Decision Making on the Fire Ground.*

[26] A copy of the list and search criteria is available from the author.

[27] William Stephenson, *The Study of Behavior: Q-Technique and its Methodology.* See Chapter Eleven for additional information on this methodology.

[28] I would like to credit Dr. Forrest Frank of the Institute for Defense Analyses for his suggestions regarding the naming convention for the categories of variables in the accompanying chart.

cases and directed to use various methods to analyze the situations and to generate final products. During the training exercises, the verbal and physical behavior of individuals and groups were observed and compared with the taxonomic model. I participated in a number of the exercises myself to gain a better perspective. This process corroborated most of the recommendations that had been made by the experts and novices and also yielded additional variables for two of the categories.

The resulting taxonomy is purely descriptive. It is not intended to demonstrate the weight or importance of each variable or category. That is, the listing is not sufficient to predict the effect of any one variable on human performance. The intention of the enumeration is to provide a framework for aggregating existing data and to create a foundation for future experimentation. Once the variables have been identified and previous findings have been aggregated, it is reasonable to consider experimental methods that would isolate and control individual variables and, in time, indicate sources of error and potential remediation

Systemic Variables

- Organization
  - Internal
    - Structure
    - Leadership
    - Culture
      - History
        - Traditions
      - Social Practice
        - Taboo
      - Group Characteristics
    - Hierarchy
    - Resources and Incentives
      - Manpower
      - Budget
      - Technology
        - Assets
        - R&D
      - Facilities
    - Work Groups-Teams
  - External
    - Consumer Needs
    - Time and Imperatives
    - Consumer Use
    - Consumer Structure
    - Consumer Hierarchy
    - Conumer Reporting
- Politics
  - Internal-Organization
    - Policy
    - Tradition
    - Taboo
    - Security/Access
  - External-National
    - Law
    - Policy
  - External-International
    - Security
      - Denial
      - Deception
    - Policy

Systemic Variables

The column of Systemic Variables incorporates items that affect both an intelligence organization and the analytic environment. Organizational variables encompass the structure of the intelligence organization; leadership, management, and management practices; history and traditions; the working culture, social practices within the organization, and work taboos; and organizational demographics. They also include internal politics, the hierarchical reporting structure, and material and human resources. Industrial and organizational psychology, sociology, and management studies in business have brought attention to the importance of organizational behavior and its effect on individual work habits and practices. The works of Allison, Berkowitz and Goodman, Elkins, Ford, Godson, and Richelson, among others, examine in general the organizational aspects of intelligence.[29]

Systematic Variables
- User Requirements
- Operations
  - Information Acquisition
    - Collection Methods
      - Overt
      - Covert
    - Information Reliability
      - Reproducible
      - Consistent
    - Information Validity
      - Historical
      - Single Source
      - Dual Source
      - Triangulation
- Information Archive
  - Storage
  - Access
  - Correlation
  - Retrieval
- Analytical Methodology
  - Approach
    - Intuitive
    - Structured
    - Semi-structured
  - Information Processing
    - Historical Information
    - Current Information
  - Decision Strategies
    - Estimative
    - Predictive
- Reporting
  - Verbal Methods
  - Written Methods

The Systemic Variables category also focuses on environmental variables. These include such external influences on the organization as consumer needs and requirements, time limitations, and methods for using the information; and the consumer's organization, political constraints, and security issues. The works of Betts, Hulnick, Hunt, Kam, and Laqueur address the environmental and consumer issues that affect intelligence analysis.[30] Case studies that touch on various systemic variables include: Allison, on the Cuban missile crisis; Betts, on surprise attacks; Kirkpatrick, on World War II tactical intelligence operations; Shiels, on government failures; Wirtz, on the Tet offensive in Vietnam; and Wohlstetter, on Pearl Harbor.[31]

Systematic Variables

The Systematic Variables are those that affect the process of analysis itself. They include the user's specific requirements, how the information was acquired, the information's reliability and validity, how the information is stored, the prescribed methods for analyzing and processing the information, specific strategies for making decisions about the information, and the methods used to report the information to consumers.

A number of authors have written about the analytic tools and techniques used in intelligence, among them Clauser and Weir, on intelligence research methods; Jones, on analytic techniques; and Heuer, on alternative competing hypotheses.

---

[29] Graham T. Allison, *Essence of Decision*; Bruce D. Berkowitz and Allan E. Goodman, *Best Truth*; Dan Elkins, *An Intelligence Resource Manager's Guide*; Harold Ford, *Estimative Intelligence*; Roy Godson, *Comparing Foreign Intelligence*; Jeffrey Richelson, *The U.S. Intelligence Community.*

[30] Richard K. Betts, "Policy-makers and Intelligence Analysts: Love, Hate or Indifference"; Arthur S. Hulnick, "The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach"; David Hunt, Com*plexity and Planning in the 21st Century*; Kam, *Surprise Attack;* Walter A. Laqueur, *The Uses and Limits of Intelligence.*

[31] Allison; Richard K. Betts, *Surprise Attack*; Lyman B. Kirkpatrick, Jr., *Captains Without Eyes: Intelligence Failures in World War II*; Frederick L. Shiels, P*reventable Disasters: Why Governments Fail*; James J. Wirtz, *The Tet Offensive: Intelligence Failure in War*; Roberta Wohlstetter, *Pearl Harbor: Warning and Decision.*

Comparatively little work has been done comparing structured techniques to intuition. Robert Folker's work is one of the exceptions; it compares the effectiveness of a modified form of alternative competing hypotheses with intuition in a controlled experimental design. His study is unique in the field and demonstrates that experimental methods are possible. Geraldine Krotow's research, on the other hand, looks at differing forms of cognitive feedback during the analytic process and makes recommendations to improve intelligence decisionmaking.[32]

Idiosyncratic Variables

- Weltanschauung (world-view)
- Affiliation
  - Familial
  - Cultural
  - Ethnic
  - Religious
  - Social
  - Linguistic
  - Political
- Psychology
  - Bias
  - Personality Profile
  - Security Trust
  - Cognitive Processing
    - Learning Style
    - Information Acquisition
    - Information Processing
    - Expertise
    - Problem-solving
    - Decisionmaking
    - Cognitive Load
    - Speed/Accuracy
  - Stress Effects
- Education
  - Domain
  - Location
  - Mentor
- Training
  - Organizational
  - Domain
  - Procedural
- Readiness
  - Resources
  - Facilities

Idiosyncratic Variables

Variables in the third column are those that influence individuals and their analytic performance. These include the sum of life experiences and enculturation—familial, cultural, ethnic, religious, linguistic, and political affiliations—that identify an individual as a member of a group. I have used the German word *Weltanschauung* (customarily rendered in English as "world view") to denote this concept. These idiosyncratic variables also encompass such psychological factors as biases, personality profiles, cognitive styles and processing, cognitive loads,[33] expertise, approach to problem-solving, decisionmaking style, and reaction to stress. Finally, there are such domain variables as education, training, and the readiness to apply knowledge, skills, and abilities to the task at hand.

The relevant psychological literature is extensive. Amos Tversky and Daniel Kahneman began to examine psychological biases in the early 1970s.[34] Their work has found its way into the intelligence literature through Butterfield,

[32] Geraldine Krotow, *The Impact of Cognitive Feedback on the Performance of Intelligence Analysts*, 176.

[33] "Cognitive loads" are the amount/number of cognitive tasks weighed against available cognitive processing power.

[34] Amos Tversky and Daniel Kahneman, "The Belief in the 'Law of Small Numbers'" and "Judgment Under Uncertainty: Heuristics and Biases."

Davis, Goldgeier, and Heuer, among others.[35] Decisionmaking and problem-solving have been studied since the early 1920s, and these topics are reflected in Heuer's work as well.[36] Personality-profiling, too, is well understood and has had an impact on recent intelligence practices and theory.[37]

Communicative Variables
- Formal
  - Inter-organization
    - Hierarchical
    - Inter-division
    - Inter-group
  - Intra-organization
    - Hierarchical
    - Intra-division
    - Intra-group
  - Individual
    - Hierarchical
    - Inter-division
    - Intra-group
- Informal
  - Inter-organization
    - Hierarchical
    - Inter-division
    - Inter-group
  - Intra-organization
    - Hierarchical
    - Intra-division
    - Intra-group
  - Individual
    - Hierarchical
    - Inter-group
    - Intra-group
  - Technology
    - Networked Analysis
    - Collaboration

Other well-researched areas, however, have yet to be studied in the context of intelligence. Acculturation and enculturation, educational factors, and training strategies, for example, may yet yield interesting results and insights into the field of intelligence.[38]

Communicative Variables

The fourth category contains variables that affect interaction within and among groups. Because communication is the vital link within the system—among processes and among individuals—this group of variables logically could be included in each of the other three categories. Its broad relevance, however, makes it seem reasonable to isolate it as a distinct area of variability. The Communicative Variables include formal and informal communications within an organization (from products to e-mails), among organizations, and between individuals and the social networks they create. In his essay on estimative probability, Kent highlights this area by describing the difficulty that producers of intelligence have in communicating the likelihood of an event to their consumers.[39] In addition to addressing organizational issues, case studies by Wohlstetter and others touch on communication and social networks and the impact that communication

[35] Alexander Butterfield, *The Accuracy of Intelligence Assessment*; Jack Davis, "Combating Mindset"; James M. Goldgeier, "Psychology and Security"; Heuer.

[36] Frank H. Knight, *Risk, Uncertainty and Profit.*

[37] Caroline Ziemke, Philippe Loustaunau, and Amy Alrich, *Strategic Personality and the Effectiveness of Nuclear Deterrence*.

[38] Acculturation is the cultural change that occurs in response to extended firsthand contact between two or more previously autonomous groups. It can result in cultural changes in groups as well as individuals.

[39] Sherman Kent, *"*Words of Estimative Probability.*"*

has on the analytic process.[40] This is an area that could benefit from additional study.

Conclusion

> *There is rarely any doubt that the unconscious reasons for practicing a custom or sharing a belief are remote from the reasons given to justify them.*
>
> —Claude Levi-Strauss[41]

As it is now practiced, intelligence analysis is art, tradecraft, and science. There are specific tools and techniques to help perform the tasks, but, in the end, it is left to individuals to use their best judgment in making decisions. This is not to say that science is not a part of intelligence analysis. Science is born of organized knowledge, and organizing knowledge requires effort and time. The work on this taxonomy is intended to help that process by sparking discussion, identifying areas where research exists and ought to be incorporated into the organizational knowledge of intelligence, and identifying areas where not enough research has been performed.

There are a number of parallels in the field of medicine, which, like intelligence, is art, tradecraft, and science. To solve problems, practitioners are trusted to use their best judgment by drawing on their expertise. What is important to remember is that there are numerous basic sciences driving medical practice. Biology, chemistry, physics, and all of the subspecialties blend together to create the medical sciences, the foundation on which modern medicine rests. The practice of medicine has been revolutionized by the sciences that underpin its workings.

Intelligence analysis has not experienced that revolution. Unlike medicine, the basic sciences that underpin intelligence are the human sciences, which are considerably more multivariate and more difficult to control. Because of these factors, it is a more complex task to measure "progress" in the human sciences. Even so, there are numerous domains from which intelligence may borrow. Organizational behavior is better understood today than ever before. Problem-solving and decisionmaking have been researched since the 1920s.

---

[40] Wohlstetter.

[41] Claude Levi-Strauss wrote *Structural Anthropology* in 1958, setting the stage for structuralism to emerge as an analytic interpretive method. Broadly, structuralism seeks to explore the interrelationships (the "structures") through which meaning is produced within a culture. This meaning, according to structural theory, is produced and reproduced through various practices, phenomena, and activities that serve as systems of "signification." A structuralist studies activities as diverse as food preparation and serving rituals, religious rites, games, literary and non-literary texts, and forms of entertainment to discover the ways in which cultural significance develops.

Structural anthropology addresses many of the enculturation and identity issues that affect individual behavior. Cognitive scientists are building models that can be tested in experimental conditions and used for developing new tools and techniques. Sociology and social theory have much to offer in studying social networks and communication.

The organization of knowledge in intelligence is not a small task, but I believe that the effort should be undertaken for the betterment of the profession. The taxonomy proposed here could serve as a springboard for a number of innovative projects, for example: development of a research matrix that identifies what is known and how that information may be of use in intelligence analysis, setting a research agenda in areas of intelligence that have been insufficiently studied, application of research from other domains to develop additional training and education programs for analysts, creation of a database of lessons learned and best practices to build a foundation for an electronic performance support system, integration of those findings into new analytic tools and techniques, and development of a networked architecture for collaborative problem-solving and forecasting. It is my hope that this taxonomy will help intelligence practitioners take steps in some of these new directions.

CHAPTER FOUR

Testing the Intelligence Cycle Through Systems Modeling and Simulation

Judith Meister Johnston[1]
Rob Johnston

Throughout the Intelligence Community, the process of analysis is represented conventionally by a model known as the Intelligence Cycle (See next page). Unfortunately, the model omits elements and fails to capture the process accurately, which makes understanding the challenges and responsibilities of intelligence analysis much more difficult. It also complicates the tasks of recognizing where errors can occur and determining methods for change based on accurate predictions of behavior. Our analysis of the Intelligence Cycle, employing a systems approach and a simulation created to represent it, demonstrated these shortcomings.[2] Because of its wide acceptance and use in training and in discussions of the analytic process, the traditional representation of the Intelligence Cycle will be closely considered in this chapter, especially with regard to its impact on analytic products, its effectiveness, and its vulnerability to error and failure.

The Traditional Intelligence Cycle

The Intelligence Cycle is customarily illustrated as a repeating process consisting of five steps.[3] ***Planning and direction*** encompasses the management of

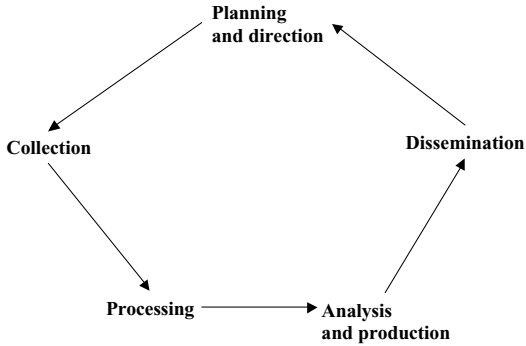
---

[1] Dr. Judith Meister Johnston is an educational psychologist with expertise in human performance technology and instructional systems design. A Booz Allen Hamilton Associate, she supports human factors work for the Intelligence Community.

[2] Simulation involves the development of a computer-based model that represents the internal processes of an event or situation and estimates the results of proposed actions.

the entire effort and involves, in particular, determining collection requirements based on customer requests. ***Collection*** refers to the gathering of raw data to meet the collection requirements. These data can be derived from any number and type of open and secret sources. ***Processing*** refers to the conversion of raw data into a format analysts can use. ***Analysis and production*** describes the process of evaluating data for reliability, validity, and relevance; integrating and analyzing it; and converting the product of this effort into a meaningful whole, which includes assessments of events and implications of the information collected. Finally, the product is ***disseminated*** to its intended audience.[4]

The Traditional Intelligence Cycle



In some ways, this process resembles many other production cycles. It is prescriptive, structured, made up of discrete steps, and expected to yield a specific product. The traditional depiction of the process in the Intelligence Cycle, however, is not an accurate representation of the way intelligence is produced. The notion of a cycle assumes that the steps will proceed in the prescribed order and that the process will repeat itself continuously with reliable results. This type of representation gives the impression that all inputs are constant and flow automatically, but it does not address elements that may influence the movement of the cycle, positively or negatively.

The most significant assumption about the Intelligence Cycle model, that it provides a means for helping managers and analysts deliver a reliable product, should be examined at the outset. This can be accomplished through two types of analyses. The first is a systematic examination of the elements of the process, the inputs it relies on, and the outcomes that can be expected. The second uses a systemic approach to identifying the relationships of the elements in the process and their influence on each other.

[3] Central Intelligence Agency, *A Consumer's Guide to Intelligence*.
[4] Central Intelligence Agency, *Factbook on Intelligence.*

Systematic Analysis

Many disciplines (for example, business process, organizational management, human performance technology, program evaluation, systems engineering, and instructional systems design) employ specific methods to analyze the effectiveness of products, programs, or policy implementation. Although they are often given different, domain-specific names and may involve varying levels of detail, these analytic methods involve the identification of *inputs*, *processes*, and *outputs*. Once these elements are identified, the evaluation process maps the relationships of the inputs, their implementation in processes, and their impact on intended—as opposed to actual—outputs.[5] The reasoning underlying this approach is that an effective product, result, or action is one that matches its objectives and that these objectives are reached by processes that logically lead from the objectives to results. Along the way, existing practices and barriers to reaching goals effectively can be identified. Finally, interventions, which can range in complexity from simple job aids to a complete restructuring of the process, can be proposed and implemented and their impacts assessed.[6]

This method of analysis has been employed successfully to evaluate processes that have characteristics similar to the Intelligence Cycle, and we use it here to examine the effectiveness of the Intelligence Cycle and its utility in representing the creation of sound analytic products while avoiding failure or error.

Findings Based on Systematic Analysis

The Intelligence Cycle is represented visually to provide an easy-to-grasp and easy-to-remember representation of a complex process. Although this type of representation may make the flow of information and the interrelationships of steps easy to identify, it does not indicate who or what may affect the completion of a step or the resources needed to begin the next step. In its concise form, then, the visual representation of the Intelligence Cycle is reduced to a map of information handling. Without explicit descriptions of the steps in the process or the benefit of prior knowledge, it can raise questions of accuracy and completeness and can occasion misconceptions, particularly concerning the roles and responsibilities of intelligence analysts.

---

[5] Marc J. Rosenberg, "Performance technology: Working the system."

[6] Roger Kaufman, "A Holistic Planning Model: A Systems Approach for Improving Organizational Effectiveness and Impact."

Inputs, Processes, and Outputs of the Intelligence Cycle

Inputs	Processes	Outputs
Policymaker and other stakeholder questions, requirements	***Direction***	Data collection requirements
Data collection requirements, assessment of available resources and capabilities	***Planning***	Task assignment, potential data sources, focus of analysis
Open-source data: foreign broadcasts, newspapers, periodicals, books; Classified data: case officer, diplomatic, and attaché reports, electronics, satellite photos	***Collection***	Potentially relevant data
Potentially relevant data	***Processing:*** Reduction of data in a variety of formats to consistent pieces of usable data	Usable Data
Usable data	***Analysis***: Integration, evaluation, assessment of reliability, validity, and relevance of data	Findings
Analytic review	*Production*: Peer review, supervisory review	Written briefs, studies, long range assessments, short range assessments, oral briefs, national intelligence estimates
Written briefs, studies, long-range assessments, short-range assessments, oral briefs, national intelligence estimates	**Dissemination**	Appropriate product to address customer's need

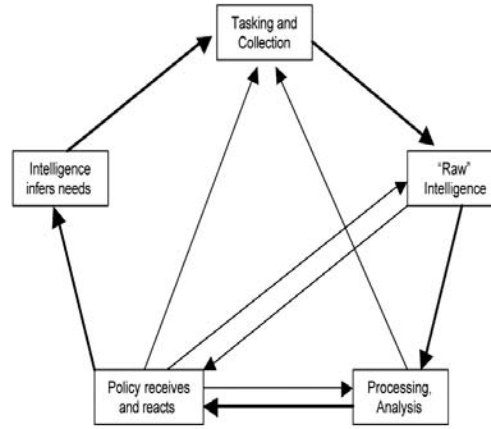
The table above depicts a more detailed input, process, and output analysis and makes some relationships clearer—for example, the steps that include two actions (planning and direction, analysis and production) have been separated into distinct processes—but it sill leaves a number of questions unanswered. It is difficult to see from this analysis specifically who is responsible for providing inputs, carrying out the processes, and producing outputs; and what requirements are expected of the inputs and outputs.

An important issue that this analysis only partly clarifies is the role of analysts. Nor does it demonstrate how great a burden the process places on them,

an especially important point. Assuming that the actions identified in the "Processes" column are ultimately the responsibility of the intelligence analyst, the steps of the process move from a heavy reliance on information coming in from sources outside the analyst's control to a heavy reliance on the analyst to produce and manage the final submission of the product.

Another important defect in this analysis is that steps in the cycle do not accurately represent the differences in the cognitive complexity involved in preparing a long-range assessment or a national intelligence estimate and that required for a two-paragraph brief on a current situation. The same can be said about the process required to develop each of the products.

Treverton's "Real" Intelligence Cycle



The Intelligence Cycle depicts a sequential process and does not provide for iterations between steps. This is not an accurate reflection of what happens, particularly in the collection and production steps, where the challenges of defining policymaker needs and shaping collection necessitate repeated refinement of requirements by policymakers or of inferences by the Intelligence Community. A more accurate picture of the steps in the process and their iterative tendencies may be seen in Greg Treverton's model, which he terms the "Real" Intelligence Cycle (above).[7]

Mark Lowenthal proposes another model.[8] Although presented in a more linear fashion than Treverton's, it focuses on the areas where revisions and reconsiderations take place, representing iteration in a slightly different light. Both models provide a more realistic view of the entire process. In addition, assuming that the analyst's role is represented by the "Processing, Analysis" box, the Treverton model allows us to focus visually and conceptually on the demands that the process can place on the analyst. However, neither model

[7] Gregory F. Treverton, *Reshaping National Intelligence in an Age of Information.*
[8] Mark W. Lowenthal, *Intelligence: From Secrets to Policy.*

provides an effective way of showing who is responsible for what, and neither reflects the impact of the work on the individuals responsible for producing the reports—particularly the analyst—nor the reliance of the analyst on a variety of factors beyond his or her control.

In sum, this brief evaluation of the Intelligence Cycle with respect to its inputs, processes, and outputs shows us that the traditional model:

- assumes the process works the same way for all objectives, regardless of complexity and cognitive demands;
- does not represent the iterative nature of the process required for meeting objectives;
- does not identify responsibilities for completing steps and allows for misconceptions in this regard;
- does not accurately represent the impact of resource availability on analysts.

To better understand these limitations and the relationships among elements in the process, it is necessary to step back and take a longer view of the process, using a different method of analysis.

Systemic Analysis

If we think of the phenomenon that is being described by the Intelligence Cycle as a system and perform a systems analysis, we may be able to derive a greater understanding of process relationships, a better representation of the variables affecting the process, and a greater level of detail regarding the process itself.

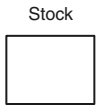
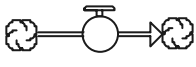
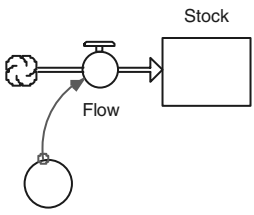
The premise that underlies systems analysis as a basis for understanding phenomena is that the whole is greater than the sum of its parts. A systems analysis allows for the inclusion of a variety of influences and for the identification of outliers that are obfuscated in other types of analyses but that often play major roles. A systems analysis is accomplished through the examination of phenomena as cause-and-effect patterns of behavior. This approach is called a "closed feedback loop" in systems analysis. It requires a close examination of relationships and their influences, provides a longer view of these relationships, and often reveals new insights based on trends rather than on discrete events.[9]

The systems model diagrammed below is a visual representation of the process. The elements of the Intelligence Cycle are identified in terms of their

[9] Fritjof Capra, "Criteria of Systems Thinking"; David L. Kaufman, Jr., *Introduction to Systems Thinking*.

relationships with each other, the flow of the process, and phenomena that influence the elements and the flow. The model uses four icons to represent actions and relationships within the system: stocks, flows, converters, and connectors. The icons and their placement within the systems model show the relationships of the elements of the analyzed phenomenon.

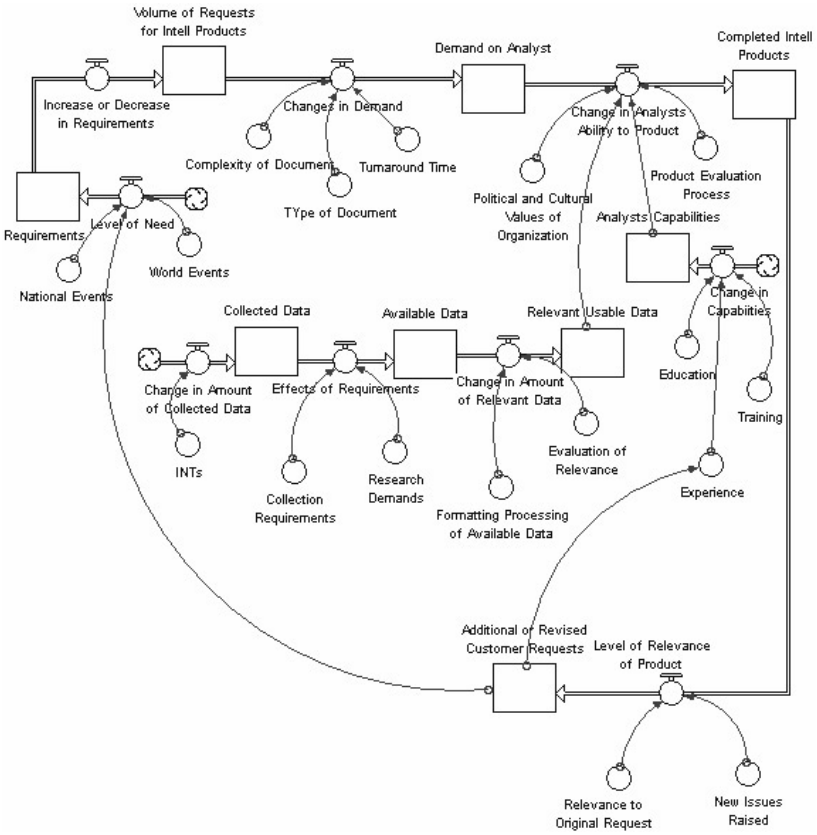
The Components of the Systems Model

Icon	Purpose
	***Stocks*** represent accumulations. These are quantities that can increase or decrease, such as the amount of work that needs to be completed, the time available in which to do it, experience one might bring to a task.
	***Flows*** represent activities. They control the filling or draining of stocks, causing conditions to change.
	Converters change inputs into outputs. They usually represent the variables that initiate change. In the example, a converter might represent a sudden and drastic world event.
	***Connectors*** link elements to other elements, representing assumptions about what depends on what.

The systems model of the Intelligence Cycle provides insights into the process of analysis as well as other factors that can influence the successful and timely completion of an intelligence task. It also provides a way to understand the impact of change in any area of the Intelligence Cycle on other elements, either through reflection or by applying mathematical values to the influences and relationships and running simulations of the model.

Demand. As in the traditional Intelligence Cycle model, the systems model begins with requirements for information that generally come from policymakers. These requirements are represented by a *stock* (found in the upper left-hand quarter of the diagram) because they can increase or decrease based on the level of need for information (a *flow*). The change in level of need is influenced by national and world events, as well as by new questions or requests for clarification of items in previously delivered products. Each request does not contribute equally to the amount of work, which is influenced by the types of documents or products requested, the complexity of the prod-

Systems Model of the Intelligence Cycle



ucts, and the turnaround time imposed. All of these factors determine the level of demand placed on the analyst.

Production. This section focuses on the process of producing intelligence products. The elements described are tied, directly or indirectly, to the flow that represents changes in the analyst's ability to produce. In turn, these changes cause products to be completed and requests of policymakers to be fulfilled. It is important to note that this portion of the model deals with factors that influence the *act* of analysis and does not attempt to address *methods* of analysis.

Factors that influence the ability of analysts to produce are numerous and complex, as shown. First and foremost are the capabilities an analyst brings to the task. This is represented by a *stock*—usually an increasing one—that derives from an analyst's education, training, and experience.

Another influence is the number and frequency of evaluations and revisions imposed on a work in progress. That a draft of the product must be reviewed and edited by a number of others places variable constraints on the time available for creating the original draft. This factor increases in significance when the product requested has a short deadline.

Political and cultural values of the organization also have an influence, usually constraining. Strictly following traditional heuristics and methods and meeting organizational or management expectations may influence both an analyst's ability to produce and the quality of the output. The weight of these influences will vary depending on the experience of the analyst.

Another factor that influences the analyst's ability to produce is the amount of relevant, usable data (a *stock*) available. The term "relevant, usable data" describes all collected intelligence that is relevant to meeting the request and that exists in a format that can be used to develop the product. To become usable, the data must go through steps that are influenced by a variety of *other* people, organizations, systems, and technologies. This process is represented by the stock and flow chain that appears across the middle of diagram.

Data are collected from a variety of sources, represented by the INTs converter.[10] These data add to the stock of collected data. The ways in which accumulated collected data are converted to the stock of available data are influenced by internal research demands and specific collection requirements imposed by analysts, policymakers, and others. Once the data are processed and put into an agreed format for use by intelligence producers and consum-

[10] INT is an abbreviation for intelligence, usually contained in acronyms for the various types of intelligence collected by the Intelligence Community, for example, HUMINT (human intelligence) and SIGINT (signals intelligence).

ers, they add to the accumulation of material that affects the ability of an analysts to produce.

Product Influences. The accumulation of completed intelligence products, which is represented as a *stock*, is not in practice an end-state for analysis. A customer may respond to a delivered product by levying additional or revised tasking. In all instances, this information influences the level of need for policymaker requirements and causes the process to begin again. Each iteration of the process is different, not because the steps in the process change, but because those responsible for carrying out the steps have changed as a result of their participation in the previous run. These changes can include a greater level of experience with the process, with the customer, with the topic area, or with the quirks of the organization and its processes. The changes are a manifestation of the concept that the system is greater than the sum of its parts.

Findings Based on Systems Analysis

Systems analysis clearly demonstrates the defects of the traditional Intelligence Cycle model. To recapitulate briefly, the traditional model merely represents a simple list of steps rather than a dynamic closed feedback loop. In addition, although the steps are meant to be performed by several different actors, the model does not provide useful information about what each actually contributes to the cycle, nor does it accurately represent the path a request takes as it is addressed. Another problem with the traditional model is that none of its features help identify ways of developing a consistent product. For example, there is no allowance for a statement of objectives or for any formative or summative evaluations to check that objectives have been met.

On the other hand, the model that resulted from a systems analysis provides a more complex view. That model shows cause and effect, and it shows what other elements have an impact on the development of intelligence products and how and why elements depend on other elements. These advantages of the systems model are clearly apparent in considering the role of analysts in production, a crucial element of the cycle that the traditional model all but ignores.

Impact on Production and Analyst's Control. Study of the systems model shows that the "Analyst's Ability to Produce" (upper right-hand quarter of the diagram) is the central factor in the production cycle and the driver of the feedback loop. The systems view also makes us aware of a less obvious fact that is critically important to a discussion of analytic failure.

A look at the entire system makes readily apparent the number of factors of varying complexity that influence an analyst's ability to produce: the analyst's capabilities; the product evaluation process; the political and cultural values of

the organization; the amount of relevant, usable data and actions related to transforming collected data to relevant, usable data; and the level of demand on the analyst. Of these five factors, only one—the analyst's capabilities—is an internal factor and somewhat under the analyst's control.[11] Yet, even though the other factors are out of the analyst's control, the analyst must rely on them to accomplish the goal and to meet the expectations of customers and the organization. When the proportion of external factors to internal factors is as unbalanced as the systems model of the Intelligence Cycle demonstrates, the causes of stress in the analytic environment increase, as does the possibility that stress will occur.

In such a high stress environment, where the critical person is responsible for delivering a product whose development relies on a great number of factors beyond his or her control, there is greater risk of error, with an increased likelihood of incomplete or incorrect products. Tendencies to use shortcuts, to avoid creative thinking, and to minimize the perceived impact of certain events or actions become more apparent in this situation, especially if their implementation means reducing the workload and the stressors. Results of working in such an environment can include increased personnel turnover, missed or undervalued information, lack of attention to detail, decreased motivation, and a lack of creativity in approaching analysis. Moreover, with analysts so central to the process, their actions may have a widespread and, thus, powerful influence on the entire system. This change can be positive or negative. Given the number of elements influencing the analyst that are out of his or her control, however, it is unlikely that the changes would positively affect the quality, accuracy, and number of intelligence products created.

Recommendations

Revisit the traditional intelligence model. The traditional Intelligence Cycle model should either be redesigned to depict accurately the intended goal, or care should be taken to discuss explicitly its limitations whenever it is used. Teaching with an inaccurate aid merely leads to misconceptions that can result in poor performance, confusion, and a need for unlearning and reteaching. If the objective is to capture the entire intelligence process, from the request for a product to its delivery, including the roles and responsibilities of Intelligence Community members, then something more is required. This should be a model that pays particular attention to representing accurately all the elements of the process and the factors that influence them.

---

[11] Even the factors that contribute to the analyst's capabilities, notably experience and training, may be seen to be under the control of others when access to, and selection of, them are considered.

Further Study. The use of simulation allows us to determine flaws in the system that basic informational models cannot address. A simulation moves the image of the Intelligence Cycle from a picture that selectively and indiscriminately illustrates a series of events to a holistic and realistic representation of events, responsibilities, processes, and their impact on each other. The simulation of the Intelligence Cycle developed for this analysis is merely a first step. Further work should be done with it to validate the representations, test for vulnerabilities, predict outcomes, and accurately recommend changes.

Lightening the Analyst's Load. The systems model reveals a serious imbalance in the work processes analysts can and cannot control. It is unrealistic and unnecessary to consider reorganizing the process to correct this defect. However, there are actions that could be taken to provide analysts more control over external factors without significantly altering their roles. These actions would also reduce the amount of potential influence that one group could have over the entire process.

First, analysts might be designated as reports or research analysts. The former would prepare products that address short-term tasks, such as writing for the PDB. As the process of collection and analysis is different for short- and long-term products, this might be a responsibility assigned primarily to more junior analysts. Research analysts might be those with more experience. Freed from the obligation to prepare short-term reports, senior analysts would be available for more intense research efforts, such as those required for an NIE. In addition, cross-training or experience in creating both products and the flexibility to switch from one process to another would provide greater depth of personnel. If appropriate, movement to a long-term research position could be viewed as professional development.

Second, personnel responsible for formatting and processing raw data might be included on accounts. Through association with a particular group, people in this role would have a reasonable idea of analysts' requirements. This would allow the preselection and preparation of data, so that analysts could focus on "connecting the dots." The skills requirement for this role would be akin to those of a research librarian.

Third, tools to help the analyst identify, manage, and fuse relevant data could be identified and deployed. These tools, which need not be limited to those that are technology-based, should be used to support analysts' labor-intensive tasks, thereby freeing them to focus on the analysis of data.

Employ alternative methods for examining work processes. Just as we used alternative methods to examine the Iintelligence Cycle, and as managers press analysts to use alternative analyses in assessing their targets, so should managers employ alternative methods for examining work processes. These methods

should not simply test effectivenss; they should also identify vulnerabilities and potential sources of other problems in the community's analytical methods.

PART III

Potential Areas for Improvement

CHAPTER FIVE

Integrating Methodologists into Teams of Experts[1]

Intelligence analysis, like other complex tasks, demands considerable expertise. It requires individuals who can recognize patterns in large data sets, solve complex problems, and make predictions about future behavior or events. To perform these tasks successfully, analysts must dedicate years to researching specific topics, processes, and geographic regions.

Paradoxically, it is the specificity of expertise that makes expert forecasts unreliable. While experts outperform novices and machines in pattern recognition and problem solving, expert predictions of future behavior or events are seldom as accurate as Bayesian probabilities.[2] This is due, in part, to cognitive biases and processing-time constraints and, in part, to the nature of expertise itself and the process by which one becomes an expert.

Becoming an Expert

Expertise is commitment coupled with creativity. By this, I mean the commitment of time, energy, and resources to a relatively narrow field of study and the creative energy necessary to generate new knowledge in that field. It takes a great deal of time and regular exposure to a large number of cases to become an expert.

---

[1] A version of this chapter originally appeared as "Integrating Methodologists into Teams of Substantive Experts in *Studies in Intelligence* 47, no. 1 (2003): 57–65.

[2] Method for estimating the probability of a given outcome developed by Thomas Bayes (1702–61), an English mathematician. See Thomas Bayes, "An Essay Toward Solving a Problem In the Doctrine of Chances."

Entering a field of study as a novice, an individual needs to learn the heuristics and constraints—that is, the guiding principles and rules—of a given task in order to perform that task. Concurrently, the novice needs to be exposed to specific cases that test the reliability of such heuristics. Generally, novices find mentors to guide them through the process of acquiring new knowledge. A fairly simple example would be someone learning to play chess. The novice chess player seeks a mentor who can explain the object of the game, the number of spaces, the names of the pieces, the function of each piece, how each piece is moved, and the necessary conditions for winning or losing a game.

In time, and with much practice, the novice begins to recognize patterns of behavior within cases and, thus, becomes a journeyman. With more practice and exposure to increasingly complex cases, the journeyman finds patterns not only within but also among cases and, more important, learns that these patterns often repeat themselves. Throughout, the journeyman still maintains regular contact with a mentor to solve specific problems and to learn more complex strategies. Returning to the example of the chess player, the individual begins to learn patterns of opening moves, offensive and defensive strategies, and patterns of victory and defeat.

The next stage begins when a journeyman makes and tests hypotheses about future behavior based on past experiences. Once he creatively generates knowledge, rather than simply matching patterns, he becomes an expert. At this point, he becomes responsible for his own knowledge and no longer needs a mentor. In the chess example, once a journeyman begins competing against experts, makes predictions based on patterns, and tests those predictions against actual behavior, he is generating new knowledge and a deeper understanding of the game. He is creating his own cases rather than relying on the cases of others.

The chess example in the preceding paragraphs is a concise description of an apprenticeship model. Apprenticeship may seem to many a restrictive, old-fashioned mode of education, but it remains a standard method of training for many complex tasks. In fact, academic doctoral programs are based on an apprenticeship model, as are such fields as law, music, engineering, and medicine. Graduate students enter fields of study, find mentors, and begin the long process of becoming independent experts and generating new knowledge in their respective domains.

To some, playing chess may appear rather trivial when compared, for example, with making medical diagnoses, but both are highly complex tasks. Chess heuristics are well-defined, whereas medical diagnoses seem more open ended and variable. In both instances, however, there are tens of thousands of potential patterns. A research study discovered that chess masters had spent between 10,000 and 20,000 hours, or more than 10 years, studying and play-

ing chess. On average, a chess master acquires 50,000 different chess patterns.[3]

Similarly, a diagnostic radiologist spends eight years in full-time medical training - four years of medical school and four years of residency—before being qualified to take a national board exam and begin independent practice.[4] According to a 1988 study, the average diagnostic radiology resident sees 40 cases per day, or around 12,000 cases per year.[5] At the end of a residency, a diagnostic radiologist has acquired an average of 48,000 cases.

Psychologists and cognitive scientists agree that the time it takes to become an expert depends on the complexity of the task and the number of cases, or patterns, to which an individual is exposed. The more complex the task, the longer it takes to build expertise, or, more accurately, the longer it takes to experience a large number of cases or patterns.

The Power of Expertise

Experts are individuals with specialized knowledge suited to perform the specific tasks for which they are trained, but that expertise does not necessarily transfer to other domains.[6] A master chess player cannot apply chess expertise in a game of poker; although both chess and poker are games, a chess master who has never played poker is a novice poker player. Similarly, a biochemist is not qualified to perform neurosurgery, even though both biochemists and neurosurgeons study human physiology. In other words, the more complex a task, the more specialized and exclusive is the knowledge required to perform that task.

Experts perceive meaningful patterns in their domains better than do nonexperts. Where a novice perceives random or disconnected data points, an expert connects regular patterns within and among cases. This ability to identify patterns is not an innate perceptual skill; rather, it reflects the organization of knowledge after exposure to and experience with thousands of cases.[7]

Experts have a deeper understanding of their domains than do novices, and they utilize higher-order principles to solve problems.[8] A novice, for example, might group objects together by color or size, whereas an expert would group

---

[3] W. Chase and H. Simon, "Perception in Chess."

[4] American College of Radiology. Personal communication, 2002.

[5] A. Lesgold et al., "Expertise in a Complex Skill: Diagnosing X-Ray Pictures."

[6] M. Minsky and S. Papert, *Artificial Intelligence*; J. Voss and T. Post, "On the Solving of Ill-Structured Problems."

[7] O. Akin, *Models of Architectural Knowledge*; D. Egan and B. Schwartz, "Chunking in Recall of Symbolic Drawings"; K. McKeithen et al., "Knowledge Organization and Skill Differences in Computer Programmers."

the same objects according to their function or utility. Experts comprehend the meaning of data better than novices, and they weigh variables with different criteria within their domains better. Experts recognize variables that have the largest influence on a particular problem and focus their attention on those variables.

Experts have better domain-specific short-term and long-term memory than do novices.[9] Moreover, experts perform tasks in their domains faster than novices and commit fewer errors while solving problems.[10] Interestingly, experts also go about solving problems differently. At the beginning of a task, experts spend more time thinking about a problem than do novices, who immediately seek to find a solution.[11] Experts use their knowledge of previous cases as context for creating mental models to solve given problems.[12]

Because they are better at self-monitoring than novices, experts are more aware of instances where they have committed errors or failed to understand a problem.[13] They check their solutions more often and recognize when they are missing information necessary for solving a problem.[14] Experts are aware of the limits of their knowledge and apply their domain's heuristics to solve problems that fall outside of their experience base.

The Paradox of Expertise

The strengths of expertise can also be weaknesses.[15] Although one would expect experts to be good forecasters, they are not particularly good at it. Researchers have been testing the ability of experts to make forecasts since the 1930s.[16] The performance of experts has been tested against Bayesian probabilities to determine if they are better at making predictions than simple statistical models. Seventy years later, after more than 200 hundred experiments in different domains, it is clear that the answer is no.[17] Supplied with an equal amount of data about a particular case, Bayesian probability data are as

---

[8] M. Chi, P. Feltovich, and R. Glaser, "Categorization and Representation of Physics Problems by Experts and Novices"; M. Weiser and J. Shertz, "Programming Problem Representation in Novice and Expert Programmers."

[9] W. Chase and K. Ericsson, "Skill and Working Memory."

[10] W. Chase, "Spatial Representations of Taxi Drivers."

[11] J. Paige and H. Simon, "Cognition Processes in Solving Algebra Word Problems."

[12] Voss and Post.

[13] M. Chi, R. Glaser, and E. Rees, "Expertise in Problem Solving"; D. Simon and H. Simon, "Individual Differences in Solving Physics Problems."

[14] J. Larkin, "The Role of Problem Representation in Physics."

[15] C. Camerer and E. Johnson, "The Process-Performance Paradox in Expert Judgment."

[16] H. Reichenbach, *Experience and Prediction*; T. Sarbin, "A Contribution to the Study of Actuarial and Individual Methods of Prediction."

good as, or better than, an expert at making calls about the future. In fact, the expert does not tend to outperform the actuarial table, even if given more specific case information than is available to the statistical model.[18]

There are few exceptions to these research findings, but these are informative. When experts are given the results of the Bayesian probabilities, for example, they tend to score as well as the statistical model if they use the statistical information in making their own predictions.[19] In addition, if experts have privileged information that is not reflected in the statistical table, they will actually perform better than does the table. A classic example is the case of the judge's broken leg. Judge X has gone to the theater every Friday night for the past 10 years. Based on a Bayesian analysis, one would predict, with some certainty, that this Friday night would be no different. An expert knows, however, that the judge broke her leg Thursday afternoon and is expected to be in the hospital until Saturday. Knowing this key variable allows the expert to predict that the judge will not attend the theater this Friday.

Although having a single variable as the determining factor makes this case easy to grasp, analysis is seldom, if ever, this simple. Forecasting is a complex, interdisciplinary, dynamic, and multivariate task wherein many variables interact, weight and value change, and other variables are introduced or omitted.

During the past 30 years, researchers have categorized, experimented, and theorized about the cognitive aspects of forecasting and have sought to explain why experts are less accurate forecasters than statistical models. Despite such efforts, the literature shows little consensus regarding the causes or manifestations of human bias. Some have argued that experts, like all humans, are inconsistent when using mental models to make predictions. That is, the model an expert uses for predicting X in one month is different from the model used for predicting X in a later month, although precisely the same case and same data set are used in both instances.[20] A number of researchers point

---

[17] R. Dawes, D. Faust, and P. Meehl, "Clinical Versus Actuarial Judgment"; W. Grove and P. Meehl, "Comparative Efficiency of Informal (Subjective, Impressionistic) and Formal (Mechanical, Algorithmic) Prediction Procedures."

[18] R. Dawes, "A Case Study of Graduate Admissions"; Grove and Meehl; H. Sacks, "Promises, Performance, and Principles"; T. Sarbin, "A Contribution to the Study of Actuarial and Individual Methods of Prediction"; J. Sawyer, "Measurement and Prediction, Clinical and Statistical"; W. Schofield and J. Garrard, "Longitudinal Study of Medical Students Selected for Admission to Medical School by Actuarial and Committee Methods."

[19] L. Goldberg, "Simple Models or Simple Processes?"; L. Goldberg, "Man versus Model of Man"; D. Leli and S. Filskov, "Clinical-Actuarial Detection of and Description of Brain Impairment with the Wechsler-Bellevue Form I."

[20] J. Fries, et al., "Assessment of Radiologic Progression in Rheumatoid Arthritis."

to human biases to explain unreliable expert predictions.[21] There is general agreement that two types of bias exist:

- *Pattern bias*: looking for evidence that confirms rather than rejects a hypothesis and/or filling in—perhaps inadvertently—missing data with data from previous experiences;
- *Heuristic bias*: using inappropriate guidelines or rules to make predictions.

Paradoxically, the very method by which one becomes an expert explains why experts are much better than novices at describing, explaining, performing tasks, and solving problems within their domains but, with few exceptions, are worse at forecasting than are Bayesian probabilities based on historical, statistical models. A given domain has specific heuristics for performing tasks and solving problems, and these rules are a large part of what makes up expertise. In addition, experts need to acquire and store tens of thousands of cases in order to recognize patterns, generate and test hypotheses, and contribute to the collective knowledge within their fields. In other words, becoming an expert requires a significant number of years of viewing the world through the lens of one specific domain. This concentration gives the expert the power to recognize patterns, perform tasks, and solve problems, but it also focuses the expert's attention on one domain to the exclusion of others. It should come as little surprise, then, that an expert would have difficulty identifying and weighing variables in an interdisciplinary task, such as forecasting an adversary's intentions. Put differently, an expert may know his specific domain, such as economics or leadership analysis, quite thoroughly, but that may still not permit him to divine an adversary's intention, which the adversary may not himself know.

The Burden on Intelligence Analysts

Intelligence analysis is an amalgam of a number of highly specialized domains. Within each, experts are tasked with assembling, analyzing, assigning meaning to, and reporting on data, the goals being to describe an event or observation, solve a problem, or make a forecast. Experts who encounter a case outside their field repeat the steps they initially used to acquire their expertise. Thus, they can try to make the new data fit a pattern previously acquired; recognize that the case falls outside their expertise and turn to their domain's heuristics to try to give meaning to the data; acknowledge that the

[21] J. Evans, *Bias in Human Reasoning*; R. Heuer, *Psychology of Intelligence Analysis*; D. Kahneman, P. Slovic, and A. Tversky, *Judgment Under Uncertainty*; A. Tversky and D. Kahneman, "The Belief in the 'Law of Small Numbers'."

case still does not fit with their expertise and reject the data set as an anomaly; or consult other experts.

An item of information, in and of itself, is not domain specific. Imagine economic data that reveal that a country is investing in technological infrastructure, chemical supplies, and research and development. An economist might decide that the data fit an existing spending pattern and integrate these facts with prior knowledge about a country's economy. The same economist might decide that this is a new pattern that needs to be stored in long-term memory for some future use, or he might decide that the data are outliers of no consequence and may be ignored. Finally, the economist might decide that the data would be meaningful to a chemist or biologist and, therefore, seek to collaborate with other specialists, who might reach different conclusions regarding the data than would the economist.

In this example, the economist is required to use his economic expertise in all but the final option of consulting other experts. In the decision to seek collaboration, the economist is expected to know that what appears to be new economic data may have value to a chemist or biologist, domains with which he may have no experience. In other words, the economist is expected to know that an expert in some other field might find meaning in data that appear to be economic.

Three disparate variables complicate the economist's decisionmaking:

- *Time context*. This does not refer to the amount of time necessary to accomplish a task but rather to the limitations that come from being close to an event. The economist cannot say a priori that the new data set is *the* critical data set for some future event. In "real time," they are simply data to be manipulated. It is only in retrospect, or in long-term memory, that the economist can fit the data into a larger pattern, weigh their value, and assign them meaning.

- *Pattern bias*. In this particular example, the data have to do with infrastructure investment, and the expert is an economist. Thus, it makes perfect sense to try to manipulate the new data within the context of economics, recognizing, however, that there may be other, more important angles.

- *Heuristic bias*. The economist has spent a career becoming familiar with and using the guiding principles of economic analysis and, at best, has only a vague familiarity with other domains and their heuristics. An economist would not necessarily know that a chemist or biologist could identify what substance is being produced based on the types of equipment and supplies that are being purchased.

This example does not describe a complex problem; most people would recognize that the data from this case might be of value to other domains. It is one isolated case, viewed retrospectively, which could potentially affect two other domains. But, what if the economist had to deal with 100 data sets per day? Now, multiply those 100 data sets by the number of domains potentially interested in any given economic data set. Finally, put all of this in the context of "real time." The economic expert is now expected to maintain expertise in economics, which is a full-time endeavor, while simultaneously acquiring some level of experience in every other domain. Based on these expectations, the knowledge requirements for effective collaboration quickly exceed the capabilities of the individual expert.

The expert is left dealing with all of these data through the lens of his own expertise. Let's assume that he uses his domain heuristics to incorporate the data into an existing pattern, store the data in long-term memory as a new pattern, or reject the data set as an outlier. In each of these options, the data stop with the economist instead of being shared with an expert in some other domain. The fact that these data are not shared then becomes a potentially critical case of analytic error.[22]

In hindsight, critics will say that the implications were obvious—that the crisis could have been avoided if the data had been passed to one or another specific expert. In "real time," however, an expert often does not know which particular data set would have value for an expert in another domain.

The Pros and Cons of Teams

One obvious solution to the paradox of expertise is to assemble an interdisciplinary team. Why not simply make all problem areas or country-specific data available to a team of experts from a variety of domains? This ought, at least, to reduce the pattern and heuristic biases inherent in relying on only one domain. Ignoring potential security issues, there are practical problems with this approach. First, each expert would have to sift through large data sets to find data specific to his expertise. This would be inordinately time-consuming and might not even be routinely possible, given the priority accorded gisting and current reporting.

Second, during the act of scanning large data sets, the expert inevitably would be looking for data that fit within his area of expertise. Imagine a chemist who comes across data that show that a country is investing in technologi-

[22] L. Kirkpatrick, *Captains Without Eyes: Intelligence Failures in World War II*; F. Shiels, *Preventable Disasters*; J. Wirtz, *The Tet Offensive: Intelligence Failure in War*; R. Wohlstetter, *Pearl Harbor.*

cal infrastructure, chemical supplies, and research and development (the same data that the economist analyzed in the previous example). The chemist recognizes that these are the ingredients necessary for a nation to produce a specific chemical agent, which could have a military application or could be benign. The chemist then meshes the data with an existing pattern, stores the data as a new pattern, or ignores the data as an anomaly.

The chemist, however, has no frame of reference regarding spending trends in the country of interest. He does not know if the investment in chemical supplies represents an increase, a decrease, or a static spending pattern—answers the economist could supply immediately. There is no reason for the chemist to know if a country's ability to produce this chemical agent is a new phenomenon. Perhaps the country in question has been producing the chemical agent for years, and these data are part of some normal pattern of behavior.

If this analytic exercise is to begin to coalesce, neither expert must treat the data set as an anomaly and both must report it as significant. In addition, each expert's analysis of the data—an increase in spending and the identification of a specific chemical agent—must be brought together at some point. The problem is, at what point? Presumably, someone will get both of these reports somewhere along the intelligence chain. Of course, the individual who gets these reports will be subject to the same three complicating variables described earlier—time context, pattern bias, and heuristic bias—and may not be able to synthesize the information. Thus, the burden of putting the pieces together will merely have been shifted to someone else in the organization.

In order to avoid shifting the problem from one expert to another, an actual collaborative team could be built. Why not explicitly put the economist and the chemist together to work on analyzing data? The utilitarian problems with this strategy are obvious: not all economic problems are chemical, and not all chemical problems are economic. Each expert would waste an inordinate amount of time. Perhaps one case in 100 would be applicable to both experts, but, during the rest of the day, they would drift back to their individual domains, in part, because that is what they are best at and, in part, just to stay busy.

Closer to the real world, the same example may also have social, political, historical, and cultural aspects. Despite an increase in spending on a specific chemical agent, the country in question may not be inclined to use it in a threatening way. For example, there may be social data unavailable to the economist or the chemist indicating that the chemical agent will be used for a benign purpose. In order for collaboration to work, each team would have to have experts from many domains working together on the same data set.

Successful teams have very specific organizational and structural requirements. An effective team requires discrete and clearly stated goals that are

shared by each team member.[23] Teams also require interdependence and accountability, that is, the success of each individual depends on the success of the team as a whole as well as on the individual success of every other team member.[24]

Effective teams require cohesion, formal and informal communication, cooperation, shared mental models, and similar knowledge structures.[25] Putting combinations such as this in place is not a trivial task. Creating shared mental models may be fairly easy within an air crew or a tank crew, where an individual's role is clearly identifiable as part of a clearly-defined, repetitive team effort, such as landing a plane or acquiring and firing on a target. It is more difficult within an intelligence team, given the vague nature of the goals, the enormity of the task, and the diversity of individual expertise. Moreover, the larger the number of team members, the more difficult it is to generate cohesion, communication, and cooperation. Heterogeneity can also be a challenge; it has a positive effect on generating diverse viewpoints within a team, but it requires more organizational structure than does a homogeneous team.[26]

Without specific processes, organizing principles, and operational structures, interdisciplinary teams will quickly revert to being simply a room full of experts who ultimately drift back to their previous work patterns. That is, the experts will not be a team at all; they will be a group of experts individually working in some general problem space.[27]

---

[23] Dorwin Cartwright and Alvin Zander, *Group Dynamics: Research and Theory*; P. Fandt, W. Richardson, and H. Conner, "The Impact of Goal Setting on Team Simulation Experience"; J. Harvey and C. Boettger, "Improving Communication within a Managerial Workgroup."

[24] M. Deutsch, "The Effects of Cooperation and Competition Upon Group Process"; D. Johnson and R. Johnson, "The Internal Dynamics of Cooperative Learning Groups"; D. Cartwright and A. Zander, *Group Dynamics: Research and Theory;* David Johnson and Roger Johnson, "The Internal Dynamics of Cooperative Learning Groups"; D. Johnson et al., "Effects of Cooperative, Competitive, and Individualistic Goal Structure on Achievement: A Meta-Analysis"; R. Slavin, "Research on Cooperative Learning"; R. Slavin, *Cooperative Learning*.

[25] J. Cannon-Bowers, E. Salas, S. Converse, "Shared Mental Models in Expert Team Decision Making"; L. Coch and J. French, "Overcoming Resistance to Change"; M. Deutsch, "The Effects of Cooperation and Competition Upon Group Process"; L. Festinger, "Informal Social Communication"; D. Johnson et al., "The Impact of Positive Goal and Resource Interdependence on Achievement, Interaction, and Attitudes"; B. Mullen and C. Copper, "The Relation Between Group Cohesiveness and Performance: An Integration"; W. Nijhof and P. Kommers, "An Analysis of Cooperation in Relation to Cognitive Controversy"; J. Orasanu, "Shared Mental Models and Crew Performance"; S. Seashore, *Group Cohesiveness in the Industrial Work-group*.

[26] T. Mills, "Power Relations in Three-Person Groups"; L. Molm, "Linking Power Structure and Power Use"; V. Nieva, E. Fleishman, and A. Rieck, *Team Dimensions: Their Identity, Their Measurement, and Their Relationships*; G. Simmel, *The Sociology of Georg Simmel*.

[27] R. Johnston, *Decision Making and Performance Error in Teams: Research Results*; J. Meister, "Individual Perceptions of Team Learning Experiences Using Video-Based or Virtual Reality Environments."

Can Technology Help?

There are potential technological alternatives to multifaceted teams. For example, an Electronic Performance Support System (EPSS) is a large database that is used in conjunction with expert systems, intelligent agents, and decision aids.[28] Although applying such a system to intelligence problems might be a useful goal, at present, the notion of an integrated EPSS for large complex data sets is more theory than practice.[29] In addition to questions about the technological feasibility of such a system, there are fundamental epistemological challenges. It is virtually inconceivable that a comprehensive computational system could bypass the three complicating variables of expertise described earlier.

An EPSS, or any other computational solution, is designed, programmed, and implemented by a human expert from one domain only, that of computer science. Historians will not design the "historical decision aid," economists will not program the "economic intelligent agent," chemists will not create the "chemical agent expert system." Computer scientists may consult with various experts during the design phase of such a system, but, when it is time to sit down and write code, the programmer will follow the heuristics with which he is familiar.[30] In essence, one would be trading the heuristics of dozens of domains for those that govern computer science. This would reduce the problem of processing time by simplifying and linking data, and it might reduce pattern bias. It would not reduce heuristic bias, however; if anything, it might exaggerate it by reducing all data to a binary state.[31]

This skepticism is not simply a Luddite reaction to technology. Computational systems have had a remarkable, positive effect on processing time, storage, and retrieval. They have also demonstrated utility in identifying patterns within narrowly defined domains. However, intelligence analysis requires the expertise of so many diverse fields of study and is not something a computational system handles well. Although an EPSS, or some other form of computational system, may be a useful tool for manipulating data, it is not a solution to the paradox of expertise.

---

[28] An *Expert System* is a job-specific heuristic process that helps an expert narrow the range of available choices. An *Intelligent Agent* is an automated program (bot) with built-in heuristics used in Web searches. A *Decision Aid* is an expert system whose scope is limited to a particular task.

[29] R. Johnston, "Electronic Performance Support Systems and Information Navigation."

[30] R. Johnston and J. Fletcher, *A Meta-Analysis of the Effectiveness of Computer-Based Training for Military Instruction*.

[31] J. Fletcher and R. Johnston, "Effectiveness and Cost Benefits of Computer-Based Decision Aids for Equipment Maintenance."

Analytic Methodologists

Most domains have specialists who study the scientific process or research methods of their discipline. Instead of specializing in a specific substantive topic, these experts specialize in mastering the research and analytic methods of their domain. In the biological and medical fields, these methodological specialists are epidemiologists. In education and public policy, they are program evaluators. In other fields, they are research methodologists or statisticians. Whatever the label, each field recognizes that it requires experts in methodology who focus on deriving meaning from data, recognizing patterns, and solving problems within a domain in order to maintain and pass on the domain's heuristics. They become in-house consultants—organizing agents—who work to identify research designs, methods for choosing samples, and tools for data analysis.

Because they have a different perspective than do the experts in a domain, methodologists are often called on by substantive experts to advise them on a variety of process issues. On any given day, an epidemiologist, for example, may be asked to consult on studies of the effects of alcoholism or the spread of a virus on a community or to review a double-blind clinical trial of a new pharmaceutical product. In each case, the epidemiologist is not being asked about the content of the study; rather, he is being asked to comment on the research methods and data analysis techniques used.

Although well over 160 analytic methods are available to intelligence analyst, few methods specific to the domain of intelligence analysis exist.[32] Intelligence analysis has few specialists whose professional training is in the process of employing and unifying the analytic practices within the field. It is left to the individual analysts to know how to apply methods, select one method over another, weigh disparate variables, and synthesize the results—the same analysts whose expertise is confined to specific substantive areas and their own domains' heuristics.

Conclusion

Intelligence agencies continue to experiment with the right composition, structure, and organization of analytic teams. Yet, although they budget significant resources for technological solutions, comparatively little is being

[32] Exceptions include: S. Feder, "FACTIONS and Policon"; R. Heuer, *Psychology of Intelligence Analysis*; R. Hopkins, *Warnings of Revolution: A Case Study of El Salvador*; J. Lockwood and K. Lockwood, "The Lockwood Analytical Method for Prediction (LAMP)"; J. Pierce, "Some Mathematical Methods for Intelligence Analysis"; E. Sapp, "Decision Trees"; J. Zlotnick, "Bayes' Theorem for Intelligence Analysis."

done to advance methodological science. Methodological improvements are left primarily to the individual domains, a practice that risks falling into the same paradoxical trap that currently exists. What is needed is an intelligence-centric approach to methodology that will include the methods and procedures of many domains and the development of heuristics and techniques unique to intelligence. In short, intelligence analysis needs its own analytic heuristics that are designed, developed, and tested by professional analytic methodologists.

The desired outcome would be a combined approach that includes formal thematic teams with structured organizational principles, technological systems designed with significant input from domain experts, and a cadre of analytic methodologists. These methodologists would act as in-house consultants for analytic teams, generate new methods specific to intelligence analysis, modify and improve existing methods of analysis, and promote the professionalization of the discipline of intelligence. Although, at first, developing a cadre of analytic methodologists would require using specialists from a variety of other domains and professional associations, in time, the discipline would mature into its own subdiscipline with its own measures of validity and reliability.

CHAPTER SIX

The Question of Foreign Cultures: Combating Ethnocentrism in Intelligence Analysis

The intelligence literature often cautions intelligence professionals to be wary of mirror imaging.[1] Although the term is a misnomer (a mirror image is a reverse image), the concept is that individuals perceive foreigners—both friends and adversaries of the United States—as thinking the same way as Americans.[2] Individuals do, in fact, have a natural tendency to assume that others think and perceive the world in the same way they do. This type of projective identification, or ethnocentrism, is the consequence of a combination of cognitive and cultural biases resulting from a lifetime of enculturation, culturally bound heuristics, and missing, or inadequate, information.[3]

Ethnocentrism is a phenomenon that operates on a conscious level, but it is difficult to recognize in oneself and equally difficult to counteract. In part, this is because, in cases of ethnocentric thinking, an individual does not recognize that important information is missing or, more important, that his worldview and problem-solving heuristics interfere with the process of recognizing information that conflicts or refutes his assumptions.

Take, for example, the proposition that others do not think like Americans. It seems only intuitive that other tribes, ethnic groups, nationalities, and states

---

[1] Alexander Butterfield, *The Accuracy of Intelligence Assessment;* Richards J. Heuer, Jr., *Psychology of Intelligence Analysis*; Lisa Krizan, *Intelligence Essentials for Everyone*; J. R. Thompson, R. Hopf-Weichel, and R. Geiselman, *The Cognitive Bases of Intelligence Analysis*.

[2] In this work, I use the broader term "ethnocentrism" to refer to the concept represented by mirror imaging and projective identification .

[3] In anthropology, ethnocentrism is the tendency to judge the customs of other societies by the standards of one's own culture. This includes projecting one's own cognition and norms onto others.

have different histories, languages, customs, educational practices, and cultures and, therefore, must think differently from one another.

The problem, however, is that the cognitive process of understanding or even recognizing that there are cultural and cognitive differences is not intuitive at all. Intuition is the act of immediate cognition, that is, perceiving something directly through the use of culturally dependent heuristics and cognitive patterns accumulated through a lifetime without requiring the use of rational or formal processes. This effort appears doomed to failure, because "trying to think like them" all too often results in applying the logic of one's own culture and experience to try to understand the actions of others, without knowing that one is using the logic of one's own culture. This, however, does not have to be the case. Through acculturation and the use of specific strategies, tools, and techniques, it is possible to combat the effects of ethnocentrism without trying to "think like them." This text includes two short case studies on failures to recognize ethnocentrism, both drawn from the author's own experience and told from his perspective. These failures are then examined with the goal of developing strategies and techniques to combat ethnocentric bias.

Case Study One: Tiananmen Square

At the time of the prodemocracy protests of the Chinese students and, to a lesser extent, workers, between April and June of 1989, I too was a college student. I mention this because American college students and Chinese college students tend to perceive themselves in very different ways, and they are perceived by their societies as having very different social roles. Chinese students perceive themselves as having moral authority, and they are perceived as controlling social capital and possessing public status. There is a cultural norm in China that students, as the future elite, have a morally superior role in society. I remember thinking at the time that, with the obvious exception of those in power, who risked losing their privileged positions, any "right-minded" person in China would support democracy. A movement for democratic reform would liberalize the policies of a repressive regime, encourage personal freedom, and give the Chinese people a voice in their lives.

When the university students went on strike and took over Tiananmen Square, the popular view in the United States, reflected in the US media, was that they were college students protesting for democratic reform. There were images of thousands of students rallying and camping out on and around the statue of the People's Heroes. Throughout the square, banners and posters from universities supported democracy and freedom. The statue of the Goddess of Democracy erected by the demonstrators looked very much like our Statue of Liberty. Labor groups offered to join the students, people paraded in front of the Great Hall of the People, and citizens donated blankets and food.

Student leaders began a hunger strike to force a dialogue between the students and the government. All signs seemed clearly to point to a popular movement for democracy, for which there was a groundswell of support.

The Chinese government seemed hesitant or unsure. The People's Liberation Army (PLA) was sent to surround the square, but citizens blocked their advance and tried to persuade the troops to be neutral. A curfew order was not obeyed; martial law was declared and ignored. Another PLA move on Tiananmen Square was repelled. It appeared that the students had forced a stalemate and that their demands would be heard.

At that point, my assumption was that the government was weakened and would be forced to respond to the protesters' demands, at least to some degree. I anticipated a dialogue and concessions on both sides. Although I imagined the government was capable of resorting to violence, I assumed that it would not. It seemed inconceivable that the citizens of Beijing—10–12 million people—would not intervene on behalf of the students. That many people could have overwhelmed the PLA had they chosen to do so. I also assumed that the soldiers of the PLA would be reluctant to fire on their own people, partly because the majority of both groups were from the same, dominant ethnic group of China, the Han, and, in part, because the soldiers represented a lower rung of Chinese society then did the students. The notion of soldiers killing students would be an affront to the sensibilities of the Han, or so I thought. I was wrong.

In the end, when the PLA carried out its orders to clear the square with force and end the protest, support for the protesters turned out to be relatively slight. The Chinese "middle class" never came to the students' aid; the great majority of the Beijing populace simply watched the events unfold. Moreover, it turned out that the labor groups participating in the demonstration were actually protesting against corporate corruption and the lack of job stability brought about by market reforms and not in support of the students' demands for a loosening of restrictions on expression. What I perceived to be a groundswell of popular support for the students had been exaggerated and wishful thinking on my part.

My failure to anticipate the way events would actual unfold in Tiananmen Square was tied to ethnocentric thinking and a lack of accurate and contextual information. Students in the United States are encouraged to be politically active, and their protests are often seen merely as minor inconveniences that need to be endured. In China, however, the protesting students were seen as a direct challenge to political authority and, much more so than in the United States, their actions were viewed as an outright conflict between the future elite and the current leadership. The protest itself was viewed as a violation of a taboo, upsetting the cultural order and the stability of society.

As an observer, I missed the cultural context that was necessary to view the events as an actual conflict and could not convince myself that a violent solution was a possibility. I had discounted the hypothesis that violence would occur, because I could not imagine it occurring in the United States. This led me to discount raw data that would have refuted a hypothesis that the two factions would reach a compromise. In addition, at that time, I had no formal grounding in Chinese studies, nor had I been to China. Thus, I had not acquired information that would have helped me create a meaningful context for the event.

Years later, my wife and I were in China doing ethnographic fieldwork on the socioeconomic effects of the spread of the English language and American culture in urban and rural China.[4] While there, we spent a great deal of time talking with others about the events of Tiananmen, and we decided to include in our research questions about the student protests, if for no other reason than to satisfy our own curiosity.

What we found stood in contrast to media reports and the opinions expressed by many pundits and scholars in the US and the West. After hundreds of interviews with a wide variety of people in and around Beijing, we found a consistent preoccupation among the "silent majority." That was the Cultural Revolution, which had affected all of the people we interviewed. They had been participants, observers, or survivors, and, often, all three.

In the mid-1960s, Mao Zedong sought to recapture power from reform-minded opponents within the Communist Party. Using radical party leaders as his instruments, he created the Red Guard, which was made up primarily of college students (although others followed suit in time). The image of the Cultural Revolution was not simply the image of Mao; it was also the image of angry, violent, and powerful college students, who were the most visible proponents of the "Cult of Mao." According to the people we interviewed, it was the students who had chanted slogans, raised banners, paraded in public spaces, resisted older forms of social control, and seized power. With that power and the blessings of Mao, the youth and university students had committed many of the atrocities of the Cultural Revolution and plunged China into a decade of chaos, during which many institutions, including schools, were closed and many of the country's cultural and historical artifacts were destroyed.

---

[4] American anthropology is based on the ethnographic method and direct interaction with the people who are being studied. This interaction includes direct and participant observation and interviews, or fieldwork, where one lives with the people being investigated. Continental European schools of anthropology are not as obsessed with methodology and hands-on experience and tend to the more theoretical.

At the height of the Cultural Revolution, any dissent was sufficient to bring accusations of counterrevolutionary sympathies and to qualify one for "re-education," which could mean public denunciation, job loss, incarceration, forced labor, relocation, and even murder, torture, and rape. The traditional values of respect and honor were replaced with violence and terror, and the historical social unit of the family had been disrupted and replaced with the cult of Mao.

For those who had lived through the Cultural Revolution, the student challenge to the government in Tiananmen in 1989 was also a challenge to social order and stability. The people we interviewed remembered, correctly or not, that the faction of the Communist Party then in power and the PLA had stopped the Red Guard and the Cultural Revolution, arrested its highest ranking proponents and beneficiaries, the Gang of Four, and eventually restored order to the nation. The point of view of the people we interviewed was that the PLA, despite the low social status of soldiers, had stopped the chaos. Although they did not approve of killing students, the threat of another cultural revolution, democratic or otherwise, was more disturbing to them than the bloody climax in the square. Social order was the higher virtue.

Tiananmen Square: Discussion

> *We cut nature up, organize it into concepts, and ascribe significances as we do, largely because we are parties to an agreement to organize it in this way—an agreement that holds throughout our speech community and is codified in the patterns of our language.*
>
> Benjamin Whorf[5]

In 1987, a Chinese academic, Min Qi, performed the first national survey of Chinese political culture.[6] Respondents were asked, among other things, to select statements that best described their understanding of democracy. Of the 1,373 respondents, 6.6 percent responded that democracy meant that people could elect their political leaders and 3.4 percent that power was limited and divided. These replies tended to be from individuals under 25 years of age, in college, and living in urban centers.

---

[5] Benjamin Whorf, along with fellow anthropologist Edward Sapir, developed the linguistic relativity hypothesis, asserting that different speech communities had different patterns of thought. Although challenged by linguist/philosopher Noam Chomsky and others with the Universal Grammar hypothesis, linguistic relativity still has a significant amount of empirical research support. Benjamin Whorf, *Language, Thought, and Reality.*

[6] Min Qi, *Zhongguo Zhengzhi Wenhua* [Chinese Political Culture]. Translation courtesy of a friend of the author who prefers to remain anonymous.

In contrast, 25 percent responded that democracy was guided by the center (the party and the cadres), 19.5 percent that democracy meant that the government would solicit people's opinions (the party would ask people what they thought), and 11 percent that democracy meant the government would make decisions for the people based on the people's interests but not including the people's direct vote. These three responses were more in line with then-current party doctrine and tended to be from individuals over 36 years of age living in both urban and rural settings. This was the same demographic that experienced the Cultural Revolution.

The election of representatives and the division and limitation of those representatives' power—what I would have considered to be two key aspects of democracy—were chosen by 10 percent of the sample, only slightly larger than the 6.3 percent of Chinese respondents who reported that they didn't know what the word "democracy" meant. My own perception of democracy fit with a young, urban, elite, college educated population, not with the majority of Chinese citizens.

There was a very small sample of citizens in Tiananmen Square demanding what looked and sounded like my American version of democracy. Yet, however much the students' message resonated in the West, it did not do so in China. My expectations notwithstanding, there was a cognitive disconnect between students and average citizens, which, along with the visceral semiotics of the Cultural Revolution, kept the two apart.[7] It was not just the message that had kept people in their homes during the PLA siege on Tiananmen; it was also the messengers.

The label "ethnocentrism" might be accurate, but it does not diagnose the root of the problem. I did not use a variety of tools or techniques to question my underlying assumptions and, therefore, I failed to make an accurate forecast. There were obvious statistical and analytic flaws. The former was principally a sampling error, both frame and selection bias (the students at Tiananmen did not represent the general population in Beijing or China at large). More significant than simple technical or statistical flaws, however, my frame of reference and my assumptions about meanings, context, and values (or culture) misled me.

The assumptions I made about the Tiananmen protests were products of my own enculturation, and I am not convinced that anything short of the experience of analytic failure would have been sufficient for me to examine the process underpinning my reasoning. I never would have reexamined my mental mode without experiencing failure. Failure is an event that is easily remem-

[7] Semiosis is the production of cultural signifiers or signs and the cultural or contextual meaning of those signs. This includes all modes of visual and auditory production.

bered; it affects the ego and drives one to investigate errors and to adapt or change behavior based on those investigations. Failure is a learning event and results in a teachable moment.[8]

There seems to be little reason to perform a postmortem when events unfold as predicted. The natural assumption is that the mechanisms of analysis were valid, because the results of the analysis were accurate. The obvious danger is that this assumption discounts the possibility that one may be accurate purely by accident. Moreover, by focusing only on failure, one risks sampling bias by only choosing cases in which there was error. The risk of ignoring success is that potential lessons may go undiscovered. An alternative to relying on failure to challenge one's assumptions is to create a standard practice of reviewing each case regardless of outcome, principally through the use of a formal After Action Review (AAR).

Case Study Two: The Red Team

Recently, I was asked to serve on a newly formed red team within the Department of Defense. I agreed to participate, despite a number of serious concerns having to do both with the nature and structure of red teams in general and with my own experience with ethnocentrism and its effects on analysis. These concerns are applicable not only to red teams, but also to any analyst put in the position of trying to "think like them."[9]

This particular red team was part of a constructive/conceptual war game in which there were 11 participants, seven of whom had doctorates. Of the seven doctorates, three were psychologists, one was a historian, one was an economist, one was a political scientist, and one was an anthropologist. The other four participants had extensive military backgrounds. There were no physical scientists or engineers. Nine of the 11 participants were white males, one was a male born in the region of interest, and one was a white female. All were middle class. Seven of the 11 were raised in nominally Christian homes and three in nominally Jewish homes. (I say nominally because it was not possible to determine their level of religious commitment during this exercise.)

I mention the demographics of the group because it was not representative of the adversary we were intended to simulate. Although the group had

---

[8] Charles Perrow, *Normal Accidents.*

[9] Military red teams are meant to simulate the actions of an adversary in some type of war game or crisis simulation, usually with the goal of generating scenarios for training and readiness or for logistics and planning. These war games may be *live*, e.g., force-on-force simulations like those of the US Army Combat Training Centers; *virtual*, as in flight simulators; or *constructive*, either digital theater-level simulations or purely conceptual games centered on strategic, tactical, or operational issues.

numerous domain matter experts, very few had first-hand knowledge of the region of interest. Only one participant was from the area, had spent formative years there, spoke the languages, and experienced the culture firsthand. As this group was assembled to simulate the behavior and decisionmaking of a foreign adversary, this aspect was more important than it would have been for a substantive team developing threat assessments around a specific topic or target. Consequently, the scenarios developed by the red team often reflected an adversary whose behavior and decisionmaking resembled those of educated, white, middle class Americans.

The one member of the red team who had been born in and spent formative years in the region of interest regularly stopped the scenario development process by saying, "They wouldn't do that" or "They don't think that way." On several occasions, he objected, "This scenario is way too complex" or "They wouldn't use that tactic; it requires too much direct communication." His objections were not usually based on military considerations; rather, they were based on the cultural norms and mores of the adversary. He talked of kinship relationships as a specific type of social network in the region and of the value of kinship for understanding the adversary's intentions. In short, he brought an ethnographic perspective to the exercise.

Having no personal or professional experience with this region or its cultures, I thought it appropriate to defer to his first-person experience. Ultimately, however, it proved difficult to convince the group that this man's cultural knowledge was, in fact, an area of specialized knowledge that needed to be factored into each scenario. This difficulty was born out of another type of ethnocentric bias.

Inviting an anthropologist to a red team exercise presupposes that the red team takes seriously the notion that cultural differences matter and that those cultural factors ought to be made explicit in the analytic process. The problem in this case was that the anthropologist was not an area expert for this region and its cultures, and the one area expert who was there lacked the academic credentials to be taken seriously by the other members of the group. Had I been able to assert the same concepts that the other individual asserted, it would have had a certain academic, or scientific, imprimatur because of my training and experience. Because he lacked these credentials, many of the other individual's insights were lost, and the analytic product suffered as a result.

The Red Team: Discussion

I am reluctant to fault the organizers for the ethnocentric bias in the demographic composition of the red team. It is very difficult to assemble a truly

representative red team. There is the obvious problem of security. Someone fully able to represent the adversary culturally would very likely be unable to obtain requisite clearances for participation in a classified red team exercise. In fact, even if it were possible to find someone both culturally representative *and* sympathetic to the goals of the red team, such as the participant born in the region, the conflicts triggered by that sympathy, cultural identity, and cultural allegiance could well lead to unforeseen cognitive biases that would be difficult to counteract.[10]

An alternative is to find an ethnic American citizen with similarities to the people of the region of interest, but simply finding a US citizen with the same ethnicity as those of the region of interest does not guarantee any special insight into their thinking. Ethnicity is not the same as sharing culture or identity. Not all ethnic groups in the US are isolated and self-perpetuating. Many, in fact, put great effort into trying to assimilate into the larger "American culture" by distancing themselves from their culture of origin. These people often struggle with their own concept of cultural identity and the broader issues of community affiliation.[11] Many immigrants and most first-generation offspring have already begun the process of acculturation. More striking, their offspring display a process of enculturation in the US by learning the language, attending the schools, assimilating local and national values, and establishing ties to a diverse community outside of their own ethnic enclave. In fact, the children of recent immigrants share many of the same cognitive filters as those who are generations removed from migration. That said, there are American citizens born in the region of interest, like the member of the red team in which I participated, who do have insight into specific cultures, principally because their enculturation was affected by being born in, and living in, a foreign region.

The participant in that red team was a foreign-born American citizen, but foreign birth is not a necessary condition for enculturation.[12] Living in a foreign region, speaking the language, interacting with the people, developing community ties, and establishing an identity within that community are all part of the acculturation process and allow one to alter the cognitive filters through which one interprets the world. Time spent on a US military base, in a US embassy, or in a Western hotel overseas does not lead to acculturation.

---

[10] Philip Cushman, *Constructing the Self, Constructing America*; John Lucy, *Language Diversity and Thought*; Douglass Price-Williams, *Explorations in Cross-Cultural Psychology*; Marshall Segall, *Cross-Cultural Psychology*; Richard Shweder, *Thinking Through Cultures*; Yali Zou and Enrique Trueba, *Ethnic Identity and Power*; and Benjamin Whorf.

[11] David Levinson and Melvin Ember, *American Immigrant Cultures*. For raw data covering 186 cultural groups since 1937, including immigrants, see the Human Relations Area Files at Yale University.

[12] Some anthropologists have argued that enculturation is specific to childhood but the evidence supports that it is a lifelong process. See Segall.

Quite the contrary, each of these is a "virtual" America, an approximation of life in the United States on some foreign soil, and it is the time spent away from these institutions that is important.

The red team experience reinforced lessons I learned from my own analytic failures and biases. Watching the struggle between the man enculturated in the region of interest and the academic experts was a frustrating experience. It was clear that the experts would not, or could not, hear what he was saying and that neither he nor I knew how to get the other experts to listen. I doubt this communication failure was the result of stubbornness or arrogance on anyone's part. It seemed rather that the experts' thinking naturally defaulted to their own cultural reference points, which interfered with his attempts to communicate his cultural knowledge.

Specific cultural knowledge is a skill and the foundation for forecasting the behavior and decisionmaking of foreign actors. Acquiring cultural knowledge should be taken as seriously as learning any other facet of one's analytic capabilities. Moreover, it is incumbent on analysts to educate their own leadership and policymakers about the value and utility of cultural knowledge for intelligence analysis.

Conclusion and Recommendations

Ethnocentrism is a normal condition, and it results in analytic bias. The analytic community and intelligence researchers need to develop tools and techniques to combat analytic ethnocentrism. I believe that using cultural diversity as a strategy to combat ethnocentrism has much to recommend it.[13]

Security concerns may make it very difficult, if not impossible, to hire people who are genuinely representative of a given culture. As an alternative to focusing on hiring practices, I recommend a formal cultural training program to facilitate acculturation. The program would include language acquisition and a classroom segment centered on specific cultures, but it would go beyond these by having the students go to countries of interest and interact with the

[13] Some social action groups have appropriated the words "cultural diversity" from Levi-Strauss and the French school of structural anthropology as a rallying cry to advance an agenda of equal access to resources and power. That is, the concept has been politicized, and, invoking the words "cultural diversity" in a public forum ensures that people will have some emotional reaction. This is not my intention. The use of the words in this work is meant strictly in the technical sense, specifically, that is, to refer to individuals whose enculturation occurs among different cultures or individuals who have experienced acculturation. Acculturation is not specific to any one group, all people can and do experience acculturation to one degree or another through cultural contact and cultural diffusion, defined as the spreading of a cultural trait (e.g., material object, idea, or behavior pattern) from one society to another without wholesale dislocation or migration. Moreover, acculturation can be accomplished purposefully through training and fieldwork.

people in their own setting and on their own terms. Students would be encouraged to investigate the rituals, norms, taboos, kinship systems, and social networks of the cultures being studied. There would also be provision for continuing on-line education and an on-line community of practice for mentoring, problem solving, and peer-to-peer interaction.

In my view, a stand-alone training program would be insufficient to affect analytic processes without specific follow-on programs. Retention of training requires repetition, problem solving, application, and evaluation. People must use what they learn and then determine if what they have learned can improve the quality of their work. To this end, I recommend a formal After Action Review (AAR) process.

The AAR is used by the US Army to capture lessons learned after a training exercise or a live operation. Unlike conventional postmortems and traditional performance critiques, the AAR is used to evaluate successes as well as failures. Although failure generally receives more scrutiny and attention than success, an approach that only examines failure results in sampling error. If one only scrutinizes mistakes, otherwise effective methods may be blamed for the errors. That those techniques were successful in 99 out of 100 cases can go unnoticed, with the result that the failures receive disproportionate attention and bias the statistical results of the postmortem. The AAR was specifically designed to avoid this problem.

The AAR process was introduced in the mid 1970s, but it is based on the oral history method of "after combat interviews" employed by S.L.A. Marshall during World War II, the Korean War, and the Vietnam War. As soon as possible after a battle, regardless of the outcome, Marshall would assemble soldiers who were involved and, using a semistructured interview technique, would engage them in a group discussion about their individual and team roles and actions during combat.

The current AAR method also includes such objective data as tactics, logistics, kill ratios, time-to-task, accuracy-of-task, and operational outcomes.[14] Informed by the objective data, a group discussion led by a facilitator trained in the elicitation process ensues. The AAR, along with supporting documents, such as historical studies and relevant doctrinal materials, is then stored in a knowledge repository at the US Army's Center for Army Lessons Learned (CALL).[15]

With some customization, an AAR process and a lessons learned repository could be created for intelligence analysts. Although seemingly time-consuming and cumbersome, with training and expert facilitators, the AAR process could be modified and streamlined for use by analysts at the end of a production cycle. As

---

[14] John Morrison and Larry Meliza, *Foundations of the After Action Review Process*.

a practical matter, the process would be used mostly with longer works, such as assessments or estimates. The intelligence product, along with AAR notes, would then be incorporated in a community knowledge repository. This knowledge repository would also help in the development and refinement of advanced analytic courses by providing course developers with baseline analytic data. In short, the repository becomes a tool for continuous educational needs analysis and links training directly to the actual work practices of analysts. These data can be used as a test bed for research on the effectiveness of analytic methodology. In this way, the lessons learned are not lost to future generations of analysts.

[15] See the US Army Center for Army Lessons Learned Web site, which has links to numerous other repositories. Although each organization has customized the concept to meet its unique needs, all of the US military services, the National Aeronautics and Space Administration, the Department of Energy, the Environmental Protection Agency, the North Atlantic Treaty Organization, the United Nations, and the ministries of defense of Australia and Canada, currently have Lessons Learned repositories.

CHAPTER SEVEN

Instructional Technology: Effectiveness and Implications for the Intelligence Community

J. D. Fletcher[1]
Rob Johnston

The Intelligence Community has begun to invest substantial resources in the training and education of its analysts. With the exception of a few advanced courses available through distance learning networks, this instruction is delivered using a conventional classroom model. This model possesses a number of inherent inefficiencies, including inconsistent instruction, strict ties to time and place of instruction, large student-to-instructor ratios, and limited active participation by students due to class size and scheduling.

Research suggests that significant improvements can be achieved through the use of computer-based instructional technology. According to these studies, this technology can increase instructional effectiveness and reduce time needed to learn. It can achieve these efficiencies, moreover, while both lowering the cost of instruction and increasing its availability.[2] This chapter summarizes evidence on the promise of instructional technology for intelligence analysis training.

---

[1] Dr. J. D. Fletcher is a research staff member at the Institute for Defense Analyses, where he specializes in issues of manpower, personnel, and training. He holds graduate degrees in computer science and educational psychology from Stanford University.

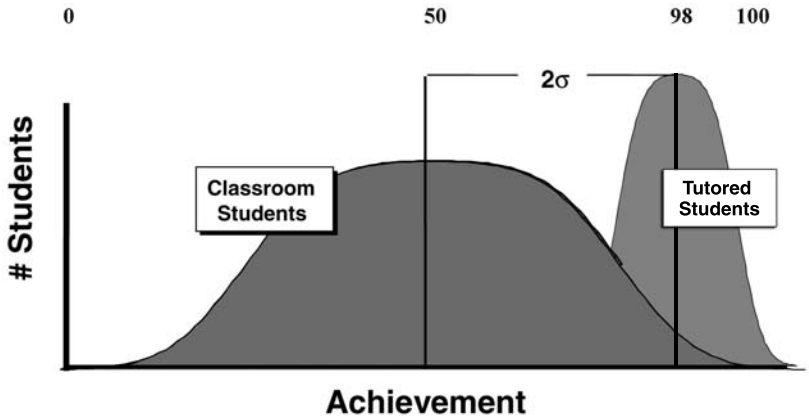
[2] Because instructional technology makes few distinctions between formal education and professional training, the term "instruction" will be used for both in this chapter.

Background

The argument for the use of instructional technology usually begins with a comparative examination of the effectiveness of classroom instruction and individual tutoring. For instance, the graph below illustrates the combined findings of three dissertation studies that compared one-on-one tutoring with one-on-many classroom instruction.[3]

It is not surprising that such comparisons would show that tutored students learned more than those taught in classrooms. What is surprising is the magnitude of the difference. Overall, as the figure shows, it was two standard deviations. This finding means, for example, that with instructional time held fairly constant one-on-one tutoring raised the performance of 50th percentile students to that of 98th percentile students. These, and similar empirical research findings, suggest that differences between one-on-one tutoring and typical classroom instruction are not only likely, but also very large.

Individual Tutoring Compared to Classroom Instruction



Why then do we not provide these benefits to all students? The answer is straightforward and obvious. With the exception of a few critical skills, such as aircraft piloting and surgery, we cannot afford it. One-on-one tutoring has been described as an educational imperative and an economic impossibility.[4]

---

[3] Benjamin S. Bloom, "The 2 Sigma Problem: The Search for Methods of Group Instruction as Effective as One-to-One Tutoring." The dissertation studies were performed under Bloom's direction.

[4] M. Scriven, "Problems and Prospects for Individualization."

The success of one-on-one tutoring may be explained by two factors. First, measured in terms of questions asked and answered, tutors and their students engage in many more instructional interactions per unit of time than is possible in a classroom. Second, one-on-one tutoring can overcome the substantial spread of ability, measured by the time needed to reach minimal proficiency, that is found in practically every classroom. Tutoring reduces time-to-learn by adapting each interaction to the needs of each student. Less time is spent on material the student has already learned, and more time is spent on material remaining to be mastered.

To investigate the intensity of instructional interactions, Art Graesser and Natalie Person compared questioning and answering in classrooms with those in tutorial settings.[5] They found that classroom groups of students ask about three questions an hour and that any single student in a classroom asks about 0.11 questions per hour. In contrast, they found that students in individual tutorial sessions asked 20–30 questions an hour and were required to answer 117–146 questions per hour. Reviews of the intensity of interaction that occurs in technology-based instruction have found even more active student response levels.[6]

Differences in the time needed by individuals in any classroom to meet instructional objectives are also substantial. Studies on this issue have reported ratios varying from 1:3 to 1:7 in the times the fastest learners need to learn compared to the times needed by the slowest learners. Although these differences may be due initially to ability, these studies suggest that such ability is quickly overtaken by prior knowledge of the subject matter.[7] This effect is particularly evident in instruction for post-secondary-school students, because prior knowledge rapidly increases with age and experience. Technology-based instruction has long been recognized for its ability to adjust the pace of instruction to individual needs, advancing through instructional material as quickly or as slowly as required. The overall result has been substantial savings in the time required to meet given instructional objectives.[8]

It should be emphasized that these benefits are not achieved at the expense of instructional quality. Research has found that many instructional technologies have a positive impact on learning across a wide variety of student populations, settings, and instructional subject matters.[9]

This research suggests that technology-based instruction results in substantial savings of time and money. Studies have shown that the times saved aver-

---

[5] Art Graesser and Natalie Person, "Question-Asking During Tutoring."
[6] J. D. Fletcher, *Technology, the Columbus Effect, and the Third Revolution in Learning*.
[7] Sigmund Tobias, "When Do Instructional Methods Make a Difference?"
[8] J. D. Fletcher, "Evidence for Learning From Technology-Assisted Instruction."
[9] Ken Spencer, "Modes, Media and Methods: The Search for Educational Effectiveness."

age about 30 percent, as seen in the table below. The reduction in overhead expenses averages 20–30 percent.[10] Research has shown that the cost ratios (calculated as the ratio of experimental intervention costs over the costs of a control group) for interactive multimedia technology (computer-based instruction with enhanced audio, graphics, and/or video; CD-ROM and DVD-based instruction; interactive video, etc.) favor it over conventional instruction along with time savings of about 31 percent.[11] Simulation of such systems as helicopters, tanks, and command-control systems for training combat skills has also proven to be cost-effective.[12] The operational costs for simulation are, on average, 10 percent of the costs of using the actual systems to train.[13]

Time Savings for Technology-Based Instruction

Study (Reference)	Number of Studies Reviewed	Average Time Saved (Percent)
Military Training - Orlansky	13	54
Higher Education - Fletcher	8	31
Higher Education - Kulik	17	34
Adult Education - Kulik	15	24

Meta-analysis Demonstrates the Effectiveness of Instructional Technology

Researchers often use a meta-analytic approach to review and synthesize quantitative research studies on a variety of issues, including instructional effectiveness.[14] This method involves a three-step process, which begins with the collection of studies relevant to the issue using clearly defined procedures that can be replicated. Next, a quantitative measure, "effect size," is used to tabulate the outcomes of all the collected studies, including those with results that are not statistically significant. Finally, statistical procedures are used to

---

[10] Jesse Orlansky and Joseph String, *Cost-Effectiveness of Computer-Based Instruction in Military Training*; H. Solomon, *Economic Issues in Cost-Effectiveness Analyses of Military Skill Training*; James Kulik, "Meta-Analytic Studies of Findings on Computer-Based Instruction"; Rob Johnston, "The Effectiveness of Instructional Technology"; Ruth Phelps et al., "Effectiveness and Costs of Distance Education Using Computer-Mediated Communication"; J. D. Fletcher *Effectiveness and Cost of Interactive Videodisc Instruction in Defense Training and Education*.

[11] J. D. Fletcher, "Computer-Based Instruction: Costs and Effectiveness."

[12] Jesse Orlanksy et al., *The Cost and Effectiveness of the Multi-Service Distributed Training Testbed (MDT2) for Training Close Air Support*.

[13] Jesse Orlansky et al., *The Value of Simulation for Training.*

[14] Gene Glass, "Primary, Secondary, and Meta-Analysis of Research."

synthesize the quantitative measures and describe the findings of the analysis. Meta-analysis appears to be especially suited for synthesizing the results of instructional research, and it has been widely used for this purpose since its introduction in 1976.

Meta-analysis is still being developed as a technique, and some matters concerning its use, notably the "file-drawer" problem and calculation of effect size, remain unsettled. Chapter Twelve presents a more detailed explanation and these considerations. Briefly, however, meta-analytic reviews of instructional technology effectiveness have found substantial results favoring its use over traditional technologies of classroom instruction.

Overall, effect sizes for post-secondary school instruction average about 0.42, which is roughly equivalent to raising the achievement of 50th percentile students to that of 66th percentile students.[15] Reviews of more elaborate forms of instructional technology, such as those using applied artificial intelligent techniques, have found effect sizes in excess of 1.0, which is roughly equivalent to raising the achievement of 50th percentile students to that of the 84th percentile.[16] It seems reasonable to conclude that the reduced costs and reduced time to learn obtained in applications of instructional technology are not achieved at the expense of instructional effectiveness.

Encouraging as these favorable results are, our ability to apply instructional technology efficiently may be in its infancy. Findings thus far have been based on instructional applications intended to teach facts (e.g., What is the capital of Brazil? What is the Spanish word for chapel? Who was the first director of the Central Intelligence Agency?) concepts (e.g., What is a mass spectrometer used for? What is the difference between micro- and macro-economics? When must you use a torque wrench?), and procedures (e.g., How do you record a movie from television? How do you prepare a purchase requisition? How do you calibrate a radar repeater?). All intelligence analysts must possess a repertoire of facts, concepts, and procedures to perform their craft, and instructional technology holds great promise for increasing both the efficiency with which they might develop this repertoire and their access to instructional resources for doing so.

However, the capabilities analysts may seek through instruction are likely to include more abstract, or "higher," cognitive processes. For instance, in addition to learning a procedure, analysts may need the capability to recognize

---

[15] Chen-Lin Kulik., James Kulik and Barbara Shwalb, "Effectiveness of Computer-Based Adult Education: A Meta-Analysis"; Chen-Lin Kulik and James Kulik, "Effectiveness of Computer-Based Education in Colleges"; Rob Johnston and J. D. Fletcher, *A Meta-Analysis of the Effectiveness of Computer-Based Training for Military Instruction*; J. D. Fletcher, "Evidence for Learning from Technology-Assisted Instruction."

[16] Sherrie P. Gott, R. S. Kane, and Alan Lesgold , *Tutoring for Transfer of Technical Competence*.

the procedure's applicability in unfamiliar situations, modify it as needed, and use it to develop new approaches and procedures. Early on, Bloom discussed learning objectives as a hierarchy beginning with knowledge at the most rudimentary level and ascending through comprehension, application, analysis, and synthesis to evaluation.[17] Bloom's is not the only such hierarchy to emerge from research on instructional design, but it seems to be the best known, and it describes as well as any the various levels of knowledge, skill, and ability to which learners may aspire.

Current Research on Higher Cognitive Abilities

Analysts have begun to discuss development of the higher cognitive abilities needed to deal with unanticipated and novel challenges.[18] Components of such "cognitive readiness" may include:

- *Situation awareness*—the ability to comprehend the relevant aspects of a situation and use this understanding to choose reasonable courses of action.[19] Practice and feedback in complex, simulated environments have been shown to improve situation awareness.
- *Memory*—the ability to recall and/or recognize patterns in a situation that lead to likely solutions. It may be supported by two underlying theoretical mechanisms: *encoding specificity,*[20] which stresses the importance of responding to relevant external and internal perceptual cues, and *transfer-appropriate processing,*[21] which stresses the actions performed during encoding and retrieval. Some instructional techniques, such as overlearning,[22] have been shown to enhance long-term retention.[23]
- *Transfer*—the ability to apply what is learned in one context to a different context. It can be perceived either as the ability to select and apply procedural knowledge gained in one context to another ("low road" transfer) or as the ability to apply the principles abstracted from a set of contexts to another ("high road" transfer).[24] Extensive practice, with feedback, will

---

[17] Benjamin. S. Bloom, *Taxonomy of Educational Objectives.*
[18] J. E. Morrison, and J. D. Fletcher, *Cognitive Readiness*.
[19] M. R. Endsley, "Design and Evaluation for Situation Awareness Enhancement."
[20] E. Tulving and D. M. Thomson, "Encoding Specificity and Retrieval Processes in Episodic Memory."
[21] C. D. Morris, J. D. Bransford, and J. J. Franks, "Level of Processing Versus Transfer-Appropriate Processing."
[22] The use of specific problem-solving methods repetitively.
[23] R. A. Wisher, M. A. Sabol, and J. A. Ellis *Staying Sharp: Retention of Military Knowledge and Skills*.

enhance the former. Instruction in developing mental abstractions will enhance the latter.

- *Metacognition*—the executive functions of thought, more specifically, those needed to monitor, assess, and regulate one's own cognitive processes.[25] Meta-cognitive skills can be enhanced by exercises designed to increase awareness of self-regulatory processes.[26]
- *Pattern Recognition*—the ability to distinguish the familiar from the unfamiliar. It may be accomplished by "template matching," which involves comparing retained images with incoming sensory impressions; or by "feature comparison," which involves recognizing and generalizing from distinctive features of a structure held in memory with incoming sensory impressions.[27] Pattern recognition can be taught through a combination of extensive practice, with feedback, and instruction in forming abstractions.
- *Automaticity*—processes that require only limited conscious attention.[28] Automaticity can be taught by providing extensive practice, with feedback.
- *Problem Solving*—the ability to analyze a situation and identify a goal or goals that flow from it, identify tasks and subtasks leading to the goal, develop a plan to achieve them, and apply the resources needed to carry out the plan. Practice, with feedback, and overlearning can enhance problem-solving ability in many tasks. Techniques for problem solving can be successfully taught, as can the knowledge base needed to implement them.[29]
- *Decisionmaking*—a component of problem solving, but the emphasis in decisionmaking is on recognizing learned patterns, reviewing courses of action, assessing their impact, selecting one, and allocating resources to it.[30] Instruction in assessing courses of action has been shown to improve decisionmaking, but some aspects of successful decisionmaking are more likely to be inborn than trained.
- *Mental Flexibility and Creativity*—the ability to generate and modify courses of action rapidly in response to changing circumstances.[31] It

---

[24] G. Salomon and D. N. Perkins "Rocky Roads to Transfer: Rethinking Mechanisms of a Neglected Phenomenon."
[25] J. H. Flavell, "Metacognitive Aspects of Problem Solving."
[26] D. J. Hacker, *Metacognition: Definitions and Empirical Foundations* [On-line Report].
[27] M. H. Ashcraft, *Fundamentals of Cognition*.
[28] R. M. Shiffrin and W. Schneider, W. "Controlled and Automatic Human Information Processing: II. Perceptual Learning."
[29] J. R. Hayes, *The Complete Problem Solver*.
[30] P. Slovic, S. Lichtenstein, and B. Fischoff, "Decision-making."
[31] D. Klahr, & H. A. Simon, "What Have Psychologists (and Others) Discovered About the Process of Scientific Discovery?"

includes the ability to devise plans and actions that differ from and improve upon "school solutions." Capabilities that widen the range of options can be taught, but higher levels of creativity are more likely to be inborn than trained.

The above review suggests, first, that the creative processes needed by analysts can, to some extent, be broken down into components, and second, that these components can, again to some extent, be taught. Instructional technology can now substantially aid analysts in acquiring the facts, concepts, and procedures needed to perform their craft. However, it must become increasingly "intelligent" if it is to compress the years of experience analysts now need to become proficient and help them more rapidly acquire the advanced cognitive capabilities—those higher in Bloom's hierarchy—that they also need. To do this successfully, instruction must be tailored to the specific background, abilities, goals, and interests of the individual student or user. Instructional technology must provide what has been called "articulate expertise." Not only must it supply helpful and relevant guidance in these more advanced levels of knowledge, skills, and abilities, it must do so in a way that learners and users with varying levels of knowledge and skill can understand.

Discussion

At this point, it may be worth reviewing the capabilities provided by "non-intelligent" instructional technology since the 1950s. It has been able to:[32]

- accommodate the rate of progress of individual students, allowing as much or as little time as each needs to reach instructional objectives;
- tailor both the content and the sequence of instructional content to each student's needs;[33]
- make the instruction easy or difficult, specific or abstract, applied or theoretical as necessary;
- adjust to students' most efficient learning styles (collaborative or individual, verbal or visual, etc.).

Intelligent tutoring systems are a different matter. They require quite specific capabilities that were first targeted in the 1960s.[34] Two key capabilities are that intelligent tutoring systems must:

---

[32] E. Galanter, *Automatic Teaching*; R. C. Atkinson and H. A. Wilson, *Computer-Assisted Instruction*; P. Suppes and M. Morningstar, *Computer-assisted Instruction at Stanford 1966-68*; J. D. Fletcher and M. R. Rockway, "Computer-based Training in the Military."

[33] J. S. Brown, R. R. Burton, and J. DeKleer, "Pedagogical, Natural Language and Knowledge Engineering in SOPHIE I, II, and III."

- allow either the system or the student to ask open-ended questions and initiate instructional, "mixed-initiative" dialogue as needed or desired;
- generate instructional material and interactions on demand instead of requiring developers to foresee and store all the materials and interactions needed to meet all possible eventualities.

Mixed-initiative dialogue requires a language for information retrieval, tools to assist decisionmaking, and instruction that is shared by both the system and the student/user. The system must have the capability (referred to as "generative capability") to devise, on demand, interactions with students that do not rely on predicted and prestored formats. This capability involves more than generating problems tailored to each student's needs. It must also provide the interactions and presentations that simulate one-on-one tutorial instruction, including coaching, hints, and critiques of completed solutions.

Cost containment is one motivation for wanting to generate responses to all possible student states and actions instead of attempting to anticipate and store them. Another arises from basic research on human learning, memory, perception, and cognition. As documented by Neisser among others, during the 1960s and 1970s, the emphasis in basic research on human behavior and on the way in which it is understood shifted from the strict logical positivism of behavioral psychology, which focused on directly observable actions, to consideration of the internal, cognitive processes that were needed to explain empirically observed behavioral phenomena and are assumed to mediate and enable human learning.[35]

The hallmark of this approach is the view that seeing, hearing, and remembering are all acts of *construction,* making more or less use of the limited stimulus information provided by our perceptual capabilities. Constructivist approaches are the subject of much current and relevant discussion in instructional research circles, but they are firmly grounded in the foundations of scientific psychology.[36] For instance, in 1890, William James stated his General Law of Perception: "Whilst part of what we perceive comes through our senses from the object before us, another part (and it may be the larger part) always comes out of our mind."[37]

In this sense, the generative capability sought by intelligent instructional systems is not merely something nice to have. It is essential if we are to

---

[34] J. R. Carbonell, "AI in CAI: An Artificial Intelligence Approach to Computer-Assisted Instruction"; J. D. Fletcher & M. R. Rockway.

[35] U. Neisser, *Cognitive Psychology.*

[36] For example, T. M. Duffy, and D. H. Jonassen, *Constructivism and the Technology of Instruction*; S. Tobias and L. T. Frase, "Educational psychology and training."

[37] William James, *Principles of Psychology: Volume I.*

advance beyond the constraints of the prescribed, prebranched, programmed learning and ad hoc principles commonly used to design technology-based instruction. The long-term vision is that training, education, and performance improvement will take the form of human-computer conversations.

There has been progress toward this end. This conversational capability has been realized in systems that can discuss issues with students using a formal language, such as computer programming or propositional calculus.[38] More recent research suggests that significantly improved natural-language dialogue capabilities can be achieved by instructional technology.[39] Such an interactive, generative capability is needed if we are to deal successfully with the extent, variety, and mutability of human cognition. Much can now be accomplished by instructional technology, but much more can be expected.

Conclusion

The research discussed above suggests that instructional technology can:

- reduce costs of instruction;
- increase the accessibility of instruction;
- increase instructional effectiveness for analysts;
- reduce the time analysts need to learn facts, concepts, and procedures;
- track progress and ensure that all learners achieve instructional targets;
- provide opportunities for helping analysts to compress experience and achieve the higher cognitive levels of mastery demanded by their craft.

In addition, the findings suggest a rule of "thirds." This rule posits that the present state-of-the-art in instructional technologies can reduce the cost of instruction by about a third and *either* increase achievement by about a third *or* decrease time to reach instructional objectives by a third. Eventually, instructional technology should provide a conversation between the analyst and the technology that will tailor instruction in real time and on demand to the particular knowledge, skills, abilities, interests, goals, and needs of each individual. This capability, now available in rudimentary forms, can be expected to improve and develop with time. Even in its current state of development, however, instructional technology deserves serious attention within the Intelligence Community.

---

[38] For example, BIP and EXCHECK, respectively. For the first, see A. Barr, M. Beard, and R. C. Atkinson, "A rationale and description of a CAI Program to teach the BASIC Programming Language"; for the second, see P. Suppes and M. Morningstar.

[39] A. C. Graesser, M. A. Gernsbacher, and S. Goldman, *Handbook of Discourse Processes*.

CHAPTER EIGHT

Organizational Culture: Anticipatory Socialization and Intelligence Analysts

Stephen H. Konya[1]
Rob Johnston

I know it sounds silly, but I had this image of James Bond before I started working here. The truth is, I just sit in a cubicle, and I write reports.

Every organization has a unique culture that is defined partly by its individual members and partly by its structure, history, and policies. For that culture to endure, it must be transmitted from current members to new members. This process, known as organizational socialization, is especially important in organizations with strong, insular cultures, as those with weak cultures have less to transmit and will tend to experience culture changes as members come and go.

Although socialization begins prior to a person's first day on the job and is a continuous process, it is experienced most intensely by new employees. The cultural symbols acquired and interpreted during their initial interaction with the institution create potent and lasting impressions.[2] For them, socialization

---

[1] Stephen Konya is a Research Associate at the Institute for Defense Analyses, currently examining multimodal interfaces for the dismounted for the DARPA/Army Future Combat Systems program. He holds an MS in industrial and organizational psychology from Rensselaer Polytechnic Institute.

[2] Umberto Eco, *A Theory of Semiotics*; Clifford Geertz, *The Interpretation of Cultures*; Jacques Lacan, *Ecrits*; Ferdinand de Saussure, *Course in General Linguistics*.

is the process of learning the ropes; training; and becoming formally and informally acquainted with what is actually of value within the organization.[3] It is also the time when one learns the organization's norms and taboos and the extent of its social capital.[4] In sum, formal and informal socialization are types of control mechanism for maintaining the norms, or status quo, within any organization.[5]

Organizational Socialization

According to Daniel Feldman, organizational socialization is "the process through which individuals are transformed from outsiders to participating, effective members of an organization."[6] As shown in Figure 1, Feldman divides this process into three stages: getting in (or anticipatory socialization), breaking in (or accommodation), and settling in (often referred to as role management). During the getting-in stage, potential employees try to acquire information about an organization from available sources, such as Web sites, professional journals, and corporate annual reports. The breaking-in stage includes orientation and learning organizational as well as job-related proce-

Feldman's three stages of organizational socialization.

dures. The settling-in stage concludes when an individual attains full member status in the organization.

While each of the three stages of socialization is important, the focus of this chapter is on the first, or anticipatory, stage. There are several reasons for this. Clearly, the expectations people develop about an organization they are joining are important to a new recruit's eventual satisfaction, retention, and performance. Moreover, because it can control several aspects of the recruitment process, this stage is often the easiest for an organization to change. This chapter will take both a descriptive and prescriptive approach to easing the socialization of new employees.

---

[3] William G. Tierney and Robert A. Rhoads, *Faculty Socialization as Cultural Process.*

[4] See footnote 7 in Chapter Two.

[5] John P. Wanous, *Organizational Entry.*

[6] Daniel C. Feldman, "The Multiple Socialization of Organization Members."

Anticipatory Socialization

Anticipatory socialization encompasses all of the learning that occurs prior to a recruit's entering on duty.[7] At this stage, an individual forms expectations about the job and makes decisions about the suitability of fit between himself and the organization. What a person has heard about working for a particular organization, such as an intelligence agency, provides an idea of what to expect if hired. Conversely, individuals who do not believe they would fit in may decide not to apply.

There are two variables that are particularly useful for tracking a potential employee's progress through the anticipatory stage: The first is *realism*, or the extent to which an individual acquires an accurate picture of daily life in the organization. Realism is influenced by the level of success recruits achieve during the information-sharing and information-evaluation part of their recruitment. The second is *congruence*, or the extent to which the organization's resources and the individual's needs and skills are mutually satisfying. Congruence is influenced by the level of success an individual has achieved in making decisions about employment. Although it cannot directly influence congruence, which is an inherently personal experience, an organization can present relevant information in order to provide a realistic and accurate description of the work performed and the work environment.

Organizations often use interviews to begin the socialization of new recruits. For example, an interviewer will attempt to provide an accurate description of what to expect from the job and the organization, the purpose being to reduce the likelihood that a recruit will be disturbed by unanticipated situations. Interviewing is also used to determine the degree to which there is a match between the values of potential recruits and the values of the organization. New recruits with personal values matching those of the organization have been found to adjust to the organization's culture more quickly than recruits with nonmatching values.[8]

Organizations also send cultural messages to new recruits during interviews. When there are several rounds of interviews with progressively senior members of the organization, for example, the message conveyed is that finding the best person for the position is important. In contrast, hiring for a part-time job at the lowest level of the organization is often accomplished quickly, to the extent that a person having minimally acceptable qualifications may

---

[7] This stage is termed "pre-arrival" in Lyman W. Porter, Edward E. Lawler, and J. Richard Hackman, *Behavior in Organizations*.

[8] Jerald Greenberg and Robert A. Baron, *Behavior in Organizations*: *Understanding the Human Side of Work.*

often be hired on the spot. The cultural message in this case is that such employees are easily let in to and out of the organization.

Another, particularly pertinent example is intelligence work, which requires that recruits undergo employment screenings unlike those found in most civilian jobs. Potential CIA analysts must submit to a thorough background investigation, a polygraph examination, and financial and credit reviews. Further, a battery of psychological and medical exams must be passed prior to a formal employment offer. The timeframe for the background check eliminates the possibility of a rapid hiring decision. Even more important are the nonverbal messages sent to the recruit that this is a position of secrecy and high importance.

Several sources of information contribute to beliefs about any organization. Friends or relatives who are already part of the organization might share their experiences with the person considering employment. Information might also be acquired from other sources, such as professional journals, magazines, newspaper articles, television, governmental and private Web sites, public statements or testimony, and annual reports. While these sources of information about an organization are far from perfect (all may contain positive and negative hyperbole), they are still useful from the point of view of forming preliminary ideas about what it might be like to work for that organization.

Because competition for highly qualified employees is fierce, successful recruitment usually involves a skillful combination of salesmanship and diplomacy. Recruiters tend to describe their organizations in glowing terms, glossing over internal problems and external threats, while emphasizing positive features. The result is that potential employees often receive unrealistically positive impressions of conditions prevailing in a specific organization. When they arrive on the job and find that their expectations are not met, they experience disappointment, dissatisfaction, and even resentment that they have been misled. In fact, research findings indicate that the less employees' job expectations are met, the less satisfied and committed they are and the more likely they are to think about quitting or actually to do so.[9]

These negative reactions are sometimes termed entry shock, referring to the confusion and disorientation experienced by many newcomers to an organization. In order to avoid entry shock, it is important for organizations to provide job candidates with accurate information about the organization. Research supports the notion that people exposed to realistic job previews later report higher satisfaction and show lower turnover than those who receive glowing, but often misleading, information about their companies.[10] Moreover, having

[9] John P. Wanous et al., "The Effects of Met Expectations on Newcomer Attitudes and Behavior: A Review and Meta-analysis."

[10] Bruce M. Meglino et al., "Effects of Ralistic Job Previews: A Comparison Using an Enhancement and a Reduction Preview."

realistic expectations helps to ease the accommodation stage of the socialization process.

Consequences of Culture Mismatch

> *When I got here, I felt like a rabbit stuck in headlights. Now, I feel like a deer.*
>
> *It took me a while to figure out that this place runs more like a newspaper than a university.*
>
> *It's pretty solitary work. I spend all day in my head. I really wasn't expecting that.*

There are several consequences of a cultural mismatch between an employee and an organization. Among these consequences are culture shock, low job satisfaction, low employee morale, increased absenteeism, increased turnover, and increased costs.

Culture Shock. People often have to be confronted with different cultures before they become conscious of their own culture. In fact, when people are faced with new cultures, it is not unusual for them to become confused and disoriented, a phenomenon commonly referred to as culture shock.

Beryl Hesketh and Stephen Bochner, among others, have observed that the process of adjusting to another culture generally follows a U-shaped curve.[11] At first, people are optimistic about learning a new culture. This excitement is followed by frustration and confusion as they struggle to learn the new culture. After six months or so with the organization, people adjust to their new cultures, become more accepting of them, and are more satisfied by them. For those who enter a mismatched culture, the productivity issue is clear: the several months required to adjust and accept the new work style results in several months of even lower productivity than is obtainable with those who fit in right away.

Job Satisfaction. Job satisfaction is defined by one scholar as "people's positive or negative feelings about their jobs."[12] It is hardly surprising that dissatisfied employees may try to find ways of reducing their exposure to their jobs. This is especially significant when one considers that people spend roughly one-third of their lives at work.

---

[11] Beryl Hesketh and Stephen Bochner, "Technological Change in a Multicultural Context: Implications for Training and Career Planning"; Maddy Janssens, "Interculture Interaction: A Burden on International Managers?"

[12] Edwin A. Locke, "The Nature and Causes of Job Satisfaction."

Interestingly, research suggests that the relationship between satisfaction and task performance, although positive, is not especially strong.[13] Thus, while job satisfaction may be important to the longevity of any individual career cycle, it is not a major factor in individual job performance. It does, however, increase absenteeism, which has a negative effect on overall organizational productivity.

Absenteeism and Turnover. Research indicates that the lower an individual's job satisfaction, the more likely he or she is to be absent from work.[14] As with job satisfaction and task performance, this relationship is modest but also statistically significant. An employee may even choose to leave an organization altogether. This voluntary resignation is measured as employee turnover and has fiscal consequences for both the individual and the organization.

Fiscal Cost. Employee turnover is a critical cost element. The expense of recruiting and training new employees, along with lost productivity from vacant positions and overtime pay for replacement workers, increases operating costs and also reduces employee organizational output.

A 2002 study by the Employment Policy Foundation found that the estimated turnover cost is $12,506 per year per full-time vacancy for the average employee with total compensation (wages and benefits) of $50,025.[15] As the average annual turnover benchmark within the Fortune 500 is 23.8 percent, one can clearly see how critical it is for organizations to lessen the number of employees who leave voluntarily. Even unscheduled absences can be expensive—averaging between $247 and $534 per employee, per day, according to the same study.

Anticipatory Socialization in the Intelligence Community

> *The secrecy is strange. I thought it would be romantic, but it turns out that it is just strange.*
>
> *I was sold on the cool factor. It's still sort of cool, I guess.*

Accepting a job with one of the 14 members of the Intelligence Community differs from other professions in that it is difficult for new employees to have a clear and precise understanding of the roles and responsibilities they are about

---

[13] The correlation is 0.17 according to Michelle T. Iaffaldano and Paul M. Muchinsky in their "Job Satisfaction and Job Performance: A Meta-Analysis."

[14] Lyman W. Porter et al., "Organizational Commitment, Job Satisfaction and Turnover Among Psychiatric Technicians."

[15] This number does not take into account the additional costs within the Intelligence Community for background and security investigations.

to assume. This is all the more pronounced because, for the most part, the Intelligence Community organizations lack a civilian counterpart.

Occasionally, the anticipatory socialization of people entering the intelligence analysis discipline will derive from accounts of current or former practitioners. More generally, however, a newcomer's initial impressions stem from the fictional media portrayals, which tend to emphasize the supposed glamour of operational tasks and pay little attention to the reality of research-based analytic work. The absence of hard knowledge about intelligence work is attributable, in part, to the organizational secrecy of the Intelligence Community and, in part, to the actual socialization process that occurs after one has been accepted for employment and has passed the required background investigation.

A newcomer's experience is often contrary to initial expectations. Employees are discouraged from talking about the specifics of their work outside of the organization or with those who have not been "cleared." On an individual level, this experience translates into professional culture shock and social isolation. Organizationally, an intentionally closed system of this kind has a number of potential performance-related consequences, among them perpetuation of the existing organizational culture by hiring familial legacies or those most likely to "fit in," job dissatisfaction, low morale and consequent reduction in employee readiness, increased employee turnover, greater likelihood of "groupthink," and strong internal resistance to organizational change.[16]

Since the attacks of 11 September, the Intelligence Community has become more open about its role in government, its day-to-day working environment, and its employees' functions and responsibilities. While this openness is an extension of an ongoing trend toward public outreach—an example is the CIA's Officer-in-Residence program established in 1985—the community has accelerated this trend toward openness in an effort to help the public, and its representatives, understand the missions and value of the Intelligence Community.[17]

This trend toward openness has improved employee retention by counteracting the culture shock of misinformed anticipatory socialization and resultant employee turnover. This trend also helps prepare the organization for the inevitable changes to come by increasing the potential recruitment pool, expanding the intellectual diversity of its staff, and fostering better relations with its broader constituency, the American public.

---

[16] Irving Janis, *Groupthink*.

[17] See CIA Officer in Residence Program in Web Resources in bibliography.

Conclusion and Recommendations

As noted, there is something of a disconnect between the largely fictionalized portrayal of the Intelligence Community in the popular media and the actual experience of intelligence analysts. This disconnect can be exacerbated once a recruit is on the job and can lead to negative consequences and behaviors, such as organizational culture shock, employee dissatisfaction, and increased employee absenteeism and turnover. This has an obvious effect on individual analysts, but it has a direct effect on the efficiency and effectiveness of the Intelligence Community.

Since the September 2001 attacks, some members of the Intelligence Community have acted to change the socialization process by providing accurate and realistic career information. One of the most widely used media for this is the Internet. For example, the Central Intelligence Agency's (CIA) Web site contains a section on "Life at the CIA."[18] This section contains information about the Agency and its culture, several analyst profiles and job descriptions written in the analyst's own words, and information concerning employee benefits and social and intellectual diversity. Although the "Employment" section of the Federal Bureau of Investigation's (FBI) Web site is less detailed than the "Life at the CIA" section of the CIA Web site, it does illustrate a typical first assignment.[19] In contrast, the "Careers" section of the Defense Intelligence Agency's (DIA) Web site contains detailed information on current job openings and the application process, but it provides no information about the actual work of a DIA analyst.[20] Steps such as these are encouraging, but they are still insufficient. There are more active things that can be done to facilitate the socialization of new employees.

To begin, Intelligence Community components should accept that what most people know about a job is often false and that it is incumbent on the organization and its recruiters to present accurate pictures and to work diligently to dispel myths. This will help to counteract the effects of culture shock. Instead of overselling a particular job or organization, recruiters should focus on facilitating the anticipatory socialization of potential employees by providing accurate information about the job and about the culture of the organization itself. Early in the selection process, applicants should be provided with realistic job previews, presented in either written or oral form. Previews should contain accurate information about the specific conditions within an organization and the specific requirements of the job. Research has shown that providing accurate descriptions of tasks is important in increasing job commitment and job satisfaction, as well as decreasing initial turnover of new

[18] See Central Intelligence Agency Web site in Web Resources.
[19] See Federal Bureau of Investigation Web site in Web Resources
[20] See Defense Intelligence Agency and US Intelligence Community Web sites in Web Resources.

employees.[21] The job preview allows candidates to make an informed decision to continue with the recruitment process or to withdraw from it if they feel the job is not appropriate. Realistic previews also lower unrealistically high expectations. A particularly good example of such an effort can be found on the CIA's Office of General Counsel Web site. This Web site includes a section titled "Misconceptions about working for the CIA," which tries to dispel prejudices and biases about employment at the CIA by addressing them in a straightforward manner.[22] In addition, the authors explain the benefits of having work experiences with the CIA for future employment endeavors in other areas.

Interview screenings of applicants should be reviewed and improved where needed. Hiring interviews are not very effective predictors of job performance; even so, there are ways to improve their reliability and validity. Numerous cognitive measurement instruments are available that help predict a match between an individual's knowledge, skills, and abilities and specific behavioral, cognitive, and psychomotor tasks.[23] In addition, the use of structured interviewing - posing the same questions to all applicants - is more effective than unstructured interviewing. Structured interviews allow for consistent comparisons among applicants.[24] Organizations should also consider using panel interviews. Differences among individual interviewers may result in inaccurate judgment of an applicant, but the overall decision of a team of evaluators may improve reliability.[25]

The use of situational exercises should be included in the recruitment process. These exercises usually consist of approximations of specific aspects of a job. They can be used to evaluate candidates' job abilities and to provide candidates with simulated work tasks. The former can facilitate organizational evaluations of candidates' performance on a job-related task; the latter may help candidates to decide whether the job would be a good match.[26]

A desirable additional step would be the creation and expansion of academic degree programs with a focus on intelligence and intelligence analysis. Further, an enhanced effort to improve public awareness and understanding of the Intelligence Community through greater community outreach, internships,

---

[21] Glenn M. McEvoy and Wayne F. Cascio, "Strategies for Reducing Employee Turnover: A Meta-analysis."

[22] See Central Intelligence Agency, Office of General Counsel Web site.

[23] The Buros Institute of Mental Measurements tracks and reports the statistical validity and reliability of thousands of measurement instruments.

[24] Richard D. Arvey and James E. Campion, "The Employment Interview: A Summary of Recent Research."

[25] P. L. Roth and James E. Campion, "An Analysis of the Predictive Power of the Panel Interview and Pre-Employment Tests."

[26] Wayne F. Cascio, *Applied Psychology in Human Resource Management*.

research fellowships, professional workshops, and academic forums will help to facilitate better employee relations by providing potential employees with a clearer perspective on what to expect after receiving their badge.

CHAPTER NINE

Recommendations

The First Step: Recognizing A Fundamental Problem

It is far too early in the research process to determine if any one organizational model for the Intelligence Community is more or less effective than any other, but I believe there is a fundamental structural question that needs to be addressed at the outset. This is, in my view, that current reporting competes for time and resources with indications and warning (I&W) intelligence. This emphasis is unlikely to change, for several reasons. First, current intelligence reporting results in significant "face-time" for the Intelligence Community with policy makers, who, in turn, provide the resources that fund and support community activities. This is a significant contributor to the social capital that the Intelligence Community commands.

The second reason is that in-depth research of the kind that contributes to I&W intelligence is a long-term investment whose payoff is often an abstraction. Not infrequently, successful warnings are taken for granted. Those that fail, however, may well involve the community in public recriminations that cost the Intelligence Community significant social capital. In this sense, the Intelligence Community's focus on current reporting is understandable. The problem is that producing current intelligence tends to become an all-consuming activity. The majority of analysts who participated in this study said that their time was spent on current reporting. Unfortunately, this does little to improve I&W intelligence, which requires long-term research, in-depth expertise, adoption of scientific methods, and continuous performance improvement. The return for the Intelligence Community, in terms of social capital, may be quite limited and even, as noted above, negative. Thus, the analytic area most in need of long-term investment often gets the least.

As the resources available to intelligence analysis are limited, it needs to be determined if those resources are better spent on the reporting functions of the Intelligence Community or on warning functions. It also needs to be determined whether these functions should be performed by the same analysts or if they are two separate career tracks. To make this determination, the Intelligence Community will need to invest in what I call a Performance Improvement Infrastructure as well as basic and applied analytic research.

Performance Improvement Infrastructure

The first step in improving job or task-specific performance is the establishment of a formal infrastructure designed explicitly to create an iterative performance improvement process. Such a process would include:

- measuring actual analytic performance to create baseline data;
- determining ideal analytic performance and standards;
- comparing actual performance with ideal performance;
- identifying performance gaps;
- creating interventions to improve analytic performance;
- measuring actual analytic performance to evaluate the effectiveness of interventions.

Several organizational, or infrastructure, assets should be developed to support this process. These should include:

- basic and applied research programs;
- knowledge repositories;
- communities of practice;
- development of performance improvement techniques.

The performance improvement process would be repeated throughout the life cycle of an organization in order to encourage continuous improvement. With the infrastructure and process in place, an organization would be capable of adapting to new or changing environmental conditions.

Infrastructure Requirements

Institutional changes, such as corporate reorganizations, are often enacted without a clear understanding of their potential or actual impact. What is most often missing in such changes is a basic research plan or a systems approach

to determine and predict the effect on organizational performance. The same is true with the Intelligence Community. Although there have been numerous proposals to reorganize the Intelligence Community—including those that resulted from the hearings of the Kean 9/11 commission—few have addressed the question of why one change would be any more effective than any other change. Merely asserting, based on some a priori notion of effectiveness, that organizational scheme X is more effective than organizational scheme Y is insufficient evidence. What is needed is a posteriori data, such as case studies, to support or refute the proposed change.[1]

Organizational Requirements. Many large organizations distribute performance improvement responsibilities throughout the organization at a supervisory or midlevel of management, but the group most often charged with collecting and analyzing performance data is the human resources department. This task generally involves developing task-specific performance standards and metrics based on expert performance models and in accordance with corporate policy.

The human resources department also becomes the central repository for pre-, periodic, and post-performance measurements. As this department generally has contact with employees throughout their careers, this is the most efficient way to manage, analyze, and inform senior leadership about aggregate changes in performance over time. Although data are collected at the individual level, it is the aggregation of performance data that allows leadership to determine the effectiveness of any organizational change or job-related intervention.

Baseline Data. Measuring actual analytic performance is essential to the establishment of a data driven performance infrastructure. The analysts in this study perceived their performance to be tied directly to the quantity of written products they produced during each review period. Counting the number of analytic publications is one metric, of course, but it is hardly indicative of analytic quality. Surgeons are a useful example of this problem.. They may count the number of patients they treat, but this metric says more about system throughput and salesmanship than it does about surgical performance. Unlike the purely cognitive work of intelligence analysts, surgeons have the advantage of multiple physical outputs, which makes measurement an easier task. In particular, surgeons have patient outcomes, or morbidity and mortality ratios, which become a grounded end-state for all measurements.[2] Other things being equal, these data then ought to inform a prospective patient about where to take his or her business.

---

[1] William Nolte, a deputy assistant director of central intelligence for analysis and production proposed such an idea in "Preserving Central Intelligence: Assessment and Evaluation in Support of the DCI " in *Studies in Intelligence* 48, no. 3 (2004): 21–25.

For intelligence analysts, the question may be put as, "What is an analytic morbidity and mortality ratio?" The process of describing and identifying morbidity and mortality, or error and failure in analytical terms, is a necessary step in identifying mechanisms to develop, test, and implement performance improvement interventions. There was little consensus among the participants in this study about what comprises failure, or even if failure was possible. There was greater consensus regarding the nature of analytic error, which was generally thought to be a consequence of analytic inaccuracy.

Metrics. One could reasonably conclude that compounded errors lead to analytic failure. Conversely, one could conclude that failure is the result of analytic surprise, that its causes are different from the causes of error, and that it needs to be treated as a separate measurement. This subject is open to debate and will require further research. It is still possible, however, to use both accuracy and surprise as metrics in evaluating analytic performance on a case-by-case basis.

The advantage of an error and failure metric is that it is observable in a grounded state separate from the analytic process. Any analytic product can be reviewed to determine levels of accuracy, and any unexpected event can be traced back through analytic products to determine if there was an instance of surprise.

Once levels of error and failure are calculated, along with measures of output, it is possible to determine expert levels of performance and to derive performance models based on successful processes. In any organization, there will be those individuals with the greatest output—in this case, the greatest number of written products. There will also be individuals with the highest levels of accuracy—in this case, factual consistency. There will also be individuals who have the lowest incident of surprise—in this case, those who generate the greatest number of potential scenarios and track and report probabilities most reliably. Using data-driven metrics means that expertise is not a function of tenure; rather, it is a function of performance.

Once expert performers are identified, it is possible to capture their work processes and to develop performance models based on peak efficiency and effectiveness within the Intelligence Community. Through the use of cognitive, behavioral, and linguistic task analyses, ethnography, and controlled experiments, it is possible to generate process metrics to identify analytic methods that are more effective for specific tasks than other methods. This is not to say that there is one analytic method that is the most effective for intel-

[2] Grounded Theory is the development of theoretical constructs that result from performing interpretive analysis on qualitative data rather than relying on a priori insights. The theory is then derived from some grounded data set. Barney Glaser and Anselm Strauss, *Discovery of Grounded Theory*; Barney Glaser, *Theoretical Sensitivity*; Barney Glaser, *Basics of Grounded Theory Analysis*.

ligence analysis; rather, each type of task will have an analytic method that is best suited to accomplishing it in an efficient and effective manner.

Developing these metrics is no small task. It is a job that will require numerous researchers and research programs within, or with access to, the Intelligence Community. These programs will need formal relationships with human resource departments, analytic divisions, organizational leadership, and developers of training and technology interventions in order to have a positive effect on analytic performance.

Research Programs

The results of this research indicate that the Intelligence Community needs to commit itself to performance research that is rigorous, valid (in that it measures what it proposes to measure), and replicable (in that the method is sufficiently transparent that anyone can repeat it). Within some intelligence organizations, this has been an ongoing process. The problem is that most of the internal research has concentrated on historical case studies and the development of technological innovations. What is missing is focused study of human performance within the analytic components of the Intelligence Community. Questions about the psychology and basic cognitive aptitude of intelligence analysts, the effectiveness of any analytic method, the effectiveness of training interventions, group processes versus individual processes, environmental conditions, and cultural-organizational effects need to be addressed.

This effort will require commitment. Researchers will have to be brought into the Intelligence Community, facilities will have to be dedicated to researching analytic performance, expert analysts will have to give some percentage of their time to participating in research studies, managers and supervisors will have to dedicate time and resources to tracking analytic performance within their departments, human resource staffs will have to dedicate time and resources to developing a performance repository, and there will have to be formal interaction between researchers and the community.

Analytic Performance Research. In the previous section, I discussed the need for analytic standards as part of the Performance Improvement Infrastructure. In terms of a research program, this will require, as a first step, the collection of baseline analytic performance data and a clear and measurable description of ideal analytic behavior. Next, there should be a determined effort by human performance researchers to develop, test, and validate analytic performance metrics and measurement systems. This will be a lengthy process. The accuracy and surprise measures suggested in this text require large historical and comparative data sets and are cumbersome and time consuming to perform. Conducting behavioral, cognitive, and linguistic task

analyses requires significant research expertise, ample time, and broad organizational access.

In time, analytic performance research will become a highly specialized domain and will require continuous organizational access not normally available to outsiders. It will become necessary for the Intelligence Community to establish internal or cooperative research centers in order to acquire the research expertise necessary to analyze and effect performance improvement. There are numerous community outreach efforts on which these centers can be built. Those efforts need to be expanded, however, and those programs need to include domains beyond the traditional relationship between the Intelligence Community and political or geographic area experts.[3]

Institutional Memory. The results of this research program indicate that there is a loss of corporate knowledge in the Intelligence Community due to employee attrition and the lack of a central knowledge repository for capturing "lessons learned." A number of industries and government organizations, including the Departments of Defense and Energy and the National Aeronautics and Space Administration, already maintain centers for lessons learned as an information hub for its employees.[4]

These centers act as information repositories for successful and unsuccessful operations and interventions. Their purpose is to reduce the amount of organizational redundancy and levels of error and failure by tracking, analyzing, and reporting on after-action reviews and analytic outcome data.[5] The other primary function of these repositories is to establish networks for communities of practice within and among organizations.

Networked communities of practice allow professionals to interact, exchange methodological information, post and respond to individual case studies, and develop ad hoc teams of experts for specific problem solving tasks. With simple search tools, basic database software, and a simple network visualization interface, any analyst in the Intelligence Community would be able to identify any other expert whose domain specialty was needed to answer a specific question or solve a specific problem. Another advantage of this model is the development of formal and informal mentoring within the network. Any novice would be able to find an expert within the Intelligence Community and establish a relationship that would be beneficial to both. With appropriate incentives, experts would be encouraged to contribute to the network and make available their time and expertise for the purpose of mentoring.

---

[3] An example of researching the validity and reliability of metrics can be found in the *Buros Mental Measurement Yearbook* at the Buros Institute of Mental Measurements Web site.

[4] See the US Army Center for Army Lessons Learned (CALL) Web site, which has links to numerous other repositories.

[5] See Chapter Six for a more detailed explanation of the After Action Review process.

Intelligence analysis, like other fields of science, is a cognitive process. Although tools and technologies may be available to assist cognitive processes, such as measurement devices for physical scientists, technology is ultimately merely a tool to be designed and developed using a human-centered approach. As such, any new technology needs to be a passive tool, employed by analysts to solve specific problems or answer specific questions, rather than a restrictive reinterpretation of cognition according to the rules of binary computation and artificial intelligence theorists.[6]

Analytic Psychology and Cognition. As evidenced by the work of Richards Heuer and others, there is significant research to be conducted into the cognitive mechanisms involved in intelligence analysis.[7] Understanding and defining the heuristics used in performing intelligence analysis, as well as cognitive-load thresholds, multitasking requirements, mechanisms that generate cognitive biases, and the utilization of pattern recognition strategies and anomaly detection methods are all areas that will prove fundamental to improving analytic performance.

In addition to researching basic cognitive functions and intelligence analysis, this area of research will be valuable for understanding how external variables, such as time constraints and analytic production methods, affect the cognitive processing of individual analysts. Another result will be the development of future employee screening and selection tools that will match the specific cognitive requirements of intelligence analysis with each applicant's individual knowledge, skills, and abilities.

Analysts employ cognitive strategies that are time efficient in order to cope with the demands of producing daily written products, but such strategies are not necessarily the most effective analytic methods for increasing analytic accuracy and decreasing the occurrence of analytic surprise. In fact, improving analytic accuracy and avoiding surprise may require mutually exclusive analytic strategies. This line of inquiry will require baseline performance data generated through the development of performance metrics and conducted in conjunction with research in analytic methodology effectiveness. The results would then be integrated into a knowledge repository.

These types of studies will require experimental psychologists and cognitive scientists working in controlled laboratory environments with consistent access to working professional analysts.

---

[6] See Chapter Five for a more detailed description of the limitations of technological solutions.

[7] Richards J. Heuer, Jr., *Psychology of Intelligence Analysis*; William Brei, *Getting Intelligence Right*; Isaac Ben-Israel, "Philosophy and Methodology of Intelligence: The Logic of Estimate Process"; Klaus Knorr, *Foreign Intelligence and the Social Sciences*; Abraham Ben-Zvi, "The Study of Surprise Attacks." See also Marjorie Cline, Carla Christiansen and Judith Fontaine, *Scholar's Guide to Intelligence Literature*.

Development and Validation of Analytic Methods. The Intelligence Community routinely generates ad hoc methodologies to solve specific analytic problems or crises. However, once the problem has been solved, or the crisis averted, the new analytic method may or may not become part of the institutional memory. Often these new methods are lost and need to be re-created to address the next problem or crisis. In addition, these methods are seldom tested against other competing analytic methods for validity or reliability. It is difficult for an analyst to know which analytic method to employ in a given situation or requirement.

There are obvious inefficiencies in the current model. First, there is the loss of corporate knowledge each time an innovative analytic method is generated and subsequently abandoned. Second, there is no effectiveness testing center where analytic methods can be compared for specific cases. Although there are hundreds of analytic strategies, there is no way to determine which strategy is the most effective for any particular problem set.

The lack of an analytic methodology research agenda leads analysts to choose methods with which they are most familiar or to choose those dictated by circumstance, such as deadlines. Moreover, instead of advancing the concept that intelligence analysis is science and needs to be engaged in like any other scientific discipline, the paucity of effectiveness data supports a deep-seated community bias that analytic methods are idiosyncratic and, therefore, akin to craft.

The development of a research agenda for analytic methodology that is focused on collecting effectiveness and validation data is the first step in moving intelligence analysis from a tradecraft model to a scientific model. This may be the most culturally difficult recommendation to implement: there is cultural resistance to adopting a science-based model of intelligence analysis that is rooted in the traditions, norms, and values of the Intelligence Community. Another difficult step will be to introduce effectiveness data and corresponding analytic methods to the community at large and to incorporate these in future training programs.

Training Effectiveness. Successful analysis demands group cohesion and the implementation of consistent, effective analytic methods within the Intelligence Community. The best way to achieve this is through formal basic and advanced training programs. As noted earlier, several agencies within the community have invested resources in formal training programs, but these programs are unique to each agency and are often missing evaluations of student performance. Although most formal courses include a written subjective evaluation of the instructor, as well as the student's perception of the value of the course, the evaluation of student performance has yet to be formalized.

Without evaluating preintervention, or precourse, performance and following that with a postintervention evaluation, it is difficult to determine the effect that any training intervention will have on employee performance. In addition to formal measurements based on course objectives, it is important to collect performance data from managers and supervisors to evaluate the retention of training and the impact that training has had on actual day-to-day performance.

Developing performance metrics will inform and advance the training interventions currently employed in the Intelligence Community and will determine the gap between ideal performance and actual performance. As such, the system is an iterative process of setting performance standards, measuring actual performance, designing training interventions to improve performance, and evaluating the effects of those interventions on actual performance. The data derived from these interventions and measurements will then contribute to the growth of the knowledge repository and strengthen the ties created through the communities of practice.

Organizational Culture and Effectiveness. Identifying existing organizational norms and taboos is the first step to creating an internal dialogue about the future of an organization and its place in a competitive environment. Culture drives the operations of an organization, determines the people who are hired, enculturates new employees, establishes standards of behavior and systems of rewards, shapes an organization's products, and determines the social capital that any organization may possess. In short, culture defines an organization's identity to itself and to others.

Understanding the culture of the Intelligence Community and analyzing the effects of any performance intervention on that culture contributes to the evaluation of intervention effectiveness. Effective performance interventions will have a positive effect on the organization's culture and become themselves measurement instruments.

Developing cultural markers to track organizational change and performance improvement requires baseline ethnographic data and the identification of key cultural indicators. Once identified, cultural indicators such as language use, norms, and taboos would be measured at regular intervals and would serve as grounded data to determine levels of change within the organization. This would permit interventions to be modified before they became ritualized within the Intelligence Community.

The Importance of Access

The improvement of human performance often requires an organization to change its culture, and organizational leaders seldom possess sufficient power to mandate cultural change by edict. At best, management can introduce

agents or agencies of change and manage their organization's culture in the same way they manage physical and financial resources. An organization's culture shapes individual behavior by establishing norms and taboos and, ultimately, determines the quality and character of an organization's products. Culture and product are inseparable, and one cannot be changed without affecting the other. The choice confronting any organization is to manage its institutional culture or to be managed by it.

There is no single path to carrying out the research recommended in this work. It could be performed at a single center or coordinated through several specific centers; it could be purely internal to the Intelligence Community; a cooperative effort among the community, academe, and national laboratories; or some combination of these. What is most important to effective implementation is that there be regular and open access among researchers and the Intelligence Community. This may appear simple enough, but access equals trust, and trust is difficult to establish in any domain. This is especially the case within the Intelligence Community. The Intelligence Community needs to increase its commitment to community outreach efforts. This study is one such effort.

During the course of my research, the value of access and the premium the community places on trust quickly became evident. At agency after agency, physical access restrictions, security clearances, forms, interviews, phone calls, questions, vetting, and more vetting were all signs of the value, not of secrecy per se, but of trust and access. Without this sort of cooperation, this research would have been impossible, and this is an important lesson that ought to inform future research programs.

PART IV

Notes on Methodology

CHAPTER TEN

Survey Methodology

This study included 489 interviews with intelligence professionals, academics, and researchers throughout the Intelligence Community. It also involved participation in intelligence training programs, workshops, and focus groups; direct observation of intelligence analysts performing their duties, and participant observation in a variety of analytic tasks. My access was not restricted to specific people, locations, or organizations. I was allowed to observe, interview, and participate in whatever manner I thought would be most beneficial to the research project.

Unlike other academic studies of the intelligence discipline (case studies or topic-specific postmortems, for example), this study was process oriented. It also differed from the work of Sherman Kent, Richards Heuer, and other intelligence professionals concerned with the process of intelligence analysis.[1] Rather than having an intelligence professional looking *out* to the social and behavioral sciences, this study had a social scientist looking *in* at the intelligence profession. Although some of the conclusions of this work may be similar to previous studies, the change in perspective has also led to some different findings.

It is important to keep in mind that cultural anthropology is a qualitative discipline and that, in general, its findings are descriptive and explanatory rather than inferential or predictive. The use of ethnographic methods to describe a culture, the environment in which that culture operates, and the work processes that culture has adopted is designed to generate testable theory that can be investigated experimentally or quasi-experimentally using other

[1] Sherman Kent, *Strategic Intelligence for American World Policy;* Richards J. Heuer, Jr., *Psychology of Intelligence Analysis.*

research methodologies. Additionally, ethnography is used to identify and describe the influence of different variables on cultural phenomena, again with a focus on developing testable theory. Unlike more quantitative disciplines, cultural anthropology is not traditionally employed experimentally to test theory or to generate predictive measures of statistical significance.

The findings in this work describe the data collected during this study, but they do not indicate the weight or general statistical effect of any one variable as opposed to any other variable. Although a single variable might have more effect on the error or failure rate of intelligence analysis, further quantitative research will be needed to determine those statistical values. Without additional quantitative support, it may not be possible to generalize from these findings.

Methodology

This study used an applied anthropological methodology for the collection and analysis of qualitative data.[2] A traditional approach to ethnography, the descriptive documentation of living cultures, was modified for use in post-industrial organizational settings.[3] This method included conducting interviews, directly observing analysts performing their jobs, participating in analytic tasks and training, and conducting focus groups. The settings for this research included the 14 members of the Intelligence Community, related government agencies, universities, think tanks, national laboratories, the National Archives and related presidential libraries, and private and corporate locations.

The background data were collected using a Q-sort literature review method, which is discussed in more detail in Chapters Three and Eleven. This procedure was followed by semi-structured interviews, direct observation, participant observation, and focus groups. The Q-sort method was employed specifically because of its utility for developing taxonomic categories.[4]

The identity of the research participants will not be revealed. Participant responses and observational data gathered during the research process have been tabulated and made anonymous or aggregated according to context and

---

[2] Erve Chambers, *Applied Anthropology: A Practical Guide;* Alexander Ervin, *Applied Anthropology*: *Tools and Perspectives for Contemporary Practice.*

[3] Russell Bernard, *Research Methods in Anthropology: Qualitative and Quantitative Approaches;* Robert Bogdan, *Participant Observation in Organizational Settings;* Norman Denzin and Yvonna Lincoln, *Handbook of Qualitative Research*; Jean Schensul and Margaret LeCompte, *Ethnographer's Toolkit. Vol. I - Vol. VII;* James Spradley, *Participant Observation;* Robert Yin, *Case Study Research: Design and Methods.*

[4] William Stephenson, *The Study of Behavior: Q-Technique and its Methodology.*

content and, thus, are not attributable to any specific individual. This is not simply the result of security procedures within the Intelligence Community; it is also the professional obligation of every member of the American Anthropological Association, as stated in the American Anthropological Association Code of Ethics.[5]

The interview technique employed in this study was semi-structured. Several specific questions about the participant's perception of the nature of intelligence, the analytic process, the intelligence production cycle, and intelligence errors and failures were standard throughout the interviews. Other questions, specific to the individual's job responsibilities, were tailored to each respondent. This method allowed for a more open-ended approach, which surveys and highly structured interviews do not. The semi-structured method is more akin to an open conversation (with consistent data collection constructs and probing questions) than to a formal interview, which helps put the respondents at ease and makes the entire process seem somewhat less contrived.

Access to interview participants was made possible through the Center for the Study of Intelligence. Individuals at CSI introduced me to their contacts throughout the Intelligence Community, including active and retired senior analysts, managers and senior leadership, as well as to academics and researchers. The various intelligence-training centers put me in touch with new hires and novice analysts. Each interviewee was asked to make recommendations and provide contact information for others who might be interested in participating in this research project. In addition, numerous interviewees were approached without a formal or informal introduction from a previous participant. Only four of the 489 individuals contacted to date have declined to participate in this study. This constitutes a participation rate of greater than 99 percent, which is unusually high for this type of research. Although a participation rate this high may be an artifact of the sampling method or of an organizational pressure to participate, it also may indicate a general desire within the Intelligence Community to support performance improvement research.

Unlike random sampling, purposive sampling is an attempt to collect data from specific data sources. In anthropological studies, purposive sampling is regularly used to address specific issues and to answer specific questions. Normally, this approach requires finding a "key informant" or someone on the inside of a specific culture who will become the researcher's ally and access agent. In this particular study, the CSI staff acted as access agents to the Intelligence Community at large.

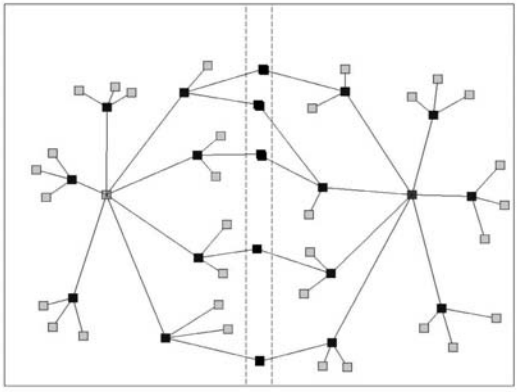
---

[5] American Anthropological Association, *Code of Ethics of the American Anthropological Association*.

Relying on such a "social network" sampling method for collecting interview data does pose potential statistical biases.[6] The likelihood that each new interviewee was referred to me because of a friendly relationship with a previous interviewee may mean that those references are "like minded" and not necessarily representative of the population of intelligence professionals. In order to counteract that bias, efforts were also made to enlist individuals without any social network-based introduction. The "cold" contacts were informed of the nature of the research project, its sponsorship, and its goals, given reference information for verification, and then invited to participate. The "cold" contact interviewees were also asked to make recommendations and provide contact information for others who might be interested in participating in the study.

This strategy was used in an attempt to reduce the affects of sampling bias by generating parallel social network samples. The figure below is a visual representation of a parallel social-network sampling model. The central, or first-order, node on the left is a "cold" contact or unknown individual who recommends several second-order contacts, each represented as a node within the left box. The second-order "cold" contacts then make additional recommendations for third-order contacts, and so on. The central (first-order) node on the right is a "hot" contact or a known individual who recommends several second-order contacts, each represented as a node within the right box. The second-order "hot" contacts then make recommendations for third-order contacts, and so on.

Social Network Mapping



In many instances, the contacts from both social network samples overlapped or converged on specific individuals, as represented by the overlapped fourth-order nodes in the central column. There are several possible explanations for this convergence. It may indicate that there are a number of respected "thought leaders" in the Intelligence Community whom each contact believed I should interview for this project, or the convergence of nodes

[6] Social network sampling is also known as "snowball" sampling in sociology and psychology.

might merely serve to emphasize the small size of Intelligence Community. In any case, this approach to sampling may help to ameliorate the sampling bias inherent in qualitative research.

In addition to semi-structured interviews, both direct and participant observation data collection methods were employed. The direct observation method involved watching Intelligence Community analysts perform their tasks in both actual and training environments, recording the physical and verbal interactions they had with one another, and observing the steps used to create intelligence products. Direct observation occurred over the course of two years by observing 325 individual analysts and teams of analysts performing their specific tasks. The data collected from observing the 325 analysts were not included in the semi-structured interview data because I did not use the formal semi-structured interview process to structure those interactions. These observational data were recorded separately in field notes and used for triangulating the findings from the interviews.

The participant observation method is employed to give the researcher a "first-person" understanding of the context and nuances associated with a task and the culture in which that task occurs. Although the researcher possesses only an approximation of the knowledge and understanding of the actual practitioners of the task and their culture, this "first-person" perspective can lead the researcher to new insights and new hypotheses.

During this study, the participant observation was conducted during analytic production cycles, scenario development, and red cell exercises. This included monitoring my own analytic strategies, the analytic strategies of others as diagramed or verbalized, the physical and verbal social interactions among the participants, the environment in which the tasks occurred, and the steps used to create a final intelligence product. These data, along with notes on social dynamics, taboos, and social power, were recorded in field notes and created a separate data source for triangulation.

With modern anthropology, these data normally would be captured on film, audiotape, or in some digital format. Due to the security requirements of the Intelligence Community, however, the data were captured only in the written form of field notes. As is the case with the field notes, the identity of the interview participants will not be disclosed. This is in keeping with both the security practices of the Intelligence Community and the professional standards described in the American Anthropological Association Statement on the Confidentiality of Field Notes.[7]

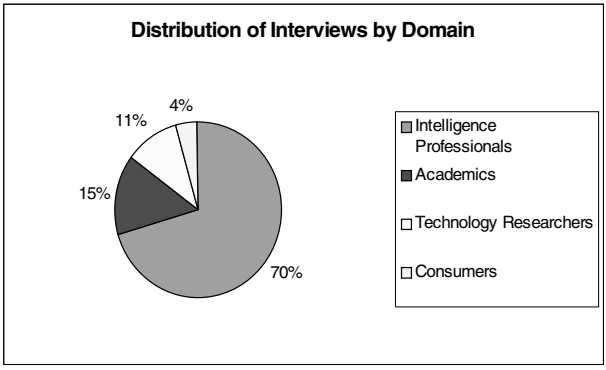
The data from the interviews were analyzed using a method called interpretational analysis.[8] This approach included segmenting the interview data into

[7] American Anthropological Association, *Statement on the Confidentiality of Field Notes.*

analytic units (or units of meaning), developing categories, coding the analytic units into content areas, and grouping the analytic units into categories. From these categories, general trends and specific instances can be identified. As noted, the direct and participant observational data were analyzed separately in order to triangulate the findings from the interview data. The purpose of using multiple data sources for triangulation is to uncover internal inconsistencies in the data, to cross-check those inconsistencies with the available literature, and to verify the content validity for each category.

Demographics

As of this writing, 489 semi-structured interviews have been conducted with active and retired intelligence professionals, intelligence technology researchers, academics who teach the intelligence discipline or have published in it, and consumers of intelligence products.[9] Of the 489 individuals interviewed, 70-percent were newly hired, active, or retired intelligence professionals; 15-percent were academics; 11-percent were intelligence technology researchers; and the remaining four percent were policy makers or senior consumers of intelligence products. The graph here shows the distribution of interviews by percentage for each professional category.



The table below lists each professional category and the corresponding total number (N) of individuals interviewed. The intelligence professional category is further divided into three sub-groups. The "novice" sub-group includes new hires and those with less than two years of experience.[10] The "active" sub-

[8] Leonard Bickman and Debra Rog, *Handbook of Applied Social Research Methods;* Meredith Gall et al., *Educational Research;* Jonathan Gross, *Measuring Culture: A Paradigm for the Analysis of Social Organization*; Ernest House, *Evaluating with Validity;* Jerome Kirk and Marc Miller, *Reliability and Validity in Qualitative Research, Qualitative Research Methods, Volume 1*; Delbert Miller, *Handbook of Research Design and Social Measurement;* Michael Patton, *Qualitative Evaluation and Research Methods*; Peter Rossi and Howard Freeman, *Evaluation*. *A Systematic Approach*.

[9] Additional interviews are being conducted.

group includes all those currently working in the Intelligence Community with more than two years of experience. The "retired" sub-group includes those who have spent more than fifteen years in the intelligence profession and have since gone on to either full retirement or other organizations outside of the Intelligence Community.

Of the 345 intelligence professionals interviewed, 20 percent were novices, 65 percent were active, and 15 percent were retired. The active and retired sub-groups include senior managers.

Interview Categories and Numbers

Category	**N**
Intelligence Professionals	345
Novice	(60)
Active	(233)
Retired	(52)
Academics	73
Technology Researchers	53
Consumers	18
Total Interviewed	**489**

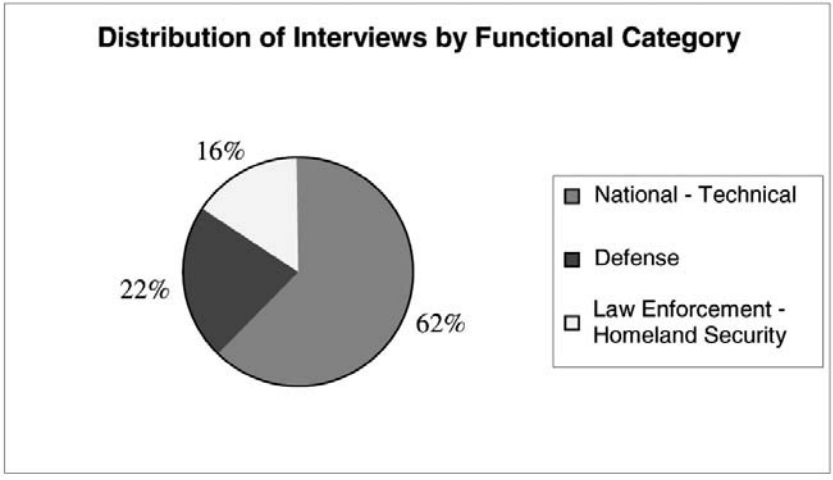
In order to assure anonymity for the participants, I have created broader job-related functional categories and associated the number of individuals interviewed with the broader categories rather than linking them to specific organizations within the Intelligence Community. This is in contrast to aggregating the agencies according to each agency's specific mission, process, or product. Although not an official member of the Intelligence Community, the Drug Enforcement Administration is included because of its intelligence function and resources. The table on the next page shows how I aggregated the agencies into National-Technical, Defense, and Law Enforcement-Homeland Security categories according to the professional functions of interview participants.

[10] The use of two years as a divide between novice and active is derived from the total amount of experience it is possible to gain in that time. See the discussion of expertise in Chapter Five.

Agency Aggregation According to Interviewee Job-type

National-Technical	Defense	Law Enforcement-Homeland Security
Central Intelligence Agency	Defense Intelligence Agency	Department of Homeland Security
National Security Agency	Army Intelligence	Federal Bureau of Investigation
National Reconnaissance Office	Air Force Intelligence	Department of Energy
National Geospatial Intelligence Agency	Navy Intelligence	Department of Treasury
Department of State (INR)	Marine Corps Intelligence	*Drug Enforcement Administration*

The figure below shows the distribution of intelligence professionals interviewed for this study according to each broader functional category. Of the 345 intelligence professionals interviewed, 214 work within the National-Technical Intelligence category, 76 in the Defense Intelligence category, and 55 in the Law Enforcement—Homeland Security category.



CHAPTER ELEVEN

Q-Sort Methodology

Observations always involve theory.

Edwin Hubble[1]

As described earlier, this work reflects triangulation of the data derived from the literature Q-sort, interview responses, and observations.[2] The data include 489 interviews, direct and participant observation of 325 analysts performing their jobs, participation in a variety of analytic tasks, and focus groups conducted to generate the taxonomy of variables that guided this study.

The first Q-sort of the data was aggregated according to the function of each intelligence organization, as listed in Table 1. The data were then analyzed to determine response context according to job type and to develop variable categories.

The organizational Q-sort generated the broad variable groupings used to create the second Q-sort parameters. The variable categories that emerged during the interpretive analysis of the first Q-sort of the data were compiled again, and a second Q-sort was performed based on those categories. The data was then aggregated according to categorical or variable groupings of the second Q-sort, Table 2.

The use of two separate Q-sort strategies generated the variables and then de-contextualized the data in order to find consistent trends throughout the Intelligence Community. That is, this strategy resulted in broad categories of findings that apply across many agencies. In those cases where interview and

---

[1] Edwin Hubble discovered the first evidence to support the Big Bang theory that the universe is expanding and that the Milky Way is not the only galaxy in the universe. He also developed the Hubble Galaxy Classification System and Hubble's Law (the farther away a galaxy is from Earth, the faster its motion away from Earth). Edwin Hubble, *The Realm of the Nebulae*.

[2] William Stephenson, *The Study of Behavior: Q-Technique and its Methodology.*

observational data could have been sorted into several categories, I based the placement of the data on the question that generated the interview response.

Table 1. Q-Sort 1. Data Grouping According to Organizational Function.

National – Technical	Defense	Law Enforcement – Homeland Security
Central Intelligence Agency	Defense Intelligence Agency	Department of Homeland Security
National Security Agency	Army Intelligence	Federal Bureau of Investigation
National Reconnaissance Office	Air Force Intelligence	Department of Energy
National Geospatial Intelligence Agency	Navy Intelligence	Department of the Treasury
Department of State (INR)	Marine Corps Intelligence	*Drug Enforcement Administration*

In several instances throughout the text, the quotes that were used may well fit in a number of other categories. Once the data were sorted by variable, the coding and context identifier notes were removed from all data in order to assure participant anonymity, in keeping with the American Anthropological Association *Code of Ethics*, section III, A.[3]

Table 2. Q-Sort 2. Data Grouping According to Variable Categories.

Time Constraints	Analytic Methods	Organizational Norms	Analytic Identity	Analytic Training
Products	Tradecraft	Taboos	Reportorial	Formal
Interactions	Science	Biases	Academic	Informal

The quotes that appear throughout the text are exemplars from each variable category and indicate trends found in the data-set. Although the exemplar quotes are not universal, nor are they necessarily subject to generalization, they do represent consistent findings from the interview and observation data. Utilizing this approach to develop theory is similar to the method in which grounded theory is employed in sociology, specifically, using grounded data to generate theory rather than using some a priori technique. The significant advantage to this approach is that the theory is directly tied to data, providing it additional validity. Another advantage is that the individuals who allowed me to interview and observe them are given some voice in the final product by way of direct quotes, which also provides some qualitative context.

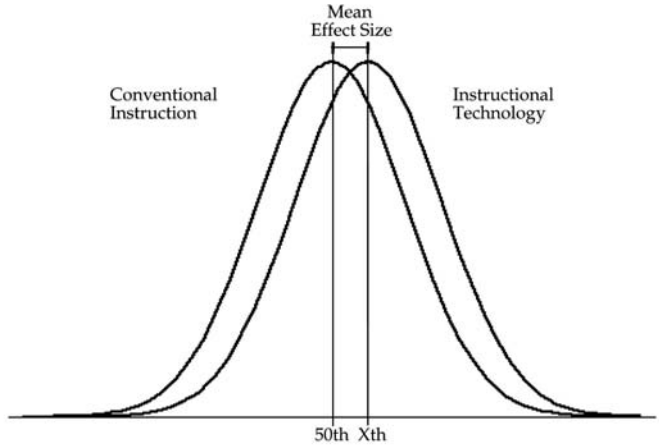
[3] American Anthropological Association, *Code of Ethics of the American Anthropological Association*.

CHAPTER TWELVE

The "File-Drawer" Problem and Calculation of Effect Size

The file-drawer problem appears to have two causes: the reluctance of researchers to report their null results and the reluctance of professional journal editors to include studies whose results fail to reach statistical significance. Such studies remain in the "file-drawers" of the researchers. How much would these inaccessible studies affect the results of our meta-analysis? The answer seems to be not much.[1]

Effect Size - Difference Between Two Means



[1] Gene Glass, and Barry McGaw, "Choice of the Metric for Effect Size in Meta-Analysis"; Larry Hedges, "Estimation of Effect Size from a Series of Independent Experiments"; Larry Hedges and Ingram Olkin, "Vote-Counting Methods in Research Synthesis."

Effect size is usually defined as the difference between the means of two groups divided by the standard deviation of the control group $\left(\Delta = \frac{\overline{X}_e - \overline{X}_c}{\sigma_c}\right)$.[2]

Effect sizes calculated in this way estimate the difference between two group means measured in control group standard deviations as seen in the figure above. Glass et al. suggest that the choice of the denominator is critical and that choices other than the control group standard deviation are defensible.[3] However, they endorse the standard choice of using the control group standard deviation.

Alternatively, Hedges and Olkin show that, for every effect size, both the bias and variance of its estimate are smaller when standard deviation is obtained by pooling the sample variance of two groups instead of using the control group standard deviation by itself.[4] An effect size based on a pooled standard deviation estimates the difference between two group means measured in standard deviations estimated for the full population from which both experimental and control groups are drawn: $\left(g = \frac{\overline{X}_e - \overline{X}_c}{S}\right)$,[5] where

S is the pooled standard deviation: $S = \sqrt{\frac{(N_e - 1)(S_e)^2 + (N_c - 1)(S_c)^2}{N_e + N_c - 2}}$.[6]

Most commentators suggest that effect sizes can be treated as descriptive statistics and entered into standard tests for statistical significance. Hedges and Olkin have shown that the error variance around estimates of effect size is inversely proportional to the sample size of the studies from which the effect sizes are drawn. If the effect size in any review is drawn from studies employing widely different sample sizes, then the heterogeneity of variance among effect sizes prohibits their use in conventional t-tests, analyses of variance, and other inferential tests. This is the case in most of these reviews; therefore, effect sizes reported in this study are treated only with descriptive statistics.

The effect sizes for computer-based training range from 0.20 to 0.46 depending on the population.[7] The effect size for distance instruction (television) is

---

[2] Δ = Glass's Effect Size, $\overline{X}_e$ = Experimental Mean, $\overline{X}_c$ = Control Mean, σ_c = Control Standard Deviation

[3] Gene Glass, Barry McGaw and Mary Lee Smith, *Meta-Analysis in Social Research*.

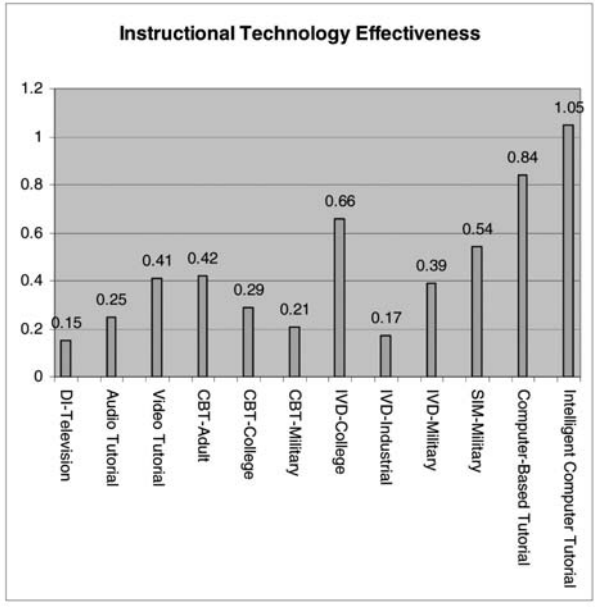
[4] Larry Hedges and Ingram Olkin, *Statistical Methods for Meta-Analysis*.

[5] g=Hedge's Effect Size, S=Hedge's Pooled Standard Deviation

[6] Ne=Number of experimental subjects, Nc=Number of control subjects, Se=Standard deviation of experimental group, Sc=Standard deviation of control group

0.15 and for interactive videodiscs, the effect sizes range from 0.17 to 0.66 depending on the population.[8] The effect size for flight simulation is 0.54 and the effect size for tutorials range from 0.25 to 0.41 depending on the presentation of the tutorial material.[9]

Although the effect sizes for instructional technology range from 0.15 to 0.66 standard deviations, they all report favorable findings when compared to conventional instruction. There are many possible explanations for the differences in instructional technology effectiveness; it might be the result of population differences, system differences, interactivity or individualization. From a purely utilitarian point of view, the reason may not be all that important. If, at the very least, using instructional technology forces the producer to rethink the content of the course to match the delivery system, then revisiting the pedagogy may be enough to produce the positive effect sizes. Whatever reason for the changes in effectiveness, the use of instructional technology saves instructional time, overhead costs, and results in a higher level of achievement for the students in a variety of domains.



[7] The abbreviations in figure one: CBT=Computer Based Training, DI=Distance Instruction, IVD=Interactive Video Disc, SIM=Simulation. More than 300 research studies were used to develop these effect sizes, see Chen-Lin Kulik., James Kulik and Barbara Shwalb, "Effectiveness of Computer-Based Adult Education: A Meta-Analysis"; Chen-Lin Kulik and James Kulik, "Effectiveness of Computer-Based Education in Colleges"; Rob Johnston and J. Dexter Fletcher, *A Meta-Analysis of the Effectiveness of Computer-Based Training for Military Instruction*.

[8] Godwin Chu and Wilbur Schramm, *Learning from Television*; J. Dexter Fletcher *Effectiveness and Cost of Interactive Videodisc Instruction in Defense Training and Education*; J. Dexter Fletcher, "Computer-Based Instruction: Costs and Effectiveness."

[9] R. T. Hays, J. W. Jacobs, C. Prince and E. Salas, "Flight Simulator Training Effectiveness: A Meta-Analysis"; Peter Cohen, James Kulik and Chen-Lin Kulik, "Educational Outcomes of Tutoring."

APPENDIX

Selected Literature

Intelligence Tools and Techniques

Jerome K. Clauser and Sandra M. Weir, *Intelligence Research Methodology: An Introduction to Techniques and Procedures for Conducting Research in Defense Intelligence* (Washington, DC: US Defense Intelligence School, 1976).

Stanley Feder, "FACTIONS and Policon: New Ways to Analyze Politics," (1987) in H. Bradford Westerfield, ed., *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal* (New Haven: Yale University Press, 1995).

Craig Fleisher and Babette Bensoussan, *Strategic and Competitive Analysis. Methods and Techniques for Analyzing Business Competition* (Upper Saddle River, NJ: Pearson Education, 2003).

Leonard Fuld, *The New Competitor Intelligence. The Complete Resource for Finding, Analyzing, and Using Information About Your Competitors* (New York: John Wiley & Sons, 1995).

Ronald Garst, ed., *A Handbook of Intelligence Analysis*, 2nd ed (Washington, DC: Defense Intelligence College, 1989).

R. Hopkins, *Warnings of Revolution: A Case Study of El Salvador* (Washington, DC: Center for the Study of Intelligence, 1980) TR 80-100012.

Morgan Jones, *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving* (New York, NY: Times Business, 1998).

Larry Kahaner, *Competitive Intelligence. How to Gather, Analyze, and Use Information to Move Your Business to the Top* (New York: Touchstone, Simon and Schuster, 1996).

Jonathan Lockwood and K. Lockwood, "The Lockwood Analytical Method for Prediction (LAMP)," *Defense Intelligence Journal* 3, no. 2 (1994): 47–74.

Douglas J. MacEachin, et al., *The Tradecraft of Analysis: Challenge and Change in the CIA* (Washington, DC: Consortium for the Study of Intelligence, 1994).

Don McDowell, *Strategic Intelligence: A Handbook for Practitioners, Managers and Users* (Canberra, Australia: Istana Enterprises, 1998).

Marilyn Peterson, *Applications in Criminal Analysis* (Westport, CT: Greenwood Press, 1995).

———, Bob Morehouse, and Richard Wright, eds. *Intelligence 2000: Revising the Basic Elements* (Sacramento CA: LEIU and IALEIA, 2000).

John Pierce, "Some Mathematical Methods for Intelligence Analysis," *Studies in Intelligence* 21 (Summer 1977, declassified): 1–19.

John Prescott and Stephen Miller, eds. *Proven Strategies in Competitive Intelligence* (New York: John Wiley & Sons, 2001).

Edwin Sapp, "Decision Trees," *Studies in Intelligence* 18 (Winter 1974, declassified): 45–57.

David Schum, *The Evidential Foundations of Probabilistic Reasoning* (Evanston, IL: Northwestern University Press, 1994).

Jack Zlotnick, "Bayes' Theorem for Intelligence Analysis," (1972), in H. Bradford Westerfield, ed. *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal* (New Haven: Yale University Press, 1995).

Cognitive Processes and Intelligence

Edgar Johnson, *Effects of Data Source Reliability on Inference* (Alexandria, VA: Army Research Institute for the Behavioral and Social Sciences, Technical Paper #251, 1974).

Robert Mathams, "The Intelligence Analyst's Notebook," in Douglas Dearth and R. Thomas Goodden, eds., *Strategic Intelligence: Theory and Application*, 2nd ed. (Washington, DC: Joint Military Intelligence College, 1995).

Avi Shlaim, "Failures in National Intelligence Estimates: The Case of the Yom Kippur War," *World Politics* 28, no. 3 (1976): 348–80.

Tools and Techniques as Cognitive Processes

Bruce D. Berkowitz and Allan E. Goodman, *Best Truth: Intelligence in the Information Age* (New Haven: Yale University Press, 2000).

———, and Allan E. Goodman, *Strategic Intelligence for American National Security* (Princeton: Princeton University Press, 1989).

Sherman Kent, "Words of Estimative Probability," *Sherman Kent and the Board of National Estimates: Collected Essays* (Washington, DC: Center for the Study of Intelligence, 1994).
Lisa Krizan, *Intelligence Essentials for Everyone* (Washington, DC: Joint Military Intelligence College, 1999).

Intelligence Analysis as Individual Cognitive Process

Alexander Butterfield, *The Accuracy of Intelligence Assessment: Bias, Perception, and Judgment in Analysis and Decision* (Newport, RI: Naval War College, 1993).
Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999).
Robert Jervis, *Perception and Misperception in International Politics* (Princeton: Princeton University Press, 1977).
Ephraim Kam, *Surprise Attack: The Victim's Perspective* (Cambridge, MA: Harvard University Press, 1988).
Geraldine Krotow, *The Impact of Cognitive Feedback on the Performance of Intelligence Analysts* (Monterey, CA: Naval Postgraduate School, 1992).
Mark Lowenthal, *Intelligence: From Secrets to Policy* (Washington, DC: CQ, 2000).
David Moore, Creating Intelligence: Evidence and Inference in the Analysis Process. Unpublished Masters Thesis (Washington DC: Joint Military Intelligence College, 2002).
J. R. Thompson, R. Hopf-Weichel, and R. Geiselman, *The Cognitive Bases of Intelligence Analysis* (Alexandria, VA: Army Research Institute, Research Report 1362, 1984).

Error

Daniela Busse and Chris Johnson "Using a Cognitive Theoretical Framework to Support Accident Analysis," in *Proceedings of the Working Group on Human Error, Safety, and System Development* (Seattle, WA: International Federation for Information Processing, 1998, 36–43).
Peter Fishburn, *Utility Theory for Decision Making* (New York: John Wiley, 1970).
Paul Fitts and Michael Posner, *Human Performance* (Belmont, CA: Brooks Cole, 1967).
John Hammond, Ralph Keeney, and Howard Raiffa, "The Hidden Traps in Decision Making," *Harvard Business Review*, Sept.– Oct. 1998: 47–58.

Hede Helfrich, "Human Reliability from a Social-Psychological Perspective," *International Journal Human-Computer Studies* 50 (1999): 193–212.
Erik Hollnagel, "The Phenotype of Erroneous Actions," *International Journal of Man-Machine Studies* 39 (1993): 1–32.
Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision Under Risk," *Econometrica* 47, no. 2 (1979): 263–91.
Duncan Luce and Howard Raiffa, "Utility Theory" in Paul Moser, ed. *Rationality in Action: Contemporary Approaches* (New York: Cambridge University Press, 1990).
Judith Orasanu and Lynne Martin, "Errors in Aviation Decision Making: A Factor in Accidents and Incidents" in *Proceedings of the Working Group on Human Error, Safety, and System Development* (Seattle, WA: International Federation for Information Processing, 1998, 100–107).
James Reason, *Human Error* (New York: Cambridge University Press, 1990).
John Senders and Neville Moray, *Human Error: Cause, Prediction and Reduction* (Hillsdale, NJ: Earlbaum, 1991).
Neville Stanton and Sarah Stevenage, "Learning to Predict Human Error: Issues of Acceptability, Reliability and Validity," *Ergonomics* 41, no. 11 (1998): 1737–56.

Language and Cognition

Terry K. Au, "Chinese and English Counterfactuals: The Sapir-Whorf Hypothesis Revisited," *Cognition* 15 (1983): 155-187.
Alfred Bloom, *The Linguistic Shaping of Thought: A Study in the Impact of Language on Thinking in China and the West* (Hillsdale, NJ: Lawrence Erlbaum Associates, 1981).
Lera Boroditsky, "Does Language Shape Thought? Mandarin and English Speakers' Conceptions of Time," *Cognitive Psychology* 43 (2001):1–22.
Ernest Cassirer, "Le Langage et le Monde des Objets," *Journal de Psychologie Nomale et Pathologique* 30, 1(4) (1933): 18–44.
John Gumperz and Dell Hymes, *Directions in Sociolinguistics: The Ethnography of Communication* (Oxford: B. Blackwell, 1986).
———, and Stephen Levinson, *Rethinking Linguistic Relativity* (Cambridge: Cambridge University Press, 1996).
Harry Hoijer, "The Relation of Language to Culture" in Alfred Kroeber, ed. *Anthropology Today* (Chicago: University of Chicago Press, 1953).
Wilhelm von Humboldt *"Uber die Verschiedenheit des Menschlichen Sprachbaues*" in B. Bohr, ed. *Gesammelte Schriften* (Berlin: Verlag, 1907).
Earl Hunt and Franca Agnoli, "The Whorfian Hypothesis. A Cognitive Psychology Perspective," *Psychological Review* 98, no. 3 (1991): 377–89.

Dell Hymes, ed. *Language in Culture and Society: A Reader in Linguistics and Anthropology* (New York: Harper and Row, 1977).
Penny Lee, *The Whorf Theory Complex: A Critical Reconstruction* (Amsterdam: Benjamins, 1996).
Lisa Liu, "Reasoning Counterfactually in Chinese: Are There any Obstacles?" *Cognition* 21 (1985): 239–70.
John Lucy, *Grammatical Categories and Cognition* (Cambridge: Cambridge University Press, 1992) and *Language Diversity and Thought* (Cambridge: Cambridge University Press, 1992).
George Miller and Philip Johnson-Laird, *Language and Perception* (Cambridge, MA: Harvard University Press, 1976).
Richard Nisbett and Ara Norenzayan, "Culture and Cognition" in Douglas Medin and Hal Pashler, eds. *Stevens' Handbook of Experimental Psychology*, 3rd ed. (New York: John Wiley & Sons, 2002).
Edward Sapir, *Language* (New York: Harcourt Brace, 1949).
Jost Trier, *Der deutsche Wortschatz im Sinnbezirk des Verstandes* (Heidelberg: Carl Winter, 1931).
Leo Weisgerber, *Vom Weltbild der Deutschen Sprache* (Dusseldorf: Padagogischer Verlag Schwann, 1953).
Benjamin Whorf, *Language, Thought, and Reality* (New York: John Wiley, 1956).

BIBLIOGRAPHY

Published Sources

Akin, Omer. *Models of Architectural Knowledge.* London: Pion, 1980.

Allen, Charles, *Comments of the Associate Director of Central Intelligence for Collection at a Public Seminar on Intelligence at Harvard University*, spring 2000. (<http://pirp.harvard.edu/pdf-blurb.asp? id+518>.)

Allison, Graham T. *Essence of Decision: Explaining the Cuban Missile Crisis.* Boston: Little, Brown and Company, 1971.

American Anthropological Association. *Code of Ethics of the American Anthropological Association.* Arlington, VA, 1998. (http://www.aaanet.org/committees/ethics/ethcode.htm.)

———. *Statement on the Confidentiality of Field Notes.* Arlington, VA, 2003. (http://www.aaanet.org/stmts/fieldnotes.htm.)

American College of Radiology. Written communications between staff and Johnston, 2002.

Arvey, Richard D., and James E. Campion. "The Employment Interview: A Summary of Recent Research," *Personnel Psychology* 35 (1982): 281–322.

Ashcraft, M.H. *Fundamentals of Cognition.* New York: Addison Wesley Longman, 1998.

Atkinson, R. C., and H. A. Wilson. *Computer-Assisted Instruction: A Book of Readings,* New York: Academic Press, 1969.

Au, Terry K. "Chinese and English Counterfactuals: The Sapir-Whorf Hypothesis Revisited," *Cognition* 15 (1983): 155–87.

Barr, A., M. Beard, and R. C. Atkinson. "A Rationale and Description of a CAI Program to Teach the BASIC Programming Language." *Instructional Science* 4 (1975): 1–31.

Bayes, Thomas. "An Essay Toward Solving a Problem in the Doctrine of Chances," *Philosophical Transactions of the Royal Society of London* 53: 370–418. (http://plato.stanford.edu/entries/bayes-theorum/#Bib.)

Ben-Israel, Isaac. "Philosophy and Methodology of Intelligence: The Logic of Estimate Process," *Intelligence and National Security* 4, no. 4 (1989): 660–718.

Ben-Zvi, Abraham. "The Study of Surprise Attacks," *British Journal of International Studies* 5 (1979).

Berkowitz, Bruce D., and Allan E. Goodman. *Best Truth: Intelligence in the Information Age*. New Haven, CT: Yale University Press, 2000.

———. *Strategic Intelligence for American National Security.* Princeton, NJ: Princeton University Press, 1989.

Bernard, Russell. *Research Methods in Anthropology: Qualitative and Quantitative Approaches*. Thousand Oaks, CA: Sage, 1994.

Betts, Richard K. "Policy-Makers and Intelligence Analysts: Love, Hate or Indifference," *Intelligence and National Security* 3, no. 1 (January 1988): 184–89.

———. *Surprise Attack*. Washington, DC: The Brookings Institution, 1982.

Bickman, Leonard, and Debra Rog. *Handbook of Applied Social Research Methods*. Thousand Oaks, CA: Sage, 1997.

Bloom, Alfred. *The Linguistic Shaping of Thought: A Study in the Impact of Language on Thinking in China and the West*. Hillsdale, NJ: Lawrence Erlbaum Associates, 1981.

Bloom, Benjamin S., ed. *Taxonomy of Educational Objectives: The Classification of Educational Goals: Handbook I, Cognitive Domain*. New York: Longmans, Green, 1956.

———. "The 2 Sigma Problem: The Search for Methods of Group Instruction as Effective as One-to-One Tutoring," *Educational Researcher*, 13 (1984): 4–16.

Boas, Franz. "An Anthropologist's Credo," *The Nation* 147 (1938): 201–4.

Bogdan, Robert. *Participant Observation in Organizational Settings*. Syracuse, NY: Syracuse University Press, 1972.

Boroditsky, Lera. "Does Language Shape Thought? Mandarin and English Speakers' Conceptions of Time," *Cognitive Psychology* 43 (2001): 1–22.

Bourdieu, Pierre. "The Forms of Capital" in John Richardson, ed. *Handbook of Theory and Research for the Sociology of Education*. New York: Greenwood Press, 1986.

Brei, William. *Getting Intelligence Right: The Power of Logical Procedure.* Washington, DC: Joint Military Intelligence College, 1996.

Brinberg, David, and Joseph McGrath. *Validity and the Research Process*. Beverly Hills, CA: Sage, 1985.

Brown, J.S., R.R. Burton, and J. DeKleer. "Pedagogical, Natural Language, and Knowledge Engineering in SOPHIE I, II, and III" in D. Sleeman and J.S. Brown, eds. *Intelligent Tutoring Systems*, New York: Academic Press, 1982.

Busse, Daniela, and Chris Johnson. "Using a Cognitive Theoretical Framework to Support Accident Analysis," *Proceedings of the Working Group on Human Error, Safety, and System Development*. Seattle, WA: International Federation for Information Processing, 1998, 36–43.

Butterfield, Alexander. *The Accuracy of Intelligence Assessment: Bias, Perception, and Judgment in Analysis and Decision*. Newport, RI: Naval War College, 1993, AD-A266.

Camerer, Colin, and Eric Johnson. "The Process-Performance Paradox in Expert Judgment: How Can Experts Know so Much and Predict so Badly?" in K. Anders Ericsson and Jacqui Smith, eds. *Toward a General Theory of Expertise: Prospects and Limit.* Cambridge: Cambridge University Press, 1991.

Cannon-Bowers, Janis, Eduardo Salas, and S. Converse. "Shared Mental Models in Expert Team Decision Making" in J. N. John Castellan, ed. *Current Issues in Individual and Group Decision Making*. Hillsdale, NY: Lawrence Erlbaum Associates, 1983.

Capra, Fritjof. "Criteria of Systems Thinking," *Futures,* October 1985: 475–78.

Carbonell, J. R. "AI in CAI: An Artificial Intelligence Approach to Computer-Assisted Instruction" in *IEEE Transactions on Man-Machine Systems*, 11 (1970): 190–202; J. D. Fletcher and M. R. Rockway loc. cit.

Carmines, Edward, and Richard Zeller. *Reliability and Validity Assessment*. Newbury Park, CA: Sage, 1991.

Cartwright, Dorwin, and Alvin Zander. *Group Dynamics: Research and Theory.* New York: Harper & Row, 1960.

Cascio, Wayne F. *Applied Psychology in Human Resource Management*. 5th ed. Englewood Cliffs, NJ: Prentice Hall, 1998.

Cassirer, Ernest. "Le Langage et le Monde des Objets," *Journal de Psychologie Nomale et Pathologique* 30, 1(4) (1933): 18–44.

Central Intelligence Agency. *A Consumer's Guide to Intelligence*. Washington, DC: Central Intelligence Agency, 1993.

———. *Factbook on Intelligence* (http://www.cia.gov/cia/publications/factfell/index.html.)

Chambers, Erve. *Applied Anthropology: A Practical Guide*. Prospect Heights, IL: Waveland Press, 1989.

Chase, William G. "Spatial Representations of Taxi Drivers" in Don Rogers and John Slobada, eds. *Acquisition of Symbolic Skills*. New York: Plenum, 1983.

———, and Herbert Simon. "Perception in Chess," *Cognitive Psychology* 4 (1973): 55–81.

———, and K. Anders Ericsson. "Skill and Working Memory" in Gordon Bower, ed. *The Psychology of Learning and Motivation.* New York: Academic Press, 1982.

Chi, Michelene, Robert Glaser, and Ernest Rees. "Expertise in Problem Solving" in Robert Sternberg, ed. *Advances in the Psychology of Human Intelligence*. Hillsdale, NJ: Lawrence Erlbaum Associates, 1982.

———, Paul Feltovich, and Robert Glaser. "Categorization and Representation of Physics Problems by Experts and Novices," *Cognitive Science* 5 (1981): 121–25.

Chu, Godwin, and Wilbur Schramm. *Learning from Television: What the Research Says.* Stanford, CA: Stanford University, Institute for Communication Research, 1968.

Clauser, Jerome K., and Sandra M. Weir. *Intelligence Research Methodology: An Introduction to Techniques and Procedures for Conducting Research in Defense Intelligence*. Washington, DC: US Defense Intelligence School, 1976.

Cline, Marjorie, Carla Christiansen, and Judith Fontaine. *Scholar's Guide to Intelligence Literature: Bibliography of the Russell J. Bowen Collection.* Frederick, MD: University Publications of America, 1983.

Coch, Lester, and John French. "Overcoming Resistance to Change," Dorwin Cartwright and Alvin Zander, eds. *Group Dynamics: Research and Theory.* New York: Harper & Row, 1960.

Cohen, Peter, James Kulik, and Chen-Lin Kulik. "Educational Outcomes of Tutoring: A Meta-Analysis of Findings," *American Educational Research Journal* 19 (1982): 237–48.

Cushman, Philip. *Constructing the Self, Constructing America*. Reading, MA: Addison-Wesley, 1995.

Davis, Jack. "Combating Mindset," *Studies in Intelligence* 35 (Winter 1991): 13–18.

Dawes, Robyn. Written communications between Dawes and Johnston, 2002.

———. "A Case Study of Graduate Admissions: Application of Three Principles of Human Decision Making," *American Psychologist* 26 (1971): 180–88.

———, David Faust, and Paul Meehl. "Clinical Versus Actuarial Judgment," *Science* 243 (1989): 1668–74.

Dearth, Douglas, and R. Thomas Goodden, eds. *Strategic Intelligence: Theory and Application*, 2nd ed. Washington, DC: Joint Military Intelligence College, 1995.

Denzin, Norman, and Yvonna Lincoln, eds. *Handbook of Qualitative Research*. Thousand Oaks, CA: Sage, 1994.

Deutsch, Morton. "The Effects of Cooperation and Competition Upon Group Process" in Dorwin Cartwright and Alvin Zander, eds. *Group Dynamics: Research and Theory.* New York: Harper & Row, 1960.

Duffy, T. M., and D. H. Jonassen, eds. *Constructivism and the Technology of Instruction: A Conversation*. Hillsdale, NJ: Erlbaum, 1992.

Eco, Umberto. *A Theory of Semiotics*. Bloomington, IN: Indiana University Press, 1979.

Egan, D., and B. Schwartz. "Chunking in Recall of Symbolic Drawings," *Memory and Cognition* 7 (1979): 149–58.

Elkins, Dan. *An Intelligence Resource Manager's Guide*. Washington, DC: Joint Military Intelligence College, 1997.

Endsley, M.R. "Design and Evaluation for Situation Awareness Enhancement," *Proceedings of Human Factors Society 32nd Annual Meeting*, Santa Monica, CA: Human Factors Society, 1988.

Ervin, Alexander. *Applied Anthropology. Tools and Perspectives for Contemporary Practice*. Boston: Allyn and Bacon, 2000.

Evans, Jonathan St. B. T. *Bias in Human Reasoning: Causes and Consequences*. Hove, UK: Lawrence Erlbaum Associates, 1989.

Fandt, Patricia, W. Richardson, and H. Conner. "The Impact of Goal Setting on Team Simulation Experience," *Simulation and Gaming* 21, no. 4 (1990): 411–22.

Feder, Stanley. "FACTIONS and Policon: New Ways to Analyze Politics," (1987), in H. Bradford Westerfield, ed. *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal*. New Haven, CT: Yale University Press, 1995.

Feldman, Daniel C. "The Multiple Socialization of Organization Members." *Academy of Management Review* 6, no. 2 (1981): 309–18.

Feldman, Tine, and Susan Assaf. *Social Capital: Conceptual Frameworks and Empirical Evidence. An Annotated Bibliography.* Social Capital Initiative Working Paper No. 5. Washington, DC: The World Bank, 1999.

Festinger, Leon. "Informal Social Communication" in Dorwin Cartwright and Alvin Zander, eds. *Group Dynamics: Research and Theory.* New York: Harper & Row, 1960.

Fishburn, Peter. *Utility Theory for Decision Making*. New York. John Wiley, 1970.

Fitts, Paul, and Michael Posner. *Human Performance*. Belmont, CA: Brooks Cole, 1967.

Flavell, J.H. "Metacognitive Aspects of Problem Solving" in L. Resnick, ed. *The Nature of Intelligence*. Hillsdale, NJ: Lawrence Erlbaum Associates, 1976.

Fleisher, Craig, and Babette Bensoussan. *Strategic and Competitive Analysis. Methods and Techniques for Analyzing Business Competition.* Upper Saddle River, NJ: Pearson Education, 2003.

Fleishman, Edwin, and Marilyn Quaintance. *Taxonomies of Human Performance*. New York: Academic Press, 1984.

Fletcher, J. Dexter. "Computer-Based Instruction: Costs and Effectiveness" in Andrew Sage, ed. *Concise Encyclopedia of Information Processing in Systems and Organizations*. Elmsford, NY: Pergamon Press, 1990.

———. *Effectiveness and Cost of Interactive Videodisc Instruction in Defense Training and Education*. Alexandria, VA: Institute for Defense Analyses, 1990, IDA P-2372.

———. "Evidence for Learning From Technology-Assisted Instruction" in Harold F. O'Neil, Jr. and Ray Perez, eds. *Technology Applications in Education: A Learning View.* Hillsdale, NJ: Lawrence Erlbaum Associates, 2003.

———. *Technology, the Columbus Effect, and the Third Revolution in Learning*. Alexandria, VA: Institute for Defense Analyses, 2001, D-2562.
———, and Rob Johnston. "Effectiveness and Cost Benefits of Computer-Based Decision Aids for Equipment Maintenance," *Computers in Human Behavior* 18 (2002): 717–28.
———, and M. R. Rockway. "Computer-based Training in the Military" in J. A. Ellis, ed. *Military Contributions to Instructional Technology.* New York: Praeger Publishers, 1986.
Folker, Robert D. *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods*. Washington, DC: Joint Military Intelligence College, Occasional Paper #7, 2000.
Ford, Harold. *Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating*. Lanham, MD: University Press of America, 1993.
Freud, Sigmund. "A Philosophy of Life: Lecture 35," *New Introductory Lectures on Psycho-Analysis*. London: Hogarth Press, 1933.
Fries, J., et al. "Assessment of Radiologic Progression in Rheumatoid Arthritis: A Randomized, Controlled Trial," *Arthritis Rheum* 29, no. 1 (1986): 1–9.
Fuld, Leonard. *The New Competitor Intelligence: The Complete Resource for Finding, Analyzing, and Using Information About Your Competitors*. New York: John Wiley & Sons, 1995.
Galanter, E., ed. *Automatic Teaching: The State of the Art.* New York: John Wiley & Sons, 1959.
Gall, Meredith, Walter Borg, and Joyce Gall. *Educational Research,* Sixth Edition. White Plains, NY: Longman, 1996.
Garst, Ronald, ed. *A Handbook of Intelligence Analysis*, 2nd ed. Washington, DC: Defense Intelligence College, 1989.
Geertz, Clifford. *The Interpretation of Cultures*. New York: Basic Books, 1973.
Giddens, Anthony. *Modernity and Self-Identity.* Stanford, CA: Stanford University Press, 1991.
Glaser, Barney, and Anselm Strauss. *Discovery of Grounded Theory: Strategies for Qualitative Research*. Hawthorne, NY: Aldine de Gruyter, 1967.
———. *Theoretical Sensitivity: Advances in the Methodology of Grounded Theory.* Mill Valley, CA: Sociology Press, 1978.
———. *Basics of Grounded Theory Analysis: Emergence vs. Forcing*. Mill Valley, CA: Sociology Press, 1992.
Glass, Gene. "Primary, Secondary, and Meta-Analysis of Research." *Educational Researcher* 5 (1976): 3–8.
———, and Barry McGaw. "Choice of the Metric for Effect Size in Meta-Analysis." *American Educational Research Journal* 17 (1980): 325–7.
———, Barry McGaw, and Mary Lee Smith. *Meta-Analysis in Social Research*. New York: Sage, 1981.

Godson, Roy, ed. *Comparing Foreign Intelligence: The U.S., the USSR, the U.K. and the Third World*. Washington, DC: Pergamon-Brassey, 1988.

Goldberg, Lewis. "Simple Models or Simple Processes? Some Research on Clinical Judgments," *American Psychologist* 23 (1968): 483–96.

———. "Man versus Model of Man: A Rationale, Plus Some Evidence, for a Method of Improving on Clinical Inferences," *Psychological Bulletin* 73 (1970): 422–32.

Goldgeier, James M. "Psychology and Security," *Security Studies* 6, no. 4 (1997): 137–66.

Gott, Sherrie, P.R.S. Kane, and Alan Lesgold. *Tutoring for Transfer of Technical Competence*. Brooks AFB, TX: Armstrong Laboratory, Human Resources Directorate, 1995, AL/HR-TP-1995-0002.

Graesser, A.C., M.A. Gernsbacher, and S. Goldman, eds. *Handbook of Discourse Processes*, Mahwah, NJ: Lawrence Erlbaum Associates, 2003.

———, and Natalie Person. "Question-Asking During Tutoring." *American Educational Research Journal* 31 (1994): 104–37.

Greenberg, Jerald, and Robert A. Baron. *Behavior in Organizations: The Human Side of Work*. Upper Saddle River, NJ: Prentice-Hall, 2002.

Grimes, Barbara, ed. *Ethnologue,* 14th ed. Dallas, TX: Summer Institute of Linguistics, 2000.

Gross, Jonathan. *Measuring Culture: A Paradigm for the Analysis of Social Organization*. New York: Columbia University Press, 1985.

Grove, William, and Paul Meehl. "Comparative Efficiency of Informal (Subjective, Impressionistic) and Formal (Mechanical, Algorithmic) Prediction Procedures: The Clinical-Statistical Controversy," *Psychology, Public Policy, and Law* 2, no. 2 (1996): 293–323.

Gumperz, John, and Dell Hymes. *Directions in Sociolinguistics: The Ethnography of Communication*. Oxford: B. Blackwell, 1986.

———, and Stephen Levinson. *Rethinking Linguistic Relativity.* Cambridge: Cambridge University Press, 1996.

Hacker, D.J. *Metacognition: Definitions and Empirical Foundations* [On-line report]. Memphis, TN: The University of Memphis, 2001. Retrieved 30 May 2001 from the World Wide Web. (http://www.psyc.memphis.edu/trg/meta.htm.)

Hammond, John, Ralph Keeney, and Howard Raiffa. "The Hidden Traps in Decision Making." *Harvard Business Review*, September–October 1998, 47–58.

Harvey, J., and C. Boettger. "Improving Communication Within a Managerial Workgroup," *Journal of Applied Behavioral Science* 7 (1971): 164–74.

Hayes, J.R. *The Complete Problem Solver*, Philadelphia: The Franklin Institute, 1981.

Hays, R. T., et al. "Flight Simulator Training Effectiveness: A Meta-Analysis." *Military Psychology* 4, no. 2 (1992): 63–74.

Hedges, Larry. "Estimation of Effect Size From a Series of Independent Experiments," *Psychological Bulletin*, 7 (1982): 119–37.

———, and Ingram Olkin. "Vote-Counting Methods in Research Synthesis," *Psychological Bulletin* 88 (1980): 359–69.

———, and Ingram Olkin. *Statistical Methods for Meta-Analysis*. New York: Academic Press, 1985.

Helfrich, Hede. "Human Reliability From a Social-Psychological Perspective," *International Journal Human-Computer Studies* 50 (1999): 193–212.

Hesketh, Beryl, and Stephen Bochner. "Technological Change in a Multicultural Context: Implications for Training and Career Planning" in Marvin Dunnette and Leaetta Hough, eds. *Handbook of Industrial and Organizational Psychology.* Palo Alto, CA: Consulting Psychologists Press, 1994.

Heuer, Richards J., Jr. *Psychology of Intelligence Analysis.* Washington, DC: Center for the Study of Intelligence, 1999.

Hewitt, John P. *Self and Society,* 7th ed. Boston: Allyn and Bacon, 1997.

Hinchman, Lewis P., and Sandra K. Hinchman, eds. *Memory, Identity, Community.* Albany, NY: State University of New York Press, 1997.

Hoijer, Harry. "The Relation of Language to Culture" in Alfred Kroeber, ed. *Anthropology Today.* Chicago: University of Chicago Press, 1953.

Hollnagel, Erik. "The Phenotype of Erroneous Actions." *International Journal of Man-Machine Studies* 39 (1993): 1–32.

Hopkins, R. *Warnings of Revolution: A Case Study of El Salvador.* Washington, DC: Center for the Study of Intelligence, 1980, TR 80-100012.

House, Ernest. *Evaluating with Validity.* Beverly Hills, CA: Sage, 1980.

Hubble, Edwin. *The Realm of the Nebulae*. New Haven, CT: Yale University Press, 1936.

Hulnick, Arthur S. "The Intelligence Producer-Policy Consumer Linkage: A Theoretical Approach," *Intelligence and National Security* 1, no. 2 (May 1986): 212–33.

Hunt, David. *Complexity and Planning in the 21st Century: Intelligence Requirements to Unlock the Mystery.* Newport, RI: Naval War College, 2000.

Hunt, Earl, and Franca Agnoli. "The Whorfian Hypothesis. A Cognitive Psychology Perspective," *Psychological Review* 98, no. 3 (1991): 377–89.

Hymes, Dell, ed. *Language in Culture and Society: A Reader in Linguistics and Anthropology.* New York: Harper and Row, 1977.

Iaffaldano, Michelle T., and Paul M. Muchinsky. "Job satisfaction and Job Performance: A Meta-Analysis," *Psychological Bulletin* 97 (1985): 251–73.

James, William. *Principles of Psychology: Volume I*. New York: Dover Press, 1890/1950.

Janis, Irving. *Groupthink*, 2nd ed. Boston: Houghton Mifflin, 1982.

Janssens, Maddy. "Interculture Interaction: A Burden on International Managers?" *Journal of Organizational Behavior* 16 (1995): 155–67.

Jervis, Robert. *Perception and Misperception in International Politics*. Princeton, NJ: Princeton University Press, 1977.

Johnson, David, and Roger Johnson. "The Internal Dynamics of Cooperative Learning Groups" in Richard Slavin, et al., eds. *Learning to Cooperate, Cooperating to Learn*. New York: Plenum, 1985.

———, et al. "Effects of Cooperative, Competitive, and Individualistic Goal Structure on Achievement: A Meta-Analysis," *Psychological Bulletin* 89, no. 1 (1981): 47–62.

———, et al. "The Impact of Positive Goal and Resource Interdependence on Achievement, Interaction, and Attitudes," *Journal of General Psychology* 118, no. 4 (1996): 341–47.

Johnson, Edgar. *Effects of Data Source Reliability on Inference*. Alexandria, VA: Army Research Institute for the Behavioral and Social Sciences, Technical Paper #251, 1974.

Johnston, Rob. *Decision Making and Performance Error in Teams: Research Results*. Arlington, VA: Defense Advanced Research Projects Agency, 1997.

———. "The Effectiveness of Instructional Technology," *Proceedings of the Virtual Reality in Medicine and Developers' Exposition*. Cambridge, MA: VRS, 1995.

———. "Electronic Performance Support Systems and Information Navigation," *Thread* 2, no. 2 (1994): 5–7.

———, and Sunil Bhoyrul. "A Preliminary Report of a Task Analysis of Laparoscopic Cholecystectomy Used to Assess the Effectiveness of a Virtual Reality Surgical Simulator," *Journal of Virtual Reality in Medicine* 2, no. 1 (1996): 16–19.

———, et al. "Assessing a Virtual Reality Surgical Skills Simulator" in Suzanne Weghorst, Hans Sieburg, and Karen Morgan, eds. *Health Care in the Information Age: Future Tools for Transforming Medicine*. Washington, DC: IOS Press, 1996.

———, and J. Dexter Fletcher. *A Meta-Analysis of the Effectiveness of Computer-Based Training for Military Instruction*. Alexandria, VA: Institute for Defense Analyses, 1998.

———, J. Dexter Fletcher, and Sunil Bhoyrul. *The Use of Virtual Reality to Measure Surgical Skill Levels*. Alexandria, VA: Institute for Defense Analyses, 1998.

Jones, Morgan. *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*. New York: Times Business, 1998.

Jung, Carl. *The Undiscovered Self*. Translated by R.F.C. Hull. Princeton, NJ: Princeton University Press, 1990.

Kahaner, Larry. *Competitive Intelligence. How to Gather, Analyze, and Use Information to Move Your Business to the Top*. New York: Touchstone, Simon and Schuster, 1996.

Kahneman, Daniel, and Amos Tversky. "Prospect Theory: An Analysis of Decision Under Risk," *Econometrica* 47, no. 2 (1979): 263–91.

———, Paul Slovic, and Amos Tversky. *Judgment Under Uncertainty: Heuristics and Biases*. Cambridge: Cambridge University Press, 1982.

Kam, Ephraim. *Surprise Attack. The Victim's Perspective*. Cambridge: Harvard University Press, 1988.

Kaufman, David L., Jr. *Introduction to Systems Thinking*. Minneapolis: Future Systems, 1978.

Kaufman, Roger. "A Holistic Planning Model: A Systems Approach for Improving Organizational Effectiveness and Impact," *Performance and Instruction Journal*, October 1983: 3–10.

Kent, Sherman. *Strategic Intelligence for American World Policy.* Princeton: Princeton University Press, 1966.

———. "Words of Estimative Probability," *Sherman Kent and the Board of National Estimates: Collected Essays*. Washington, DC: Center for the Study of Intelligence, 1994.

Kirk, Jerome, and Marc Miller. *Reliability and Validity in Qualitative Research. Qualitative Research Methods, Volume 1*. Newbury Park, CA: Sage, 1986.

Kirkpatrick, Lyman B., Jr. *Captains Without Eyes: Intelligence Failures in World War II*. London: MacMillan Company, 1969.

Klahr, D., and H.A. Simon. "What Have Psychologists (and Others) Discovered About the Process of Scientific Discovery?" *Current Directions in Psychological Science* 10.

Klein, Gary, Roberta Calderwood, and A. Clinton-Cirocco. *Rapid Decision Making on the Fire Ground.* Yellow Springs, OH: Klein Associates, 1985, KA-TR-84-41-7 (prepared under contract MDA903-85-G-0099 for the US Army Research Institute, Alexandria, VA).

Knight, Frank H. *Risk, Uncertainty and Profit.* Boston: Houghton Mifflin, 1921.

Knorr, Klaus. "Foreign Intelligence and the Social Sciences." (Research monograph, Center of International Studies, Princeton University, 1964.)

Krizan, Lisa. *Intelligence Essentials for Everyone*. Washington, DC: Joint Military Intelligence College, 1999.

Krotow, Geraldine. *The Impact of Cognitive Feedback on the Performance of Intelligence Analysts*. Monterey, CA: Naval Postgraduate School, 1992, AD-A252.

Kuhn, Thomas. *The Structure of Scientific Revolutions*. Chicago: The University of Chicago Press, 1970.

Kulik, Chen-Lin, and James Kulik. "Effectiveness of Computer-Based Education in Colleges," *AEDS Journal*, Winter/Spring 1986: 81–108.

———, and Barbara Shwalb, "Effectiveness of Computer-Based Adult Education: A Meta-Analysis," *Journal of Educational Computing Research* 2, no. 2 (1986): 235–52.

Kulik, James. "Meta-Analytic Studies of Findings on Computer-Based Instruction" in Eva Baker and Harold O'Neil, eds. *Technology Assessment in Education and Training*. Hillsdale, NJ: LEA Publishers, 1994.

Lacan, Jacques. *Ecrits.* Translated by Alan Sheridan. New York: W.W. Norton, 1977.

Laqueur, Walter A. *The Uses and Limits of Intelligence*. New Brunswick, NJ: Transaction Publishers, 1993.

Larkin, Jill. "The Role of Problem Representation in Physics" in Debra Gentner and Albert Stevens, eds. *Mental Models*. Hillsdale, NJ: Lawrence Erlbaum Associates, 1983.

Lee, Penny. *The Whorf Theory Complex: A Critical Reconstruction*. Amsterdam: Benjamins, 1996.

Leli, D., and S. Filskov. "Clinical-Actuarial Detection of and Description of Brain Impairment with the Wechsler-Bellevue Form I," *Journal of Clinical Psychology* 37 (1981): 623–29.

Lesgold, Alan, et al. "Expertise in a Complex Skill: Diagnosing X-Ray Pictures" in Michelene Chi, Robert Glaser and Marshall Farr, eds. *The Nature of Expertise*. Hillsdale, NJ: Lawrence Erlbaum Associates, 1988.

Levi-Strauss, Claude. *Structural Anthropology.* New York: The Penguin Press, 1968. (Originally published in 1958.)

Levine, George, ed. *Constructions of the Self.* Brunswick, NJ: Rutgers University Press, 1992.

Levinson, David, and Melvin Ember, eds. *American Immigrant Cultures: Builders of a Nation. Vol. I and II*. New York: Macmillan Reference, 1997.

Litwin, Mark. "How to Measure Survey Reliability and Validity" in Arlene Fink, ed. *The Survey Kit. Volume 7*. Thousand Oaks, CA: Sage, 1995.

Liu, Lisa. "Reasoning Counterfactually in Chinese: Are There Any Obstacles?" *Cognition* 21 (1985): 239–70.

Locke, Edwin A. "The Nature and Causes of Job Satisfaction" in Marvin Dunnette, ed. *Handbook of Industrial and Organizational Psychology.* Chicago: Rand McNally, 1976.

Lockwood, Jonathan, and K. Lockwood. "The Lockwood Analytical Method for Prediction (LAMP)," *Defense Intelligence Journal* 3, no. 2 (1994): 47–74.

Lowenthal, Mark. *Intelligence: From Secrets to Policy.* Washington, DC: CQ, 2000.

Luce, Duncan, and Howard Raiffa. "Utility Theory." Paul Moser, ed. *Rationality in Action. Contemporary Approaches*. New York. Cambridge University Press, 1990.

Lucy, John. *Grammatical Categories and Cognition*. Cambridge: Cambridge University Press, 1992.

———. *Language Diversity and Thought*. Cambridge: Cambridge University Press, 1992.

MacEachin, Douglas J., et al. *The Tradecraft of Analysis: Challenge and Change in the CIA*. Washington, DC: Consortium for the Study of Intelligence, 1994.

Marrin, Stephen. *CIA's Kent School. A Step in the Right Direction*. Paper presented at the International Studies Association Annual Convention, New Orleans, LA, 2002. (http://www.isanet.org/noarchive/marrin.html.)

———. "Improving CIA Analysis by Overcoming Institutional Obstacles" in Russell G. Swenson, ed. *Bringing Intelligence About: Practitioners Reflect on Best Practices.* Washington, DC: Joint Military Intelligence College, 2003.

Mathams, Robert. "The Intelligence Analyst's Notebook" in Douglas Dearth and R. Thomas Goodden, eds. *Strategic Intelligence: Theory and Application*, 2nd ed. Washington, DC: Joint Military Intelligence College, 1995.

Mauss, Marcel. *The Gift: The Form and Reason for Exchange in Archaic Societies*. Translated by W. D. Halls. New York: W. W. Norton, 2000.

Mayo, Elton. *The Human Problems of an Industrial Civilization*. New York: MacMillan, 1933.

McDowell, Don. *Strategic Intelligence: A Handbook for Practitioners, Managers and Users*. Canberra, Australia: Istana Enterprises, 1998.

McEvoy, Glenn M., and Wayne F. Cascio. "Strategies for Reducing Employee Turnover: A Meta-Analysis," *Journal of Applied Psychology* 70, no. 2 (1985): 342–53.

McGuire, Hunter, et al. "Measuring and Managing Quality of Surgery: Statistical vs. Incidental Approaches," *Archives of Surgery* 127 (1992): 733–37.

McKeithen, Katherine, et al. "Knowledge Organization and Skill Differences in Computer Programmers," *Cognitive Psychology* 13 (1981): 307–25.

Mead, George. *Mind, Self, and Society.* Charles Morris, ed. Chicago: University of Chicago Press, 1967.

Meglino, Bruce M., et al. "Effects of Realistic Job Previews: A Comparison Using an Enhancement and a Reduction Preview." *Journal of Applied Psychology* 71 (1988): 259–66.

Meister, David. *Behavioral Analysis and Measurement Methods*. New York: Wiley, 1985.

———. *Human Factors: Theory and Practice*. New York: Wiley, 1971.

Meister, Judith. "Individual Perceptions of Team Learning Experiences Using Video-Based or Virtual Reality Environments," *Dissertation Abstracts International*, UMI No. 9965200, 2000.

Miller, Delbert. *Handbook of Research Design and Social Measurement*. Newbury Park, CA: Sage, 1991.

Miller, George, and Philip Johnson-Laird. *Language and Perception*. Cambridge: Harvard University Press, 1976.

Mills, Theodore. "Power Relations in Three-Person Groups" in Dorwin Cartwright and Alvin Zander, *Group Dynamics: Research and Theory.* New York: Harper & Row, 1960.

Min Qi, *Zhongguo Zhengzhi Wenhua* [Chinese Political Culture]. Kunming, China: Yunnan People's Press, 1989.

Minsky, Marvin, and Seymour Papert. *Artificial Intelligence.* Eugene: Oregon State System of Higher Education, 1974.

Molm, Linda. "Linking Power Structure and Power Use" in Karen Cook, ed. *Social Exchange Theory.* Newbury Park, CA: Sage, 1987.

Moore, David. "Creating Intelligence: Evidence and Inference in the Analysis Process." Unpublished Masters Thesis. Washington, DC: Joint Military Intelligence College, 2002.

Morris, C.D., J.D. Bransford, and J.J. Franks. "Level of Processing Versus Transfer-Appropriate Processing," *Journal of Verbal Learning and Verbal Behavior* 16 (1977).

Morrison, J.E., and J.D. Fletcher. *Cognitive Readiness*. Alexandria, VA: Institute for Defense Analyses, 2001, IDA Paper P-3735.

———, and Larry Meliza. *Foundations of the After-Action Review Process*. Alexandria, VA: Institute for Defense Analyses, 1999.

Mullen, Brian, and Carolyn Copper. "The Relation Between Group Cohesiveness and Performance: An Integration," *Psychological Bulletin*, 115 (1994): 210–27.

National Aeronautics and Space Administration. *Astronaut Fact Book*. NP-2000-09-008JSC. Washington, DC: NASA, 2000.

Neisser, U. *Cognitive Psychology.* New York: Appleton, Century Crofts, 1967.

Nieva, V., E. Fleishman, and A. Rieck. *Team Dimensions: Their Identity, Their Measurement, and Their Relationships,* RN 85-12. Alexandria, VA: US Army Research Institute for the Behavioral and Social Sciences, 1985.

Nijhof, W., and P. Kommers. "An Analysis of Cooperation in Relation to Cognitive Controversy" in Richard Slavin, Shlomo Sharan, Spencer Kagan, et al., eds. *Learning to Cooperate, Cooperating to Learn*. New York: Plenum, 1985.

Nisbett, Richard, and Ara Norenzayan. "Culture and Cognition" in Douglas Medin and Hal Pashler, eds. *Stevens' Handbook of Experimental Psychology*, 3rd ed., New York: John Wiley & Sons, 2002.

Nolte, William. "Preserving Central Intelligence: Assessment and Evaluation in Support of the DCI, " *Studies in Intelligence* 48, no. 3 (2005): 21–25.

Orasanu, Judith. "Shared Mental Models and Crew Performance." Paper presented at the 34th annual meeting of the *Human Factors Society*, Orlando, FL, 1990.

———, and Lynne Martin. "Errors in Aviation Decision Making: A Factor in Accidents and Incidents," *Proceedings of the Working Group on Human Error, Safety, and System Development*. Seattle, WA: International Federation for Information Processing, 1998: 100–107.

Orlansky, Jesse, and Joseph String. *Cost-Effectiveness of Computer-Based Instruction in Military Training.* Alexandria, VA: Institute for Defense Analyses, 1979. IDA P-1375.

———, et al. *The Cost and Effectiveness of the Multi-Service Distributed Training Testbed (MDT2) for Training Close Air Support.* Alexandria, VA: Institute for Defense Analyses, 1997.

———. *The Value of Simulation for Training*. Alexandria, VA: Institute for Defense Analyses, 1994. IDA P-2982.

Paige, Jeffery, and Herbert Simon. "Cognition Processes in Solving Algebra Word Problems" in Benjamin Kleinmuntz, ed. *Problem Solving*. New York: Wiley, 1966.

Patton, Michael. *Qualitative Evaluation and Research Methods,* 2nd ed. Beverly Hills, CA: Sage, 1990.

Perrow, Charles. *Normal Accidents: Living with High Risk Technologies*. Princeton, NJ: Princeton University Press, 1999.

———. Written communications between Perrow and Johnston, 2002.

Peterson, Marilyn. *Applications in Criminal Analysis.* Westport, CT: Greenwood Press, 1995.

———, Bob Morehouse, and Richard Wright, eds. *Intelligence 2000: Revising the Basic Elements.* Sacramento, CA: LEIU and IALEIA, 2000.

Phelps, Ruth, et al. "Effectiveness and Costs of Distance Education Using Computer-Mediated Communication," *American Journal of Distance Education* 5, no. 3 (1991): 7–19.

Pierce, John. "Some Mathematical Methods for Intelligence Analysis," *Studies in Intelligence* 21 (Summer 1977) (declassified): 1–19.

Popper, Karl. *The Logic of Scientific Discovery.* London: Hutchinson, 1959.

———. *Conjectures and Refutations: The Growth of Scientific Knowledge.* New York: Routledge, 2002 reprint.

Porter, Lyman W., Edward E. Lawler, and J. Richard Hackman. *Behavior in Organizations.* New York: McGraw-Hill, 1975.

———, et al. "Organizational Commitment, Job Satisfaction and Turnover Among Psychiatric Technicians," *Journal of Applied Psychology* 59 (1974): 603-609.

Prescott, John, and Stephen Miller, eds. *Proven Strategies in Competitive Intelligence.* New York: John Wiley & Sons, 2001.

Price-Williams, Douglass. *Explorations in Cross-Cultural Psychology.* San Francisco: Chandler and Sharp, 1975.

Putnam, Robert. *Bowling Alone: The Collapse and Revival of American Community.* New York: Simon and Schuster, 2000.

———. "The Prosperous Community: Social Capital and Public Life," *The American Prospect 4, no.* 13 (1993): 35–42.

Quirk, John, et al. *The Central Intelligence Agency: A Photographic History.* Guilford, CT: Foreign Intelligence Press, 1986.

Reason, James. *Human Error.* New York: Cambridge University Press, 1990.

Reichenbach, Hans. *Experience and Prediction.* Chicago: University of Chicago Press, 1938.

Richelson, Jeffrey. *The U.S. Intelligence Community*, 4th ed. Boulder, CO: Westview Press, 1999.

Roethlisberger, Fritz J., and William J. Dickson. *Management and the Worker: An Account of a Research Program Conducted by the Western Electric Company, Hawthorne Works, Chicago.* Boston: Harvard University Press, 1939.

Rosenberg, Marc J. "Performance Technology: Working the System," *Training,* January 1990: 5–10.

Rossi, Peter, and Howard Freeman. *Evaluation. A Systematic Approach,* 5th ed. Newbury Park, CA: Sage, 1993.

Roth, P. L. ,and James E. Campion. "An Analysis of the Predictive Power of the Panel Interview and Pre-Employment Tests," *Journal of Occupational and Organizational Psychology* 65 (1992): 51-60.

Sacks, H. "Promises, Performance, and Principles: An Empirical Study of Parole Decision-Making in Connecticut," *Connecticut Law Review* 9 (1977): 349–422.

Salomon, G., and D.N. Perkins. "Rocky Roads to Transfer: Rethinking Mechanisms of a Neglected Phenomenon," *Educational Psychologist* 24 (1998).

Sapir, Edward. *Language*. New York: Harcourt Brace, 1949.

Sapp, Edwin. "Decision Trees," *Studies in Intelligence* 18 (Winter 1974) (declassified): 45–57.

Sarbin, Theodore. "A Contribution to the Study of Actuarial and Individual Methods of Prediction," *American Journal of Sociology* 48 (1943): 593–602.

Saussure, Ferdinand. *Course in General Linguistics.* Translated by W. Baskin. New York: McGraw-Hill, 1959.

Sawyer, J. "Measurement and Prediction, Clinical and Statistical," *Psychological Bulletin* 66 (1966): 178–200.

Schensul, Jean, and Margaret LeCompte, eds. *Ethnographer's Toolkit*. *Vol. I–Vol. VII.* Walnut Creek, CA: Alta Mira Press, 1999.

Schofield, W., and J. Garrard. "Longitudinal Study of Medical Students Selected for Admission to Medical School by Actuarial and Committee Methods," *British Journal of Medical Education* 9 (1975): 86–90.

Schum, David. *The Evidential Foundations of Probabilistic Reasoning.* Evanston, IL: Northwestern University Press, 1994.

Scriven, M. "Problems and Prospects for Individualization" in H. Talmage, ed. *Systems of Individualized Education*. Berkley, CA: McCutchan, 1975.

Seashore, S. *Group Cohesiveness in the Industrial Workgroup*. Ann Arbor: University of Michigan Press, 1954.

Segall, Marshall. *Cross-Cultural Psychology: Human Behavior in Global Perspective.* Monterey, CA: Brooks/Cole, 1979.

Senders, John, and Neville Moray. *Human Error: Cause, Prediction and Reduction.* Hillsdale, NJ: Lawrence Earlbaum Associates, 1991.

Shiels, Frederick L. *Preventable Disasters: Why Governments Fail.* Savage, MD: Rowman and Littlefield Publishers, 1991.

Shiffrin, R.M. and W. Schneider. "Controlled and Automatic Human Information Processing: II. Perceptual Learning," *Psychological Review* 84 (1977).

Shlaim, Avi. "Failures in National Intelligence Estimates: The Case of the Yom Kippur War," *World Politics* 28, no. 3 (1976): 348–80.

Shweder, Richard. *Thinking Through Cultures.* Cambridge, MA: Harvard University Press, 1991.

Simmel, Georg. *The Sociology of Georg Simmel.* Translated by K. Wolff. Glencoe, IL: Free Press, 1950.

Simon, D., and Herbert Simon. "Individual Differences in Solving Physics Problems" in Robert Siegler, ed. *Children's Thinking: What Develops?* Hillsdale, NJ: Lawrence Erlbaum Associates, 1978.

Slavin, Robert. "Research on Cooperative Learning: Consensus and Controversy," *Educational Leadership* 47, no. 4 (1989): 52–55.

———. *Cooperative Learning*. New York: Longman, 1983.

Slovic, P., S. Lichtenstein, and B. Fischoff. "Decision-Making" in R.C. Atkinson et al. eds. *Steven's Handbook of Experimental Psychology (2nd ed.), Volume 2: Learning and Cognition*, New York: John Wiley & Sons, 1988.

Solomon, H. *Economic Issues in Cost-Effectiveness Analyses of Military Skill Training.* Alexandria, VA: Institute for Defense Analyses, 1986, IDA P-1897.

Spencer, Herbert. *The Study of Sociology.* New York: D. Appleton. 1874.

Spencer, Ken. "Modes, Media and Methods: The Search for Educational Effectiveness," *British Journal of Educational Technology* 22, no. 1 (1991): 12–22.

Spradley, James. *Participant Observation.* New York: Rinehart and Winston, 1980.

Stanton, Neville, and Sarah Stevenage. "Learning to Predict Human Error: Issues of Acceptability, Reliability and Validity," *Ergonomics*, 41, no. 11 (1998): 1737–56.

Stephenson, William. *The Study of Behavior: Q-Technique and its Methodology.* Chicago: University of Chicago Press, 1953.

Suppes, P., and M. Morningstar. *Computer-Assisted Instruction at Stanford, 1966-68: Data, Models, and Evaluation of the Arithmetic Programs.* New York: Academic Press, 1972.

Thompson, J. R., R. Hopf-Weichel, and R. Geiselman. *The Cognitive Bases of Intelligence Analysis*. Alexandria, VA: Army Research Institute, Research Report 1362, 1984, AD-A146.

Tierney, William G., and Robert A. Rhoads. *Faculty Socialization as Cultural Process: A Mirror of Institutional Commitment*. Washington, DC: ASHE-ERIC Higher Education Report No. 6, 1993.

Tobias, Sigmund. "When Do Instructional Methods Make a Difference?" *Educational Researcher* 11, no. 4 (1982): 4–9.

———, and L. T. Frase. "Educational Psychology and Training" in S. Tobias and J. D. Fletcher, eds. *Training and Retraining: A Handbook for Business, Industry, Government, and the Military.* New York: Macmillan Library Reference, 2001.

Treverton, Gregory F. *Reshaping National Intelligence in an Age of Information.* Cambridge: Cambridge University Press, 2001.

Trier, Jost. *Der deutsche Wortschatz im Sinnbezirk des Verstandes.* Heidelberg: Carl Winter, 1931.

Trochim, William. *The Research Methods Knowledge Base.* Cincinnati, OH: Atomic Dog, 2001.

Tulving, E., and D.M. Thomson. "Encoding Specificity and Retrieval Processes in Episodic Memory," *Psychological Review* 80 (1973).

Tversky, Amos, and Daniel Kahneman. "The Belief in the 'Law of Small Numbers,'" *Psychological Bulletin* 76 (1971): 105–10.

———. "Judgment Under Uncertainty: Heuristics and Biases," *Science* 185 (1974): 1124–31.

US Joint Forces Command. *Department of Defense Dictionary of Military and Associated Terms*. USJFCOM Joint Publication 1-02. Amended through June 5, 2003. (http://www.dtic.mil/doctrine/jel/doddict/index.html.)

von Humboldt, Wilhelm. "Uber die Verschiedenheit des Menschlichen Sprachbaues" in B. Bohr, ed. *Gesammelte Schriften*. Berlin: Verlag, 1907.

Voss, James, and Timothy Post. "On the Solving of Ill-Structured Problems" in Michelene Chi, Robert Glaser and Marshall Farr, eds. *The Nature of Expertise.* Hillsdale, NJ: Lawrence Erlbaum Associates, 1988.

Vygotsky, Lev. *Mind and Society*, Cambridge: Harvard University Press, 1930.

Wanous, John P. *Organizational Entry: Recruitment, Selection, Orientation, and Socialization.* Reading, MA: Addison-Wesley, 1992.

———, et al. "The Effects of Met Expectations on Newcomer Attitudes and Behavior: A Review and Meta-Analysis," *Journal of Applied Psychology* 77 (1992): 288–97.

Warner, Michael. "Wanted: A Definition of 'Intelligence,'" *Studies in Intelligence* 46, no. 3 (2002):15–22.

Weiser, M., and J. Shertz. "Programming Problem Representation in Novice and Expert Programmers," *Instructional Journal of Man-Machine Studies* 14 (1983): 391-96.

Weisgerber, Leo. *Vom Weltbild der Deutschen Sprache.* Dusseldorf: Padagogischer Verlag Schwann, 1953.

White, Robert. *Task Analysis Methods: Review and Development of Techniques for Analyzing Mental Workload in Multiple Task Situations*. St. Louis, MO: McDonnell Douglas Corporation, 1971, MDC J5291.

Whorf, Benjamin. *Language, Thought, and Reality.* New York: John Wiley, 1956.

Wirtz, James J. *The Tet Offensive: Intelligence Failure in War.* Ithaca, NY: Cornell University Press, 1991.

Wisher, R.A., M.A. Sabol, and J.A. Ellis. *Staying Sharp: Retention of Military Knowledge and Skills*. Alexandria, VA: US Army Research Institute for the Behavioral and Social Sciences, 1999, ARI Special Report 39. (<http://www.ari.army.mil>.)

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision.* Stanford, CA: Stanford University Press, 1962.

Wolf, Eric. *Pathways of Power. Building an Anthropology of the Modern World.* Berkeley: University of California Press, 2001.

Yin, Robert. *Case Study Research: Design and Methods* 2nd ed. Thousand Oaks, CA: Sage, 1994.

Ziemke, Caroline, Philippe Loustaunau, and Amy Alrich. *Strategic Personality and the Effectiveness of Nuclear Deterrence.* Washington, DC: Institute for Defense Analyses, 2000, D-2537.

Zlotnick, Jack. "Bayes' Theorem for Intelligence Analysis" (1972) in H. Bradford Westerfield, ed. *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal.* New Haven, CT: Yale University Press, 1995.

Zou, Yali, and Enrique Trueba. *Ethnic Identity and Power.* Albany: State University of New York, 1998.

Web resources

Buros Institute of Mental Measurements (http://www.unl.edu/buros/).
Central Intelligence Agency main website (http://www.cia.gov).
Central Intelligence Agency Office of General Council (http://www.cia.gov/ogc/best.htm).
Central Intelligence Agency Officer in Residence Program (http://www.cia.gov//csi/officer.html).
Defense Intelligence Agency (http://www.dia.mil).
Federal Bureau of Investigation (http://www.fbijobs.com or http://www.fbi.gov).
Human Relations Area Files. Yale University. (http://www.yale.edu/hraf/).
National Aeronautics and Space Administration-Johnson Space Center career astronaut biography. (http://www.jsc.nasa.gov/Bios/astrobio_activemgmt.html).
National Imagery and Mapping Agency (http://www.nima.mil/).
National Reconnaissance Office (http://www.nro.gov/).
National Security Agency (http://www.nsa.gov/).
US Air Force (http://aia.lackland.af.mil/aia/).
US Army (http://usaic.hua.army.mil/index.htm).
U.S. Army Center for Army Lessons Learned (http://call.army.mil/).
US Coast Guard (http://www.uscg.mil/USCG.shtm).
US Department of Energy (http://www.energy.gov/engine/content.do).
US Department of Homeland Security (http://www.dhs.gov/dhspublic/).
US Department of State (http://www.state.gov/s/inr/).
US Department of the Treasury (http://www.treasury.gov/).
US Intelligence Community (http://www.intelligence.gov/index.shtml).
US Marine Corps (http://www.usmc.mil/).
US Navy (http://www.nmic.navy.mil/).

AFTERWORD

Joseph Hayes[1]

The unexamined life is not worth living

Socrates.

A very popular error: having the courage of one's convictions; rather, it is a matter of having the courage for an attack on one's convictions!

Nietzsche

Rob Johnston has written a superb book, a study of intelligence as it is actually practiced. Rob's book is alive with specific, practical recommendations about how the practice of intelligence could be made better. The literature of intelligence is overwhelmingly devoted either to studies which, however rigorous in their academic structure, fail to convey the humanness of the enterprise or to books and articles, too often self congratulatory or self promoting, which are little more than assemblages of entertaining anecdotes. Rob's study deserves a place of honor on the very small bookshelf reserved for analytically sound, deeply insightful works on the conduct of intelligence. Any serious discussion of reform or significant change in the ways in which US intelligence is organized, structured, and carried out will need to take this book as a starting point.

Rob's work bears witness to the imagination and commitment to excellence on the part of the senior intelligence officials who made it possible for a cultural anthropologist to carry out his field work in the secret, sometimes hermetically

[1] Joseph Hayes is a retired senior officer of the Central Intelligence Agency Directorate of Operations. He served more than 30 years in the clandestine service.

sealed, world of intelligence. Rob's work also bears witness to the tremendous passion among intelligence professionals to understand better what they do, why they do it, and how their work could be improved. There is, in this community, a palpable desire to do better.

Since the tragedy of 9/11 and the bitter controversies surrounding Iraqi WMD, the world of intelligence analysis has been scrutinized with an intensity of almost unprecedented dimensions. The focus of scrutiny, however, has been on the results, not on the process by which the results were produced and certainly not on the largely anonymous corps of civil servants whose work was at the heart of the issue. Those people, and how and why they do what they do, are at the heart of Rob's important study. If we are ever to make the improvements that must be made in the quality of our intelligence work, then we must begin with a more mature and nuanced understanding of who actually does the work, how, and why. There is a context within which the work is done, a definite culture with values, traditions, and procedures that help shape important outcomes.

Rob has characterized a world that I find all too familiar. It is a world in which rewards and incentives are weighted heavily in favor of filling in gaps in conventional knowledge rather than in leading the way to alternative points of view. It is a world in which confirming evidence is welcome and rewarded and disconfirmatory evidence is, at best, unwelcome and, at worst, discounted. It is a world in which the legitimate and often necessary resort to secrecy has served, all too often, to limit debate and discussion. It is a world in which the most fundamentally important questions—what if and why not—are too often seen as distractions and not as invitations to rethink basic premises and assumptions.

Much of the recent discussion concerning the performance of intelligence organizations has been conducted in almost mechanical terms. "Connecting the dots," "mining the nuggets" are phrases offered as a way of understanding the exquisitely subtle, complex business of making intelligence judgments. As Rob Johnston's book makes abundantly clear, this is first and foremost a human enterprise. All of the intellectual power, biases, and paradigms that inform the thinking of the people who actually do the work need to be understood in the organizational context in which they do their work. In the finest tradition of anthropological field research, Rob has observed, collected data rigorously, reflected with deep insight upon it, and produced a study both sophisticated and extremely useful.

I worked myself for more than 30 years in the clandestine operations area of CIA, a part of the Intelligence Community that calls out for the same kind of understanding, professional, and constructive scrutiny this book has devoted to the analytic realm. My fervent hope is that the human intelligence service will benefit from the same kind of rigor and constructive understanding the analytic side has now experienced. My real hope is that Rob is available for the job.

The Author

Dr. Rob Johnston is an ethnographer who specializes in the cultural anthropology of work. He has been a research staff member at the Institute for Defense Analyses and a Director of Central Intelligence Postdoctoral Research Fellow at the Central Intelligence Agency's Center for the Study of Intelligence, where he is now a member of the staff.

Dr. Johnston is a Fellow of the Royal Anthropological Institute, the Society for Applied Anthropology, and the Inter-University Seminar on Armed Forces and Society.

This Page Is Intentionally Left Blank

Studies in Intelligence

Journal of the American Intelligence Professional

Unclassified articles from *Studies in Intelligence* Volume 55, Number 2
(June 2011)

Cultural Topography: A Research Tool for Intelligence Analysis

Improving Policymaker Understanding of Intelligence

The Pursuit of Intelligence History in the United Kingdom

From the Archives—At cia.gov only
The Evolution of US Army HUMINT

Reviews

Grappling with Covert Action after the Cold War

Takes on Intelligence and the Vietnam War

Intelligence Officer's Bookshelf

Center *for the* Study *of* Intelligence

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2011		**00-00-2011 to 00-00-2011**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Studies in Intelligence. Volume 55, Number 2	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Center for the Study of Intelligence,Central Intelligence Agency,Washington,DC,20505**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**Same as Report (SAR)**	**102**	

This publication is prepared primarily for the use of US government officials. The format, coverage, and content are designed to meet their requirements. To that end, complete issues of *Studies in Intelligence* may remain classified and are not circulated to the public. These printed unclassified extracts from a classified issue are provided as a courtesy to subscribers.

All statements of fact, opinion, or analysis expressed in *Studies in Intelligence* are those of the authors. They do not necessarily reflect official positions or views of the Central Intelligence Agency or any other US government entity, past or present. Nothing in the contents should be construed as asserting or implying US government endorsement of an article's factual statements and interpretations.

Studies in Intelligence often contains material created by individuals other than US government employees and, accordingly, such works are appropriately attributed and protected by United States copyright law. Such items should not be reproduced or disseminated without the express permission of the copyright holder. Any potential liability associated with the unauthorized use of copyrighted material from *Studies in Intelligence* rests with the third party infringer.

Studies in Intelligence is available on the Internet at: https:// www.cia.gov/library/center-for-the-study-of-intelligence/ index.html.

Requests for subscriptions should be sent to:

Center for the Study of Intelligence
Central Intelligence Agency
Washington, DC 20505

ISSN 1527-0874

The Mission

The mission of *Studies in Intelligence* is to stimulate within the Intelligence Community the constructive discussion of important issues of the day, to expand knowledge of lessons learned from past experiences, to increase understanding of the history of the profession, and to provide readers with considered reviews of public literature concerning intelligence.

The journal is administered by the Center for the Study of Intelligence, which includes the CIA's History Staff, CIA's Lessons Learned Program, the CIA Museum, and the Agency's Historical Intelligence Collection of Literature. The center also houses the Emerging Trends Program, which seeks to identify the impact of future trends on the work of US intelligence.

Contributions

Studies in Intelligence welcomes articles, book reviews, and other communications. Hardcopy material or data discs (preferably in .doc or .rtf formats) may be mailed to:

Editor
Studies in Intelligence
Center for the Study of Intelligence
Central Intelligence Agency
Washington, DC 20505

Awards

The Sherman Kent Award of $3,500 is offered annually for the most significant contribution to the literature of intelligence submitted for publication in *Studies*. The prize may be divided if two or more articles are judged to be of equal merit, or it may be withheld if no article is deemed sufficiently outstanding. An additional amount is available for other prizes.

Another monetary award is given in the name of Walter L. Pforzheimer to the graduate or undergraduate student who has written the best article on an intelligence-related subject.

Unless otherwise announced from year to year, articles on any subject within the range of *Studies*' purview, as defined in its masthead, will be considered for the awards. They will be judged primarily on substantive originality and soundness, secondarily on literary qualities. Members of the *Studies* Editorial Board are excluded from the competition.

The Editorial Board welcomes readers' nominations for awards.

CENTER *for the* STUDY *of* INTELLIGENCE
Washington, DC 20505

EDITORIAL POLICY

Articles for *Studies in Intelligence* may be written on any historical, operational, doctrinal, or theoretical aspect of intelligence.

The final responsibility for accepting or rejecting an article rests with the Editorial Board.

The criterion for publication is whether, in the opinion of the Board, the article makes a contribution to the literature of intelligence.

EDITORIAL BOARD

Peter S. Usowski, Chairman
Pamela S. Barry
Nicholas Dujmovic
John McLaughlin
Philip Mudd
Wayne M. Murphy
Matthew J. Ouimet
Valerie P.
Michael Richter
Michael L. Rosenthal
Barry G. Royden
Ursula M. Wilder

Not listed are three members who are under cover. Members of the board are drawn from the Central Intelligence Agency and other Intelligence Community components.

EDITORIAL STAFF

Andres Vaart

CONTENTS

Improving Analysis
Cultural Topography: A New Research Tool for Intelligence Analysis **1**
Jeannie L. Johnson and Matthew T. Berrett

Improving Policymaker Understanding of Intelligence
An Educated Consumer Is Our Best Customer **23**
Dennis C. Wilder

Coming to Clarity
The Pursuit of Intelligence History: Methods, Sources, and Trajectories in the United Kingdom **33**
Christopher R. Moran

From the Archives—At cia.gov only.
The Evolution of US Army HUMINT: Intelligence Operations in the Korean War **57**
John P. Finnegan

Grappling with Covert Action after the Cold War **71**
Matthew P.

Takes on Intelligence and the Vietnam War **73**
Clayton Laurie

Intelligence Officer's Bookshelf **79**
Compiled and reviewed by Hayden Peake

Contributors

Matthew Berrett is the Assistant Deputy Director for the DNI President's Daily Brief. He has served as an analyst and manager of analysts covering Middle East issues in the CIA's Directorate of Intelligence.

Jeannie Johnson is a lecturer in the Political Science Department at Utah State University. Ms. Johnson worked in the CIA's Directorate of Intelligence on Balkans issues during 1998–99. Her primary research interest, strategic culture, is the role of national and organizational cultures on the formation of security policy.

Clayton Laurie is a CIA historian. He also teaches military and intelligence history at the University of Maryland Baltimore County.

Dr. Christopher R. Moran is a research scholar at the University of Warwick. He focuses on the development of government secrecy in Cold War Britain. Interests include spy fiction and growth of intelligence communities in the 20th century.

Hayden Peake is curator of the CIA Historical Intelligence Collection. He has served in the CIA's Directorates of Science and Technology and the Directorate of Operations.

Matthew P. is a clandestine service officer assigned to the CIA History Staff.

Dennis Wilder is a senior officer in the CIA's Directorate of Intelligence. He has served as an analyst, a manager of analysts, a Special Assistant to the President and Senior East Asia Director on the National Security Council, and a senior reviewer of the President's Daily Briefing.

On the Web:

John P. Finnegan was a US Army historian who focused on military intelligence history. He died two years after his unclassified article appeared in a classified issue of *Studies* in 2000. Unfortunately, it was not extracted for an unclassified issue at the time.

Cultural Topography: A New Research Tool for Intelligence Analysis

Jeannie L. Johnson and Matthew T. Berrett

> ***"American decisionmakers have shown a need for help in isolating and understanding the complexity, weight, and relevance of culture as they consider foreign policy initiatives."***

In the third edition of his "History of the World," J.M. Roberts notes that "Historical inertia is easily underrated…the historical forces molding the outlook of Americans, Russians, and Chinese for centuries before the words capitalism and communism were invented are easy still to overlook."[1] In this article, Jeannie Johnson and I offer a variation on Roberts's view: Cultural inertia is easily underrated, and American decisionmakers have shown a need for help in isolating and understanding the complexity, weight, and relevance of culture as they consider foreign policy initiatives.

The view I bring to this discussion is not one of an anthropologist but rather one of a former economic analyst in US intelligence who has been a senior manager of analysts in various disciplines for a decade. My analytic and management positions have repeatedly brought me into indirect and sometimes direct interaction with top-level US decisionmakers including several US presidents. As I witnessed these decisionmakers in action and tried to help deliver insights they needed, I came to conclude that the "inertia of culture" was often underrated in their assessments of opportunities and obstacles, in part because few if any of their information sources offered a systematic and persuasive methodology for addressing this inertia and its implications for their policy options. I also came to conclude from direct observation and some readings out of the academic field of strategic culture that America's cultural view features the notion that Americans can achieve anything anywhere including going to the moon—if they just invest enough resources.

This notion is understandable but perhaps hazardous. America's remarkable history of achievement includes being the first nation actually to go to the moon, but the we-can-do-anything part of American self-identity also leads some to argue still that US failures in

The endnotes and an appendix are available in the digital version of the article in cia.gov.

All statements of fact, opinion, or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

Vietnam were not the consequence of a poorly managed investment; they were the consequences of investing too little.[2] How many resources and over what period would have been sufficient to strike "success"—particularly if success would have required changes in Vietnam at the cultural level? I have rarely seen American policymakers ask "Will our desired foreign policy outcome require change over there at the cultural level? Over what period and with what resources is such cultural change achievable?"

The more I observed the policy-intelligence dynamic, the more I perceived a need for an analytic construct designed exclusively to illustrate clearly and persuasively the inertia of culture. Cultural influences are typically touched on within US Intelligence Community (IC) analyses as peripheral factors, described with passing references, and often in general and superficial terms. Although the IC is full of world-class expertise on foreign peoples, places, and organizations, this industry rarely isolates and illustrates culture as a factor deserving its own sophisticated and thorough treatment.

To remedy this perceived deficiency, I teamed with Jeannie Johnson—formerly an intelligence analyst at CIA and now with Utah State University—who had brought her academic training in strategic culture to a pursuit similar to mine. For some time she had been amassing training ideas in the area of cultural analysis for IC experts, and our combined efforts, along with significant input from other members of my former office,[3] trial runs of intelligence products, research, and continued refinements over the past four years have resulted in a process we call "Cultural Mapping." This process, or methodology, is designed to isolate and assess cultural factors at play on issues of intelligence interest and to distinguish the degree to which those factors influence decisionmaking and outcomes. Mapping exercises done across time, spanning multiple issues, and on diverse groups within a society may aid in understanding that society's "Cultural Topography." We describe the process below.-mtb

---

Target Audience: Intelligence Analysts

Understanding this methodology and its specific structure requires a grasp of the users for whom it was designed: intelligence analysts. Anthropologist Rob Johnston was hired in the wake of 9/11 to complete an ethnographic analysis of the IC's analytic cadre and to offer suggestions for improving its performance. He observed biases produced by both ethnocentrism and expertise, which resulted in rather serious cognitive gaps, and he noted a lack of systematic tools for going after cultural data.[4]

Johnston defines ethnocentrism as the tendency to project "one's own cognition and norms onto others." Intuition, a compass regularly employed by career analysts, is culturally encoded and, by nature, ethnocentric. Johnston warns of its use as a barometer for analyzing or predicting the behavior of foreign agents.[5] According to Edward Stewart and Milton Bennett, American cultural tendencies are particularly unhelpful in this regard. Despite vast information resources and exposure to exotic cultures, Americans continue to overemphasize similarity and assume that other social groups have values and aspirations in line with their own.[6]

It may seem counterintuitive to see expertise as a source of bias but Johnston points out that "becoming an expert requires a significant number of years viewing the world through the lens of one specific domain. This concentration gives the expert the power to recognize patterns, perform tasks, and solve problems, but it also focuses the expert's attention on one domain to the exclusion of others."[7]

Johnston's cautionary counsel regarding the habits of experts echoes that penned by Richards Heuer two decades earlier:

> *Once people have started thinking about a problem one way, the same mental circuits or pathways get activated and strengthened each time they think about it. This facilitates the retrieval of informa-*

tion. These same pathways, however, also become the mental ruts that make it difficult to reorganize the information mentally so as to see it from a different perspective.[8]

A third form of observed bias among analysts, which might be added to Johnston's list, has roots in academic training and is an institutional legacy that tends to leave culture out in the "all-source" approach to analysis. The academic backgrounds of most intelligence analysts stem from disciplines that emphasize power and wealth as the primary human motivators, leaving underexplored other motivators such as identity, preservation of social institutions, alternative value structures, powerful narratives, or perceptions of the security environment distinctive to a person's or group's region and history. Due to institutional habits, the educational paradigms of many of our experts, and the reticence of members of the anthropological community to accept positions within US security institutions, culture has received limited attention as a variable. Most analysts have simply not been introduced to the training or the research tools for going after cultural data effectively.

This bias also affects intelligence collection, which aims disproportionately at foreign

Despite vast information resources and exposure to exotic cultures, Americans continue to overemphasize similarity and assume that other social groups have values and aspirations in line with their own.

leaders and the elite cadres that surround them. We have, institutionally, very few tools aimed at understanding national populations or specific subcultures, a point General Michael Flynn made in his public rebuke of intelligence practices in Afghanistan in January 2010.[9] The emphasis on elites has produced cognitive gaps in our analysis—perhaps illustrated anew by the surprise over the political tumult that erupted across North Africa and the Middle East in early 2011. Johnston observes:

[An] analyst, while accounting successfully for an adversary's capability, may misjudge that adversary's intention, not because of what is cognitively available, but because of what is cognitively absent. The failure to determine an adversary's intention may simply be the result of missing information or, just as likely, it may be the result of missing hypotheses or mental models about an adversary's potential behavior.[10]

Noting that the lack of cultural data in mental models is a problem not only for analysts but also for the policymakers they support, Johnston exhorts:

Specific cultural knowledge is a skill and the foundation for forecasting the behavior and decisionmaking of foreign actors. Acquiring cultural knowledge should be taken as seriously as learning any other facet of one's analytic capabilities. Moreover, it is incumbent on analysts to educate their own leadership and policymakers about the value and utility of cultural knowledge for intelligence analysis.[11]

Johnston's advice may sound rather obvious, but given the scope and complexity of the phenomenon we call "culture," attempting its research and determining—with no prior training in this field—which aspects have policy relevance can be an intimidating task even for the most talented political, economic, or military analyst. Interviews with analysts have often revealed a sense of being overwhelmed by the scope of cultural data that are relevant to their accounts—and of dismay at the length and depth of the historical knowledge necessary to capture a grand strategic profile of any region or group. One reaction is to subconsciously search for reasons why cultural data are not necessary—a position that ana-

Interviews with analysts have often revealed a sense of being overwhelmed by the scope of cultural data that are relevant to their accounts, and of dismay at the length and depth of the historical knowledge necessary to capture a grand strategic profile of any region or group.

lysts schooled in the international relations paradigms of realism and neorealism are already trained to take.

Analysts also face institutional obstacles to in-depth cultural study. The organizations they work for are required to produce large volumes of often tactical pieces on a daily basis. For some analytic assignments, this pace can be relentless. IC institutions simply do not have the manpower to pursue the type of cultural research employed by professional anthropologists: living in the region for extended periods in order to conduct ethnography (participant observation) and to refine fluency in the local language. Many analysts move from one account to another during their careers and must conduct cultural research via short-term stays in theater, brief stints of language training, and information that can be accessed from their desk or in library holdings.

Given this particular organizational backdrop, our aims have been modest but effective, we hope, in moving cultural research and analysis forward within the community. Our research tool is designed to broaden the IC's grasp of the factors that drive outcomes, specifically cultural factors, and to help IC analysts be creative in their collection of cultural data. We make no attempt to deliver the end point or last word in cultural research. What we offer is an accessible research tool that can produce systematic, sophisticated surveys of cultural variables, a grasp of which can greatly help US policymakers achieve desired outcomes and avoid surprises.

Research Philosophy

Our experience in marrying cultural data and analysis to the daily demands of defense and intelligence analysis has led to a few conclusions about best practice. The most overriding of these is that sweeping cultural profiles of a region or a national group are of limited value in the intelligence industry for a number of reasons. As has been effectively argued by Christopher Twomey, security studies that attempt to draw predictive power from the amorphous and often internally contradictory substance we call "national culture" often suffer follies of overgeneralization and static analysis, and they reach, as a consequence, questionable conclusions about the sources of security policy.[12] Patrick Porter heaps heavy criticism on many of the West's nascent efforts at cultural analysis for making this mistake. He accuses military and intelligence analysts of drawing static portraits of Eastern cultures rather than recognizing them as moving, flexing, human creations—and, in so doing, introducing dangerous sources of error.[a 13]

To reference "culture" in the singular for any particular polity is typically an error; there is rarely just one internal variety. Walter Russell Mead identifies four distinct narratives within US strategic culture and posits that our various foreign policies are formed from the "collisions and debates" those narratives inspire.[14] The idea of composite cultures is not restricted to analysis of the US, of course. Authors writing on Germany, China, India, and Iran, to name a few, all note the internal conflict of competing cultural narratives about national security within these countries.[15] The existence of

[a] Porter's warnings are valid but may be a bit overstated. Today's Department of Defense is not entirely uninitiated in doctrines of cultural change. Leading-edge training methods emphasize "practice theory"—an approach to culture which treats the change dynamic as central. Practice theory explains culture as a product of interaction between agent and structure and trains analysts to expect change rather than stasis.

multiple cultures is present not only at the national level; it is true right down to the ordinary individual. As Kevin Avruch quips, "for any individual, culture always comes in the plural."[16] The cultural influences at play on a single actor could derive from a background that features Northern European, Catholic, engineering school, and family-specific influences.

Most academic work examining the impact of culture on security policy mirrors the biases of the IC by privileging elite-level culture (usually at the organizational level) over other types. The typical justification of this approach is that while public opinion may play a peripheral role, "it is arguably the elite—owing to its role as gatekeeper, its expert knowledge and its privileged access to means of communication—that ultimately decides which way security policy goes."[17] But this logic breaks down when one is assessing the impact of culture within the context of counterinsurgency and stability operations, for instance. Given the pivotal role of local popular opinion in this type of military engagement, understanding public culture, the cultures of significant substate groups, and how these affect security policy becomes paramount.

The research method presented here asks analysts to step outside the biases of the institutional and academic work already done on their topic and assess afresh which actors and cultural influences are most relevant for the policy issue they are researching. In some cases this may be a vastly understudied section of the population, one which has received little attention within official channels, and one whose research will require unorthodox (for the institution) survey and collection methods.

Most academic work examining the impact of culture on security policy mirrors the biases of the IC by privileging elite-level culture (usually at the organizational level) over other types.

Culture at any level—organizational, tribal, ethnic, regional, or national—is a dynamic human creation and subject to change, but this should not discourage analysts from its study. Any tool devised to track cultural influences must employ questions that challenge previous assumptions, unearth fresh data, and highlight possible areas of change, but as Barak A. Salmoni and Paula Holmes-Eber remind Marines who may be intimidated by the complexity and movement of the cultures they are studying:

> *Although people are, by nature, variable and unpredictable, they still need to work with others in social and cultural groups. These groups —and their associated beliefs and structures—are organized according to logical, understandable principles that every person living in the culture must understand, at least intuitively, in order to get along with each other. With some basic study,* [others] *can also recognize and understand these principles and apply that understanding to their operations.*[18]

It is with our specific audience and these basic assumptions about culture in mind that we constructed the Cultural Mapping method. It is presented here in the step-by-step process we have provided recently to groups of analysts.

Cultural Mapping Exercise

Step 1: Identify an Issue of Intelligence Interest

The first injunction to analysts is to narrow the scope of cultural inquiry by isolating a particular policy question of interest. The narrower the issue, the more targeted the cultural research, and the more likely it will yield actionable data. The issue selected may reflect a frequently asked question that needs examining from a new angle, or a question that policymakers are not asking—perhaps due to ethnocentric blinders, habit, or limited

knowledge of the region—but should be.

Step 2: Select an Actor

Analysts are urged in the this step to isolate a particular population for study. All "players" within this issue arena are identified for consideration, stretching to include some not typically examined. A sampling of possible actors might include prosperous urban elites, an ethnic subgroup, a particular government institution, a dissident group, a village council, housewives across a region, a youth bulge, or the cadre around a leadership figure. From among these subgroups, or actors, one is selected for focused study. This actor may be the one expected to play the most pivotal role in a particular outcome on the issue selected or one that is dangerously understudied and may present a wild card for the future.

The actor in question need not have a discernible "group culture." The important question here is not "what is this actor's culture?" but rather "what cultural influences will weigh in on decisionmaking on this issue for members of this group?"

The mapping exercise is designed as a looping process. The actor who seems most relevant initially may fade into the background as research progresses and the salience of other actors becomes apparent. Conversely, the initial actor may remain of interest but emerge as a far more complex entity once research magnifies group properties. Analysts are invited to loop back to this stage after an initial round of research in order to disaggregate, refine, or switch actor sets in a way most profitable for intelligence analysis.

Continued refinement occurs to the central policy question as well. Analysts may find that they were as captive to ethnocentric blinders as the clients they serve when crafting the initial intelligence question. Looped-back refinements on this front are to be expected.

Step 3: Amass a Range of Cultural Influences

Assuming Avruch's logic that all individuals and groups possess culture in the plural, analysts are asked to map out the various cultural influences which may guide the behavior of members of this group—again, *within the context of the issue they are assessing.* These influences range from the local, such as clan, tribal, or organizational cultures, to wider cultural influences, such as regional, ethnic, religious, national, gendered, socioeconomic, or generational. Analysts need not confine themselves to fleshing out "typical" cultural influence sets but rather think expansively and creatively about the specific group they are studying.

New forms of social media have norms embedded and learned by new users; a leadership cadre hailing from a similar educational institution may espouse a common view of how the world works; and foreign youth who work part time at America's franchises may be internalizing a strong dose of capitalist work ethic. We encourage analysts to consider all plausible influences initially, pursuing this as an exploratory stage. Decisions about which influences are most relevant will come later.

Step 4: Explore the Cultural Data from Four Perspectives

In order to supply structure to the cultural exploration encouraged in Step 3, we suggest the following four categories for assessing cultural data: *Identity, Norms, Values*, and *Perceptual Lens*. This is not an exhaustive list of important cultural factors but is a useful starting point in examining culture from four policy relevant perspectives. The categories are distinctive enough from one another to inspire different sets of questions and elastic enough to capture a wide range of data:

***Identity*:** The character traits the group assigns to itself, the reputation it pursues, and individual roles and statuses it designates to members.

***Norms*:** Accepted and expected modes of behavior.

***Values*:** Material or ideational goods that are honored or that confer increased status to members.

***Perceptual Lens*:** The filter through which this group determines "facts" about others.

Unearthing and isolating factors that might be captured as identity, norms, values, and perceptual lens is a messy business.

Analysts receive an in-depth list of questions for each category.[a] The magnitude of cultural data unearthed in answering the questions in these four categories may be managed by keeping a litmus test for policy relevance in mind. An initial short list of questions might examine the issue selected in Step 1 in the ways below.

Identity.

- Which factors surrounding this issue would cause this actor's identity to be threatened? Alternatively, which might provide the US common ground for co-option?
- Is group cohesion strong along identity lines in response to this issue? What would cause the group to fracture or to unite behind a common front?
- What individual roles and statuses might group members seek to protect?

Norms.

- Does this issue place social institutions or common practices under threat?
- Which practices are deeply internalized and likely to inspire resistance?
- Which practices are compatible with US interests on this issue?
- Would our proposed changes in this policy area offer group members a way out of increasingly unpopular normative practices? Which members?

Values.

- What is considered "honorable" behavior in this issue area?
- Which local values may be in conflict with our approach to this issue?
- Which values might be co-opted in moving US interests forward?
- Where might value differences between target groups present an opportunity to exploit cleavages?

***Perceptual Lens*:**

- What are the preconceived notions of this group concerning the behavior and character of the United States?
- What are group's beliefs about the future?
- What hurdles must we overcome in messaging to this group on this issue?

This tidy and rather simple list of questions may provide the false impression that the answers are readily apparent and attainable. The reality is that unearthing and isolating factors that might be captured as identity, norms, values, and perceptual lens is a messy business. It involves doing heavy amounts of open-source reading, using the research skills honed in graduate school (rather than the typical day-to-day practices of the intelligence business), and wading through a lot of data of questionable relevance.

Most analysts need to take themselves off-line for a period in order to accomplish this task with any effectiveness. This sort of research does not mix well with the often frenetic pace of producing current intelligence. Some offices have been particularly proactive in this regard and have offered their analysts short sabbaticals in order to get them away from their desks. These intelligence officers remove themselves to a separate location—in most instances to an institution with significant holdings on their area of interest—to conduct research. Other offices have assigned analysts into research or methodology teams where they can focus on a long-term research endeavor with the necessary consistency.

[a] The questions are contained in an appendix available in digital versions of this article.

Most analysts need to take themselves off-line for a period in order to accomplish this task with any effectiveness.

After immersing themselves in what cultural data is available through official channels, open-source searches, and (ideally) visits to the region, analysts begin to identify cognitive gaps in previous modes of analysis. In addition to benefitting from new data accumulated on their account, they become far more attuned to what they don't know—what information the institution is not collecting. Identifying key knowledge gaps means coming up with creative solutions for going after the target data. Time constraints limit the ability of intelligence analysts to employ extended ethnography as a tool, and institutional restraints can limit the ability to employ methods pursued by academic or other institutions. The following is a collection of cultural research strategies proffered by a variety of analysts representing the full range of experience, with some residing in academic venues and others in policymaking forums.

Historical Narratives

Nearly all analysts begin with the assumption that one must conduct a thorough background investigation to become familiar with a regime's history, geography, internal social codes, and general interactions with other states. If not conducted with strategic efficiency, this task can be overwhelming. One way to gauge those aspects of history relevant to the issue being tracked is to pay attention to historic references made when the policy issue is addressed, whether in political rhetoric, private conversation, lessons in school, or expressions from the artistic community. Which narratives do politicians draw on to legitimize their behavior on this issue and to pacify the public? Which narratives work? Which do not?

Physical manifestations such as architecture, street names, statues, and memorials demonstrate which aspects of a nation's history it chooses to preserve and celebrate. Finding and understanding the selection of heroes, for example, lends itself to understanding national values.[19] Of particular interest are those symbols that people voluntarily display in their homes.[20]

Understanding historic narratives can be critical to making sense of the strategic choices of foreign populations. The 1999 bombing campaign against Serbia supplies an example. US analysts vastly underestimated the duration and expense of the 1999 engagement, in part because they undervalued the role of historic narratives of victory and defeat. Serbia's national holiday is not a celebration of a past battlefield victory but of a glorious defeat in 1389 at the hands of the Ottoman Turks. Serbs celebrate the valor of the war's hero, Prince Lazar, who received a heavenly visitation on the eve of battle and was told that unless he surrendered he faced certain defeat the next day. Given the choice, Lazar declared that it was better to die in battle than to live in shame.[21] He did precisely that—and became cemented in Serbian legend.

This tale permeates Serbian society. It is taught to youngsters in school and is represented in homes and offices in the renowned painting "Kosovo Girl." Most analysts working this issue were familiar with these aspects of Serbian culture but lacked a method for tracking and weighing them systematically and thus acquiring the footing necessary to articulate persuasively to policymakers the potential impact on Serbian behavior: that is, that Serbia would find victory by standing up to an overpowering military force when the world expected it to fold.

Understanding the weight of this narrative for Serbs in defining honorable conduct during war would probably have disabused planners of the idea that the bombing campaign would be over quickly. Instead of projecting a three-day campaign, we might have helped policymakers plan for a cam-

paign closer to the almost 80 days it eventually took.[22]

Tapping into the Population

Useful interaction with the population under survey can range from rudimentary (daily records of anecdotal interaction) to highly institutionalized methods (sophisticated polling conducted nationwide).[23] One popular method for both institutions and individual researchers is targeted focus groups. Much has been written on this particular survey technique, but the advice of analysts in the field is that effective focus groups must be preceded by an in-depth study of the issue at hand so that the interviewer can select a sampling of *relevant* focus group participants and frame questions appropriately.[24]

One selection device employed by ethnographers is to narrow interviews to "key informants" of local culture.[25] Key informants can range from subject matter experts to those who are cynical about their own culture and are therefore observant, reflective, and articulate.[a 26]

A variation on key informants is "key keepers" of culture. These people are defined by frequent contact and extended conversation with other members of the community. As a result, the key keepers tend to harbor the notions, language modes, and perceptual lens of the local community.[27] A key keeper may be institutional. In determining core values within Israeli society, Greg Giles looked first to shared, institutionalized socialization processes. He pinpointed the Israeli Defense Force (IDF) since universal conscription requires that all Israeli citizens experience socialization and training through this institution. Giles points out that it is not just contact with the institution that matters, but institutional legitimacy. The IDF meets these criteria based on the high number of young people polled who said they would be willing to serve in the IDF even if it were an all-volunteer force.[28]

Useful interaction with the population under survey can range from rudimentary (daily records of anecdotal interaction) to highly institutionalized methods (sophisticated polling conducted nationwide).

An important window into norms and the color of a group's perceptive lens is the "conventional wisdom"—the things "everybody knows."[29] Compiling and analyzing oral traditions may take a number of different forms. The author of a recent popular survey of Iran attempted to do this by engaging in dialogue with persons from a sampling of all of the society's castes and factions and starting each conversation with the same request: "Tell me your story."[30] The patterns and themes developed across conversations helped uncover generally accepted notions about self and others. Additional probing may reveal notions of identity—what is taken for granted as a natural role for the nation, what is expected, and what is controversial.[31]

One inventive young scholar from Monterey's Naval Postgraduate School proposed an alternative to official polling—the systematic study of "RUMINT" (rumor intelligence).[32] She surveyed and prioritized the issues on the minds of Iraqis by tracking the frequency of rumors that appeared in local print. One of her findings, a surprise for US forces at the time, was that a large swath of Iraqis believed the United States was *behind* the insurgency. Their belief stemmed not so much from an assumption that the United States was malicious but from the perception that it was impossible that a superpower with the might of America could not stop the insurgency if it wanted to. Therefore, the United States must be behind it. Her work produced a number of timely insights for US

[a] Bernard claims that cynical informants have consistently been his best sources over the years.

Those not in-theater could use alternative approaches to tracking gossip networks.

officials concerning Iraqi attitudes and priorities.

Those not in-theater could use alternative approaches to tracking gossip networks. Dr. Deborah Wheeler, a specialist in Middle East studies, has focused her research on online discussions across her region—particularly among women who otherwise do not speak out. Chat rooms and editorials posted in pseudonymous blogs may be one way to evaluate the thinking of otherwise reticent populations.[33] Christine Fair, an analyst writing on Iran, suggests another alternative to firsthand interviews with citizens of a repressive regime:

> *Utiliz*[e] *consulates of countries where Iranians seek US visas (India and Turkey) to collect and develop information during the visa interview process. Defense attachés may also engage their in-country counterparts in countries where military cooperation with Iran are ongoing to gain insights into Iran.*[34]

Expatriates are a self-selected group, often coming from within a limited segment of society not representative of the broader base. Despite this sampling drawback, interviews with this group offer some value. Students from the region of interest living abroad are often better at identifying beliefs and norms in their home lands than fellow citizens left behind because the students have experienced the contrast between their national beliefs and those of people in their host countries.[35]

Secondhand interviews—interviewing those who frequently interact with members of the culture—are also very useful, especially in cases where the populace does not feel comfortable speaking openly about its thoughts and opinions.[36] In some cases it is politically incorrect to speak of one's historic culture, especially where security policy is concerned, so there is an absence of civil or political rhetoric on the topic. Rodney Jones notes the case of Japan, where Jesuit priests who lived there for extended periods were more likely than Japanese statesmen to speak freely of Japan's history and predilections.[37]

Joe Bermudez, a longtime Korea analyst, notes that when information is hard to come by, as it is with North Korea, even interviews with travelers and a careful look at their photographs can prove beneficial. In North Korea's case, it helps unveil the genuine state of affairs for the state's population (regarding, for example, roads, electricity, phone service, and health conditions) in contrast to state claims about its situation.[38]

Content Analysis of Texts

When evaluating national-level cultural threads, texts taught in school deserve special attention. Classroom textbooks explain perceptions of a nation's own history, its view of others, acceptable methods of warfare, and common justifications for past behavior (norms). Societal values are taught to children explicitly, particularly in the early stages of education. Their texts may include hero legends, songs, rhymes, fables and oversimplified anecdotes from the nation's history.[39] Valuable cultural or political insights can be drawn from noting which figures are celebrated, which are despised, and why.[40] Education and other socialization processes also result in a body of shared literature considered "classic." What are the messages in this body of work? How widely are the classics read? How often are they referenced?[41]

Military texts are essential sources of information on the values, identity, and acceptable methods of achieving security within a regime. Twomey recommends a deep survey of all sorts of doctrinal texts—telegrams, military orders, descriptions of training regimens, diaries, memoirs, and communications between military leaders.[42] This study would

Military texts are essential sources of information on the values, identity, and acceptable methods of achieving security within a regime.

reveal national aspirations over time (identity), accepted norms for achieving them, and perhaps more particular values such as views on the use of manpower and loss of life.[43]

Tracking Political Rhetoric

The key to analyzing political rhetoric effectively is understanding, in local context, the role it plays in communicating with the population of interest. Russia analyst Fritz Ermarth notes that a first step in weighing the value of political rhetoric within a nation is to track its correlation with actual behavior in the past. Tracking over time and across politicians may yield useful generalizations about government speeches as indicators of sincere goals and security objectives.[44] On China, Twomey points out that the culture tends to weigh private comments more heavily than public statements and that inflammatory public statements need to be qualified accordingly.[45]

Once understood, public rhetoric may represent a rich data field for assessing norm strength or identity trends. The work of Andrew Cortell and James Davis, as well as that of Paul Kowert and Jeffrey Legro, suggests measuring a norm's strength by the frequency with which it is referenced by statesmen proposing a course of action or legitimizing one already taken.[46] On the identity front, Glenn Chafetz, Hillel Abramson, and Suzette Grillot employ content analysis of leaders' speeches in order to explain the weapons acquisitions patterns of diverse states. Their research presents a strong correlation between four identity typologies and a "marked tendency toward nuclear acquisition."[47] The method Chafetz et al. suggest for coding role conception can easily be duplicated for other issues.

Extended Observation of Public Behavior

Public reactions to the moves made by state leadership may highlight areas of congruence or cleavage between the understanding of values and norms fostered by the populace and the behavior of state officers. Disaffection may come in the form of protest, local grumbling, or biting humor pointed at political officials, while congruence might manifest itself through strong turnout for state events and parades, voluntary displays of state insignia, or healthy membership in state-related organizations.[48] Congruence or cleavage between separate identity groups may be manifest in part by the degree to which the target group is willing to accumulate and incorporate traditions of food, dress, verbal expression, names given to children, and entertainments originating elsewhere.[49]

In order to understand identity distinctions within large regions, one might systematically observe social ceremonies and rituals. What is the purpose of the ceremony? Who attends?[50] Which norms violations are publicly punished? Which achievements publicly celebrated? One daily ritual that often sheds light on identity and value structure is the protocol of salutations, especially in conversations between members of the population meeting for the first time. How does one introduce oneself? Is it by way of profession, clan ties, or religious affiliation?[51] Which aspects of personal identity are most valued?

Humor can serve as a useful test for one's grasp of the culture under study. What does this group find funny? Why? Which alternative group is consistently used as the object of ridicule? Which of the alternative group's characteristics are subjected to mockery? How does this illuminate the values of the group being tracked? What does it say about their perception of others?

Language is an indispensable source of cultural information. Not every analyst is going to have the opportunity to become

Entertainment media provides valuable insights for those seeking to understand the current state of a particular set of norms within a society.

fluent in the local tongue but will find that pursuing even novice-level language competence may yield cultural insights. Concepts that a population values are often assigned more words than those that are not. Recent research suggests that language has a profound impact on our perceptual lens. It registers the content of our memories—the aspects of reality that we record, and how we record them.[52]

Evaluating the Output of the Media and the Artistic Community

Depending on the level of independence enjoyed by news, entertainment, and artistic producers within a population, these may yield significant insight into a group's identity and its core norms and values. Twomey notes the onerous level of work involved in a comprehensive review of these sources and commends two authors who have tackled it: Peter Hays Gries on China, and Ted Hopf, on Russia.[53] Even completely controlled media may still offer material for cultural analysis. State propaganda illuminates the identity, norms, and values that the state hopes to achieve, as well as the narrative it hopes will dominate popular perception.

In a free society, the bounds and content of political debates channeled through the press can identify not only cleavages in the strategic and political culture but also points of popular congruence.[54] Sometimes what is *not* addressed is as interesting as what is. Christopher Meyer and Adrian Zdrada isolated a pronounced identity aspect to Poland's willingness to ally with the United States in our runup to the invasion of Iraq in 2003 through content analysis of press debates on the issue. Their research revealed an absence of serious security discussions relating to Iraq and strong emphasis on establishing Polish identity as a reliable US partner. The identity basis of Poland's participation helps explain why the failure to unearth weapons of mass destruction in the Iraqi theater did not diminish the enthusiasm for the US alliance in Poland as it did in Great Britain.[55]

Free media may also serve as a reliable watchdog for norms violations within the state. For example, the flurry of reporting in the United States on excesses in Guantanamo and at Abu Ghraib manifest norms violations that are considered serious and newsworthy in the United States but may not have been treated that way in other countries. As commercial organizations, media outlets must present a worldview comfortable to their audience. The worldview captured in newscasts validating (especially controversial) state actions may illuminate popular perspectives and narratives that more formal instruments for measuring opinion would miss.[56]

Entertainment media provides valuable insights for those seeking to understand the current state of a particular set of norms within a society. The fabric of television sitcoms is the exaggerated presentation of social *faux pas* and situational conundrums.[57] Sitcoms are also a helpful reference for illustrating a culture's typical problem-solving devices and for illuminating changes underway in society by poking fun at norms that are in flux. TV dramas serve a different purpose—they most often focus on norms violations that are serious enough to be considered tragedy and represent a shared core of values across the society.

Step 5: Assemble Critical Cultural Factors

After analysts have worked to fill cognitive gaps and amassed a sizeable accumulation of cultural data, they are then presented with the painful task of setting much of it aside—honing their data down to those cultural factors that are likely to play a role in the decision-making of *this group* on *this*

issue. The analyst's instructions are to evaluate each cultural factor according to:

- ***Relevance*** for the issue selected.
- ***Robustness*** of the factor. [a] 58
  - How well established is it?
  - How widely shared is it among members of this group?
  - To what extent is opinion or behavior that is inconsistent with this aspect of identity, norms, values, or perceptual lens rewarded or punished internally by other members of this group?
- Likelihood of this cultural factor to provoke a ***Response*** (cooperative or conflictual) when external actors engage this group on this issue**.**

The cultural factors that emerge from this rigorous culling process are the Critical Cultural Factors (CCFs) for this group on this issue and will be the concepts that are addressed in the finished intelligence product. In intelligence terms, each factor must be solidly connected to a "so-what." What impact is it likely to have on outcomes of interest to US policymakers? To what degree are we confident that behavior will reflect this cultural influence? How many types of research sources or methods validate this finding?

The cultural factors that emerge from this rigorous culling process are the Critical Cultural Factors (CCFs).

Step 6: Mapping

After an analyst has isolated the relevant set of CCFs, she is asked to map the primary source of each from among the various cultural influences identified in Step 3 (national, ethnic, tribal, professional, etc.). Are the identity components on the CCFs list confined primarily to one domain (i.e., tribal), or shared across other sources of cultural influence (i.e., ethnic and religious)? What about critical norms and values? What about critical aspects of the group's perceptual lens?

The purpose of this portion of the mapping exercise is to define—for the analyst as well as the eventual audience of her intelligence product—the influence boundaries of the CCFs. Are they spread across the cultural landscape or confined to one or two key cultural influences? Is there a clear, somewhat bounded, cultural force at play on this issue (i.e., tribal, sectarian, professional/organizational), or are cultural influences widely dispersed and unlikely to provide anything close to a clear script for action?

Step 7: Writing the Paper

Based on the outcome of the mapping exercise, a finished Cultural Topography paper will define for the reader first, which aspects of identity, norms, values and perceptual lens are most important to understand when the United States engages this actor on this issue, and second, the probable influence boundaries of the CCFs identified. These CCFs provide the primary focus of the paper. The paper answers, in specific terms, the following questions:

- Which CCFs represent points of possible leverage and cooperation?
- Which CCF red lines are likely to spark resistance or even armed conflict between foreign elites and their broader populations or between foreign populations and US actors?

[a] The work of Jeffrey Legro may serve as a useful reference point for this task. He has written extensively on measurement of norm strength and his work on norms probably has some transferability to identity, values and perceptual lens. He proposes that a norm be evaluated according to three criteria: how clearly it is recorded in the rules of society (specificity), how long it has existed within this society and its strength in standing up to normative competitors (durability), and how widely it is accepted and referenced in discourse (concordance).

A handful of papers based on the Cultural Topography methodology have been produced, but they have prompted reaction to suggest the method offers a way to add analytic value.

- Do most of the CCFs stem from one cultural tradition or source of influence (i.e., ethnic, religious, tribal)? If so, what else do we need to know about this cultural domain in order to acquire adequate context for understanding the CCFs in question?
- Are the members of the group under study drawing from multiple cultural traditions/influences when they respond to this issue? Will it cause them to fracture when pressure is exerted on the myriad aspects of this issue?
- To what extent do adversarial groups in the region share the same cultural mapping on this issue as the group under study, reflecting common sources of cultural influence? Where is this not the case? How does that inform forecasting on future cooperation or divergence between these groups?
- Within which tradition will our messages to this group on this issue be most persuasive?
- How likely are other groups across the region to respond in similar fashion when presented with this issue?

Initial Impact of Cultural Topography

Only a handful of papers based on the Cultural Topography methodology have been produced, but they have prompted sufficient reaction to indicate that the insights they offer get beyond the general body of information already grasped by most analysts and policymakers, and early reactions to such insights suggest that the methodology offers a way to add analytic value:

- In a meeting that was part of a US policy review on a specific country, an attendee not familiar with this methodology reported that several analysts, authors of a Cultural Topography paper on this country, "quickly proved themselves to be as smart or smarter on [country of focus] than anyone else in the room…on history, ethnic topography." It is worth adding that the room was filled with experts who had spent significantly more years on the subject than had these analysts.
- While traveling abroad, a special envoy with significant expertise selected one of the Cultural Topography papers as one of only two items—from a large pile of intelligence materials—he wanted sent back to his office for further study. Several senior commanders also expressed significant interest in this paper.

Additional reactions have been consistent with those noted above, but only the continued application and refinement of this tool will fully display whether its potential is great or limited. The methodology is being taught in at least one IC institution, and several new Cultural Topography papers are in motion now. The main challenge to pursuing and exploiting this approach within the IC is the pressure of daily production driven mostly by conventional collection and analysis. Cultural Topography holds no promise of advancing the understanding of cultural influences on foreign perceptions and actions unless researchers are given the time to find additional, often novel data and then to incorporate them into the tool.

(The appendix and endnotes. are available in the digital version of this article.)

❖ ❖ ❖

Appendix A

Cultural Analysis

Concepts and Questions

Identity

- Is individual identity seen as comprising one's distinct, unique self, or is it bound up in a larger group (family, clan, tribe)?[59]
- Does this group see itself as responsible for and capable of solving social problems? Are problems responded to with energy or left to fate?
- Which myths and national narratives compose the stories everyone knows? How do these speak about group identity?
- What is this group's origin story? Does it inform group members of their destiny?
- What would this group list as defining traits of its national, tribal, ethnic character?
- Is one aspect of identity being overplayed, not because it is foundational for most decisions but because it is being threatened or diminished?

Values

- For the linguist, which concepts/things are described in nuanced ways (meaning that many words have been assigned to them)? Which concepts are missing from the language? (For example, the concept of "fair play" is hard to find outside of English.)
- What generates hope in this population?
- Which is viewed more highly as a communicative tool—emotion or logic? Are conversational styles which emphasize logic viewed as trustworthy?
- Is conspicuous consumption valued as a status marker? If not, what incentives exist to work hard?
- To what extent do security concerns trump liberty concerns in this society? Which parts of liberty are deemed attractive?
- Is social mobility considered a good thing, or is it deemed disruptive to a highly organized system? Would this group fight to keep a hierarchical arrangement even if offered opportunities for egalitarianism?
- To what extent does loyalty trump economic advantage?
- Which is more value-laden for this group—"progress" or "tradition"?
- Is optimism rewarded as a character trait or is it considered naive, juvenile, and possibly dangerous?
- Which character qualities are consistently praised?
- What composes the "good life"?
- What sorts of myths, hero figures, segments of history, or identity markers does the material culture celebrate? What is revealed by the decorations in homes, modes of dress, food eaten (or not eaten), monuments respected (as opposed to those covered with graffiti), gifts given, etc.?

•In describing a proposed project, what will "impress" this audience? The project's size? Its historical relevance? The technology used to produce it? How might new projects best be framed in order to win popular support?

NORMS

Political

•What is considered a legitimate pathway to power? How do "heroes" in film and other popular media obtain their power? Do they act as isolated individualists or in concert with others?

•"What gives a public the comfortable feeling that the way that decisions are reached and leaders are chosen is 'right'?"[60]

•How does the group view compromise?

•Where does "genuine" law come from? (Nature? God? A constitution? Current political institutions? Imagined, future institutions? Moral conscience? A personality from the past?)

•Is adherence to state-manufactured law admired or disdained? To what extent is state law equated with "right" and "wrong"?

Social

•Is social status in this society primarily ascribed (i.e., one is born into it) or achieved? If achieved, how so?[61]

•What are the primary markers of a person of high rank in this society? How would you recognize him/her? Does political power or intellectual prestige rank higher than economic surplus?

•What is the process for establishing trust? How does one know when it has been achieved?

•Do people perceive their own place and the dominant hierarchy as natural?

•To what extent are subordinates responsible for their own actions?[62]

•What do proverbs say about social expectations and the perceived pathway to success?

Economic

•What are the group's views on work? Which types are admired? Which are disdained? What are the economic implications?

•Which economic activities are considered immoral?

•Is it considered appropriate to "master" the natural environment and bend it to one's will?

•To what extent is the economy intertwined with kin obligations?

•What are obstacles to private property ownership?

•How does this culture group stack up when evaluated against the traits some claim are necessary for successful market economies?[63] These can include:

  •Is there trust in the individual?

  •Are wealth and resources perceived as finite or infinite? Is the focus on "what exists" or "what does not yet exist"?

  •Is competition seen as healthy or unacceptably aggressive?

  •Is this society comfortable with a questioning mind?

  •Does the education system encourage investigative learning?

- Are the "lesser virtues"—punctuality, job performance, tidiness, courtesy, efficiency – admired?
- Which are emphasized—small achievements accomplished by the end of the day (preferable for market economies) or grandiose projects (the unfinished megaworks of progress-resistant economies)?

- What is the "radius of trust" in this community? Is trust extended to family only? How far does it extend to strangers?[64]
- What are prestige commodities within this community? Why? Might these serve as stronger incentives for cooperation than direct funding?
- Is risk taking admired or negatively sanctioned? How widely spread is the "harm" of individual failure (damages family honor, potentially ignites retribution cycle, etc.)?

Security

- What defines "victory" for this group in a kinetic conflict?
- What types of battlefield behavior would result in shame?
- What level of internal destruction is acceptable?
- How do accepted myths describe this group's military history? What is its projected destiny?
- Are allies viewed as reliable, or historically treacherous? What is the resultant ethic regarding alliance loyalties?

Time/Change Orientation

- Does this group behave according to linear time? Is there a marked contrast between rural and urban regions? Do deadlines matter?[65]
- What is the future orientation of this group? Does it see itself as capable of changing the near future? Is it deemed appropriate or laudable to make aggressive efforts to do so?
- Which time frames are referenced with strong positive emotion—past or future scenarios?
- Is there a significant gap between socioeconomic expectations and reality? (This often is a precursor of social shifts.)[66]

Problem-Solving Devices

- What is the order of activities for solving a social problem (often called an action chain)? Does face-to-face confrontation happen first or last? Is violence used as a signal or is it an endgame?[67]
- How do those outside of official channels of activity (i.e. women in seclusion, youth in elder-oriented cultures) play a part in problem-solving processes?
- Which is preferred—action or deep deliberation? Is this group comfortable with trial and error as a discovery method?
- Are individuals comfortable with making a wide range of personal choices? Are individual choice and accountability practiced social norms? Would the choices present in democratic and market systems be overwhelming?
- To what extent must community consensus be reached in order for a decision to go forward?

Perceptive Lens

Cognitive processes

- What sources of information yield 'truth'? Scientific/factual processes? Dreams?[68] Inspired authority figures?

•Are most situations set into dichotomous frames? Are they made to be black and white? How comfortable are group members with situational complexity? How patient are they in working to understand it?

Of Self

•What are the basic expectations about the future? ("Poverty becomes a greater problem the moment wealth is perceived as a definite possibility.")[69] How might typical aspirations within this society be charted?

•How does this group characterize/perceive its own history? Which events are highlighted? Which are omitted?

•What does this group's history tell it about "dangerous" behaviors/circumstances for a society? (For example, Chinese—chaos, Americans—tyranny).

Of Others Generally

•How do members of this group assign intentions? What motives make the most sense to them? (If the best US intentions do not "make sense" to the host population, they will assign intentions that do. It is to our advantage to understand and then emphasize areas of cognitive congruence when embarking on joint ventures.)[70]

•What is this group's view on human nature? Are people generally trustworthy? Are they prone to excess and beset by vices, or are they able to regulate themselves? How are these views used for legitimating less or more government?

•How does this group obtain its information about the outside world? Which sources are considered most reliable? How are those sources biased or deficient?

•Are outsiders perceived as fundamentally different or fairly similar to group members?

Of the US Specifically

•What are regarded by this group as US vulnerabilities?

•What does this group believe drives Americans?[71] What do they value?

•Does this group see common ground with its American counterparts? In which areas?

•To what extent does this group believe American rhetoric matches intentions?

Cosmology (The way the world works...origin and structure of the universe)

•When explanations for events are not easily accessible, how does this group fill in the blanks?

❖ ❖ ❖

Endnotes

1. J.M. Roberts, *The Penguin History of the World* (London: Penguin Books, 1995), xi–xii.

2. See reviews in this issue of three works on Vietnam, two of which suggest this approach.

3. Special thanks go to David Newcomb.

4. Rob Johnston, *Analytic Culture in the US Intelligence Community: An Ethnographic Study,* (Washington DC: Center for the Study of Intelligence, 2005).

5. Ibid., 75–76.

6. Edward Stewart and Milton Bennett, *American Cultural Patterns: A Cross-Cultural Perspective* (Yarmouth, ME: Intercultural Press, 1991), 11.

7. Johnston, *Analytic Culture*, 66.

8. Richards Heuer, *Psychology of Intelligence Analysis (*Washington DC: Center for the Study of Intelligence, 1999), 21.

9. MG Michael T. Flynn (USA) et al., *Fixing Intel: A Blueprint for Making Intelligence Relevant to Afghanistan* (Washington, DC: Center for a New American Security, 2010)

10. Johnston, *Analytic Culture,* 8.

11. Ibid., 84.

12. Christopher Twomey, "Lacunae in the Study of Culture in International Security," *Contemporary Security Policy* 29 no. 2 (August 2008): 338–57.

13. Patrick Porter, *Military Orientalism: Eastern War through Western Eyes*, (London: Hurst & Co, 2009)

14. Walter Russell Mead, *Special Providence: American Foreign Policy and How it Changed the World* (New York: Alfred A. Knopf, 2001), xvii.

15. Anja Dalgaard-Nielsen, "The Test of Strategic Culture: Germany, Pacifism and Pre-emptive Strikes," *Security Dialogue* 36, no. 3 (September 2005): 339–59; Huiyun Feng, "A Dragon on Defense: Explaining China's Strategic Culture," in *Strategic Culture and Weapons of Mass Destruction: Culturally Based Insights into Comparative National Security Policymaking*, eds. J. L. Johnson, K. M. Kartchner, and J. A. Larsen (New York: Palgrave Macmillan, 2009), 171–88; Rodney Jones, "India's Strategic Culture and the Origins of Omniscient Paternalism," ibid., 117–36; Afshin Molavi, *The Soul of Iran: A Nation's Journey to Freedom*, (New York: W.W. Norton and Company, 2002).

16. Kevin Avruch, *Culture and Conflict Resolution*, (Washington DC: United States Institute of Peace Press, 1998), 15.

17. Dalgaard-Nielsen, "The Test of Strategic Culture," 342.

18. Barak A. Salmoni and Paula Holmes-Eber, *Operational Culture for the Warfighter: Principles and Applications*, (Quantico, VA: Marine Corps University Press, 2008), 13.

19. J. Avalos, discussion with author Jeannie Johnson, 2006.

20. C. Boyd, discussion with author Jeannie Johnson, 2006

Endnotes (cont.)

21. Tim Judah, *The Serbs: History, Myth and the Destruction of Yugoslavia,* (New Haven: Yale University Press, 2000), 39–47.

22. Author Jeannie Johnson was part of the team conducting intelligence analysis of Serbia and surrounding countries.

23. K. Moss, discussion with author Jeannie Johnson, 2006.

24. W. Stanley, discussion with author Jeannie Johnson, 2006.

25. H. Russell Bernard, *Research Methods in Anthropology: Qualitative and Quantitative Approaches* (Walnut Creek, CA: Alta Mira Press, 2002), 188–93.

26. Ibid., 190.

27. S. Kjar, discussion with author Jeannie Johnson, 2006.

28. Gregory Giles, discussion with author Jeannie Johnson, 2006. See Gregory Giles, "Continuity and Change in Israel's Strategic Culture," in Johnson et al., *Strategic Culture and Weapons of Mass Destruction*, 97–116.

29. W. Stanley, discussion with author Jeannie Johnson, 2006.

30. Molavi, *The Soul of Iran*.

31. C. Boyd, discussion with author Jeannie Johnson, 2006.

32. Stephanie Kelley, "Rumors in Iraq: A Guide to Winning Hearts and Minds," *Strategic Insights,* 4 (2005). This journal, published by the Naval Postgraduate School's Center on Contemporary Conflict, is available on that organization's website www.nps.edu/Academics/centers/ccc/publications/OnlineJournal/2005/Feb/kelleyfeb05.html

33. Deborah Wheeler, discussion with author Jeannie Johnson, 2006.

34. Christine Fair, "Iran: What Future for the Islamic state?," in Angel M. Rabasa et al., *The Muslim World After 9/11* (Santa Monica, CA: The RAND Corporation, 2004), 244.

35. V. Daniels, discussion with author Jeannie Johnson, 2006.

36. W. Stanley, discussion with author Jeannie Johnson, 2006.

37. Rodney Jones, discussion with author Jeannie Johnson, 2006.

38. Joe Bermudez, discussion with author Jeannie Johnson, 2006.

39. J. Moyes, discussion with author Jeannie Johnson, 2006.

40. S. Taylor, discussion with author Jeannie Johnson, 2006.

41. W. Stanley, discussion with author Jeannie Johnson, 2006.

42. Christopher Twomey, discussion with author Jeannie Johnson, 2006.

43. A. Haycock, discussion with author Jeannie Johnson, 2006.

44. Fritz Ermarth, discussion with author Jeannie Johnson, 2006.

45. Christopher Twomey, discussion with author Jeannie Johnson, 2006.

46. Andrew Cortell and James Davis, "Understanding the Domestic Impact of International Norms: A Research Agenda," *International Studies Review* 2, no. 1 (2000), 65–87; Paul Kowert and Jeffrey Legro, "Norms, Identity, and their

Endnotes (cont.)

Limits: A Theoretical Reprise", in *The Culture of National Security,* ed. Peter Katzenstein (New York: Columbia University Press, 1996), 451–97.

47. Glenn Chafetz, Hillel Abramson, and Suzette Grillot, "Culture and National Role Conceptions: Belarussian and Ukrainian Compliance with the Nuclear Proliferation Regime," in *Culture and Foreign Policy*, ed. Valerie Hudson (London: Lynne Rienner, 1997), 175. The authors also offer a list of seven typologies unlikely to engage in illegal proliferation. The National Role typologies are slightly modified versions of those proposed by Kal Holsti. See Kal Holsti, "National Role Conception in the Study of Foreign Policy," *International Studies Quarterly* 14 (1970): 233–309.

48. G. Lawrence, discussion with author Jeannie Johnson, 2006.

49. D. Anderson, discussion with author Jeannie Johnson, 2006.

50. L. Wilde, discussion with author Jeannie Johnson, 2006.

51. A. Richey, discussion with author Jeannie Johnson, 2006.

52. Lera Boroditsky, "Lost in Translation," *Wall Street Journal*, 24 July 2010.

53. Peter Hays Gries, *China's New Nationalism: Pride, Politics, and Diplomacy*, (Berkeley, CA: University of California Press, 2005); Ted Hopf, *Social Construction of International Politics: Identities and Foreign Policies*, (Ithaca, NY: Cornell University Press, 2002).

54. G. Giles, discussion with author Jeannie Johnson, 2006.

55. Christopher Meyer and Adrian Zdrada, "Unpacking the 'Coalition of the Willing': A Comparative Analysis of Norms in British and Polish Press Debates on the Iraq Invasion," *European Security* 15 (2006): 23–45

56. D. Anderson, discussion with author Jeannie Johnson, 2006.

57. C. Curtis, discussion with author Jeannie Johnson, 2006.

58. Jeffrey W. Legro, *Cooperation Under Fire: Anglo-German Restraint during World War II* (Ithaca, NY: Cornell Univ. Press, 1995); Legro, "Which Norms Matter? Revisiting the 'Failure' of Internationalism," *International Organization* 51 (1997): 31–63. Kowert and Legro, "Norms, Identity, and their Limits," 451–97.

59. Thomas Hylland Ericksen, *Small Places, Large Issues: An Introduction to Social and Cultural Anthropology*, 2nd ed. (Sterling, VA: Pluto Press, 2001), 54–55; Stewart and Bennett, *American Cultural Patterns*, 129–38.

60. Glen Fisher, *Mindset: The Role of Culture and Perception in International Relations*, 2nd ed. (Yarmouth, ME: Intercultural Press, 1997), 95.

61. For examples, see ibid., 52, 64.

62. For discussion, see Ericksen, *Small Places, Large Issues*, 155.

63. Mariano Grondona, "A Cultural Typology of Economic Development" in *Culture Matters: How Values Shape Human Progress*, eds. Lawrence E. Harrison and Samuel P. Huntington (New York: Basic Books, 2000).

64. The basic theory: the wider the radius of trust, the easier to engage in economies of scale market economics. See Francis Fukuyama, "Social Capital" in *Culture Matters*.

Endnotes (cont.)

65. A nice discussion of time orientations and why they matter can be found in Stewart and Bennett, *American Cultural Patterns*, 73–76.

66. For diverse examples see Fisher, *Mindset*, 52.

67. A nice discussion of this, with diverse examples, can be found in Edward T. Hall, *Beyond Culture* (New York: Anchor Books, 1989), 157–59.

68. Stewart and Bennett provide an interesting insight on this point in *American Cultural Patterns*, 62–65.

69. Ericksen, *Small Places, Large Issues*, 251.

70. For good examples, see Fisher, *Mindset*, 52.

71. Americans tend to overemphasize similarity. See Stewart and Bennett, *American Cultural Patterns*, 11.

❖ ❖ ❖

An Educated Consumer Is Our Best Customer

Dennis C. Wilder

This essay was a recipient of the top prize in the 2010 Galileo Intelligence Community Award competition. The competition, held annually since 2004, is intended to provide active members of the Intelligence Community opportunities to put forward innovative ideas.—Editor

> ***"The quality of service a consumer receives from the IC depends heavily on the expertise and experience that the policymaker or legislator brings to their interaction with the IC."***

It may seem odd to title a paper on Intelligence Community (IC) innovation in the 21st century with the commercial slogan made famous by discount clothier Sy Syms. But this slogan holds the key to solving some of the challenges vexing IC leaders that span issues from policymaker expectations to intelligence budgets to public perceptions of the IC. At the core of this paper is the contention that we have neglected the education of our customers—defined as appointed and elected officials and the American public—to our own detriment. The quality of service consumers receive from the IC depends heavily on the expertise and experience that policymakers or legislators bring to their interaction with the IC. Our chronic failure to communicate across the policy-intelligence divide has led to pent-up frustrations on both sides and, too often, charges of intelligence failure. This proposal provides a series of recommendations for the ODNI on redesigning the policy-intelligence interface and implementing a strategic communications strategy that leverages new social media so that the American people and the policy community will better understand and appreciate the centrality of the Intelligence Community to national security.

Taking Our Customers' Knowledge of Us for Granted

Policymakers who are steeped in the ways of the Intelligence Community (IC) know how to get superior service and support. Former Acting Director of Central Intelligence John McLaughlin, from his years of experience, explained the savvy policy consumer of intelligence this way:

> *Policymakers who knew how to use intelligence generally had a realistic view of what it could and could not do. They understood, for example, that intelligence is almost*

All statements of fact, opinion, or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

Too often policymakers with no or little exposure to the IC, especially in the case of the novice policymakers, find themselves in a frustrating maze.

> *always more helpful in detecting trends than in predicting specific events. They knew how to ask questions that forced intelligence specialists to separate what they actually knew from what they thought. They were not intimidated by intelligence that ran counter to the prevailing policy but saw it as a useful job to thinking about their courses of action.*[1]

My observations during more than four years of service on the National Security Council have led me to conclude that policymakers with no or little exposure to the IC, especially in the case of novice policymakers, too often find themselves in a frustrating maze that involves trial and error and dead ends in their attempts to get the right kind of intelligence support. This inexperience can, and has, led to serious policymaker disappointment with IC products not because the IC did not have the correct information or analytic insights to offer, but because the consumer did not have the sophisticated understanding of IC capabilities and limitations that would allow them to ask the right questions, of the right people and at the right moment to get the best information and analysis. Frequently, this has led to charges of intelligence failures because the policymakers had unrealistic expectations of what the IC could do.

What we have is a failure to communicate across the IC-policy community divide. Gregory Treverton, a senior RAND scholar of the intelligence-policy interface had a particularly useful explanation of why IC experts typically fail to meet the expectations of eager, new policymakers out to change the course of history.

> *Intelligence analysts are reflective by nature; they want to understand…. Policy officials, by contrast, tend to be active; they want to do, not just to think. They came to Washington to signify; they want to make a difference…. If policy officers are to signify, they have to do so quickly; the average tenure of an assistant secretary is not much more than a year.*[2]

The First Customer Will Always Come First

Who are the IC's customers? Our most important customer is and will remain the president. He is well served through his direct relationship with the director of national intelligence and he, each day, receives the finest intelligence publication in the world, the *President's Daily Briefing* (PDB). The history of the PDB is one of flexibility and remarkable adaptation of support to fit each president's needs and information acquisition styles.[3]

I would argue, however, that historically we have not done justice to the rest of our customers, from policymakers below the president to the members of the US Congress to the American public, in large measure because we have neglected educational outreach and strategic communications. Without such outreach, and in a decade when massive deficits burden the national budget and the competition for resources in the federal government will intensify, we are in danger of repeating the disaster that befell us at the

---

[1] John McLaughlin "Serving the National Policymaker," in Roger Z. George and James B. Bruce (eds.), *Analyzing Intelligence: Origins, Obstacles, and Innovations*, 2nd Edition, (Washington, DC: Georgetown University Press, 2008), 72.

[2] Gregory F. Treverton, *Intelligence for an Age of Terrorism* (Rand Corporation, Cambridge University Press, 2009), 170–71.

[3] For an excellent example of the kind of close attention that has been paid to getting analysis right for presidents, see John Helgerson, *CIA Briefings for Presidential Candidates*, (Washington, DC: Center for the Study of Intelligence, CIA, 1996).

end of the Cold War with the advent of the peace dividend—debilitating budget cuts, dangerously slashed human intelligence capabilities, and even debate about the necessity of the US Intelligence Community, the most expensive intelligence enterprise on the planet.

In the decade after 9/11, the IC has demonstrated the centrality of intelligence to policy, but that position may not be secure as the memory of 9/11 fades and as we enter an era of belt tightening. The new reality that the US foreign policy establishment, and by extension the IC, faces is spelled out in a thought-provoking book by Michael Mandelbaum in which he warns that because of domestic obligations this country faces, particularly caring for the ever increasing ranks of its older citizens, "The defining fact of foreign policy in the second decade of the 21st century and beyond will be 'less.'"[4] Thus, we are living in an era that none of us has ever experienced because, unlike most countries, our economic constraints have not affected US foreign policy decision-making for the past seven decades.

How do we encourage deeper policymaker literacy about the IC?

Informed Policymakers

How do we encourage deeper policymaker literacy about the IC? Brookings Institution in 2009 published a thoughtful study by Ken Lieberthal—a former special assistant to a president, senior director on the NSC, and a long-time student of intelligence—analyzing the strengths and shortcomings of the IC in the wake of the 2004–2005 intelligence reforms that provides some clues. Liberthal reported from his interviews with then active and former policymakers and intelligence professionals that most policymakers are undereducated in the use of intelligence and have no systematic understanding of the IC or of the products they receive from the IC. Moreover, he contended that most policymakers are ill equipped to ask the right questions and therefore ask for briefings on topics that often elicit "a relatively standard bureaucratic process that pulls together pertinent information and lays it out without serious attention being given to priorities, underlying uncertainties, and real insights."[5]

Such products, the author argued, are useful to a policymaker needing to get up to speed on a topic, but they tend not to force IC analysts to think through the implications of their data, debate the relative significance of different facts, and make explicit their levels of confidence in the responses they produce. *In short, because our consumers are not well schooled in what we can provide, we often fall short of helping them make deeply informed policy recommendations to the president and his Cabinet.*

What can be done to create intelligence-literate policy customers? First, we need to understand that educating the customer is an extremely difficult task that we have never done well. We have avoided tackling the issue because it can seem condescending and can lead to charges of attempts to politicize the relationship. Beginning with the legendary Sherman Kent, we have analyzed exhaustively every aspect of the IC side of the relationship with the policymaker, and we have set up high firewalls not to be crossed between the policymaker and the IC producers.[6] We have as a result, after each perceived intelligence failure, studied carefully what the IC did that led to that intelligence mistake and then carefully schooled our officers to

[4] Michael Mandelbaum, *The Frugal Superpower: America's Global Leadership in a Cash-Strapped Era*, (New York:Public Affairs, 2010).

[5] See Dr. Kenneth Lieberthal, *The U.S. Intelligence Community and Foreign Policy: Getting Analysis Right*, (Brookings Institution, Foreign Policy Paper Series, Number 17, September 2009), 56.

I believe some of our problems only can be ameliorated by radically revising our interaction with new administrations from the moment that presidential candidates are selected.

help them discern what constitutes success and failure in intelligence analysis.

But I am unaware of any effort to systematically study the policymaker's role in either intelligence successes or intelligence debacles. Most often, if policies work out, policymakers will assume that it was their hard work that made the difference and, unfortunately, if there is a policy debacle there is a strong tendency to blame the community.

We know what we could have done better on the Iraq WMD issue because we have written excellent studies of our shortcomings, and we have appropriately implemented systematic changes to our analytic tradecraft. *I am, however, unable to find any parallel effort, either within government or in academia, to systematically educate current and future policymakers to maximize the utility of intelligence* and to ask the right questions to avoid policy failures because of inadequately tapping of the capabilities of the IC. James Steinberg, currently deputy secretary of state, lamented this lack of attention to the issue in 2008 saying, "Given the enormous consequences of the evident breakdown apparent both in the September 11 and Iraq events, it is vital that practitioners on both sides try to understand the challenges inherent in the policy-intelligence interaction and how to overcome the gulf and suspicion that haunts this critical relationship."[7]

Designing a New Relationship with the White House

I believe some of our problems only can be ameliorated by radically revising our interaction with new administrations from the moment that presidential candidates are selected by their political parties and are given their first national security briefing. This is the point at which the relationship with the next president and his core national security team—in effect, his national security players in waiting—forms and needs to be shaped with briefings not only on top national security concerns, but on how we would propose to help the team prepare to use intelligence more efficiently and effectively than any past administration through a deliberate and thoughtful education process.

Obviously, this new process of education is far more complex than what I just outlined and so let me present some of the foundational work that needs to be done in advance of such an opportunity. Now in our third year of the Obama administration and with a new Congress, we have new faces involved in security policy. If the past is any indicator, too many of these new officials will have come into office, eagerly been read into their top secret codeword clearances, and started reading daily intelligence with only the most superficial understanding of what it is they are reading. Many will immediately be disappointed because they had convinced themselves that, once they got their clearances, they would see the "real secrets." If they are lucky enough to have a personal briefer, this will help but too often the briefers themselves are young and only steeped in the intelligence analysis side of this question.

Creating Intelligence Connoisseurs

What is required is the equivalent of the course now taught for analysts on the art of intelligence analysis, but this would

[6] For an example, see the incisive article written by CIA analyst Jack Davis on the history of the debates over how to serve the policymaker, "The Kent-Kendall Debate of 1949," in *Studies in Intelligence* 1992, Issue 5.

[7] James B. Steinberg, "The Policymaker's Perspective: Transparency and Partnership" in George and Bruce, *Analyzing Intelligence*, 83.

be for policymakers and members of Congress—let's call it, *Applied Intelligence for the Savvy Policymaker.* With today's technology we are capable of deploying such a course in various appealing media formats to include interactive online presentations. This course would not just be given by intelligence professionals but co-taught with former policymakers willing to share the lessons they have learned in working with the IC. Ideally, new policymakers in the future would want to take this course because it would be known to provide them a sophisticated understanding of the IC under the ODNI. Demand for the course would be high if it were known that the president and his cabinet had endorsed it.

Any attempt to design this course for new policymakers and members of Congress that in exclusively done in-house is vulnerable to charges of IC attempts at propaganda and proselytizing. Also, we have simply not developed a deep enough understanding of the topic ourselves to provide a rich and systematic briefing at this point. Thus, the director of national intelligence should ask prominent former officials from both major parties to lead a task force to develop such a course. Former officials such as Congressman Lee Hamilton, Deputy Secretary of Defense John Hamre and National Security Advisor Steve Hadley,

To provide the intellectual rigor needed to undergird a course for new policymakers and Congress, the DNI also should seek out a partnership with prominent think tanks and relevant academic institutions.

Director of National Intelligence John Negroponte, Deputy Secretary of State Thomas Pickering, US Trade Representative Charlene Barshevsky, Chairman of the Joint Chiefs of Staff Peter Pace, DCIA Michael Hayden, DCI George Tenet, and Acting DCI John McLaughlin spring to mind but there are, of course, many others with the requisite expertise.

Partnering with the Private Sector

To provide the intellectual rigor needed to undergird a course for new policymakers and Congress, the DNI also should seek out a partnership with prominent think tanks and relevant academic institutions that span the political spectrum to design case study materials from past policy successes and failures analyzing how policymakers either got the best or inadequate support from the IC.

This process would require extensive interviews with those who were intimately involved in the intelligence support and policymaking during the period studied. Such an effort would be open to suspicion if it was done in house and the academics would need access to the classified record. *To avoid rancor, the case studies might avoid recent politically charged controversies such as the issue of intelligence support to decision making on Iraq WMD but could be just as useful if done on such issues as IC support to policymakers on the Soviet Union or intelligence support during the Kosovo conflict.*[8]

Once case studies are drafted, it would be in the best interest of the IC to present them to a conference of academics and policymakers, current and former, at a symposium for a reality check and fine-tuning. Such a symposium might be appropriately convened at one of the presidential libraries and perhaps carried on CSPAN television, providing the added benefit of educating the general public on this new initiative.

Net Gens and Unauthorized Disclosures

One final important aspect of this tutorial would be a frank discussion of the damage

[8] IC assessment of the Soviet Union is attractive as a topic because it has already been extensively studied from the IC side. For example, see Douglas J. MacEachin, *CIA Assessments of the Soviet Union: The Record Versus the Charges*, (Washington, DC: Center for the Study of Intelligence, CIA, 1996).

The general public's understanding of the IC and its mission and capabilities is equally worrisome.

caused by unauthorized public disclosure. We should take heed of the implications of the recent arrest and arraignment of the 22-year-old member of the US military on charges of unauthorized disclosure of the classified information revealed through Wikileaks. He is a member of Net Gen, the generation of children, teens, and young adults aged 11 to 31 who have grown up immersed in digital technology. He allegedly downloaded a staggering 260,000 documents because he hoped their release would lead to a "worldwide discussion, debate, and reform" of the tactics in the war on terror.[9] The younger generation, whether policymakers or members of the IC, come into government with much more opens view of information and information sharing and need help understanding our unique issues.[10] Thus, the course should include a discussion of the enormous damage to US security and the financial costs to the American taxpayer when unauthorized disclosures result in damage to sensitive intelligence collection capabilities. To be effective, such a course should be open with policymakers and members of Congress in discussing the specific, recent examples of unauthorized leaks and the damage they have inflicted.

An Informed Public

The general public's understanding of the IC and its mission and capabilities is equally worrisome. All of us have experienced the uneasy feeling as we watched our profession personified by Hollywood as either the omnipotent Jack Bauer or the bumbling Maxwell Smart. At times we are portrayed as flagrantly violating the US Constitution and abusing the human rights of US citizens and foreigners alike. At other times, we are portrayed as laughingly incompetent or, worse yet, creating wars and crises because we act in secret without oversight. Few and far between are the accurate portrayals of the critical mission of the IC as the "Silent Service," going where others cannot go, risking our lives to protect Americans from harm, and providing the needed raw and finished intelligence products to inform and elevate policy deliberations.

Middling Public Approval Ratings

It is therefore not surprising that public opinion polling consistently shows that elements of the IC typically glean only about a 50-percent approval rating from the general public. This contrasts starkly with the various armed services and the FBI, which routinely poll at least 15 percentage points higher than the CIA in public opinion surveys.[11] Surveys do not even try to measure the public approval for the ODNI since there is very little public recognition of the name and almost no general understanding of its role. In the aftermath of 9/11, it seems counterintuitive and surprising that we have gained little in public approval ratings despite our large role in the battle with terrorists and the fact that intelligence has played a vital role in making sure that another 9/11 has not happened. Many IC officials have pointed to the large number of excellent resumes received each year by the IC to demonstrate that our public image is strong, but this indicator may say as much about the state of the job market and the glamorized Hollywood vision of the IC as it says about public attitudes.

Why does our public image pale in comparison to that of the armed services? To be fair, a part of our problem is simply

[9] Kevin Poulsen, Kim Zetter, "I can't believe what I am confession to you: The Wikileaks Chats," *Wired Magazine online*, 6 June 2010.

[10] For an excellent study of the challenges we face in the information age see *Where Tomorrow Will Take Us: The New Environment for Intelligence,* (Washington, *DC:* Center for the Study of Intelligence, CIA, 2010).

[11] See for example, "Distrust, Discontent, Anger and Partisan Rancor: The People and Their Government," Pew Research Center for the People and the Press http://people-press.org/2010/04/18/distrust-discontent-anger-and-partisan-rancor/ (accessed 9 May 2011).

Part of the problem is that we have not worked hard enough at strategic communications with the general public.

that we must operate under the cloak of secrecy and are therefore perceived as a bad fit for an open democracy. As Secretary of Defense Robert Gates recently put it when speaking about the CIA, "The truth is, across the political spectrum, it has had relatively few supporters other than presidents who find they like its clandestine powers. It's just an itch in our system that's hard to scratch."[12] *Secretary Gates may be a bit too fatalistic about our lot, and I believe it is this kind of presumption that holds us back from exploring new ways to convince Americans that we are not an anomaly but a necessity in American democracy.* To me, part of the problem is again that we have not worked hard enough at strategic communications with the general public. Too often, we allow others to define us (mostly negatively) by making it sound as if the sum total of our role can be summarized by referring to such controversies as Abu Ghraib and water boarding.

Reengineering Our Public Profile

Although some argue that the IC by its very nature should not have a public profile, that philosophy may be outdated in the age of new social media**.** *Frankly speaking, we only need to look at the outmoded design of www.dni.gov website in comparison to the websites of the Department of Defense or even the Defense Intelligence Agency to see that we are not communicating as well as we could with the public. Here are a few other ideas on developing stronger public insight into the IC:*

- *Internet Chats with IC experts.* Many executive branch agencies, including the White House, offer the public the opportunity for periodic on-line chats with administration officials on topics of wide interest. This is also being done with regularity by major academic think tanks. There is no reason that the ODNI and other IC leaders could not do the same under carefully controlled circumstances. National intelligence officers (NIOs) and other top-notch experts could provide on-line chat opportunities on important topics of the day to the general public. For example, the NIO for South Asia might field questions from the public on the implications of the floods in Pakistan or the NIOs for economics and East Asia might discuss the implications of China's recent emergence as the world's second largest economy. On-line chatting of this sort allows for the public to submit questions in advance so that they can be screened for any politically sensitive or inappropriate questions.

- *Outreach to Local Officials and Emerging Leaders.* It is striking when meeting with officials at the state and city level around this nation how little contact most have with the IC, beyond the FBI. Similarly, most politicians only have an association with the IC if they serve in Washington. Although there is a natural IC reluctance to hold town-hall meetings with the general public on intelligence, by invitation seminars for local officials and emerging politicians would expose them to our issues long before they became Washington policymakers. This kind of seminar is a proven formula that IC elements have used for recruiting sessions with students at universities and colleges.

- *An Official Guidebook to Intelligence***.** The CIA *World Factbook* is a wonderful resource to the general public that is heavily used on line. Although the DNI publishes the "A Consumer's Guide" to intelligence, the document is primarily intended for senior intelligence consumers in the US government and is not particularly user friendly for the general public. Creation of a general guidebook might be best accomplished by commissioning a prominent, profes-

[12] David Ignatius, "Gates: The Pentagon's Accountability Cop," *The Washington Post*, 9 September 2010.

There is one major aspect of intelligence policy that needs a clear rethinking…the bright line we have drawn over the years between intelligence and policy.

sional writer outside of the IC to write an unclassified guide that captures more fully what the uninitiated would want to know.[13]

- *Greater Publicity to Our Role in Supporting the Military.* Part of the public's high respect for the armed forces comes from their long traditions of service to the nation. Most Americans can hum the tune of the Marine Corps Hymn. The tradition of intelligence support to the military began with General George Washington, but the public perception is that the IC is only about 60 years old. While I am not suggesting uniforms and salutes, I am suggesting that we look harder at those things we might do to make ourselves more associated with proven, military traditions. One such effort is a recent *Studies* special edition, *CIA at War,* which commemorates the work of CIA men and women in conflict zones around the world since the Agency's creation.

Perceived Intelligence Failures Are Inevitable

A final reason I would cite on why strategic communications to the public is important going forward is this simple fact —there will be successful terror strikes on US soil in our future, and they may even involve the use of weapons of mass destruction. *We need only look at the major outcry against the IC that occurred after the failed terrorist attempt to blow up a commercial airliner last December to see a glimpse of the kind of blame game that is likely to engulf the IC when the next successful foreign terrorist attack occurs.* As two prominent British observers of our profession sagely put it, "Intelligence failure is a matter of expectations, and seeking to adjust expectation of what intelligence can and cannot do is surely essential to informed democratic debate. Yet if and when a catastrophic terrorist attack succeeds, public confidence in the intelligence and security services will inevitably be tested."[14] We cannot afford to wait passively for that test to come before we try to shape public expectations and understanding of what we do.

Confronting a Taboo

As we begin a new century there is one major aspect of intelligence policy that needs a clear rethinking in consultation with the Executive Branch and the US Congress. This is the bright line we have drawn over the years between intelligence and policy. Sherman Kent was adamant in his belief that intelligence analysis is a service arm to policymakers and that it should not be a formulator of objectives, a drafter of policy, or a maker of plans. But increasingly today, policymakers and legislators find that the intelligence analysts' adherence to this article of faith robs the policymaker of the ideas and suggestions for policy that a highly informed analyst can provide. They often complain that briefings that provide just the facts are simply not relevant and helpful enough. They can get the facts off of the Internet at a greater speed than we can deliver them, but what they crave from us is analytic insight and our thoughts on how US foreign policy can be advanced.

I believe former DNI Dennis Blair took a large step toward toning down the bright line when in a media roundtable in March 2009 he told the press that he had mandated that every piece of analysis on important issues not only have a threat analysis section but also an opportunities analysis section. He described opportunity analysis as helping policymakers "find the levers…which will enable us to advance our interests and our common interests."[15] Despite his pronouncement, opportunities analysis remains uncomfortable and controversial in many IC

[13] The DNI guide is located at http://www.dni.gov/reports/IC_Consumers_Guide_2009.pdf.

[14] Len Scott and R. Gerald Hughes, "Intelligence in the 21st Century," *Intelligence and Security* 24, No. 1 (February 2009), 24.

components. Analytic managers are far too concerned that providing some suggestion on policy options will taint analysis and destroy its purity. Yet in most of the advanced intelligence services around the globe no such bright line is drawn. And, I would argue, this bright line robs the policymaker of some of the most useful byproducts of analytic depth and sophistication.

We have consistently not prepared our customers to use intelligence wisely, and thus we are afraid of what they will do with even guarded policy inputs. Were we better at in-depth communication with our customers, we could jointly set parameters on opportunity analysis that would protect the IC from accusations of politicization or meddling in policy. In this regard, I am reminded of Secretary of State Colin Powell's famous adage that demonstrates his sophisticated understanding of the role of intelligence:

> *I will hold you* [the intelligence expert] *accountable for what you tell me is a fact; and I will hold you accountable for what you tell me is not going to happen because you have the fact on that, or you don't know what's going to happen, or you know what your body of ignorance is and you told me what that is. Now when you tell me what's most likely to happen, then I, as the policymaker, have to make a judgment as to whether I act on that, and I won't hold you accountable for it because that is a judgment; and judgments of this kind are made by policymakers, not by intelligence experts.*[16]

I recognize that many will argue that, if we cross the divide, we will lose our analytic objectivity and integrity. I think that this was more of a problem when we were just beginning after World War II to create the craft of intelligence analysis. That craft is now well developed, and we have a keen sense of how to keep our integrity**.** *My worry is that, if we continue to defend a rigid line of detachment from policy, we will lose our reason for existence—the opportunity to elevate the policy debate.* Policymakers have often stated that, when the IC becomes a part of a policy-intelligence task force working a particular problem, the intelligence provided becomes much better targeted to assist the policymaker. This is in part because, when we stay outside the policy circles, we have less understanding of what is really needed. Whereas when we are in the circle, we are better able to target our resources and analysis to the exacting needs of the moment.

My worry is that, if we continue to defend a rigid line of detachment from policy, we will lose our reason for existence—the opportunity to elevate the policy debate.

This brings me to my final recommendation and that is the need for a *Center for the Study of the Intelligence Innovation administered by the ODNI.* As noted above, we can do a great deal by reaching out to former officials, the academic community and think tanks for help on educating our consumers. But ultimately we should have a permanent staff of professionals who study this centrally important question on a continuing basis. The Center for the Study of Intelligence (CSI) at CIA provides a good model for this activity and is adapting to widen its focus beyond CIA. CSI recently has begun assuming the IC's Lessons Learned and history functions and is thus taking a greater community role. Policymaker needs are dynamic and change quickly because of the flow of world events and rapid technological advances. If we are to remain relevant, we cannot neglect serious study of the policy-intelligence interface.

❖ ❖ ❖

[15] Media roundtable with DNI Dennis Blair. 26 March 2009. Available at: http//www.dni.gov/interview/20090326_interview.pdf. For another challenge to the taboo, see Josh Kerbel and Anthony Olcott, "The Intelligence-Policy Nexus: Synthesizing with Clients, Not Analyzing for Customers," *Studies in Intelligence* 54, No. 4 (December 2010).

[16] Secretary Colin L. Powell, "Testimony before the Senate Governmental Affairs Committee," 13 September 2004.

The Pursuit of Intelligence History: Methods, Sources, and Trajectories in the United Kingdom

Christopher R. Moran

This article is an overview of the history of the academic study of intelligence in the United Kingdom since 1945, a time marked by three distinctive periods of historiography. Each, labelled here as Absence, Emergence, and Efflorescence, has contained unique themes and approaches to intelligence history as it has been practiced in Britain.[a]

> ***"Clarity has come to intelligence history much like the restoration of an aged fresco."***

Clarity has come to intelligence history much like the restoration of an aged fresco in which hidden details are gradually revealed through repeated cleansings until a full-bodied picture emerges. Attempts to establish the history of British intelligence have ranged greatly in style and quality, from the lurid works served up by the media and by the purveyors of conspiracy theory (appropriately described by Nicholas Hiley as "lightweight meals that sit so heavily on the stomach"),[1] *to the tomes, written by official historians and born of patient work in archives and historical scholarship.*

Writers on intelligence have been a fissiparous bunch, their focus and approach shaped to a large extent by forces and events in the real world. In the 1960s and 1970s, as public fascination with and fear about espionage grew exponentially following a string of high-profile fiascoes (including the U-2 spy plane incident in May 1960, the abortive Bay of Pigs invasion in April 1961, the John Vassall spy case in 1962, and the Profumo Affair in 1963), many authors made their names by looking at scandal.

For the likes of Andrew Boyle— whose book The Climate of Treason: Five who Spied for Russia *led to the public unmasking in 1979 of Anthony Blunt as a former Soviet agent—writing intelligence history was both a professional and a political activity, designed to shake the Establishment by shining a harsh and bright light on its unethical*

---

[a] This article is an adaptation of a chapter written by the author for *Spooked: Britain, Empire and Intelligence since 1945* (Cambridge, UK: Cambridge Scholar Publishers, 2009). Prepared with the permission of the publisher.

The endnotes are available in the digital version of the article in cia.gov.

All statements of fact, opinion, or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

Secret service work was wreathed in a miasma of secrecy; its practitioners were spectral figures, known only to their exclusive fraternal initiates.

practices.[2] *In the mid- to late 1970s and then into the 1980s, as governments lifted the lid on Allied codebreaking successes during the Second World War, so historians paid much closer attention to the role of intelligence. Similarly, in the 1990s, as the British intelligence services themselves began to edge toward the light—they were first listed in the statute books, for example, and began declassifying hitherto secret records—so the nascent discipline of intelligence studies entrenched itself in academia.*

In the 21st century, the history of Britain's intelligence services has enjoyed a revival in the wake of the terrorist attacks of 9/11, Madrid, and London, as well as the conflicts in Iraq and Afghanistan. Thanks to the spooks of today, the spies of the past are no longer the supporting cast in some larger drama of international relations but are front and center on the historical stage.

Intelligence history, while presently booming, is fast approaching another tipping point. With the official histories of the Security Service (MI5), the Secret Intelligence Service (SIS/MI6) and the Joint Intelligence Committee (JIC) hitting bookshops in 2009, 2010, and 2013 respectively, much of the original fresco will have been restored. For the intelligence historian, therefore, plotting the future of the past has never been more important.

Absence

For a long time, intelligence history was the Cinderella of disciplines of history, starved of recognition and marginalized by its more successful scholarly sisters. In 1984, Christopher Andrew and David Dilks famously described intelligence as the "missing dimension" in historical inquiry, conspicuous in its absence from the literature of both modern government and international relations.[3] Filling this significant lacuna was a task for which few serious historians had the stomach. Throughout much of the 20th century, the UK intelligence community was the "invisible man" of government, a state within a state, and an entity about which questions were never asked, even in Parliament.

Secret service work was wreathed in a miasma of secrecy; its practitioners—like members of a collegiate society—were spectral figures, known only to their exclusive fraternal initiates. "It is the essence of a Secret Service," declared Sir Austen Chamberlain (then foreign secretary) in December 1924, "that it must be secret, and if you once begin disclosure it is perfectly obvious to me as to honorable members opposite that there is no longer any Secret Service and that you must do without it."[4]

Governments, irrespective of their political persuasion, refused to avow the very existence of the intelligence agencies. As Sir Frank Newsam (then Home Office permanent undersecretary) wrote in October 1952: "I was brought up in the tradition that the existence of the Security Service should never be mentioned save in the highest circles, and, for a very long time, I never knew its address and have only recently entered its portals."[5] It was often said that the British attitude toward intelligence mirrored societal attitudes toward marital sex; that is, everyone knew that it went on, but to "speak, write or ask questions about it" was not done.[6]

Much to the chagrin of independent historians, the taboo of secrecy surrounding intelligence was undergirded by the indefinite closure of service records. No matter how old or how sensitive, all documents that referred to intelligence found themselves in a historical never-never land, withheld indefinitely from release to the Public Record Office (PRO), now The National Archives (TNA).[7] Section 3 (4) of the Public Records Act (1958, 1967), otherwise known as the "blanket" exemption, gave the

With historians deprived of documents and governments determined to choke off public debate, the "history" of Britain's intelligence services was written largely by investigative journalists and "exposé merchants."

lord chancellor discretionary power to hold back any file related to intelligence or the intelligence services. In 1982, the Wilson Committee on Modern Public Records highlighted absurd examples of closed material, including postal intercept files from the 18th century and intelligence bulletins from the Battle of Waterloo. The dearth of primary source material discouraged even the most intrepid historian, to whom accessible documentation was the lifeblood of good scholarship.

Keeping the intelligence services walled off from public view was generally defended on the grounds of operational security. The agencies claimed, with some justification, that intelligence gathering would be jeopardized if its sources or methods were disclosed. In the field of human intelligence (HUMINT), for example, the identification of an individual as a secret agent is very often a matter of life or death.

Indeed, since the danger of retribution against a spy is not necessarily restricted to a single generation, one should not assume that the passage of time concurrently diminishes the hazards of disclosure. Without a promise of absolute secrecy, moreover, it was feared that agent recruitment would diminish and service morale plummet. "Secrecy is the breath of life to the clandestine warrior," intoned RAdm. A. H. Taylor in June 1945: "It is necessary for his own morale as well as for his security that he should know it will be faithfully observed."[8]

Whitehall's commitment to keeping intelligence matters secret was so unyielding that officials often went to remarkable lengths to prevent disclosures from occurring. Nothing illustrates this better than the *Spycatcher* affair of 1986–88, when then Prime Minister Margaret Thatcher tried unsuccessfully to suppress the memoir of Peter Wright, an embittered former assistant director of MI5. Ghost written by Paul Greengrass (who would later direct the Jason Bourne films), *Spycatcher* alleged that the late Sir Roger Hollis, a past director general of the service, had been a Soviet mole, and it accused MI5 of plotting against, snooping on, and defaming then Prime Minister Harold Wilson in the mid-1970s.[9]

Wright's allegations were neither novel nor discernibly damaging to national security. In March 1981, Fleet Street's greatest scoop-merchant, Chapman Pincher, published *Their Trade is Treachery*, which forced Thatcher to admit in Parliament that Hollis had been investigated some years earlier as a possible Russian spy.[10] Unlike Pincher, however, Wright was an insider who had taken a lifelong oath of silence and whose account was less easily "deniable." In 1987, therefore, Her Majesty's Government (HMG) banned *Spycatcher* in the UK, prohibited newspaper reportage with a series of gag orders, and sought a court injunction to halt the book's publication in Australia.

The insistence on a blanket ban was ludicrous. *Spycatcher* had already been published in the United States and ranked first on *The New York Times* best sellers list; thousands of copies had crossed the Atlantic and were washing up in second-hand bookstores.[11] The affair descended into complete farce when Cabinet Secretary Sir Robert Armstrong was dispatched to an Australian court to present the government's case.

Famously, Armstrong endured a torrid time, harried by a brash young advocate and ridiculed by the world's media for refusing to accept that SIS existed. Armstrong's credibility was fatally undermined when, under cross-examination, he was forced to concede, in a priceless admission, that he had been "economical with the truth." Since open sales of *Spy-*

"Toffs to a man, Guy Burgess, Donald Maclean, Philby, Blunt and John Cairncross had all advanced because they had attended the right schools and the right gentlemen's clubs." (Guy Burgess on left, Kim Philby on the right.)

Images © Bettmann/Corbis

catcher overseas had rendered moot the question of secrecy, attempts to squelch publication ultimately failed and brought mockery upon intelligence taboos.

With historians deprived of documents and governments determined to choke off public debate, the "history" of Britain's intelligence services was written largely by investigative journalists and "exposé merchants," relying on inside information obtained from well-connected friends in Whitehall. With an impish pleasure in wreaking havoc, authors such as Pincher, Nigel West, and Andrew Boyle focused on subjects perfectly calculated to rile the Establishment, including the Wilson Plot, the Cambridge Five, and the purported duplicity of Roger Hollis. (Now in his nineties, Pincher remains convinced that Hollis was a Soviet agent.)[12]

Sometimes referred to pejoratively as the "airport bookstall" school of intelligence historiography,[13] this genre of spy literature first came to prominence in the 1960s, a period known as the "era of exposure" for the intelligence and security agencies.[14] In the United States, the CIA's ill-fated attempt to overthrow Cuban dictator Fidel Castro at the Bay of Pigs made front-page news, as did the shoot-downs of the U-2 and the RB-47 in 1960. Later in the decade, as the public became increasingly disillusioned with the war in Vietnam, and as stories emerged that US-sponsored covert action was propping up corrupt regimes in Central and South America, the CIA was seen in certain quarters as symbolic of a nation losing its way.

In Britain, the early 1960s were punctuated by a series of real-life spy scandals, beginning with the exposure of George Blake as a Soviet spy in 1961 and culminating with the revelation in 1963 that the secretary of state for war, John Profumo, had shared his prostitute girlfriend, Christine Keeler, with a Russian spymaster. By the late 1960s, things got worse. In 1967, the *Daily Express* revealed that the Government Communications Headquarters (GCHQ) routinely intercepted thousands of private cables, setting in motion a chain of events that brought personal obloquy upon Harold Wilson and very nearly spelled the end for the D-Notice Committee, the joint government/media body whose purpose was to prevent the public disclosure of information that would adversely affect the defense of the realm. A year later, Kim Philby, the ruthless SIS traitor and "Third Man" who had defected to the Soviet Union in January 1963, published his KGB-blessed memoir, *My Silent War*, which remorselessly revealed the details of SIS personnel and relationships and his own role as a Russian spy for over 30 years.

Philby and his band of turncoats became a "magnetic specter"[15] to a generation of sensation-seeking writers. Just about every "airport bookstall"

In the UK, the emergence of intelligence was more specifically linked to a series of accessibly written, authoritative, and revealing histories of wartime deception published by respected intelligence veterans in the early 1970s.

author with basic literary ability—and some without—tried to make a quick buck by peddling tall tales of treachery, betrayal, murder, and whatnot. In pursuit of the "Fourth Man" (eventually revealed as Anthony Blunt), accounts tended to focus on the cloistered quadrangles of Cambridge in the 1930s and on the secret societies, such as the Apostles, that became Marxist cells for the disaffected moneyed elite. The spate of books that were produced on Philby were in the main deeply critical of the spy, suggesting that he had handed over thousands of state secrets and caused hundreds of deaths.

In what many regard as an unforgivable apologia that may have cost him a knighthood and a Nobel Prize, the novelist Graham Greene was a lone voice in depicting Philby as a misunderstood idealist, or "passionate pilgrim," who sacrificed everything for the cause of the oppressed proletariat.[16] Greene—a close friend of Philby, following Greene's time in SIS during the Second World War—compared the spy to a persecuted Catholic in Elizabethan England.

By many accounts, the real sin of the Cambridge Five was not betraying their country, but betraying their class.[17] The motivation for disclosure was to expose the Establishment for being so blinded by class prejudice that it failed to spot treachery within its ranks. Toffs to a man, Guy Burgess, Donald Maclean, Philby, Blunt and John Cairncross had all advanced because they had attended the right schools and the right gentlemen's clubs. Similarly, many accounts of the Profumo Affair were not espionage yarns per se, but commentaries on Britain's moral landscape, critiquing those who had become sexually liberated and Bohemian long before it was fashionable.

By the late 1970s, the spread of "mole mania," coupled with the felicitous cresting of the James Bond phenomenon, arguably had created an unquenchable public thirst for sensational tales of espionage, a trend that continues today. As Oliver Hoare argues, "Racy histories of secret services…have often been the norm."[18] In academic circles, "airport bookstall" accounts were frequently met with ridicule or outright hostility, and served only to devalue the credibility of intelligence as a respectable field of inquiry. In the years to come, it is possible scholars will rehabilitate the "airport bookstall" school as a form of "protohistory" which, despite its flaws, facilitated the public emergence of Britain's intelligence agencies and the writings of the first professional intelligence historians.

Emergence

By the late 1980s, intelligence history had started to come of age, demonstrating how attention to the form and function of espionage could challenge existing orthodoxies about international relations and modern governance. Its ascent was in part the corollary of seismic events in the United States. In 1975, the Senate's famous Church Committee hearings exposed some of the CIA's most dubious, if not outright illegal activities, including the surveillance of domestic dissidents and the covert subversion of foreign governments. Church's festival of revelation was transformative for the US intelligence community and "provided scholars, in the Western world, at least, with hitherto absent incentives and reasons to study intelligence."[19]

Revealing World War II History

In the UK, the emergence of intelligence was more specifically linked to a series of accessibly written, authoritative, and revealing histories of wartime deception published by respected intelligence veterans in the early 1970s. In 1972, the

Published after 1945, the official histories of the Second World War were carefully doctored to maintain state security and thus contained no mention of Bletchley Park.

Oxford don, John Masterman, published *The Double-Cross System in the War of 1939–45*, an account of the highly successful XX Committee and its turning of German spies into double agents during World War II.[20] With outstanding social connections (then Prime Minister Edward Heath was a former student), Masterman was persona grata to members of the Establishment who shared the author's desire to champion the achievements of the system and to head off erroneous "outsider" histories.

Two years later, Group Captain Frederick Winterbotham, a former intelligence officer at the Government Code and Cypher School at Bletchley Park, was allowed to publish the first English-language work dedicated to the Ultra secret—"the greatest secret of World War Two after the atom bomb"[21]—and the influence of Enigma decryption on the course of the war.[22] Although hagiographic and unreliable in places (Winterbotham was accused of lacking "the most elementary technical knowledge" of cryptography, as well as downgrading the Polish and French contributions in breaking German ciphers),[23] *The Ultra Secret* represented a significant milestone in the pursuit of intelligence history. Ultra ranked as one of the best-kept secrets of all time. In July 1945, amid concerns that its revelation might preclude postwar rapprochement with Germany (whose leaders might claim that they were not "well and fairly beaten," à la 1918), the JIC had considered it "imperative that the fact that such intelligence was available should NEVER be disclosed."[24]

Published after 1945, the official histories of the Second World War were carefully doctored to maintain state security and thus contained no mention of Bletchley Park. Despite his reputation as something of a loose cannon, a man wanting in constraint and fickle in his loyalties to the rules of censorship, Winston Churchill was silent on the subject in his multivolume memoir of the conflict. As David Reynolds argues, for such a great aficionado of Signals Intelligence (SIGINT), Churchill made a "considerable sacrifice," a point not lost on Bletchley Park veterans who, should their wartime prime minister have spilled the beans, may have followed suit.[25]

Winterbotham's account opened up a brand new chapter in the public's understanding of WW II and provoked a groundswell of academic interest in the role of intelligence, counterintelligence, and deception. Knowing the Allies had been in possession of event-influencing information, military historians who had been enamored of a particular general or admiral lost faith, igniting a firestorm of historical revisionism.

Opening Archives

With the Ultra secret in the public domain, Whitehall, perhaps unexpectedly, began to reassess its approach to intelligence archives. Although spread over many years so "as to generate the minimum public interest,"[26] from the mid-1970s HMG started to declassify its Great War SIGINT record, the Room 40 O.B. archive. In 1977, the first batch of Enigma decrypts and other Ultra-related material was released to the National Archives. Two years later, ministers took a bolder step in authorizing the publication of the first volume of Professor Sir Harry Hinsley's official history, *British Intelligence in the Second World War*, researched and written with the help of several able hands who, like Hinsley, had served at Bletchley Park during the war.[27]

The brainchild of former Cabinet Secretary Sir Burke Trend, Hinsley's multivolume tome had been conceived as a "counterblast" against the deluge of salacious outsider accounts.[28] Depending upon who was spinning the tale, British intelligence was increasingly seen as a safe haven for disillusioned toffs more accustomed to dis-

Hinsley's [below] *multivolume* British Intelligence in the Second World War *had been conceived as a "counterblast" against the deluge of salacious outsider accounts.*

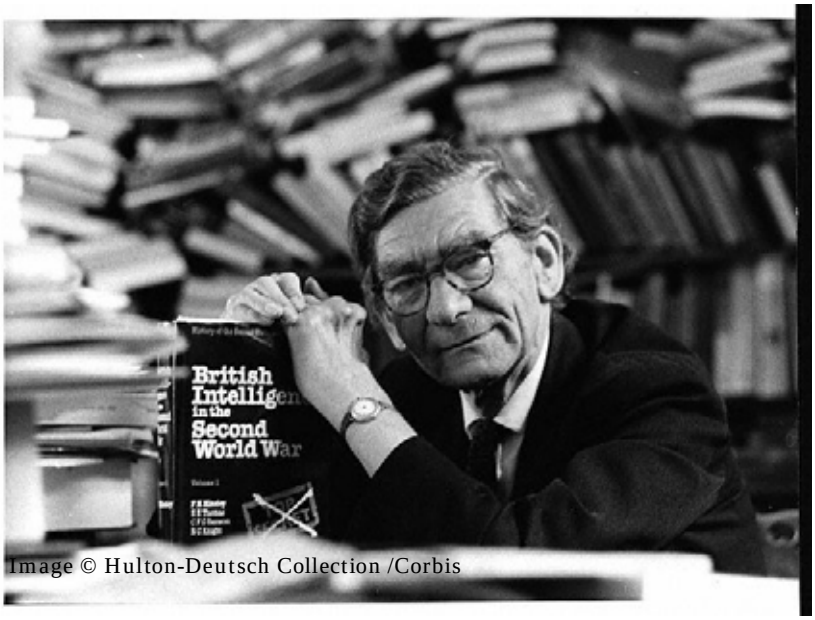


Image © Hulton-Deutsch Collection /Corbis

gorging secrets to the enemy than defending the realm. In his widely read "Karla Trilogy" (1974–79), for example, John le Carré explored a world of betrayal, treason, and murder, peopled by those who become what they behold. Fair but forthright, unfailingly well written, and meticulously researched (Hinsley and his team had been granted unrestricted access to official papers), *British Intelligence in the Second World War* won wide-ranging praise from academia's most knowledgeable and discerning commentators. CIA officer-turned-scholar Walter Pforzheimer called it "the single greatest work on intelligence ever produced," and it set the benchmark by which all other works on the subject are judged.[29]

Hacking into Other Sources

Hinsley's history firmly contested the para-historian's attempt to annex intelligence to the domain of "airport bookstall" literature and piqued the curiosity of an emerging generation of professional researchers. In the 1980s and early 1990s, scholars became less inclined to scoff and increasingly skilled at what one scholar has termed "archival intelligence hacking."[30] Hacker in chief was Christopher Andrew, Hinsley's heir apparent, but the roll also included David Stafford, Julian Lewis and Bradley Smith. Drawing upon private papers as well as so-called "adjacent" records, such as Foreign Office and Treasury files, the aforementioned demonstrated that there was sufficient declassified material to "fill in both the general outline of the missing intelligence dimension and much of its operational detail."[31]

Private collections were particularly bountiful, as long as an author was prepared to weed through, canvass, and weight each folio of inchoate documents; statesmen of the first rank, including Winston Churchill and Anthony Eden, had routinely taken copies of confidential documents home with them—copies which, unbeknownst to the Cabinet Office, were often retained among those officials' personal papers. For example, in Eden's stockpile, formally deposited in the Birmingham University Library in 1990, was the first page of Sir Edward Bridges' Top Secret report into the disappearance of SIS frogman Lionel "Buster" Crabb (not officially declassified until 2006).

Authors with a penchant for lateral thinking also started to prize UK records out of the archives and libraries of foreign states. With its sunshine laws and landmark Freedom of Information Act, signed into law by President Lyndon B. Johnson on 4 July 1966, America was increasingly seen as an Aladdin's cave—or wonderland—where any number of

In recent years, the discipline of intelligence studies has gone from strength to strength, becoming a magnet for postgraduate students and postdoctoral researchers around the world.

jewels could be found.[32] The archive of the Office of Strategic Services (OSS), the wartime counterpart of SIS and forerunner of the CIA, was said to contain "not just isolated documents," but quite often "entire files of British material."[33] In his biography of Sir Stewart Graham Menzies ("C" during and after World War Two), the globe-trotting writer Anthony Cave Brown showed that Special Operations Executive (SOE) materials were available for public inspection in the papers of C's American equivalent, William J. Donovan, which were housed at the US Army War College in Carlisle, Pennsylvania.[34]

The desire to open up the "missing dimension" enveloped Christopher Andrew in writing what became a massively detailed history of the British intelligence services. Published in 1985 and stretching to over 700 pages, *Secret Service: The Making of the British Intelligence Community* demonstrated the value of sustained and creative archival research.[35] In 1986, Andrew cofounded *Intelligence and National Security*, the first (and now preeminent) academic journal in the field. The premise of its first issue was that intelligence represented a "proper" subject of study for scholars in political history and kindred disciplines.

Others soon shared this sentiment. As Keith Jeffrey has argued, a "conclusive indicator" of the subject's newfound legitimacy was the acceptance of articles by traditional periodical outlets.[36] In 1986, for example, both *The Journal of Contemporary History* and *The English Historical Review* published articles on intelligence for the first time.[37] The proliferation of conferences was also instrumental in ushering in a growing scholarly appreciation for espionage-related topics.

This is not to say, however, that the first generation of serious scholarship was problem-free and beyond critical self-examination. As stated by John Lewis Gaddis, the "British School of Intelligence Studies" (as it became known) lent itself to "buffism," preoccupied with a love of particular and esoteric terminology.[38] Many works—framed within the parameters of organizational theory and institutional practice—elided context and expended little effort in showing how the intelligence services made a difference. In consequence, they were beyond the ken of the average student.

Published fitfully between 1979 and 1990, the five volumes produced by Hinsley and his assistants were a monument to the triumph, but also to the inherent problems of intelli-

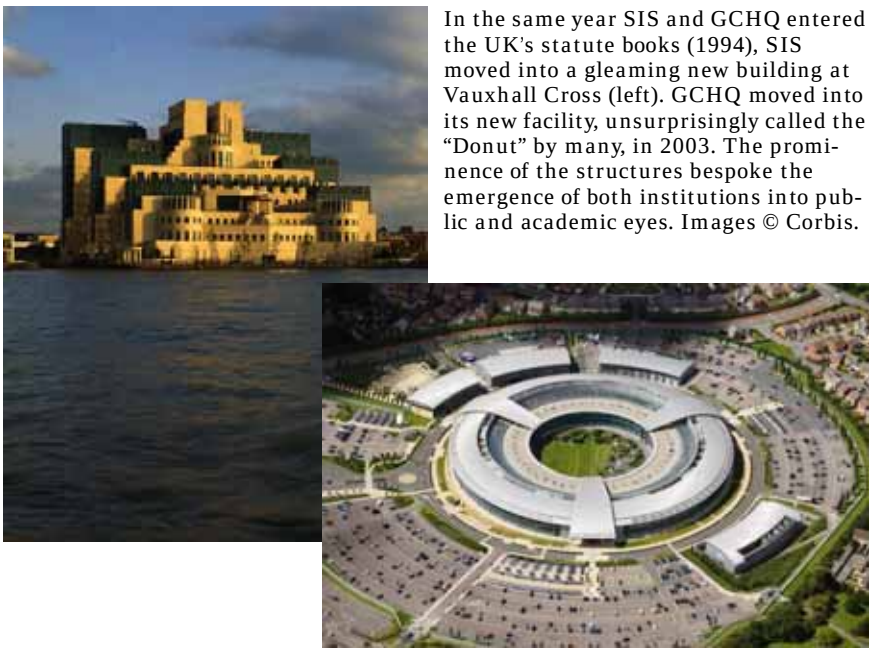
In December 1991 Stella Rimington became the first spy chief to be publicly named; the first to pose openly for cameras; and the first to publish a brochure. Image © Capital Pic/Corbis Sygma

gence history in its earliest manifestation. As Ralph Erskine noted of Volume 3, "Hinsley makes too few judgements, and his book is definitely not bedside reading. Order of battle appreciations loom all too large."[39] The pursuit of intelligence history, therefore, demanded not only the centrifugal instinct to locate minutiae in the archives, but also a centripetal inclination to contextualize those details for a readership that might not be cognizant of the basic contours and outlines.

Efflorescence

In recent years, the discipline of intelligence studies has gone from strength to strength, becoming a magnet for postgraduate students and postdoctoral researchers around the world, and producing an impressive and varied literature. The steady stream of scholarship that has accrued over the past two decades has coincided with an ever-growing public awareness about intelligence. Following the high drama of 1989 and the end of the Cold War, the intelligence and security services entered a new phase in their history. As borders opened and free elections ousted communist regimes across Eastern Europe, the UK intelligence community confidently anticipated a period of relative geopolitical calm and, in turn, placed greater emphasis on accountability and transparency.

This new era of optimism and openness had a physical metonym: the Berlin Wall.[40] During the Cold War, as made famous by John le Carré's novel *The Spy Who Came in from the Cold* (1963), the Wall was the literal and symbolic epicenter of the great game of espionage; by the early 1990s it had been torn down. The lifting of the veil in the UK began in 1989, when MI5 was placed, for the first time, on a legislative footing. The Security Service Act (1989) came into being partly as a response to complaints about unauthorized government surveillance. Four years earlier, MI5 had faced a barrage of media scrutiny when a former officer, Cathy Massiter, provided evidence before the European Court of Human Rights that the service had been illegally bugging the telephones of pressure groups, such as the Campaign for Nuclear Disarmament (CND), as well as political "high fliers," including Patricia Hewitt and Harriet Harman, then leading members of the National Council for Civil Liberties.



In the same year SIS and GCHQ entered the UK's statute books (1994), SIS moved into a gleaming new building at Vauxhall Cross (left). GCHQ moved into its new facility, unsurprisingly called the "Donut" by many, in 2003. The prominence of the structures bespoke the emergence of both institutions into public and academic eyes. Images © Corbis.

In the 18 months following her appointment as director general of MI5 in December 1991, Stella Rimington became the first spy chief to be publicly named; the first to pose openly for cameras; and the first to publish a brochure, entitled *MI5: The Security Service* (1993), describing the organization's activities.[41] Perhaps even more surprisingly, on 7 May 1992, then Prime Minister John Major acknowledged in Parlia-

Since 2001, few subjects have commanded so much attention and controversy as intelligence.

ment that Sir Colin McColl was the incumbent head of SIS.[42] Hitherto, McColl and his predecessors had been ritually referred to as "C," the fabled code name that originated with Captain Sir Mansfield Cumming, the first director of the service.

In 1994, SIS and GCHQ joined the MI5 on the statute book, while the Intelligence and Security Committee (ISC) was established to oversee the "policy, administration and expenditure" of the three agencies.[43] It should be said that the British glasnost was not in isolation; the collapse of communism prompted most Central and Eastern European secret services, previously little more than Soviet surrogates, to enshrine their responsibilities and powers in statute.

Underpinning this new spirit of openness was a perception that intelligence as a whole was becoming less important. For statesmen and practitioners alike, the passing of Marxism-Leninism from the Soviet Union, the diminution of the likelihood of large-scale conflict between states, and the purported universalization of Western liberal democracy as the final form of government all pointed to a "New World Order" in which intelligence would take a backseat.

By the early 2000s, however, this belief had been shown to be naïve. The post-Cold War era had not brought an end to conflict or instability, nor had it confirmed "the end of history," in which secular free-market democracy reigned unchallenged. The intelligence services, having lost the stabilizing force of a common enemy, found themselves required to adapt to a host of new threats, from the development of corruption, cartels, and mafias in transitioning countries, to the global spread of terrorism, organized crime, drug smuggling, and human trafficking.

Terrorism and Iraq

Since 2001, few subjects have commanded so much attention and controversy as intelligence. The terrorist attacks of 9/11, Madrid, and in London, the wars in Iraq and Afghanistan, debates about weapons of mass destruction (WMD), domestic surveillance, and secret detention and rendition have all brought unwelcome notoriety and exposure to the intelligence services. In a world of media plenty, the importance, but also the limitations and abuses of intelligence, have never been more visible. In the face of threats from militant jihadists, public expectations of intelligence have soared to an all-time high, as have calls for greater transparency about what is being done to combat this menace.[44]

The British government has played an instrumental, if not always positive, role in dragging its intelligence community into the sunlight. In the summer of 2003, members of the administration of then Prime Minister Tony Blair, in particular Downing Street's then Director of Communications and Strategy Alastair Campbell, came under heavy fire amid allegations that intelligence on Iraqi WMD had been deliberately twisted—or "sexed up"—in its representation to the public in order to present an exaggerated case for military action. The row centered on the publication of two highly contentious dossiers, which, using intelligence-derived information (including both HUMINT gathered by SIS and—for the first time—JIC assessments), claimed that Iraq had reconstituted its nuclear weapons program and could "deploy [chemical and biological] weapons within 45 minutes of a decision to do so."[45]

Asking the JIC to produce material for public consumption was an act without parallel in British politics. Blair, writes Christopher Andrew, "finally laid to rest the traditional taboo that British governments do not mention their intelligence services."[46] As the months passed without any sign of the weapons about

which Blair and his security apparatchiks had ominously warned, breaking this taboo proved disastrous. Ministers were accused of "spinning" intelligence to sell the war on a false premise, and the intelligence services, historically unswayed by the interests of any political party or class, were criticized for compromising their independence and succumbing to political influence.

As Richard Aldrich argues, "the opening up of intelligence has followed the law of unintended consequences."[47] Intending only to disclose selected snippets of information, the government instead put intelligence into a goldfish bowl, encouraging the ceaseless scrutiny of an increasingly inquisitorial Parliament and a decreasingly deferential media. Symbolizing the slide towards greater openness, the Hutton Inquiry, which reported on 28 January 2004, posted online virtually all of its evidence, including sensitive documents written only weeks before.

In a community-wide bid to restore public confidence, each intelligence service now places job advertisements in the national press, offers career presentations at academic recruitment fairs, and maintains a website delineating objectives and staffing. Generally speaking, MI5 is more open than its sister service, SIS. In a recent step towards greater transparency, on 6 January 2009 Jonathan Evans became the first serving director general in MI5's 100-year history to meet the press.

In a community-wide bid to restore public confidence, each intelligence service now places job advertisements in the national press, offers career presentations at academic recruitment fairs, and maintains a website.

New Openings

Historiography has benefited immeasurably from the two-decade waning of intelligence taboos. Declassification of documentary evidence, especially older material, has gone hand in hand with the more general opening up of intelligence agencies. The process began with the Waldegrave Initiative on Open Government in 1993, which saw the first release of historical records generated by the secret services and afforded independent historians the opportunity to assist in the formulation of retention and release policies.[48]

By the end of the second millennium, hundreds of files relating to SOE, MI5, and Ultra had been transferred to TNA, though few related to the period beyond 1945. Since then, a tsunami of declassified material has occurred. To date, MI5 has declassified approximately 4,000 "pieces" of historically significant information (in official usage, a piece may represent a whole file or a particular portion of it), including wartime material on German spies and double agents, and early Cold War files on Soviet intelligence operations.[49] SIS, despite retaining its own archive, has released a number of documents held in the files of other departments and approved the declassification of all surviving SOE records in its custody. Now, rather than retain entire documents, departments producing classified material increasingly extract or "white-out" sensitive passages (a redaction technique CIA has used since the 1970s—though it blacks out passages).

The opening of new repositories in Eastern Europe has also given historians a revealing glimpse at intelligence activities and the mindset on the other side of the Iron Curtain. Materials bearing on the work of the East German Ministry for State Security (Stasi) have revealed a web of foreign espionage in Britain during the Cold War. By referring to a vast array of German sources in his book *The Stasi Files,* Anthony Glees suggested that some 100 Britons operated—wittingly or not—as agents of influence, including prominent CND members and, most controversially, Lord Roper, former director of studies at Chatham House.[50]

It should be said, of course, that former Eastern bloc read-

In Britain, where spin doctors have a particular resonance in this field, the sincerity of declassification efforts has been the subject of much debate.

ing rooms do present problems. Although the communist system was *akribisch*—that is, obsessive about documenting itself—officials often talked "newspeak rather than brass tacks even behind closed doors." Files relating to agents and informants, moreover, are notoriously patchy.[51] In a memorably bitter review, Paul Maddrell attacked *The Stasi Files* for inflating its subject matter and accused Glees of committing a cardinal sin for any historian, failing to authenticate the reliability of his evidence.[52]

In Britain, where spin doctors have a particular resonance in this field, the sincerity of declassification efforts has been the subject of much debate. For British intelligence scholar Ken Robertson they have been tantamount to carefully coordinated publicity stunts by a government intent on "policing its past," providing officials with the opportunity to rhapsodize about transparency while it exerts control over the pace and content of disclosure. Newly released files, it is said, only disclose what governments deem safe to put on public view.[53]

Following Robertson's example, Peter Gill argues that Whitehall has become increasingly skilled at what he calls "burying," a strategy of bombarding the public with a mass of largely insignificant information.[54] The first tranche of SOE material, which included hefty batches of files on sabotage devices (e.g., incendiary cigarettes and exploding rats), and papers setting out plans to assassinate Adolf Hitler, was presented to the public as one of the biggest "windfalls" of the end of the Cold War. Such material is all well and good, auguring, as it did, a more open future. It would be well to bear in mind, however, that such programs of document release might also serve as the perfect matador's cape—waved ostentatiously to draw the eye away from more critical areas.

Richard Aldrich is another scholar who has warned against taking the Waldegrave Initiative at face value. Before entering the public domain, he reminds us, official records are meticulously "preselected, cleaned and processed" by the Whitehall machine. With no external assurance that what is released is "necessarily an analogue of reality," what is to stop the researcher from becoming an official historian, albeit once removed?[55] Documents written by actual spies require perhaps the most careful handling. As Bernard Porter writes, "all spies and secret agents are liars, trained in techniques of deception and dissimulation, who are just as likely to fake the historical record as anything else."[56]

Some researchers therefore have turned to oral history—"growing their own records"—in order to corroborate the accuracy of their archival findings.[57] This, too, of course, has inherent flaws—the inevitable diminished memory, especially when a subject worked in secrecy. Such testimony is often polluted by what has been absorbed from subsequent experience and discourse, or, in the case of the once powerful, corrupted by a self-conscious desire to entomb a good reputation. As Philip Davies convincingly argues, the most effective intelligence scholar should not use witness testimony to the exclusion of all other material but should "triangulate" research through a triad of archival, secondary, *and* oral sources.[58]

Communities of Research

Although the scope of historical writing on intelligence today is so wide that it is difficult to pigeonhole scholars into research communities or subschools, Wesley Wark's treatise *Espionage: Past, Present, Future?* notes that certain "projects" are presently being pursued and suggests a few categories.[59]

Frameworks. The first might be called the "Research Proj-

ect," the main task of which is to establish the historical framework of intelligence, rediscovering and interpreting its growth, performance, and relevance. Centered on the "episodic treatment of intelligence in peace and war" during the period from the creation of the Secret Service Bureau in 1909 to the end of the Cold War,[60] the "Research Project" involves a prolonged immersion in archival sources and favors the case study methodology. Many texts are understandably prone to narrative and description. Without such work, however, intelligence history would remain conjectural, even conspiratorial and misconceived, and laden with epistemic blind spots.

Theory. A second project works to answer the question, "What is intelligence?" The effort to define intelligence rubs shoulders with political science, gives rise to what is often referred to as "intelligence theory,"[61] and is, as Michael Warner explains, far more complicated than painting a caricature of "some shadowy figure…skulking in a dark alley." Moreover, how we define intelligence has significant implications for practitioners and scholars alike, shaping the work and remit of oversight committees, as well as influencing declassification policies by elucidating what are and are not activities that governments are required to keep secret.[62]

Until recently—in the much-quoted words of Walter Laqueur—"all attempts to develop ambitious theories of intelligence have failed."

Until recently—in the much-quoted words of Walter Laqueur—"all attempts to develop ambitious theories of intelligence have failed."[63] Officialdom stuck to a very rigid definition of intelligence as "information about things foreign"—capabilities, intentions, or activities. In academic writing, meanwhile, the term was defined de novo by each scholar who discussed it. Today we tend to think about intelligence in terms of a three-part schema.[64] The first, usually labelled "the intelligence cycle," is a series of steps that begins with a request for information, which is then collected, analyzed, and disseminated to the client. Secondly, it is seen as a "product," used by decisionmakers at several levels. Thirdly, it is seen as an "institution," encompassing the roles of related pursuits such as covert action, deception, and clandestine diplomacy.

Warner's definition—"Intelligence is secret, state activity to understand or influence foreign entities"—is as apt as it is succinct.[65] This said, in the 21st century it is arguably getting harder to build a properly encompassing taxonomy of intelligence. The increased production and consumption of surreptitiously acquired information by private groups, such as water suppliers, electricity companies, and airlines challenges the assertion that intelligence is organized by the state for the state.[66]

The recent emphasis on open source intelligence (OSINT) has further muddied the water, "blurr[ing] distinctions between intelligence and information and the barrier between secret and non-secret."[67] Although OSINT under one name or another has been around for centuries, with the rise of the Internet and global communications, the ability to search material at the click of a button has given it much greater prominence and added new components, for example, the blogosphere and social media.

The Interdisciplinary. A commitment to interdisciplinary synergies has become one of the hallmarks of intelligence historiography. The involvement of historians and political scientists, as well as partners in English, sociology, and law has made it a distinctive research cluster. Certain intelligence scholars would consider themselves as "hybrid" or "hyphenated" historians, taking their research and perspectives beyond the academy. Although those who write for nonacademic audiences are still sometimes disparaged, for many in the community, the development of a synthetic literature that connects intelligence his-

The need to relate historical analysis to contemporary problems has led to the establishment of dedicated research centers.

tory and public policy is essential.[68]

History, proponents claim, can be quarried for lessons and can inform current and future practitioners. The most vocal spokesman for the "Public Policy Project" has been Christopher Andrew. From salutary warnings about the dangers of failing to heed the lessons of history, Andrew has moved to the assertion that today's political culture suffers from "Historical Attention Span Deficit Disorder," a widespread belief that the past is "irrelevant to present and future policy and intelligence analysis."[69] For example, had decisionmakers prior to the Iraq War been familiar with failed British attempts to estimate Soviet nuclear capability during the Cold War, they would have realized that approximating WMD stocks is fraught with difficulty and potential intellectual blinkering.

"Hacker in chief," Christopher Andrew. Image courtesy C. Andrew.

The need to relate historical analysis to contemporary problems has led to the establishment of dedicated research centers, such as the Brunel Centre for Intelligence and Security Studies (BCISS) and the Buckingham University Centre for Security and Intelligence Studies (BUCSIS), that foster links with practitioners and offer degree program? in both historical and policy-oriented contexts.[70] Designed as "career-relevant" degrees, MA programs are invariably filled by those in quest of, or engaged in, security-related jobs. Academics at Brunel and Buckingham double as consultants, providing custom-made academic packages to both professional and corporate clients.

It is pleasing to note that the United States has similar centers to prepare students for careers in intelligence and provide educational tools to the intelligence community. A cluster exists, not surprisingly, among the several universities in the Washington, DC area. Exemplary outside the capital is the Center for Intelligence and Security Studies at the University of Mississippi.

The "Official History." The most common way to connect history with policy is, of course, to write full-scale histories, which analyze all stages of the intelligence cycle and seek to identify trends and themes from past to present. With their access to resources of state, including former agents and personnel, the best people to undertake such a task may be official historians: "Just as intelligence chiefs have to be able to tell policymakers what they do not want to know, so official historians have to be free, on occasion, to tell intelligence agencies uncomfortable truths."[71]

In 2009, MI5 marked its centenary with the publication of an authorized history, written by Christopher Andrew. In 2010, Keith Jeffrey's officially sanctioned history of SIS hit bookshops. It covered the history of the service from its beginnings in 1909 to the early Cold War. Yet not everyone has warmed to such works. As Len Scott and Peter Jackson explain, "For some academics the Ivory Tower should remain a sanctuary and provide a panorama on the world outside."[72] Is it not profoundly unfair, critics ask, that Professors Andrew and Jeffrey have been able to feast their eyes on materials denied to the remainder of their

It should be clear, by now, that this is an exciting time for UK students of intelligence, a subject no longer obscured by secrecy or bedecked with flights of the imagination.

profession? For Anthony Glees, the risk of whitewashing is all too great: "I don't think governments should write their own history. Academics should not become ambassadors or politicians, or work for the secret service."[73]

Christopher Andrew, having twice coauthored officially sponsored histories of the KGB (with the aid of Soviet defectors, Oleg Gordievsky and Vasili Mitrokhin), has been labelled by cynical voices as a "court historian." This is too strong. Andrew and Jeffrey, who throughout their careers have railed against the official position that there could be no middle ground between total secrecy and total disclosure, have to preserve their academic standing at all costs. Sanitizing the historical record now, knowing that documents in question will in due course enter the public domain, would be making whips for their own flogging.

The Countervailing View. A small group of intelligence historians in the UK is engaged in dissecting the seamier side of espionage. The so-called "Civil Liberties Project" (also known as the "para-political" school) conjoins two scholarly agendas.[74] The first is a program for researching intelligence history by way of nonofficial sources, including obituaries, editorials, satirical magazines (such as *Private Eye*), and other cultural miscellanea.

The second is a strategy for writing intelligence history from the "bottom up," moving beyond the intensively cultivated field of high politics to explore the private experience of spies and their most intimate details, such as sexuality, social class, and political orientation. Among the most vociferous proponents of the "Civil Liberties Project" are Robin Ramsay and Stephen Dorril. Their investigations deftly survey the heartless aspects of the secret state, upending established orthodoxy by rendering Western and Eastern European intelligence services as equally contemptuous and equally corrupt.

MI6: Fifty Years of Special Operations was in itself an exposition of the basic tenets of "para-political" approaches. In the preface, Dorril writes: "In order to unravel the activities of SIS, one has to dig deep and sift carefully, in the manner of an archaeologist, but also acculturate, like some intrepid anthropologist, to a strange and secretive society whose intricate social and professional networks are familiar to their members but quite baffling to the outsider."[75] What emerges from Dorril's 900-page tome is that SIS, determined to keep Britain at the top table in an age of postimperial decline, became a law unto itself, implicated in the surveillance and infiltration of dissident groups; the secret funding of propaganda and smearing opponents; and the formulation of "disruptive action," including assassination plots, against such leaders as Mohammed Mossadeq, Slobodan Milosevic, and Muammar Qaddafi.

Few mainstream authors support the "para-political" belief that what the intelligence services do is nefarious and disproportionate to the threat posed by the nation's enemies. Peter Hennessy, in his excellent study of the Cold War secret state and contingency planning in the event of Soviet attack, makes an impressive case for the view that the UK intelligence community, far from being a rogue elephant, comprised a noble band of skillful patriots, and was instrumental in defending the realm and keeping Britain out of nuclear war.[76] In time, he proposes, as new evidence is marshalled on communist subversion and the dirty work of the KGB, the dominant historiographical assumption will probably be that British counterintelligence was grossly inadequate.

British historiography of intelligence—having grown out of traditional British political history, which frankly precludes an interest in the non-Western world—has neglected the role of intelligence services in imperial contexts.

New Directions

It should be clear, by now, that this is an exciting time for UK students of intelligence, a subject no longer obscured by secrecy or bedecked with flights of the imagination. All the omens point to a healthy future. Fourteen British universities presently offer undergraduate or postgraduate courses explicitly on intelligence and security; at least a further dozen offer modules on terrorism and political violence.[77] As the Cold War continues to recede into history, more archival openings are anticipated. Indeed, as Donald Cameron Watt once pointed out, historians of intelligence will always be better off than scholars working on the Greco-Roman period or the Middle Ages.[78]

For the foreseeable future, intelligence will remain a cornerstone of democratic government, tasked to counter the enduring threat from al-Qa'ida and associated networks, but also used increasingly in peacekeeping, crisis management and contingency planning. For those researching contemporary matters, therefore, it is a case of "having to run to keep up."[79]

But can the same necessarily be said for intelligence historians? Leaving aside fears about whitewashing and sycophancy, the recently published official histories of MI5 and SIS are truly exhaustive in their coverage; that is the official historian's privilege. When the official history of the JIC is released, little of the general outline will be left unsaid. With this, the original raison d'être of intelligence history—namely, to rescue from oblivion the gaps in knowledge—will appear tired and slow. As is the way of things, intelligence historians will have become settlers rather than pioneers, required to think reflexively about the nature of their enterprise. Arguably, less time will be spent *doing* intelligence history, and more *reflecting* on how it is done and where it needs to go.

A handful of areas seem deserving of more attention, however. So far, British historiography of intelligence—having grown out of traditional British political history, which frankly precludes an interest in the non-Western world—has neglected the role of intelligence services in imperial contexts, especially during the period of decolonization. Contrary to popular belief, the geographical scope of MI5's work has never been restricted to the metropole. The protection of British interests worldwide (diplomatic properties and staff; businesses and investments; and citizens living abroad) has long fallen within the remit of its functions. Both Philip Murphy and Calder Walton have made initial forays into this topic, demonstrating how the intelligence services attempted to gather information about indigenous groups, to police political opponents, and to extinguish "colonial fires," albeit with diminishing success in the 1950s.[80]

Although spy fiction is a subject well traversed in literary and film studies (exploring the formulaic nature of the genre, plot conventions, and the like), there has been conspicuously little attention by historians to the genre, specifically the important question of how its products relate to and reflect the real world of intelligence.[81]

The debunking of intrigue narratives has become a compulsory practice. However, as Wark implored over 10 years ago, the relationship between social reality and popular cultural construction should be addressed.[82] Rightly or wrongly, spy fiction has to a large extent shaped public perceptions of intelligence. Many retired SIS officers, including John le Carré, often admit to joining British intelligence as young men partly because they had been brought up on a fictional diet of swashbuckling yarns.

Despite the recent appearance of GCHQ: The Uncensored History of Britain's Most Secret Intelligence Agency*, by Richard Aldrich, what one might call the "SIGINT Project" has scarcely begun.*

According to KGB defector Oleg Gordievsky, the Central Committee of the Soviet Communist Party routinely watched James Bond films in the vain hope that its scientists could replicate "Q Branch" technology.[83] In the mid-1960s, mindful of a "spy fiction gap," the KGB attempted to win the thriller war by commissioning Bulgarian author Andrei Gulyashki to write a series of spy novels in which the "cerebral powers" and "analytical mind" of a self-styled major named Zakhov were pitted against James Bond's "ruthless, intuitive violence."[84] Needless to say, Bond is ultimately slain at the hand of his superior, morally clean Soviet adversary.

Despite the recent appearance of *GCHQ: The Uncensored History of Britain's Most Secret Intelligence Agency*, by Richard Aldrich, what one might call the "SIGINT Project" has scarcely begun.[85] In part, this is because the fast-paced world of covert action has been instantly more arresting to historians, and to their publishers, than has been the mundane setting of moth-eaten desk men combing transcripts of telephone conversations and burrowing in mountains of diplomatic correspondence.

It is also the case that much of the pertinent material has not yet been released. For many in the profession, therefore, the focus on HUMINT has been more a matter of necessity than professional preference. Yet Christopher Andrew has been especially critical of intelligence historians for failing to take account of SIGINT's contribution in the Cold War. Its continued absence, he argues, reflects widespread "cognitive dissonance" within the discipline—that is, reluctance among scholars to embrace a subject that would fundamentally challenge historiographical orthodoxy, not to mention their own career-hardened patterns of thought.[86]

The current crop of intelligence historians, suggests Andrew, are not the first to display cognitive dissonance with respect to SIGINT. In 1945, Sir Edward Travis, operational head of Bletchley Park and, later, director of GCHQ, was certain that scholars would soon discover the Ultra secret: "The comparing of the German and British documents is bound to arouse suspicion in [their] minds that we succeeded in reading the enemy ciphers."[87] The clues, it was assumed, were too obvious for historians to miss.

It was widely known that British cryptographers, under the direction of intelligence officer Reginald "Blinker" Hall, had cracked German codes during the Great War; indeed, Room 40's successful interception of the Zimmermann telegram, which accelerated the United States' entry into the war, had achieved extensive notoriety and fanfare in the press.[88] Held from November 1945 to July 1946, the Congressional Inquiry into Pearl Harbor had publicly discussed the accomplishments of "Magic," the cryptonym for American efforts to break Japanese military and diplomatic communications during World War Two.

Despite allowing for the enormous benefit of hindsight, the fact that no historian, for over a quarter of century, considered the possibility that the British had enjoyed similar success against Hitler's ciphers is remarkable. Just as baffling, when intelligence officer turned author Donald McLachlan disclosed Bletchley Park's secret codename—"Station X"—in his 1968 publication, *Room 39: Naval Intelligence in Action 1939–45*, it took another 6 years before historians finally connected the dots and started to consider with confidence the contribution of British cryptography to the Allied war effort.[89]

It is very important, however, that we also cast our net beyond the relationship between British intelligence and its partner agencies in Washington.

One of the biggest challenges facing intelligence historians is to resist the urge to study the British intelligence community in geographic isolation. For its sins, much of the existing literature is parochial and Panglossian; that is, accepting of the unique and incomparable make-up of British institutions, and reluctant to analyze thematic issues in a broader transnational context.[90]

Embedding the history of the British intelligence services in a comparative history of the 20th century intelligence revolution should reveal similarities and differences between particular national systems and thereby allow us to draw conclusions about general trends and dynamics. *The Hidden Hand: Britain, America and Cold War Secret Intelligence,* by Richard Aldrich, is an exemplar of comparative history, seamlessly shifting between two intelligence cultures and their institutions. By placing intelligence in a hemispheric perspective, Aldrich reveals not only the cohesion and unities of the Anglo-American "Special Relationship," but also the moments of "rancour and suspicion" that have threatened to derail its continuance. Nuanced, archivally rich, and theoretically informed—an unusual trifecta—*Intelligence Cooperation and the War on Terror,* by Adam Svendsen, is another recent example of historical writing that successfully manages to employ a comparative methodology.[91]

It is very important, however, that we also cast our net beyond the relationship between British intelligence and its partner agencies in Washington. During the Cold War, in a bid to monitor the Soviet Union and its satellites, the UK intelligence community often liaised with a range of non-Anglo-Saxon allies, including the West German Federal Intelligence Service (BND) and the French General Directorate for External Security (DGSE). The task of unpacking these relationships still awaits its historian.

❖ ❖ ❖

Endnotes

1. N. Hiley, "Book Review of Plots and Paranoia by B. Porter," *Times Literary Supplement* (December 1989): 22–28.

2. A. Boyle, *The Climate of Treason: Five who Spied for Russia* (London: Hutchinson, 1979).

3. C. Andrew and D. Dilks, eds., *The Missing Dimension: Governments and Intelligence Communities in the Twentieth Century* (London: Macmillan, 1984).

4. *Hansard Parliamentary Debates*, 5th ser., vol. 150 (15 December 1924), col. 674.

5. F. Newsam to E. Bridges, 17 October 1952, The National Archives (hereafter cited as TNA), HO 287/1415.

6. M. Howard, "Cowboys, Playboys and Other Spies," *New York Times*, 16 February 1986.

7. W. Wark, "In Never-Never Land? The British Archives on Intelligence," *The Historical Journal* 35, no. 1 (March 1992): 195–203.

8. A.H. Taylor to the Director of Naval Intelligence, "Clandestine Warfare," 8 June 1945, TNA, ADM 223/480.

9. P. Wright, *Spycatcher: The Candid Autobiography of a Senior Intelligence Officer* (Richmond, Australia: Viking Press, 1987).

10. C. Pincher, *Their Trade is Treachery* (London: Sidgwick & Jackson, 1981).

11. L. Zuckerman, "How not to Silence a Spy," *Time*, 17 August 1987.

12. See C. Pincher, "The Far from Glorious History of MI5," *The Independent*, 11 December 2005; C. Pincher, *Treachery: Betrayals, Blunders and Cover-ups; Six Decades of Espionage Against America and Great Britain* (New York: Random House, 2009).

13. C. Andrew, "Historical Research on the British Intelligence Community," in *Comparing Foreign Intelligence: The U.S., the USSR, the U.K. and the Third World*, ed. R. Godson (London: Brassey's, 1988).

14. R.J. Aldrich, *The Hidden Hand: Britain, America, and Cold War Secret Intelligence* (London: John Murray, 2001), 606.

15. This delightful phrase is used by R. Rosenbaum in "Kim Philby and the Age of Paranoia," *New York Times*, 10 July 1994.

16. G. Greene, foreword,to *My Silent War*, by K. Philby (London: Grafton, 1968).

17. See M. Carter, *Anthony Blunt: His Lives* (London, 2001); A. Danchev, "Will the Weevil Delay?: Creative Writing and the Cold War," *Intelligence and National Security* 20, no. 3 (September 2005): 525–32.

18. O. Hoare, "Introduction," *Intelligence and National Security* 17, no. 1 (Spring 2002): 3.

19. W. Wark, "Introduction: The Study of Intelligence: Past, Present, Future?," in *Espionage: Past, Present, Future?* ed. W. Wark (Ilford: Routledge, 1994), 1.

20. J. C. Masterman, *The Double-Cross System in the War of 1939–45* (New Haven and London: Yale University Press, 1972).

Endnotes (cont.)

21. D. Kahn, "Enigma Unwrapped," *New York Times Book Review*, 29 December 1974.

22. F. W. Winterbotham, *The Ultra Secret* (Aylesbury, UK: Harper Collins, 1974).

23. See L. Tordella, review of *The Ultra Secret*, by F. W. Winterbotham, *Studies in Intelligence* 19, no. 3 (Fall 1975): 45–47.

24. United Kingdom. "Use of Special Intelligence by Official Historians," JIC (45) 223 (0) Final, 20 July 1945, TNA, CAB 103/288; "General Directive to Chief Historians for Safeguarding Special Intelligence Sources in Compiling Official Histories," 20 July 1945, TNA, CAB 103/288.

25. See D. Reynolds, "The Ultra Secret and Churchill's War Memoirs," *Intelligence and National Security* 20, no. 2 (June 2005): 209–224; D. Reynolds, *In Command of History: Churchill Fighting and Writing the Second World War* (London: Penguin, 2004), 499.

26. United Kingdom. "The Release of SIGINT Records," JIC (58) 46, 13 November 1968, TNA, PREM 13/3252.

27. F. H. Hinsley et al., *British Intelligence in the Second World War: Its Influence on Strategy and Operations* (London: Her Majesty's Stationery Office, 1979).

28. See R. J. Aldrich, "Policing the Past: Official History, Secrecy and British Intelligence since 1945," *English Historical Review* 119, no. 483 (September 2004): 922–53.

29. Cited in K. Boyd, *Encyclopedia of Historians and Historical Writing: Volume 1* (London: Routledge 1999), 592.

30. R.J. Aldrich, "The Secret State," in *A Companion to Contemporary Britain*, ed. P. Addison and H. Jones (Oxford: Wiley-Blackwell, 2005), 336.

31. Andrew and Dilks, eds., *Missing Dimension*, 4.

32. See R.J. Aldrich, "Never Never Land and Wonderland? British and American Policy on Intelligence Archives," *Studies in Intelligence* 38, no. 5 (1995): 17–26.

33. Ibid.

34. A. C. Brown, *C*: *The Secret Life of Sir Stewart Graham Menzies, Spymaster to Winston Churchill* (New York: Macmillan, 1987).

35. C. Andrew, *Secret Service: The Making of the British Intelligence Community* (London: William Heinemann, 1985).

36. K. Jeffrey, "Intelligence and Military History: A British Perspective," in *Military History and the Military Profession*, ed. D. Charters, M. Milner, and J. B. Wilson (London: Greenwood, 1992), 110.

37. B. Bridges, "Britain and Japanese Espionage in Pre-War Malaya: The Shinozaki Case," *Journal of Contemporary History* 21, no. 1 (January 1986): 23–35; N. Hiley, "Counter-Espionage and Security in Great Britain during the First World War," *English Historical Review* 101, no. 400 (1986): 635–70.

38. J. L. Gaddis, "Intelligence, Espionage and Cold War Origins," *Diplomatic History* 13, no. 2 (April 1989): 191-213. Also see D. C. Watt, "Intelligence Stud-

Endnotes (cont.)

ies: The Emergence of the British School," *Intelligence and National Security* 3, no. 2 (April 1988): 338–41.

39. R. Erskine, "Reviews and Commentary," *International Journal of Intelligence and Counterintelligence* 6, no. 2 (Summer 1993): 241-53.

40. See P. Major, *Behind the Berlin Wall: East Germany and the Frontiers of Power* (Oxford: Oxford University Press, 2009).

41. See W. Schmidt, "Britain's Spy Agencies Begin to Come Out from the Cold," *New York Times*, 22 August 1993.

42. "The Secret's Out: Top British Spy Identified," *New York Times*, 7 May 1992.

43. See the "Intelligence" page under the "National Security" header on the Cabinet Office website at http://www.cabinetoffice.gov.uk/content/intelligence/.

44. See L. Scott, "Sources and Methods in the Study of Intelligence: A British View," *Intelligence and National Security* 22, no. 2 (April 2007): 185-205.

45. United Kingdom. *Iraq's Weapons of Mass Destruction: The Assessment of the British Government* (London, 24 September 2002); *Iraq: Its Infrastructure of Concealment, Deception and Intimidation* (London, 7 February 2003).

46. C. Andrew, "Intelligence, International Relations and 'Under-theorisation,'" *Intelligence and National Security* 19, no. 2 (Summer 2004): 171.

47. C. Andrew, R.J. Aldrich, and W. Wark, "Preface: Intelligence, History and Policy," in *Secret Intelligence: A Reader*, ed. C. Andrew, R.J. Aldrich, and W. Wark, (London: Routledge, 2009), xvi.

48. See G. Bennett, "Declassification and Release Policies of the UK's Intelligence Agencies," *Intelligence and National Security* 17, no. 1 (March 2002): 21–32.

49. See the "Management and Destruction of Files" page on the MI5 website, http://www.mi5.gov.uk/output/retention-and-destruction-of-files.html.

50. A. Glees, *The Stasi Files: East Germany's Secret Operations against Britain* (London: Free Press, 2003).

51. See R. Mitter and P. Major, "East is East and West is West? Towards a Comparative Socio-Cultural History of the Cold War," in *Across the Blocs: Cold War Cultural and Social History*, ed. R. Mitter and P. Major (London: Frank Cass, 2004), 1–23.

52. P. Maddrell and A. Glees, "Debate: The Stasi Files," *Intelligence and National Security* 19, no. 3 (2004): 553–69.

53. K. G. Robertson, "The Politics of Secret Intelligence: British and American Attitudes," in *British and American Approaches to Intelligence* , ed. K. G. Robertson (Basingstoke, UK: Macmillan, 1987), 144.

54. P. Gill, "Reasserting Control: Recent Changes in the Oversight of the UK Intelligence Community," *Intelligence and National Security* 11, no. 2 (1996): 313–20.

55. See Aldrich, *Hidden Hand*, 4–6.

56. B. Porter, *Plots and Paranoia: A History of Political Espionage in Britain 1790–1988* (London: Routledge, 1989), viii.

Endnotes (cont.)

57. R.J. Aldrich, "Grow Your Own: Cold War Intelligence and History Supermarkets," *Intelligence and National Security* 17, no. 1 (Spring 2002): 135–52.

58. P. Davies, "Spies as Informants: Triangulation and the Interpretation of Elite Interview Data in the Study of the Intelligence and Security Services," *Politics* 21, no. 1 (2001): 73–80.

59. Wark, ed., *Espionage: Past, Present, Future?*

60. Ibid., 3.

61. See P. Davies, "Ideas of Intelligence: Divergent National Concepts and Institutions," in *Secret Intelligence: A Reader*, ed. C. Andrew, R. J. Aldrich, and W. Wark (London: Routledge, 2009), 12–18.

62. M. Warner, "Wanted: A Definition of 'Intelligence'," *Studies in Intelligence* 46, no. 3 (2002): 15–22.

63. W. Laqueur, *A World of Secrets: The Uses and Limits of Intelligence* (New York: Basic Books 1985), 8.

64. See M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington: CQ Press, 2002), 8.

65. Warner, "Wanted," 21.

66. For more examples, see Eamon Javers, *Broker, Trader, Lawyer, Spy: The Secret Word of Corporate Espionage* (New York: HarperCollins, 2010). For a review of Javers' book, see "The Intelligence Officer's Bookshelf," by Hayden Peake, *Studies in Intelligence* 55, no. 1 (March 2011).

67. Andrew, Aldrich, and Wark, eds., *Secret Intelligence*, 2.

68. Ibid., xv.

69. C. Andrew, "Intelligence Analysis Needs to Look Backwards before Looking Forward," *History and Policy* (June 2004), in http://www.historyandpolicy.org/papers/policy-paper-23.html.

70. The homepages for Brunel University and The University of Buckingham contain descriptions of BCISS and BUCSIS. See http://www.brunel.ac.uk/about/acad/sss/research/centres/bciss and http://www.buckingham.ac.uk/international/bucsis/.

71. Andrew, "Intelligence Analysis."

72. L. Scott and P. Jackson, "The Study of Intelligence in Theory and Practice," *Intelligence and National Security* 19, no. 2 (Summer 2004): 152.

73. D. Walker, "Just How Intelligent?" *The Guardian*, 18 February 2003.

74. Wark, "Introduction," 7.

75. S. Dorril, *MI6: Fifty Years of Special Operations* (London: Fourth Estate, 2000), xiv.

76. P. Hennessy, *The Secret State: Whitehall and the Cold War* (London: Penguin, 2002).

77. P. Maddrell, "Intelligence Studies at UK Universities: An Expanding Subject," http://users.aber.ac.uk/rbh/iss/uk.htm.

Endnotes (cont.)

78. D. C. Watt, "Intelligence and the Historian: A Comment on John Gaddis's 'Intelligence, Espionage, and. Cold War Origins'," *Diplomatic History* 14, no. 2 (Spring 1990): 199-204.

79. Andrew, Aldrich, and Wark, "Preface: Intelligence, History and Policy," xvii.

80. P. Murphy, "Creating a Commonwealth Intelligence Culture: The View from Central Africa, 1945–1965," *Intelligence and National Security* 17, no. 3 (Autumn 2002): 131-62; C. Walton, "British Intelligence and Threats to National Security, 1941-51" (PhD diss., Cambridge University, 2006).

81. A notable exception here is a special issue of the journal *Studies in Intelligence*. See "Intelligence in Contemporary Media: Views of Intelligence Officers," *Studies in Intelligence: Special Review Supplement* (Summer 2009).

82. Wark, "Introduction: Study of Espionage," 8.

83. See J. Black, "The Geopolitics of James Bond," *Intelligence and National Security* 19, no. 2 (Summer 2004): 290–303.

84. D. Schmidt, "Bulgarian Tours 007's London Dens," *New York Times*, 27 January 1966.

85. R.J. Aldrich, *GCHQ: The Uncensored History of Britain's Most Secret Intelligence Agency* (London: HarperCollins, 2010).

86. Andrew, "Under-Theorisation," 170–84.

87. United Kingdom. E. Travis, "Special Order," 7 May 1945, TNA, HW 3/29.

88. Andrew, "Under-Theorisation," 174.

89. D. McLachlan, *Room 39: Naval Intelligence in Action 1939–45* (London: Littlehampton Book Services, 1968).

90. This argument is often made in relation to British political history. See S. Pedersen, "What is Political History Now?" in *What is History Now?* ed. D. Cannadine, (Basingstoke, UK: Palgrave, 2002), 36–57.

91. A. Svendsen, *Intelligence Cooperation and the War on Terror: Anglo-American Security Relations after 9/11* (London: Routledge, 2009).

❖ ❖ ❖

The Evolution of US Army HUMINT: Intelligence Operations in the Korean War

John P. Finnegan

> ***"By the end of the Korean War, the Far East Command had fielded a large Army-controlled clandestine collection apparatus, closely linked with similarly large operations in the fields of partisan and psychological warfare."***

This article was originally published in a classified issue of Studies *(44, no. 2) in 2000. —ed.*

The traumatic experience of the Korean conflict was a watershed in the evolution of Army intelligence. Within six months, the Army found itself facing two major intelligence disasters: it was caught unprepared by the initial North Korean invasion of June 1950 and by the massive Chinese intervention in November of that year. In response, the Army hastily improvised a clandestine human intelligence (HUMINT) organization, building on a small existing intelligence unit, the Korean Liaison Office (KLO). By the end of the Korean War, the Far East Command (FECOM) had fielded a large Army-controlled clandestine collection apparatus, closely linked with similarly large operations in the fields of partisan and psychological warfare. More important, the Army had begun to take steps to create a permanent and professional HUMINT service that could carry out positive intelligence collection operations.

Lack of Intelligence

The sudden outbreak of the Korean war on 25 June 1950 came as a shock to US leaders. In hindsight, this is not surprising. Since the onset of the Cold War, the nation's intelligence assets had been targeted almost exclusively against the Soviet Union. In addition, intelligence responsibilities in the Far East were badly fragmented. General of the Army Douglas MacArthur's Far East Command (FECOM), the major theater headquarters in the area, no longer had any jurisdiction over the Korean peninsula: authority over the area had devolved to the Korean Military Advisory Group (KMAG) after the last American occupation forces left in mid-1949. Because the KMAG had no positive collection capability, Korea was an intelligence vacuum.[a1]

[a] For more on intelligence during this period, see Clayton Laurie, "A New President, a Better CIA, and an Old War," in *Studies in Intelligence* 54, No. 4 (December 2010) and CIA release of documents from the period in www.cia.gov/library/publications/historical-collections-publications/index.html.

All statements of fact, opinion, or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

In the field of intelligence, as in almost everything else, five years of peacetime occupation duty had left American forces in Japan less than well equipped to meet an outside challenge.

loughby, MacArthur's G-2, did maintain a residual intelligence organization in Korea, the KLO. The reports generated by this small office, however, received little attention in a preoccupied Tokyo. Similar reports submitted by an Air Force Office of Special Investigations (AFOSI) team that also remained in Korea were likewise disregarded. Intelligence emanating from the small CIA presence in Korea received an equally cool reception from FECOM. Intelligence that came the way of these elements was procured largely through liaison with Republic of Korea (ROK) sources. As such, it was deemed unreliable, and the information received was often conflicting. Intelligence officers back in Tokyo had heard "wolf" cried too often to believe that anything was actually going to happen. Lack of intelligence resources and hard data was paralleled by a lack of intelligence perception. Because the North Korean destabilization campaign against the South had failed, it was too easily assumed that the North would turn to political initiatives.[2]

The advance of T-34 tanks across the 38th parallel shattered the illusions of FECOM policymakers. The rapid collapse of ROK forces meant that only outside military help could prevent a communist takeover At the direction of the president and acting under the authority of the UN, FECOM quickly moved to intervene. But it found that in the field of intelligence, as in almost everything else, five years of peacetime occupation duty had left American forces in Japan less than well equipped to meet an outside challenge.[3]

On paper, FECOM controlled substantial intelligence assets. Willoughby had more than 2,500 intelligence personnel at his disposal, but these elements were organized to support an army of occupation. The largest single intelligence component within FECOM was the 441st Counter Intelligence Corps (CIC) Detachment, targeted against Japanese subversive elements. It reported to MacArthur in his capacity as Supreme Commander Allied Powers, not as head of FECOM. The four Army divisions in Japan had no organic CIC detachments.[4]

A large Military Intelligence Service Company of Japanese interpreters supported the 441st CIC Detachment, but there were only two Korean linguists at G-2's disposal. FECOM's Technical Intelligence Section had been discontinued in 1949. The PHOTINT capability of the command had shriveled. Cryptologic resources were equally lacking. The Army Security Agency, Pacific (ASAPAC) had two companies and two detachments in the Far East, but these were trained and equipped for fixed-site operations and could not easily be shifted to the field. ASA was not able to deploy a tactical unit in Korea until October, when a company was shipped from the United States.[5]

A Need for HUMINT

The adverse combat situation confronted by FECOM and the Eighth Army in Korea during the summer of 1950 created a critical need for hard intelligence. With other assets unavailable, this could only be provided by HUMINT. An organization was quickly built around the nucleus of the KLO, using personnel from the 441st CIC Detachment. To carry out its mission, the KLO hastily recruited Korean peasants, gave them sketchy training, and airdropped them behind enemy lines with instructions to return with intelligence reports. In addition, it set up Tactical Liaison Offices (TLOs) at division level to recruit Koreans as line-crossers to gather clandestine HUMINT.[a] Although it operated in support of Eighth Army and its tactical commanders, the whole structure remained firmly under Willoughby's control.[6]

Agent casualties were high, and the quality of intelligence produced unsatisfactory. But, in the early stages of the war, it

was all the UN forces had. Nonetheless, the KLO tried to improve the collection situation as early as August 1950. One basic problem was that both agent insertion techniques used by the KLO—parachute drops and line-crossing—were intrinsically hazardous, and even parachute agents had to exfiltrate through enemy lines to bring back their reports. The KLO came up with the idea of using small boats both to land its agents behind enemy lines and to retrieve them, thus bypassing the dangers of the fighting front. The cooperation of the ROK Navy was necessary for this effort, however, and this was difficult to obtain.[a] The whole idea was temporarily abandoned in September, when the needs of the forthcoming amphibious operation at Inchon absorbed all available shipping.[7]

By the time of the Inchon landing, the intelligence picture in FECOM was improving.

Some Improvement

By the time of the Inchon landing, the intelligence picture in FECOM was improving. The theater had received additional intelligence assets, and focus on the Korean problem at the national level was producing results. The rapid collapse of the North Korean Army appeared to make further efforts at establishing a permanent intelligence organization unnecessary. But the very success of UN forces exacted a price: intelligence elements repeatedly had to move to keep up with the pace of the advance, and this disorganized the intelligence structure and impaired its operational capabilities.

The Chinese Threat

The coming of November brought a new threat, the possibility of intervention by the People's Republic of China. Chinese Foreign Minister Zhou Enlai had publicly announced that China would enter the war if US forces crossed the 38th parallel. Although the United States had decided to ignore this threat as a bluff, American intelligence was aware that 400,000 troops of China's best formation, the Fourth Field Army, were being concentrated just across the Yalu River in Manchuria. Some of these forces crossed over into Korea in October and early November. Sharp clashes with UN troops ensued, and Army intelligence discovered the Chinese presence by finding that US and ROK forces had taken Chinese prisoners.[8]

The meaning of all this remained enigmatic. The Chinese soon disengaged, and the Chinese prisoners of war, when interrogated, claimed they were members of "Special Military Units" which at first were assumed to be only token cadres from the Fourth Field Army. While Army intelligence realized the Chinese did have the military capability for a full-scale intervention, it doubted they would pursue such a course. If the Chinese had failed to intervene in August, when the Eighth Army was trapped in the Pusan perimeter and intervention could have been decisive, it seemed irrational for them to intervene when North Korea had been broken. It appeared more plausible to assume the Chinese presence in Korea was in the nature of a face-saving gesture.[9]

The hard fact was that FECOM again found itself reduced to speculation about enemy intentions because it still lacked the intelligence resources needed to resolve the

---

[a] Of the early parachute agents, Marshall noted that "Frequently the Commanding General's plane was used to carry these men into nowhere." The TLO, as one officer put it, was basically a "glorified reconnaissance unit" designed to obtain order of battle information by using agents to conduct shallow penetration missions. To ensure it remained under GHQ FECOM control, the TLO was also assigned a notional strategic intelligence mission. Agents were a mixed bag whose numbers included high school-age children, women, the aged, and deserters from both the North and South Korean armies.

[a] Marshall grimly noted that in these operations, "Only the loss rate fulfilled expectations." Returning agents ran the risk of being mistaken for enemy infiltrators and shot by troops from their own side.

At this critical juncture, FECOM turned once more to clandestine HUMINT to meet its pressing need for intelligence.

problem. Manchuria was off-limits to photographic reconnaissance because of diplomatic considerations, limited aerial surveillance of Korea was unproductive, and other sophisticated collection mechanisms were targeted exclusively against the Korean problem and lacked the linguistic and technical capability to switch quickly.[10]

With his armies on the threshold of victory—the vanguards of the Eighth Army were across the Chongchon River in western Korea, those of X Corps nearing the Yalu in the East—MacArthur was in no mood to be deprived of triumph by the mere specter of a Chinese Army. He decided to subject the question of just what Chinese intentions might be to an acid test. On 24 November 1950, he ordered his widely dispersed forces to attack into the unknown.[11]

KLO Handicaps

The UN offensive ran head-on into 30 Chinese divisions that had secretly crossed over from Manchuria. The attack became a fighting retreat. The Eighth Army fell back from the Chongchon with heavy losses; X Corps began the difficult process of cutting its way back through the mountains to the port of Hungnam. By mid-December, as UN forces continued their retreat, the Chinese once more disengaged. Pursued by an overwhelming force, the Eighth Army found itself completely ignorant of how this force was disposed or where it might be attacking next.[a 12]

At this critical juncture, FECOM turned once more to clandestine HUMINT to meet its pressing need for intelligence. But the KLO organization (now officially titled the Far East Command Liaison Group, Korea) was in no condition to meet the requirements. There were no agent assets in the areas in which the Chinese were advancing. The KLO did have the capability of inserting parachute agents in "blind drops," using Air Force C-47s, but the AVIARY program, as it was called, operated under severe disabilities. The standard of agent training was low, and the KLO had no radios suitable for agent work and no agents trained in radio operation. In a desperate attempt to clarify the tactical situation, the KLO was reduced to dropping 12 two-man agent teams equipped with smoke grenades north of UN lines to establish the location of the Chinese forces. Only a few teams ever managed to signal Air Force spotter planes, all with negative results.[13]

[a] Upon assuming command of the Eighth Army, Gen. Matthew B. Ridgway recalls that all he had in the way of intelligence about the enemy north of his lines was a map showing "A big red goose egg...with '174,000' scrawled in the middle of it." The situation did not quickly improve; in February 1951, Ridgway reported that, "We have a curtain beyond the range of our immediate combat intelligence activities which I find extremely difficult to pierce."

The 442d CIC Detachment

In these darkest days of the war, FECOM responded to the intelligence challenge by setting up a new unit to conduct an expanded program of clandestine HUMINT. The 442d CIC Detachment was activated on 20 December 1950 in Seoul with 50 assigned personnel to take over operational control of the KLO central office and the division level TLOs. On paper, the 442d was a normal CIC unit, organized under a standard cellular Table of Organization and Equipment (TOE 30-500) and commanded by a regular army officer, Col. C.A. Dickey. In reality, it was a highly unusual organization assigned a positive clandestine collection mission that went far beyond the CIC's normal responsibilities.[14]

The 442d had a turbulent beginning. Two days after the unit was officially activated in Seoul, the deteriorating military situation forced it to establish a rear headquarters in the city of Taegu. The rest of the headquarters soon followed to escape the second Communist occupation of the South Korean capital. But the rapid revival of the Eighth Army's fortunes

under its new commander, Gen. Matthew B. Ridgway, put an end to further UN retreats. Working from a secure base, the 442d was able to upgrade the FECOM clandestine HUMINT program between January 1951 and the first armistice negotiations in June, making significant accomplishments in the areas of agent insertion, communications, and training.[15]

Until early 1951, agents had been inserted by line-crossing and by parachute drop. At the TLO level, hundreds of Korean peasants were sent to gather limited information about enemy dispositions in front of the UN lines. The KLO had its own line-crossers; it also paradropped smaller numbers of Korean agents on long-range collection missions, using Air Force AVIARY C-47s controlled by Eighth Army's Special Activities Mission. Both techniques resulted in heavy losses of agents.[a] To remedy this situation, the 442d began to supplement its ground and parachute insertion methods by using boats to land agents behind enemy lines, a course first suggested in the summer of 1950.[16]

At the same time, the 442d CIC Detachment's headquarters element implemented a much larger program of amphibious espionage and was given the codename SALAMANDER.

SALAMANDER

Confronted by an unacceptable loss rate among their line-crossers, the TLO teams of the 3d and 25th Infantry Divisions began transporting agents by small boats around the enemy's flank on the west coast of Korea. At the same time, the 442d CIC Detachment's headquarters element implemented a much larger program of amphibious espionage and was given the codename SALAMANDER. This involved the use of Korean-manned fishing boats to insert long-range agents deep within enemy territory. SALAMANDER operations were initially conducted from the numerous islands off the Korean west coast that were to the rear of the enemy's lines. These islands were rendered more or less secure from hostile attack by the UN naval blockade, and many were already in the hands of anti-Communist North Korean partisans.[17]

The first SALAMANDER operations were mounted from the island of Paengyong Do, just below the 38th parallel. They soon moved to a more advanced base at Cho Do, strategically located just five miles off the North Korean coast. The position gave the 442d's agents access to the whole west coast of Korea up to the Yalu River. To complement this west coast operation, the 442d later initiated plans to establish an east coast SALAMANDER base on the bleak and inhospitable island of Yodo. This move would provide intelligence coverage of another enemy flank, as well as allow agents to provide extensive lateral coverage of North Korean positions, because they could land on one coast and exfiltrate from the other. Because the native fishing boats used by the operation were both small and unseaworthy, the 442d quickly took steps to secure fast American craft.[18]

Better Communications

Agent communications were also improved. Until the end of December 1950, radios had been unavailable, and the 442d's agent handlers were forced to wait until an agent actually returned to base before they could procure any intelligence. The situation gradually improved in 1951. Radio teams equipped with SCR-300 walkie-talkies were provided for both AVIARY and SALAMANDER operations.

[a] Parachute operations were particularly costly: a former AVIARY operations officer estimated that only 20 percent of agents dispatched managed to make it back to UN lines. (However, he thought it possible that an unknown number of the agents who failed to return were stranded North Koreans who had used AVIARY as an airline ticket home.) Until agents could be furnished radios, these operations also involved long delays in procuring intelligence: because of the distances involved, paradropped agents commonly took two to three months to complete their missions.

The growing efficiency of FECOM's clandestine HUMINT operations was paralleled in other intelligence fields, as language and other problems were resolved.

agents to furnish Army intelligence with information on a real-time basis. But this was not a panacea. Voice radio had its limitations; its short range meant that relays had to be used—SALAMANDER agents passed their messages through the Cho Do base—or that aircraft had to hover in the immediate area of the agent radio teams, risking compromise of the mission. An additional complication was that some of the Air Force crews who provided communications support to AVIARY operations were inexperienced because they flew the mission for an average of only two weeks. Many agent radio teams were lost. Continuous wave (CW) radios, with their longer range, would have helped, but agents had not yet been trained in Morse code.[a] [19]

On the other hand, at least agents were now provided with some minimal training. In March 1951, the 442d set up a training school at Pusan that provided 20 agents at a time with a basic two-week course of instruction. (The facility moved to Taegu in June.) After com- went to the TLO teams and the 442d's central office. Unsurprisingly, American intelligence personnel rated the new breed of agents as "far superior" to their predecessors. For example, reports noted that the new agents "appear to be enthusiastic" and "have a basic idea of the mission."

Better training seems to have been partially offset by increased enemy security measures. Line-crossing continued to be a hazardous operation, and agent capture rates increased, although a surprisingly large number of detained agents were able to escape and make it back to UN lines. At any rate, the new recruitment and training program made it easier to obtain replacements.[20]

Improved Capabilities

The growing efficiency of FECOM's clandestine HUMINT operations was paralleled in other intelligence fields, as language and other problems were resolved. The overall improvement of intelligence capabilities took place during a period when the Eighth Army's fortunes were on the upswing. As early as mid-January 1951, UN forces had been able to mount a limited counterattack. In March, Seoul was recaptured. While MacArthur was relieved for insubordination in April and replaced by General Ridgway, UN forces continued to push the enemy back across the 38th parallel. On 23 June 1951, the Soviet UN Ambassador announced that North Korea was now interested in peace talks, and Ridgway offered armistice negotiations to the enemy commander.[21]

Peace was not at hand, however. Although peace talks began and the UN forces halted their advance, there was no ceasefire. Negotiations dragged on for two years, accompanied by a static war of attrition in which hills changed hands from time to time in bloody skirmishes while the main battleline remained stable. No longer forced to respond to the intelligence crises of the moment, FECOM began to build up an elaborate semipermanent clandestine HUMINT structure to meet the needs of a new kind of war.

The Liaison Detachment

The new effort was conducted under a revised organizational structure. The 442d CIC Detachment was inactivated on 26 July 1951, and its personnel and assets transferred to a new organization, the 8240th Army Unit. (In addition to its Korea-based assets, the 8240th consisted of a headquarters element in Tokyo and a logistic element in Sapporo, Japan.) The former KLO/TLO organization now became known as the Far East Command Liaison

[a] Twenty UHF-VHF air-sea rescue sets had been acquired in mid-December but had arrived without operating manuals and proved to be of insufficient range to be useful. Once voice radios became available, airborne radio control support was provided by the C-46s of the 438th Troop Carrier Command staging out of Japan.

Detachment, Korea. The Liaison Detachment, commanded by Col. William I. Russell, had an authorized strength of 104. Because of a shortage of intelligence specialists, and the Army's decision to return gradually all CIC personnel to their normal assignments, it took some time to gather the necessary numbers. Colonel Russell started out with only the 50-odd people he had inherited from the 442d.[22]

The tight personnel situation led to a new development in agent training—agent nets—that were set up by the summer of 1951. These consisted of permanent agent organizations behind enemy lines, linked to headquarters by radio control and supplied and reinforced by SALAMANDER and AVIARY operations. These nets were now entrusted with training, thus allowing the school at Taegu to be shut down. Under the new arrangements, each net recruited its own agents (many from the large refugee camps on the island of Koje-do), put them through a two-week training course, and sent them to the frontline TLO teams for assignment in the field. Agents who successfully completed five line-crossing missions were given two weeks of additional training and then went into the SALAMANDER or AVIARY programs.

The new approach was not completely successful. In practice, only 25 percent of agents managed to complete as many as four line-crossing missions for the TLOs. Centralized training was revived in October, when three nets were consolidated and a new school set up in Seoul. Ultimately, a compromise between the two approaches was reached: the nets provided basic agent training and the school became responsible for advanced radio and parachute training.[23]

By the summer of 1951, it was at last possible to set up a 10-week Morse code course for agents, which permitted the nets to use long-range CW radios.

New Sources of Agents

In addition, the Liaison Detachment found new sources from which to procure agents. A Korean religious group with many adherents in the North, the Chando Kyo, was tapped to provide an agent network. Chinese POWs who rallied to the UN side were dispatched on order of battle missions. Finally, the Liaison Detachment acquired 124 agents formerly employed by the ROK Army's Headquarters Intelligence Division (HID). These agents had been operating from bases on the Korean east coast, both at Yodo, where there were already Liaison Detachment operatives, and on islands in Wonsan Harbor. Because the HID had run out of funds, the US Army picked up the tab and the people.[24]

The Liaison Detachment also further improved agent communications. By the summer of 1951, it was at last possible to set up a 10-week Morse code course for agents, which permitted the nets to use long-range CW radios. By September, an elaborate communications system was in place. A network of safehouses forward of UN lines received intelligence reports from agents via voice radio. The reports were then relayed back to the various TLOs by means of Morse code. The safe houses employed SSR-5-R CW radios; the TLOs were equipped with the standard Army AN/GRC-9's. Message traffic was then passed on by the TLOs to Liaison Detachment headquarters. The main SALAMANDER base at Cho Do communicated with headquarters and its west coast agents by similar means.[25]

By the fall of 1951, the Liaison Detachment began to reevaluate its procedures for inserting long-range penetration agents. The SALAMANDER operation, which used boats to land and retrieve agents, had been very successful. By contrast, the AVIARY program, which dropped parachute agents deep within enemy territory and then required them to make it back to UN lines on their own, produced less satisfactory results. Although AVIARY operations were intensively pursued—111

The Liaison Detachment thus became a miniature Army version of the World War II OSS, with responsibilities for secret intelligence and special operations,

ing a single month—the rate of return was discouragingly low. At one point in October, the Liaison Detachment contemplated reducing its airborne operations by 50 percent. Instead, it decided to adopt a new technique. Agents would be dropped in teams close behind enemy lines, wearing enemy uniforms and carrying small arms. In this way, they could impersonate enemy patrols and, if necessary, shoot their way back to UN lines. Use of this tactic, along with better screening of agents and more specific intelligence assignments, greatly reduced losses and gave AVIARY a renewed viability.[26]

CCRAK and the Liaison Detachment

The Army's clandestine HUMINT effort in Korea had now become part of a wider secret war, waged on an extensive but uncoordinated basis. In parallel with the Liaison Detachment's operations, the Eighth US Army was supporting a growing partisan effort on the Korean west coast that was based on the same islands that served as SALAMANDER bases. These islands also provided bases for various clandestine operations undertaken by the US Air Force, which used them to gather intelligence and to support the escape and evawas another player in the secret war.[27]

To better coordinate these fragmented efforts, a new theater-level structure was created on 10 December 1951, called the Combined Command for Reconnaissance Activities, Korea (CCRAK). CCRAK was an umbrella organization set up to impose centralized control on the secret activities of the armed services, the CIA, and the ROK allies. At the same time CCRAK was formed, the Army decided to place all its covert and clandestine efforts under a single headquarters. The Eighth Army's 8086th Army Unit, which had been running the partisan effort, was dissolved. The Liaison Detachment took over its functions and assets.[28]

The Liaison Detachment thus became a miniature Army version of the World War II OSS, with responsibilities for secret intelligence and special operations, the first time these two functions had been combined in a single Army organization. The arrangement had a certain logic to it. In accordance with existing doctrine, it moved control of partisan warfare from the field army to the theater level. The reorganization also provided the Liaison Detachment with a partisan force that could protect its island bases and provide it with supplementary intelligence reports. And the Liaison Detachment was finally in a position to prevent partisan operations from inadvertently jeopardizing intelligence activities.[29]

More Manpower

This increase in the Liaison Detachment's responsibilities brought with it an increase in personnel. By February 1952, the Detachment had 150 assigned or attached personnel on board; by the time a ceasefire was finally concluded in the summer of 1953, the Detachment had a strength of 450. (Even then, there were complaints that the Detachment still had too few intelligence personnel to fulfill mission requirements.) While Army strength in Korea remained stable from 1951 on, the proportion of resources devoted to intelligence and covert activities was much expanded. Because UN policy ruled out additional territorial gains on the battlefield, the secret war was the only combat arena in which efforts could be intensified.[30]

A good part of the growth permitted by this strength increase went into expanding the clandestine HUMINT effort. By 1953, a large, formidable organization had been fielded. The Liaison Detachment's Intelligence Division controlled five separate Intelligence Commands. Each had its own geographic area of responsibility

(although one command conducted operations on both coasts of Korea and across the frontlines), but the commands were also allowed to penetrate North Korea, Manchuria, and China proper to the extent their resources permitted. The five commands directed the activities of 17 separate agent nets, all with radio links to the appropriate command headquarters.

No fewer than 2,100 agents reported to the Liaison Detachment. Badger Net alone had 450 agents. Three hundred of these were in North Korea, either in permanent cells or as temporary inserts; the rest were at headquarters, in training, or in reserve.[31]

Intelligence Production

The nature of the game meant that the structure was not perfect. The necessity of setting up a clandestine organization in a denied area under wartime conditions had forced compromises both in administration and in the caliber of recruited agents. (In light of the fact that it was not until 1953 that TLO agents received the same pay as day laborers working for the Eighth Army, the latter deficiency is particularly unsurprising.) Some nets produced only inconclusive results, and no evidence exists that any were able to supply high-level intelligence on enemy plans.

Nevertheless, by the end of the war the Liaison Detachment had become the chief producer of HUMINT for the whole CCRAK organization, furnishing up to 1,000 intelligence reports a month, most graded by consumers as being of significant importance. This represented a five-fold increase over the detachment's output in 1951. The Liaison Detachment's contribution to CCRAK was as great as that of the Air Force's clandestine service, ROK Army G-2, and the CIA's collection element combined.[32]

The Korean agents bore most of the costs and risks, and their losses had been high, especially in the first stages of the effort.

Paying a Price

This elaborate clandestine HUMINT apparatus was not built without a certain price. The Korean agents bore most of the costs and risks, and their losses had been high, especially in the first stages of the effort. But Liaison Detachment personnel also met their deaths trying to insert agents. An Air Force C-46 went down over North Korea one night in February 1952, carrying three Detachment personnel, seven Air Force crewmen, and six Korean agents and an interpreter.

In April 1953, the ill-omened Fizzle Net, operating from Yodo on the east coast under the 4th Intelligence Command, ceased to exist when the American lieutenant serving as project officer was ambushed and killed with his agent party in a landing attempt that went awry.[33]

Partisan Warfare

The expansion of the partisan operation that the Liaison Detachment had taken over from the Eighth Army at the end of 1951 was even more striking. The private army of guerrillas inherited by the Liaison Detachment originated in the various groups of anti-communist refugees from North Korea who had fled to the islands off the western coast of Korea in the winter of 1950-1951. The Eighth Army had taken these groups in hand in early 1951 and used them to form a partisan force. So-called donkey units of partisans were assembled around a hastily trained indigenous cadre and used as a raiding force against the mainland. The islands from which they operated were strategically located behind enemy lines and were protected from enemy attack by the UN naval blockade and ROK garrisons. Because the partisans required only a few American personnel as advisers, they represented an effective, inexpensive force multiplier for the Eighth Army.[34]

But when the final cease-fire was concluded in June 1953, the last radio message to reach the Liaison Division from Green Dragon was a curse.

key units on the Korean west coast had been grouped into two regiments named Leopard and Wolfpack. In addition, a company assigned the designation Kirkland had been organized on Yodo Island off the east coast of Korea. At this point, the increased activity and visibility of the partisans began to provoke a violent North Korean reaction. Some of the more vulnerable islands on the west coast came under enemy attack. This posed a threat to the partisans and to the SALAMANDER HUMINT operations of the Liaison Detachment. The end result was that the guerrillas had come under Liaison Detachment control.[35]

During the course of 1952, the Liaison Detachment expanded the initially small Kirkland force on Yodo to regimental strength. The Leopard and Wolfpack organizations on the west coast were also built up. Operating from their island safehavens and assisted by a sprinkling of American advisers and US logistic support, the partisans waged a lively little war of their own. That year, the partisans optimistically claimed to have inflicted 51,000 casualties on enemy forces. Partisan casualties, however, were not light: the partisans had to defend their own island bases in addition to mounting offen-

changed hands two or three times. More than 2,000 partisans became casualties in 1952, and more than half of these were killed or listed as missing in action.[36]

PAIR

The Army viewed this kind of amphibious warfare as a success. In the Korean War's wider context, however, the partisans were more of a nuisance to the enemy than a real threat. They were never able to establish any bases on the mainland or conduct operations larger than raids. Moreover, landing operations were hampered by the harsh Korean winters and, on the west coast, by the enormous tidal fluctuations that regularly turned beaches into vast and impassable mudflats.

Meanwhile, even more ambitious schemes were under way. In April 1952, FECOM produced a Guerrilla Operations Outline, 1952. This proposed adding an airborne dimension to the existing partisan amphibious operations. FECOM decreed that "all commands will qualify paratroops." Accordingly, paratroop trainees were taken from the existing Leopard, Wolfpack, and Kirkland formations and grouped in a unit that officially became the 1st Partisan Airborne Infantry Regiment (PAIR) in November 1952. At the same time, the Leopard, Wolfpack, and Kirkland units were redesignated respectively as the 1st, 2d, and 3d Partisan Infantry Regiments.[37]

The first contingent of the 1st PAIR's new airborne troops was committed to action in early 1953. On the night of 23 January, a flight of three Air Force C-119s guided by a B-26 Pathfinder aircraft airdropped a special 97-man "Green Dragon" unit behind enemy lines to set up an operational base for guerrilla activities. The fate of this first (and, as it turned out, only) major employment of partisans in an airborne role was not a happy one. After a long delay, the party made radio contact with headquarters and reported taking heavy casualties. Reinforcements and supplies were promptly flown in to sustain the Green Dragon force. But when the final cease-fire was concluded in June 1953, the last radio message to reach the Liaison Division from Green Dragon was a curse. The operation had been compromised and was under enemy control.[38]

The whole episode became just another part of the generally melancholy story of airborne special operations during the Korean War. The 8240th Army Unit and its Air Force counterpart repeatedly launched behind-the-lines sabotage missions. Hundreds of Koreans floated down on night drops into the black hole of

North Korea and were never heard from again. In 1952, the 8240th had paradropped "Mustang Ranger" teams of partisans behind enemy lines on half-a-dozen occasions to attack enemy railroad lines. The teams varied in size from five to 20 men. They all met the same fate. After the "Green Dragon" operation had commenced, additional large sabotage teams drawn from the ranks of the 1st PAIR were sent in. None survived.[39]

In 1951 and 1952, the Far East Air Force had dropped some 200 sabotage agents of its own on 19 separate missions directed against North Korean facilities. The agents accomplished practically nothing, and only one party ever returned safely to UN lines. Despite these unpromising precedents, the Liaison Detachment's Guerrilla Division had laid plans in the spring of 1953 to use the 1st PAIR's "Southwind" element in yet another attempt at mounting sabotage operations. It proposed to parachute in 48 two-man teams to blow up North Korean railroads. Perhaps fortunately for all concerned, the mission was never implemented.[40]

The failure of the Green Dragon operation did not become apparent until the fighting had ended. Thus, during the first part of 1953, the Liaison Detachment was encouraged to lay down plans for an ambitious and greatly expanded program of guerrilla warfare. In addition to building up the 1st PAIR, the Detachment expanded two of its original regiments to provide additional forces for seaborne raids and assaults. The overstrength 1st Partisan Infantry Regiment was split up, allowing the formation of a new 6th Partisan Infantry Regiment. In similar fashion, the 2d Partisan Infantry Regiment contributed personnel to form a new 5th Partisan Infantry Regiment. The regiment based on the Korean east coast, the 3d Partisan Infantry, was too small to break up in this way, but its members were given airborne training. (There was no 4th Partisan Infantry Regiment, because Koreans allegedly associated the number four with bad luck.) [41]

The KLO and its successor organizations, the 442d CIC Detachment and the Far East Command Liaison Detachment, Korea, occupy a unique place in the history of Army intelligence.

A Small Army

As a result of these preparations, the Liaison Detachment had fielded what amounted to its own Korean Army by the time of the July 1953 ceasefire. The six-regiment force had a strength of more than 17,000 troops. The small American cadre assigned to the partisans included 55 personnel from the Army's newly organized 10th Special Forces Group.

This guerrilla army possessed 300 trucks and trailers; was equipped with its own freighters, crash boats, and fishing vessels; and consumed 7,500 tons of supplies a month. Rice accounted for the bulk of the supply allotment; each partisan was issued 100 pounds a month, some for personal consumption, the rest for barter. The partisans also had their own chaplains, band, and travelling entertainment troupe. The Liaison Detachment even published a house magazine for them, *The Parachute.*[42]

All this was something of a triumph for American-style organization. There were, however, some liabilities. Understandably, there was a certain rivalry between the American-controlled partisans and the regular ROK forces. Also, the partisan operation had swollen to such a size that some now questioned its effectiveness. While partisan raiders had served as a useful adjunct to UN forces, their value when used in large conventional units was open to dispute, especially because of the nature of their training and equipment.

The question was never fully resolved. A ceasefire occurred before the new partisan structure could be committed to battle, the guerrillas were forced to evacuate their island bases, which lay north of the Demilitarized Zone now demarcating

North and South Korea, and most of the partisan units were disbanded.[a 43]

Psywar Activity

In 1953, the Detachment also expanded its responsibilities to include psychological warfare, or "psywar." This might seem to be an odd area of involvement for what began as an intelligence organization, but there were precedents. The OSS had conducted psychological warfare operations in World War II, and Army doctrine closely linked covert operations and psychological warfare. By mid-1953, the Liaison Detachment was providing classroom training to Koreans in psychological warfare and preparing propaganda leaflets for distribution in the enemy rear. In addition, it was using propaganda to sustain the morale of its own partisans.[44]

Evaluation

The KLO and its successor organizations, the 442d CIC Detachment and the Far East Command Liaison Detachment, Korea, occupy a unique place in the history of Army intelligence. The KLO started out as a small residual FECOM intelligence presence in Korea, increased in scope as a result of the North Korean invasion, and then was redesignated and further expanded during the darkest days of the war. Ultimately, it was redesignated once more and given responsibility for the whole Army covert and clandestine effort in Korea. Its particular pattern of organization, however, would not provide an operational model for Army intelligence in the future. The Liaison Detachment's structure was revamped almost as soon as the fighting in Korea ended.

Essentially, the Liaison Detachment was a creature of the Korean war. Its efforts produced a certain long-term impact: the Army was made aware of the potentialities for conducting positive human intelligence collection in peace as well as war. Moreover, certain Special Forces operations in Vietnam would later parallel, but not replicate, Liaison Detachment activities in Korea. Generally, however, the organization's accomplishments and the lessons learned from them went down a historical memory hole and passed into oblivion along with other aspects of America's "forgotten war" in Korea.[45]

❖ ❖ ❖

[a] Evanhoe felt that exacerbating this rivalry was the "large influx of South Korean citizens into partisan ranks whose only reason for volunteering was to escape being drafted into the South Korean Army," as well as the fact that "Many of those recruited were pimps, thieves, and other undesirables who were hiding from South Korean authorities and wanted to use duty with the partisans to escape."

Endnotes

1. John K. Singlaub, *Hazardous Duty: An American Soldier in the Twentieth Century* (New York: Summit Books, 1991), 156–66.

2. Bruce W. Bidwell, "History of the Military Intelligence Division, War Department General Staff," (US Army Center of Military History unpublished ms., Vol. VII, Chapter III), 22.

3. On the overall unreadiness of the Eighth Army in the summer of 1950, see Clay Blair, *The Forgotten War: America in Korea, 1950–1953* (New York: Times Books, 1987), 48–50.

4. US Army Intelligence Center, "History of the Counter Intelligence Corps, Volume I: Introduction and Background," (Unpublished ms., 1959), 101.

5. Office of the Assistant Chief of Staff, G-2, GHQ FEC, "Historical Report, 1 January-30 October 1950," 103, RG 338, NARA; Assistant Chief of Staff, G-2, "Summary of Major Activities Relating to the Korean Conflict, 25 June 1950-8

Endnotes (cont.)

September 1951," US Army Center of Military History; S.L.A. Marshall, *The River and the Gauntlet: Defeat of the Eighth Army by the Chinese Communist Forces, November 1950, in the Battle of the Chongchon River, Korea* (Nashville: Battery Press, 1987), 5.

6. S.L.A. Marshall, *The River and the Gauntlet*, 3–4, and author's interview with Russell K. Leick, 20 January 1985.

7. S.L.A. Marshall, *The River and the Gauntlet*, 5; 442d Counter Intelligence Corps Detachment, Historical Report, 1 March 1951, RG 319, NARA; and Ed Evanhoe, *Darkmoon: Eighth Army Special Operations in the Korean War* (Annapolis: Naval Institute Press, 1995), 13.

8. Roy E. Appleman, *United States Army in the Korean War: South to the Naktong, North to the Yalu* (Washington, DC: Office of the Chief of Military History, 1961), 761.

9. Ibid., 753, 761–64.

10. Ibid., 769–70; Historical Report, 442d CIC Detachment, 1 March 1951, RG 319, NARA.

11. James F. Schnabel, *United States Army in the Korean War: Policy and Direction: The First Year* (Washington, DC: Office of the Chief of Military History, 1972), 278.

12. *Soldier: The Memoirs of Matthew B. Ridgway, as told to Harold H. Martin* (Westport: Greenwood Press, 1974), 205; Roy E. Appleman, *Ridgway Duels for Korea* (College Station: Texas A&M Press, 1990), 312.

13. Memorandum for Record, Far East Command Liaison Group, 17 December 1950; Command Report, 442d CIC Detachment,1 January 1951, RG 319, NARA.

14. GO 86, GHQ FEC, 8 December 50-AMENDED by GO 87, GHQ FEC, 11 December 50; Foreword, Historical Report, 442d CIC Detachment,1 March 1951, RG 319, NARA.

15. Command Report-December 1950, 442d CIC Detachment.

16. Ibid. and author's interview with Winston J. Morgan, 30 January 1985.

17. Historical Report, 442d CIC Detachment, 1 March 1951.

18. Ibid.; Historical Reports, 442d CIC Detachment, April 1951, May 1951, June 1951, RG 319, NARA.

19. Memorandum for Record, Far East Command Liaison Group, 17 December 1950; Command Report-December 1950, 442d CIC Detachment; Historical Report, 442d CIC Detachment, June 1951, RG 319, NARA; and Historical Report, 442d CIC Detachment, April 1951, RG 319, NARA.

20. Historical Reports, 442d CIC Detachment, April 1951, May 1951, July 1951, RG 319, NARA.

21. Schnabel, *United States Army in the Korean War.*

22. GO 53, GHQ FEC, 24 July 1951; Historical Report, Far East Command Liaison Detachment, Korea (FEC/LD(K)), 8240th Army Unit, 1 August 1951. Eight Navy personnel were assigned to the unit in a temporary duty status.

23. Historical Reports, FEC/LD (K), 1 September 1951, 1

24. Historical Report, FEC/LD (K), l November 1951.

25. Ibid.

Endnotes (cont.)

26. Historical Reports, FEC/LD (K), 1 August 1951, 1 November 1951.

27. *Guerilla Warfare and Airpower in Korea, 1950–1953* (Maxwell Air Force Base, Aerospace Studies Institute, 1964), 64–72; Alfred H. Paddock, Jr., *US Army Special Warfare: Its Origins: Psychological and Unconventional Warfare, 1941–1952* (Washington, DC: National Defense University Press, 1982), 103.

28. *Guerrilla Warfare and Airpower in Korea*, 86; Paddock, *US Army Special Warfare*, 103. One knowledgeable Army officer dismissed CCRAK as "a hodgepodge intelligence operation." Singlaub, *Hazardous Duty*, 181–82.

29. *Guerrilla Warfare and Airpower in Korea*, 86.

30. Historical Report, FEC/LD (K), 1 April 1953, RG 319, NARA.

31. Ibid.

32. Ibid.

33. Historical Report, FEC/LD (K), 1 March 1952; Combat Command Report, Summary of Operations, Intelligence Division, FEC/LD (K), 1 June 1953, RG 319, NARA.

34. *Guerrilla Warfare and Airpower in Korea*, 64–65, 70–71, 80–84.

35. Ibid., 89; Historical Reports, FEC/LD (K), 1 November 1951, 1 March 1952, RG 319, NARA.

36. Historical Report, FEC/LD(K), 1 March 1952; Monthly Command Report, HQ, Partisan Command, FEC/LD (K), 4 April 1953, RG 319, NARA.

37. *Guerrilla Warfare and Airpower in Korea*, 96–99.

38. Ibid., 148–150.

39. Evanhoe, *Darkmoon*, 157–60.

40. *Guerrilla Warfare and Airpower in Korea*, 146–50.

41. Monthly Command Report, HQ Partisan Command, FEC/LD (K), 4 April 1953.

42. Ibid.; Combat Command Report, Summary of Operations, Intelligence Division, FEC/LD (K), 1 June 1953; Command Report No. 7, FEC/LD (K), 6 August 1953, RG 319, NARA.

43. Evanhoe, *Darkmoon*, 163. Combat Command Report, Summary of Operations, Intelligence Division, FEC/LD (K), 1 June 1953; Paddock, US Army Special Warfare, p. 103; Command Report No. 7, FEC/LD (K), 6 August 1953.

44. Monthly Command Report, HQ Partisan Command, FEC/LD (K), 4 April 1953.

45. Command Report, FEC/LD (K), September 1953, 1 October 1953, RG 319, NARA; GO 269, HQ USAFE, 27 September 53; Richard H. Shultz, Jr., *The Secret War Against Hanoi: Kennedy's and Johnson's Use of Spies, Saboteurs, and Covert Warriors in North Vietnam* (New York: HarperCollins, 1999), passim; John P. Finnegan, *The Army Lineage Series: Military Intelligence* (Washington, DC: US Army Center of Military History, 1998), 124—27.

❖ ❖ ❖

Grappling with Covert Action after the Cold War

Clinton's Secret Wars: The Evolution of a Commander in Chief, *by* Richard Sale. (New York: St. Martin's Press, 2009), 491 pp., index.

Matthew P.

Former President Bill Clinton's foreign policy reputation has suffered from charges that he was disengaged, ambivalent, and hesitant to use military force. In *Clinton's Secret Wars: The Evolution of a Commander in Chief*, journalist Richard Sale attempts to refute those charges by arguing that nonpublic initiatives, especially the use of covert action, show that Clinton was more proactive and resolute in dealing with foreign policy crises than his critics have allowed. Though the book does not succeed in making this case—at least in this reader's judgment—Sale does add to public understanding of some of the lesser-known foreign policy options available and how the first president to take office after the Cold War used them.

Sale struggles, sometimes contradicting himself, to show Bill Clinton growing steadily in knowledge and fortitude through his terms of office into a man of action. In describing the period after the infamous October 1993 Black Hawk episode in Somalia, Sale writes, "Something in Clinton had hardened, and he emerged from the crisis a different man."(88) By spring 1994, "Clinton's aggressiveness had blazed like a torch…[and] his advisors caught glimpses of some fresh, inner steel."(114) Yet, Sale continues to depict Clinton as vacillating, exhibiting a caution on Bosnia, for example, that "nearly crippled him." (137) But four pages later, in discussing Clinton's actions in July 1995, Sale alludes to "new inner toughness," (144) and by August, a "new unleashed aggressiveness."(152)

Sale provides no solid evidence for all these supposed increases in toughness. By the beginning of Clinton's second term in January 1997, the United States had failed to stop Serbian leader Slobodan Milosevic's forces from overrunning Srebrenica, and two timid regime change initiatives had failed in Iraq. At that point, Clinton still followed the lead of cautious allies on Iraq. With respect to countering terrorism, the administration had no real plan, even though Sale claims that by the summer of 1998, Clinton "was like a great sea bird, a storm petrel, swooping low over the waves alert for any prey." (302) The record shows otherwise: Clinton exerted little or no pressure on the Taliban or the government of Pakistan. Not until mid-1999 does the book show Clinton in full form, rallying allies to escalate a bombing campaign against Milosevic. But this was hardly a brazen stand, since everyone from France to Human Rights Watch to the Quakers supported military action.[1]

Sale also is given to interpreting evidence selectively in Clinton's favor. For example, when Clinton used third countries to supply arms to Bosnia—a tactic that avoided a covert action finding and its attendant congressional oversight—the move can be seen as laudably resourceful if one is sympathetic to the subject or as subversively abusive of power if not. During the 1995 Dayton negotiations, the Clinton administration agreed to keep Milosevic in power to retain a negotiating partner who could speak for the Serbs. Sale finds this bold:

[1] On the various human rights groups supporting military action, see Samantha Power, *"A Problem from Hell": America and the Age of Genocide* (New York: Basic Books, 2002), 434–35. Power's book, especially the pages that address the Clinton presidency (pages 293–502) generally support the conventional wisdom concerning Clinton's handling of foreign policy.

All statements of fact, opinion, or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of an article's factual statements and interpretations.

"To keep the peace process alive, Clinton would use Milosevic, squeeze him like a rind, then toss him away." (158) A more critical perspective might have been that the compromise laid at Clinton's feet the entire record of Milosevic's human rights atrocities from then on.

The discussion of renditions of terrorists to third countries during that period also reflects a favorable bias. Even though Clinton's White House counsel warned that such renditions violated international law, Sale depicts them as brave, in contrast to the criticism of renditions often made of the subsequent administration. Similarly, Sale blames most of Clinton's first-term foreign policy trials on his predecessor, George H.W. Bush, but he gives no indication that Clinton similarly burdened his successor by not curbing Iran's influence in the region or by delaying action against al-Qa'ida. If any single sentence in the book highlights Sale's tendency to see toughness where it might not be, it is the following quote from Clinton: "If anybody f—s with us, we'll respond. And we're going to get the UN to finally show up and take over." (88)

Whether the book salvages Clinton's foreign policy reputation or not, it does a service by exploring the important subject of covert action in the post–Cold War era. The original 1947 mandate for covert action—a US foreign policy activity in which Washington's hand remains hidden—specified that it was to be used for countering communism. Until 1991, the goal of most covert actions—even if they were not in response to a direct communist threat—was to counter communist influence or Soviet-backed governments. The fact that the United States continued a robust covert action agenda against a complex matrix of threats after the demise of the Soviet Union makes for a fascinating field of inquiry. As Sale suggests, the process by which the US government decides to undertake a covert action program is interesting in and of itself, drawing input from sometimes competing and sometimes cooperating (although not always amicably) elements of the government, including various members of the Intelligence Community.

The relationship between intelligence and policy in the covert action context deserves study, and at times in this book Sale hints at exploring it more fully. "It is a common myth that intelligence helps shape policy," Sale writes, "but the opposite is true. Policy, or the lack of it, usually shapes and fashions intelligence."(43) Sale's book also shows CIA in a role that this reviewer believes is its most underappreciated, that of serving as a shadow State Department, clandestinely engaging with foreign governments and security services on a range of unacknowledged projects and serving as a back channel to foreign leaders. This function, even if not explored in great detail, appears in the background in much of the book.

Overall *Clinton's Secret Wars* would have been better if Sale had not tried to right a perceived wrong in prior assessments of Clinton's foreign policy and had instead taken a more straightforward look at the use of covert action in the post–Cold War environment. This could have been done with only minor tweaks, namely, excising the effusive language about the president's ever-intensifying focus and his perpetually rejuvenating inner steel, observations that repeatedly detract from the more interesting material on creative foreign policy options available to him. Though his successors used these policy alternatives against similar targets, it was Clinton and his team that refined and debated them for the first time after the Cold War. By taking the reader on a tour through eight years of an administration grappling with such questions in a changed world, Sale has made a significant contribution other than the one he seems most to have intended.

❖ ❖ ❖

Takes on Intelligence and the Vietnam War

Vietnam: The History of an Unwinnable War, 1945–1975, by John Prados. (Lawrence: University Press of Kansas, 2009), 665 pp.

Why Vietnam Matters: An Eyewitness Account of Lessons Not Learned, by Rufus Phillips. (Annapolis, MD: Naval Institute Press, 2008), 398 pp.

This Time We Win: Revisiting the Tet Offensive, by James S. Robbins. (New York: Encounter Books, 2010), 364 pp.

Reviewed by Clayton Laurie

On hearing different and opposing assessments regarding US progress in Vietnam by two members of the same fact-finding team in the fall of 1963, President John F. Kennedy quipped, "The two of you did visit the same country, didn't you?" Readers of these three books seeking a better understanding of the CIA's role in Southeast Asia and the lessons of that conflict for today may well ask a similar question. Nearly 40 years after the end of the US involvement, after the publication of a score of histories describing CIA activities during that time, and after the declassification of thousands of documents, opinions regarding Agency failures and accomplishments remain far apart, as do the authors' interpretations of how the experiences of Vietnam apply to the conflicts of today.

Independent historian and self-described "engaged leftist intellectual" John Prados needs little introduction to scholars of intelligence history or of the Vietnam War, as he has written some 17 books on these subjects.[1] His latest work, published by the University Press of Kansas, will undoubtedly have a wide readership and garner acclaim from those who share his interpretations of the war and of the CIA. A large study, with a comprehensive bibliographic essay citing a wide range of archival and published sources, *Vietnam: The History of an Unwinnable War* is a recipient of the Henry Adams Prize from the Society for Historians in the Federal Government and has received numerous accolades from academic reviewers. The history, intended as a broad overview of the conflict, deals extensively with high politics and the antiwar movement, but it also frequently refers to the CIA's role at home and abroad.

Prados tends to view the CIA as an organization whose activities in Southeast Asia and at home generally contributed more to the problems of the day than to their solutions. Such critical assessments emerge throughout this work when the CIA is mentioned, starting with the Saigon Military Mission (SMM) in 1954 and extending through passing treatments of covert operations, the order-of-battle controversy, Agency activities in Laos, the Phoenix program and rural pacification, and involvement with South Vietnamese leaders. From this work, however, a reader new to CIA history would get the erroneous impression that the Agency engaged in all manner of nefarious activities in Vietnam, failed in most every Southeast Asia-related mission, and spent the

[1] Prados is affiliated with the George Washington University's National Security Archive, and he frequently blogs about the CIA on the archive website, www.gwu.edu/~nsarchiv/.

All statements of fact, opinion, or analysis expressed in this article are those of the author. Nothing in this article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

better part of its resources on illegal surveillance and collection activities against those involved in the antiwar movement at home—the latter a rare and relatively brief deviation from the Agency's traditional foreign intelligence mission, which did score numerous Cold War successes in Southeast Asia and elsewhere.

Prados has chosen to give little or no attention to publicly available CIA-commissioned histories of the period, and unfortunately his book went to press before the release in 2009 of several in-depth, formerly classified, CIA-sponsored histories written by Thomas L. Ahern, and before the release of documents on the Agency's proprietary airline, Air America.[2] Other available works, such as the National Intelligence Council's published collection of estimates produced during the Vietnam War, Ahern's published history on the CIA and rural pacification, and Harold Ford's *CIA and the Vietnam Policymakers* are cited but not extensively used in this volume.[3]

Unused and uncited are a number of well-documented and rich treatments of Agency programs that give fuller and more positive perspectives—although not without criticism—on its efforts during the period, and at the same time more accurately reflect the environment in which the Agency operated at home and abroad. For example, MHCHAOS, mentioned in passing by Prados, gets full treatment in *Richard Helms as Director of Central Intelligence*, declassified in 2006.[4] *Studies in Intelligence* also has published many now-declassified articles dealing with Southeast Asia, especially technical collection and reconnaissance programs. Other pertinent publications, such as the CIA chief historian David Robarge's monograph on the A-12 Archangel supersonic aircraft would have provided more on that technological feat.[5] Sadly, the portrayal of the CIA in Prados's work tends to reflect the antiwar, anti-Establishment view so often heard since the 1970s, when the Agency first faced lurid and media-sensationalized allegations of wrongdoing and intense congressional hearings.

In recent years, a new generation of Vietnam War scholars, many born after the conflict and whose perspectives come from scholarly research rather than direct participation in the war's events at home or in Southeast Asia, have challenged many accepted interpretations touched on in Prados's work, such as his discussion of the Phoenix program, and suggest that revisions in his thinking might be in order. But Prados dismisses those other scholars and the debate they have initiated. He writes, "this is not revisionism, it is neo-orthodoxy." (328) One would conclude from such statements that the author made up his mind about US and CIA involvement in Southeast Asia long ago and that no amount of new material will change his views. As he writes, "Ultimately I side with those who consider Vietnam an unwinnable war. I came to that view early, but extensive research and deep analysis confirm that impression." (xv) For the intelligence officer, *Vietnam: The History of an Unwinnable War* does more to reveal the author's perception of the CIA than its role in the war. For the latter, Agency-released histories provide the fullest picture.

Why Vietnam Matters: An Eyewitness Account of Lessons Not Learned, by Rufus Phillips, certainly ranks as an account that all intelligence officers should read and consider.

---

[2] The Air America material and Ahern's six studies, with one exception lightly redacted, are available in CIA's Freedom of Information Act Reading Room in its special collections section: http://www.foia.cia.gov/special_collections.asp. Ahern's volume on rural pacification was published as *Vietnam Declassified: The CIA and Counterinsurgency* (Lexington: University of Kentucky Press, 2009)

[3] Harold Ford, *CIA and the Vietnam Policymakers: Three Episodes 1962–1968* (Washington, DC: CIA Center for the Study of Intelligence, 1998). This publication is available online at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/cia-and-the-vietnam-policymakers-three-episodes-1962-1968/index.html.

[4] Robert M. Hathaway and Russell Jack Smith, *Richard Helms as Director of Central Intelligence* (Washington, DC: CIA Center for the Study of Intelligence, 1993). A scanned copy of this publication is available online at http://www.foia.cia.gov/helms.asp.

[5] David Robarge, *Archangel: CIA's Supersonic A-12 Reconnaissance Aircraft* (Washington, DC: CIA Center for the Study of Intelligence, 1997). This publication is available online at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/a-12/index.html.

Phillips's detailed memoir, which describes his service with the CIA and USAID in Vietnam and Laos between 1954 and 1968, draws on archival research, interviews, official volumes from the Department of State and CIA—including Ahern's pacification volume—plus many other pertinent scholarly publications to form a very readable account. The book makes use of many of the same sources as Prados's work, but it differs greatly in tone and in its views of the CIA's efforts, although it is still critical at times. The discursive endnotes and biographical sketches bring the reader up to date on the people who played key roles many decades ago, and an extensive bibliographical essay suggests further reading.

A US Army officer on detached service with the CIA, Phillips arrived in Southeast Asia as a member of the Agency's small SMM in July 1954. Established after a request by President Dwight Eisenhower to DCI Allen Dulles to advise and stabilize the Emperor Bao Dai's government under Prime Minister Ngo Dinh Diem, the SMM undertook what must have seemed a Herculean task. The legendary Edward G. Lansdale, a US Air Force officer assigned to the CIA and fresh from the successful repression of the Huk rebellion in the Philippines, directed the effort. In the fall of 1954, he set out to do in South Vietnam what he had done in the Philippines—stabilize, boost, and strengthen the government, while removing communist-inspired threats to the new regime.

Phillips points out early on, and frequently reiterates, that Lansdale and those small numbers concerned with the "other war" (defined as rural development and winning the support of the largely peasant southern population) worked outside the US diplomatic, military, economic, and intelligence bureaucracy in cooperation with their South Vietnamese counterparts in a relationship based on common knowledge, mutual respect, and shared goals. The SMM assisted these local efforts and never sought to dominate what was a job the Vietnamese had to do for themselves—as President Kennedy would say in an interview with correspondent Walter Cronkite in the fall of 1963. SMM personnel, in Phillips's view, from Lansdale on down, were sincere and selfless American patriots who possessed great knowledge of Asian cultures and history, superlative interpersonal skills, and a clear ability to work with, and not around, the South Vietnamese in a common fight against communism.

Perhaps most important, Phillips, like Lansdale—and unlike most American military and political leaders—recognized that the war against Ho Chi Minh represented first and foremost a political and ideological war and not a contest of arms. Victory or defeat hinged on gaining or losing adherents to the cause in both Southeast Asia and the United States. Bullets, bombs, and troops could not triumph alone, in any amount or over any length of time. Only by providing peasants with rural security, lifting them from poverty, and educating them on the merits of democracy and the evils of communism, could South Vietnam survive and the US obtain its goals. While Lansdale worked with the new regime on higher-level state stabilization matters in Saigon, Phillips worked with the peasants in the Mekong Delta, central coast, and central highlands. Phillips found the peasants amenable and loyal to Diem's government once rural development projects began and the peasants realized alternatives to the communists existed—the only other presence in the countryside prior to 1954 was the despised French. The Army of the Republic of Vietnam (ARVN), in Phillips's view, also exerted a positive influence once its units moved into the villages. Contrary to most traditional accounts, Phillips notes that the people came over to support the government, ARVN troops integrated well into the villages, and peace and stability came to the countryside.

It is here though that Phillips saw the first indications of things going seriously wrong. The SMM closed in November 1956, its mission accomplished. US efforts then went big, years before US efforts went even bigger during 1964–65. As Phillips writes, bureaucracy took over. The CIA established a station as part of a larger, ever growing State Department Country Team. The US Military Assistance and Advisory Group (MAAG)—like its 1962 successor, the Military Assistance Command-Vietnam—removed the ARVN from the villages and reconstructed the force as a conven-

tional Western-style army to counter an expected North Vietnamese invasion. The ultimate US–South Vietnamese defeat, Phillips claims, really occurred then, although he still held out hope as late as 1972 that the overall situation could be saved. Yet the cooperative connection to the South Vietnamese, both within their government and among the peasantry, was lost, never to return.

Following this early service, Phillips worked in similar programs for the CIA in Laos before returning to Agency Headquarters in Washington. Fed up with bureaucracy, especially after experiencing the independence of field work, he resigned from the Agency. When he returned to Vietnam with USAID in the early 1960s and became involved in the Strategic Hamlet Program, he noted with growing alarm the strained and distant relationship between most Americans assigned to rural areas and the South Vietnamese. Efforts to shift focus back to the classic counterinsurgency, to reintroduce Lansdale, and to influence President Kennedy's policies all failed, even though Phillips made direct appeals to Kennedy in the fall of 1963. These White House meetings were contentious, as military and civilian advisers, including Secretary of Defense Robert S. McNamara, took issue with Phillips's assessments and showed early signs of favoring a US military commitment.

Although Phillips stayed involved for several more years, the Americanization of the war after 1965 pushed rural development into the background with dire results. Phillips writes favorably of the Civil Operations and Revolutionary Development Support (CORDS) program, which began in 1967 and increased in intensity after the communist Tet offensive of 1968. To him, CORDS represented the embodiment of what he had worked towards since the mid-1950s. With rural pacification and security, nation building, and anti-Viet Cong activities all under one program, progress came swiftly. "By 1972," Phillips writes, "most of South Vietnam, particularly in the Delta area, was not only pacified but peaceful. So was most of central Vietnam." Phillips continues, "the North Vietnamese would later admit they suffered a severe reversal in the South Vietnamese countryside in the years after 1968, acknowledging that many of their bases had been wiped out in South Vietnam and that numbers of North Vietnamese and Viet Cong troops had been compelled to retreat to sanctuaries in Cambodia." (301) These firsthand observations confirm much of what newer Vietnam scholarship now shows, although improvements came too little and too late to affect the outcome of a war the American public had abandoned.

As a thoughtful participant in the events described, Phillips offers some practical lessons for those involved in today's counterinsurgencies. Foremost, Phillips stresses that Americans must know who they are as a people, and leaders must know (and be realistic) about what they are trying to attain abroad. US leaders must also know their allies and adversaries.

More important, however, Phillips maintains that if our nation is to be involved in such conflicts, we must know the "x factor"—the political and psychological nature of the struggle for hearts and minds—and the feelings of the people for whom we are fighting. We need to communicate with them on a human level, understand what motivates them, and view the conflict through their history, society, and culture. We need to know our enemies, their capabilities and motivations, as well as the level of their willingness to continue their resistance and up to what level of cost. Decisionmakers must be able to explain and connect policies and events abroad to the American public. Finally, Phillips repeatedly emphasizes that we must know whether we are fighting a conventional war or a political/ideological war—or a combination of both—so that we can bring the most suitable weapons to bear. These would include, of course, knowledgeable intelligence officers and military personnel willing to work long, hard years at the grassroots level.

James S. Robbins's *This Time We Win: Revisiting the Tet Offensive* clearly fits into the revisionist school of Vietnam War history that Prados dismisses. *This Time We Win* is not a history of the CIA in Southeast Asia, although the "Intelligence Failure" chapter accurately

speaks of the Agency, its analysis of the war in 1967, and the warning it provided before the 1968 Tet offensive. Robbins positively portrays CIA activities in a way not usually seen in most published histories.

The main value of this book for intelligence officers lies in its descriptions of how public perceptions—for better or worse—affect a nation's foreign policy and the course of its military conflicts. Focusing on public, political, and media perceptions of the Tet Offensive during its initial phase in January and February 1968, Robbins claims that most Americans saw the event negatively and today remember Tet for all the wrong reasons. The perception of loss, he argues, became a self-fulfilling prophecy, even though history shows that what happened in the offensive was a military defeat for the North. In short, the US lost in Vietnam not because of any military defeats but because US leaders, in effect, chose to lose and repeatedly avoided opportunities for victory.

Historians have long accepted that the communists suffered a major military defeat during the short but ferocious Tet offensive in 1968. At the same time, historians accept that the communists scored a major political and psychological victory as American public opinion turned against the war their leaders had consistently said they were winning. Using a wide variety of government records, published histories, interviews, and television and print news accounts, Robbins shows that Tet may have shocked the public, but it came as no surprise to US intelligence officials, soldiers, or politicians in the Johnson administration. All had anticipated a last-ditch offensive in South Vietnam months in advance, prepared for it militarily, and rapidly defeated it once it occurred, inflicting a clear military defeat on the communists, who failed to achieve any of their goals.

Robbins goes on to describe a US administration that essentially snatched defeat from the jaws of victory. President Johnson failed to explain what had happened; what the administration knew and what it had been doing beforehand; and how Tet affected or did not affect long-term US goals. This lackluster response, reinforced by media reports focusing on the spectacular, gave Tet the appearance of a major setback and served as proof that US policies had failed. The idea that Tet constituted an American catastrophe settled in the public's mind and never went away. Robbins concludes that "Tet was less a case of intelligence failure than a public relations fiasco." (123)

This all matters today, Robbins maintains, "because the Vietnam War is remembered by a large segment of the political class as pointless, immoral, and illegitimate, [and the] mere mention of Vietnam tends to delegitimize any conflict to which it is compared." (9) Because Vietnam has been so widely seen as an unwinnable war, comparisons of that conflict to the current battles in Afghanistan and Iraq are not intended to lend clarity, "but rather to couch the discussion in terms of inevitable defeat." (9)

Robbins warns that US adversaries today have drawn inspiration from the Tet offensive and hope to score similar victories. They see "America's national will as an Achilles heel" that negates its policies and power. Tet proved that a small, weak force could defeat the most powerful nation in human history by creating a big splash and the perception of power where none existed. This provided an immediate political victory that set up the North's future military triumph. Robbins concludes that the United States could just as easily lose today's conflicts if its people convince themselves that they cannot succeed.

All three books are excellent for their treatment of the history of the Vietnam War and the CIA's role in the conflict. They are less effective in their pointed analogies and comparisons of that war to the current conflicts in Afghanistan and Iraq. History is rarely so neat as to provide direct and applicable comparisons—as if times, actors, policies, and circumstances do not change. In the authors' attempts to connect what happened in Vietnam to what is happening now, one is led to wonder if writing history was their goal or if they merely intended to harness history to reinforce, or undermine, present-day policies and political agendas.

❖ ❖ ❖

Intelligence Officer's Bookshelf

Compiled and reviewed by Hayden Peake

General

***Challenges in Intelligence Analysis: Lessons from 1300 BCE to the Present**, by Timothy Walton*

***Extreme Risk Management: Revolutionary Approaches to Evaluating and Measuring Risk**, by Christina Ray*

***The Technical Collection of Intelligence,** by Robert M. Clark*

Historical

***Betrayal: Clinton, Castro and The Cuban Five**, by Matt Lawrence and Thomas Van Hare*

***Black Ops: The Rise of Special Forces in the C.I.A., the S.A.S., and Mossad,** by Tony Geraghty*

***Double Death: The True Story of Pryce Lewis, the Civil War's Most Daring Spy**, by Gavin Mortimer*

***Empire and Espionage: Spies and the Zulu War,** by Stephen Wade*

***Final Verdict: What Really Happened in the Rosenberg Case**, by Walter Schneir*

***The First War of Physics: The Secret History of the Atom Bomb 1939–1949**, by Jim Baggott*

***The Invisible Harry Gold: The Man Who Gave the Soviets the Atom Bomb**, by Allen M. Hornblum*

***The Kremlin's Geordie Spy: The Man They Swapped for Gary Powers**, by Vin Arthey*

***Radio Free Europe's "Crusade for Freedom": Rallying Americans Behind Cold War Broadcasting, 1950–1960,** by Richard H. Cummings*

***Secrets of the Cold War: US Army Europe's Intelligence and Counterintelligence Activities against the Soviets**, by Leland C. McCaslin*

***Through Hitler's Back Door: SOE Operations in Hungary, Slovakia, Romania and Bulgaria 1939–1945,** by Alan Ogden*

***Wild Bill Donovan: The Spymaster Who Created the OSS and Modern American Espionage**, by Douglas Waller*

Memoirs

All Them Cornfields and Ballet in the Evening, by John Miller

The C.I. Desk: FBI and CIA Counterintelligence As Seen from My Cubicle, by Christopher Lynch

Holding Hands with Heroes, by Jack Kassinger

Intelligence Abroad

The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB, by Andrei Soldatov and Irina Borogan

All statements of fact, opinion, or analysis expressed in this article are those of the author. Nothing in the article should be construed as asserting or implying US government endorsement of its factual statements and interpretations.

General

Challenges in Intelligence Analysis: Lessons from 1300 BCE to the Present, by Timothy Walton. (New York: Cambridge University Press, 2010), 294 pp., bibliography, maps, index.

Former CIA analyst Timothy Walton begins his book with a discussion of the basic elements and tools of intelligence analysis, which in the end supports decision making. For example, after identifying various factors an analyst must be careful to consider—uncertainty, deception, surprise, estimates of the accuracy of judgments—he describes some of the important techniques that can be applied. These include the time-line or chronology, competitive hypotheses, and various matrix models. Finally, he stresses the value of presenting the decision maker with options when no single result is directly on point.

To illustrate how analysis has functioned in the past, he provides 40 historical "lessons" from biblical times to the present. While the reader might legitimately expect the lessons to demonstrate the techniques Walton presented in the introductory chapters, that is not what the lessons do. Instead, they are historical summaries that set the stage for analyses. For example, his account of Moses sending spies into Canaan only summarizes the conflicting reports he received and the resultant disagreement among the leaders. There is nothing about fact checking or other analyses that might have led to conclusions they might have reached. Likewise, in his discussion of Hitler's surprise attack on the Soviet Union, Walton mentions Stalin's requirements for intelligence and the indicators that an attack was imminent, but he does not analyze why Stalin steadfastly refused to believe them. In the case of the run-up to the attack on Pearl Harbor, Walton provides a good summary of what happened and then acknowledges it as "the most famous and consequential example of failure in intelligence analysis." (95) But he fails to describe the analyses performed by those involved that allowed for the surprise.

A similar approach applies in the case of the atomic bomb spies. He tells how the FBI learned of the espionage through defectors and the Venona messages, but he neglects to comment on how the Bureau approached the difficult analytical problems the decrypts posed. The case also points to a major weakness of the book. None of the facts presented are sourced, and this leads to careless errors. Thus Walton writes: "shortly before Gouzenko's defection [5 September 1945] Elizabeth Bentley had volunteered information to the FBI field office in New Haven." (116) In fact, Bentley went to the Bureau office in New York on 7 November 1945. In another instance, Walton claims that Gouzenko mentioned Harry Gold, Klaus Fuchs's courier, but he did not. And Gold was not, as the book claims, the one who identified Fuchs; it was the other way around.[6]

In sum, while *Challenges in Intelligence Analysis* illustrates historical cases in which analysis was no doubt performed, the details of that analysis—how it was done, what one really needs to know—are omitted. The reader is left to resolve that.

Extreme Risk Management: Revolutionary Approaches to Evaluating and Measuring Risk, by Christina Ray. (New York: McGraw Hill, 2010), 287 pp., endnotes, charts, index.

Just days after 9/11, financial analyst Christina Ray read press allegations that Osama bin Laden collaborators with knowledge of the upcoming attacks had been trading in the market in anticipation of the impact of the attack. She hypothesized that if the story were true, analy-

[6] See Amy Knight, *How The Cold War Began: The Igor Gouzenko Affair and the Hunt For Soviet Spies* (New York: Carroll & Graf, 2005); Allen Hornblum, *The Invisible Harry Gold: The Man Who Gave the Soviets the Atom Bomb*, (New Haven, CT: Yale University Press, 2010).

sis of open source stock market transaction data would expose those involved. *Extreme Risk Management* does not reveal whether she tested her theory. Instead, it focuses on her subsequent work, which expanded the concept and explored the similarities she found in risk management techniques employed by the financial and intelligence communities. She argues that "the ability to reverse-engineer actionable market intelligence, or MARKINT," (vii) might be useful as an investigative tool in counterterrorism work and describes a number of risk management models aimed at achieving that goal. In fact, Ray points out that "the CIA is now publicly advertising" for experienced financial analysts. (viii)

Extreme Risk Management is not a book for beginners. Most of its chapters are devoted to complex financial models and the risks associated with their use. But in chapter nine, "An Alternative Path to Actionable Intelligence," she compares risk methodologies employed by financial and intelligence analysts. Here she argues that financial models, which are mainly statistical, can be adapted to show, for example, how the "intelligence community might benefit from information derived from open-source market prices converted to knowledge using quantitative sense-making models…as a metric of sovereign state instability." (151)

More generally, Ray concludes "financial warfare is arguably one of the types of unrestricted warfare for which the United States is least prepared and to which it is the most vulnerable." (254) To meet this threat, she suggests applications for MARKINT by intelligence analysts dealing with cyberthreats, counterintelligence, terrorism, insurgency, and rogue state behavior. While the practical testing of such applications remains to be done, *Extreme Risk Management* provides the basic techniques for analysts in this new field of activity.

The Technical Collection of Intelligence, by Robert M. Clark. (Washington, DC: CQ Press, 2009), 322 pp., end of chapter notes, photos, glossary, index.

Independent consultant and patent lawyer Robert Clark is a former industrial executive, Air Force intelligence officer, and CIA analyst with extensive experience in the field of technical intelligence. His previous books discussed intelligence analysis.[7] In his latest work he turns to technical collection, which he defines as the "collection, processing, and exploitation of *nonliteral* information—that is, information in a form not used for human communication" as opposed to that acquired from human agents. (xvi)

The keys to technical collection are signatures—photographic, electromagnetic, chemical, biological, acoustic, and nuclear—collected by various acquisition systems. Clark is careful to distinguish between signatures and the patterns associated with them. For example, the images of the Cuban missile sites acquired by the U-2 in 1962 are signatures. Their significance results from analysis of the patterns observed by analysts.

Chapters cover the space-, air-, sea-, and ground-based collection platforms intelligence organizations employ today. With the help of impressive color illustrations, Clark explains what each platform does and how it works. He includes, for example, several types of radar techniques, passive RF (radio frequency) collection, and digital satellite imagery. Clark also highlights the differences between active and passive systems. The final chapter looks at managing technical collection. He does not get into detailed operating procedures, though he does present a list of key management tools for consideration. One of the most important and difficult tasks Clark discusses is the allocation of collection requirements to meet time-sensitive demands that often exceed the capabilities of available systems.

Technical Collection of Intelligence is a fine, fully-documented, understandable, and comprehensive, though not elementary, introduction to

---

[7] See Robert M. Clark, *Intelligence Analysis: Estimation & Prediction* (Baltimore, MD: American Literary Press, 1996), and *Intelligence Analysis: A Target-Centric Approach* (Washington, DC: CQ Press, 2003).

a complex intelligence activity. It is an important topic not treated in such depth elsewhere.

Historical

Betrayal: Clinton, Castro and the Cuban Five, by Matt Lawrence and Thomas Van Hare. (New York: iUniverse, Inc., 2009), 217 pp., bibliography, no index.

On 24 February 1996, Cuban MiGs shot down two of three unarmed American light aircraft over international waters off the Cuban coast. The four pilots died. The third aircraft escaped and spread the word. The United States government responded with diplomatic gestures. Matt Lawrence and Thomas Van Hare think more should have been done. *Betrayal* explains why.

The authors, like the pilots flying near Cuba that day, were members of Brothers to the Rescue, a volunteer group that flew missions between Cuba and Florida searching for rafters, or *balseros*, trying to flee Castro. When the pilots spotted rafters, they radioed the US Coast Guard so they could be rescued. Between 1994 and the final mission in 2001, Brothers helped save over 17,000 lives, according to Lawrence and Van Hare.

The Castro government said the planes shot down in 1996 were in Cuban airspace, and it produced a "survivor" to prove it. The authors knew no one had survived. They also recognized the "survivor" as a fellow Brothers pilot and concluded he had penetrated the organization for Cuban intelligence.

While the story quickly dropped from public attention, many questions were left answered; for example, exactly where had the shoot-down occurred; had they actually flown into Cuban airspace? (one plane did briefly); why did the Cubans risk US Air Force retaliation; what had the three survivors said about the mission; and had any formal investigations been done by US officials? *Betrayal* offers answers to these and other questions that emerged as the authors pursued their own investigation. In a chapter titled "Cuba's Queen of Spies," the authors assert that the Pentagon did draft military responses for the president, but he chose not to implement them. Even if he had done so, the Cubans would have been prepared, and not only because of their "survivor" agent. Their principal agent in the United States, Ann Belén Montes, had been in the Pentagon group that had drawn up the options for White House consideration.

And there were other Cuban agents involved, according to this book. At least two were part of La Red Avispa (or Wasp) network, one of many such groups in the Cuban refugee community in Florida. (73ff) Five Wasps were eventually arrested, and the authors explain those agents' roles. Perhaps the most controversial conclusion of the authors is that the US government knew the Cubans were going to attack the Brothers' planes that day and for complex political reasons did nothing to warn the pilots or prevent the attacks. (189ff) The authors' evidence is not rock solid, and the reader is left to make an independent judgment.

In discussing their findings, the authors do not neglect the personalities of the Brothers pilots and their families. They present a poignant picture of Cuban refugees working against Castro while his agents work to thwart them.

Lawrence and Van Hare do not provide specific sources for key points in the book, though in the "Key References and Bibliography" section, newspaper articles, books, and persons interviewed are listed for each chapter.

Betrayal is a sad story of a humanitarian effort eventually shut down by Castro and international politics.

Black Ops: The Rise of Special Forces in the C.I.A., the S.A.S., and Mossad, by Tony Geraghty. (New York: Pegasus Books, 2010), 440 pp., endnotes, appendices, photos, index.

Arabic linguist Tony Geraghty served in the British Army, flew Nimrods in the RAF, and was a war correspondent before turning to writing books. His histories of the SAS (Special Air Service), the IRA conflict, and BRIXMIS (The British Commanders-in-Chief Mission to the Soviet Forces in Germany, which provided cover for a military intelligence unit in Cold War Europe) established him as a respected authority. In *Black Ops* he expands his outlook, first to discuss the broad historical origins of Special Forces (SF) activity, and then to focus on their use by the United Kingdom, the United States, and Israel.

To assume, however, that the book's subtitle implies that Geraghty will give equal coverage to each mentioned organization would be a mistake. After a 39-page introduction that nicely summarizes the entire book, five of the seven chapters are devoted to SF in the United States, one to Israel, and the last to the United Kingdom (the SAS and various lesser-known units). Throughout, Geraghty discusses the influence of British SF elements on their US and Israeli counterparts.

The coverage of US SF units begins with the Revolutionary War, but the focus is on their controversial development during WW II, with the OSS battling the War Department and the British Special Operations Executive (SOE). There is detailed coverage of the contentious use of SF in the Vietnam War. Geraghty goes on to describe the origins of the Delta Force and the tragic outcome of its attempted Iranian hostage rescue mission. He suggests the Delta Force finally achieved acceptance in asymmetric warfare in Iraq.

The chapter on British SF describes the often stormy evolution of operations by multiple, competing units—SAS and special military intelligence elements—that battled the IRA, supported the Falklands War, and fought in the Iraqi wars. Much of the controversy was resolved in 2005 with the formation of the UK Special Forces Group (UKSF), which included the SAS, the Special Boat Service (SBS), the 18th Signal Regiment, and various special military units designed to provide quick reaction capability.

The Israeli Chapter covers the origins of "at least thirty" (178) SF units, including the Mossad, the Aman (military intelligence), the Sayeret Matkal (an army reconnaissance and commando unit), and the Sayeret Shaldag (the Special Air-Ground Designating Team, an air force commando unit). (185) Geraghty records their effectiveness in some well known instances—for example, the aftermath of the Olympic games hostage taking, the Entebbe rescue mission, and the Vanunu case. He also asserts that in operations of this sort, the Israelis possess an advantage in that they can presume they will have the support of Jews wherever Israeli forces operate.

Geraghty takes note of the irony that three of the countries discussed in the book—Israel, the United States, and Ireland—engaged in successful resistance to British rule which "depended, initially, on irregular military forces." (177) *Black Ops* shows how SF units have since developed into a major force in the contemporary battle against terrorism. It is well documented and well worth reading.

Double Death: The True Story of Pryce Lewis, the Civil War's Most Daring Spy, by Gavin Mortimer. (New York: Walker & Company, 2010), 285 pp., endnotes, appendices, photos, index.

The late NSA analyst and jazz musician Edwin Fishel was also an authority on Civil War intelligence. Years in the archives convinced him that most Civil War intelligence memoirs qualified as subprime literature, "so heavily fictionalized that even the most believable parts are suspect." The memoirs of Allan Pinkerton, he wrote, epitomized this condition. Pinkerton "paid almost as little respect to factuality as did the authors of complete fictions."[8] Author Gavin

Mortimer agrees with Fishel's assessment of Pinkerton. Although a man of many positive qualities, writes Mortimer, "Allan Pinkerton… told the truth only when it suited him; when it didn't, he lied." (14) *Double Death* gives many examples, but the most important one concerns Pryce Lewis, one of Pinkerton's principal intelligence agents.

The first part of *Double Death* is devoted to Lewis's early life, the circumstances that brought him to America from his home in Wales, his work in America as a traveling book salesman, and his recruitment into the Pinkerton Detective Agency in 1859. When Pinkerton went to Washington to serve General McClellan as an intelligence officer, Lewis became one of his agents. He operated first in the South undercover as a traveling English gentleman.

At the same time, Pinkerton's most valuable agent, Timothy Webster, was acting as a Confederate courier but secretly carrying mail to the North. In 1862 Webster came under suspicion while in Richmond. Before he could escape he fell ill and was confined to bed. When he failed to appear as expected, Pinkerton sent Lewis and another agent, John Scully, to Richmond to see what was wrong. After meeting with Webster, they too were suspected of being agents and were arrested. In his memoir, Pinkerton writes that to save themselves, Lewis and Scully confessed that Webster was a Union agent. Webster was hanged, twice. The first attempt failed when the noose unraveled. Before the second attempt, Webster told his hangman, "I suffer a double death," hence the title of Mortimer's book. Lewis and Sully were repatriated, and their days as spies were over. This is the version of Webster's demise that Fishel recorded in his book.[9]

While researching the life of Lewis, Mortimer discovered two documents unknown to Fishel. One was a pamphlet written in 1906 by William Pinkerton, Allan's son, telling the true story of the testimony that led to Webster's death: "Scully made the confession implicating Webster… Lewis remained staunch, and did not confess." (236) No one knows why Allan Pinkerton lied. Lewis knew of the pamphlet, but so few others did that his reputation remained tainted. The second document was a copy of Lewis's memoir found in an archive in Canada. Letters indicated he had tried unsuccessfully to get it published. In the memoir, Lewis writes that he never betrayed Webster. The memoir also provides details of Lewis's life story, told in Mortimer's book for the first time.

Mortimer makes a weak case for designating Lewis the most daring spy in the Civil War. Webster is a better fit. In the end, what mattered to Lewis was his tarnished reputation. Burdened by his failure to cleanse it and by persistent financial problems, he committed suicide on 6 December 1911 in New York City. *Double Death* sets the record straight in an important Civil War intelligence case. Well written and soundly documented, it is a valuable contribution.

Empire and Espionage: Spies and the Zulu War, by Stephen Wade. (Barnsley, South Yorkshire, UK: Pen & Sword, 2010), 183 pp., endnotes, bibliography, photos, index.

The Anglo-Zulu War began in January 1879, when troops from the British colony of Natal on the East Coast of Africa invaded neighboring Zululand. Africa was not a high priority for Imperial Britain, and its army units there had few experienced officers and men and suffered from inadequate training. The Brits were counting on rigid discipline and superior weaponry to deal with the "primitive peoples' attack mode." (37) The British force of about 13,000 men—5,000 British soldiers and 8,000 Africans—advanced in three columns. Scouting parties were dispatched, but either they failed to gather intelligence about enemy positions and strength, or commanders disregarded their reports. In the event, the center column of 1,600 British and African troops was surprised and annihilated by a Zulu force 20,000 strong—one half of the Zulu

[8] Edwin C. Fishel, *The Secret War for the Union* (New York: Houghton Mifflin, 1996).
[9] Ibid., 149–49.

Army—at Isandlwana. More than 1,300 British soldiers died. Zulu losses were estimated at 2,000 dead and 1,000 injured. Author Stephen Wade examines in detail the reasons for the defeat. He goes on to describe several subsequent battles. He emphasizes the use and misuse of scouts and spies, the personalities involved, the communications employed, and the role of the media in reporting the conflict to London.

The British ultimately did overwhelm the Zulus, and after capturing the Zulu leader accepted their surrender on 1 September 1879. According to Wade, the British army learned much from the war. He describes its impact on the future of military intelligence—although he acknowledges that some of the same mistakes were made again in the Boer War.

Empire and Espionage is the only book on this topic, and it is valuable for that reason alone. But it has a major defect. Throughout, names, events, and locations are mentioned but not otherwise identified. Thus, for example, we encounter Cetshwayo (the Zulu leader), Garnet Wolseley and Chelmsford (both British generals), and Bartle Frere (the governor of South Africa) without ever learning their roles or titles. Isandlwana, though frequently mentioned in the book's opening, is not identified as a major battle until page 36. Wade offers no explanation for this awkward treatment. Thus, a reader without knowledge of the Anglo-Zulu War will find the book bumpy going.

Final Verdict: What Really Happened in the Rosenberg Case, by Walter Schneir with Preface and Afterword by Miriam Schneir. (Brooklyn, NY: Melville House Publishing, 2010), 203 pp., endnotes, photos, index.

In their 1965 book, *Invitation to an Inquest*, Walter and Miriam Schneir argued that key witnesses at the trial of Julius and Ethel Rosenberg lied and that the FBI had fabricated evidence.[10] Thus the Rosenbergs were not Soviet spies. They were innocent. In 1995, when the Venona decrypts proved the Rosenbergs had indeed been Soviet spies, the Schneirs, to their credit, revised their position in an article published in *The Nation*.[11] Julius had been a spy, they admitted, but not Ethel, her help in recruiting her brother David Greenglass notwithstanding. Then in 1999, the Schneirs read *The Haunted Wood*, by Allen Weinstein and Alexander Vassiliev,[12] and concluded it contained material that cast doubt on aspects of the government's case and might vindicate the defendants after all. *Final Verdict* reports the Schneirs' new position: Julius was only marginally involved in atomic espionage, and Ethel not at all.

Walter Schneir died before he could commit his new arguments to paper in narrative form, but his wife completed the task. She provides an eight-page timeline and a 41-page preface with background on her husband's research. In a 16-page afterword, based on material in the 2010 book *Spies*,[13] she writes that her husband's conclusions hold up. The core of *Final Verdict*—four chapters (113 pages)—is attributed to her husband. It presents his analysis of the critical discrepancies he claims to have found, though in the end his conjectures are only supported by imaginative analysis and speculation. One of the few unequivocal statements comes from Schneir himself when he writes, referring to the Rosenbergs, "Of course they lied and lied when they contended they knew nothing about espionage. Ethel knew about it and Julius practiced it." (155) In the end, Schneir's verdict is that the Rosenbergs were prosecuted for a crime they really didn't commit and not for the one they did.

---

[10] Walter and Miriam Schneir, *Invitation To An Inquest: A New Look At the Rosenberg-Sobell Case* (New York: Doubleday, 1965).
[11] Walter and Miriam Schneir, "Cryptic Answers," *The Nation*, August 14/21, 1995.
[12] Allen Weinstein and Alexander Vassiliev, *The Haunted Wood* (New York: Random House, 1999). See William Nolte's review in *Studies in Intelligence* 50, No. 2 (June 2006).
[13] John Earl Haynes, Harvey Klehr, and Alexander Vassiliev, *Spies: The Rise and Fall of the KGB in America* (New Haven, CT: Yale University Press, 2010). For Hayden Peake's review, see "The Intelligence Officer's Bookshelf," *Studies in Intelligence* 54, No. 3 (September 2010).

Nothing the Schneirs present changes the substance of the case. The final verdict remains: "guilty!"

The First War of Physics: The Secret History of the Atom Bomb 1939–1949, by Jim Baggott. (New York: Pegasus Books, 2010), 576 pp., endnotes, bibliography, photos, index.

Author Jim Baggott writes in his preface that his book contains "new materials [that] allow a single-volume popular history of the Anglo-American, German, and Soviet [atom bomb] programs to be assembled for the first time." This claim is an exaggeration. The book does portray the roles played and the controversies experienced by all the well-known scientists involved, from Oppenheimer to Teller. And it accurately chronicles the sequence of events that led to the bombings in Japan that ended WW II. With regard to intelligence, it reviews the work of the NKGB agents in the United Kingdom and the United States who gave the Soviets the plans for the US bombs. Baggott also discusses the impact those agents had on postwar relations among Britain, the Soviet Union, and the United States. But all this has been recounted by others. Baggott doesn't identify anything new in his book. The sources are all secondary, and errors made elsewhere are repeated here. For example, MI5 Director General Roger Hollis did not, as claimed, appoint Kim Philby as the principal liaison officer on the Gouzenko case, and Sir William Stephenson was not code-named *Intrepid*. (384)

The First War of Physics is a good summary of an oft-told story, but nothing more.

The Invisible Harry Gold: The Man Who Gave the Soviets the Atom Bomb, by Allen M. Hornblum. (New Haven, CT: Yale University Press, 2010), 446 pp., endnotes, bibliography, photos, index.

Defenders of Julius and Ethel Rosenberg have long argued that if Harry Gold had not confessed to being a Soviet agent, they would never have been exposed. Author John Wexley was one of many who went further by characterizing Gold's trial testimony as "fantasy… unworthy of belief."[14] With scholarly elegance, Allen Hornblum acknowledges the accuracy of the first claim and then gently demolishes Wexley's, noting that such charges followed Gold beyond the grave.

The Invisible Harry Gold is an explanation—not a defense—of Gold's actions. In explaining them, Hornblum invokes the circumstances of the Depression, growing anti-Semitism in Europe, and the struggles of Jewish immigrants in the United States. Heinrich Golodnitsky was born in 1910 near Bern, Switzerland, and became Harry Gold on arrival to the United States as a four-year-old. Hornblum describes Gold's hardscrabble early years in Philadelphia, where he endured bullying at school, worked jobs to help the family survive, and gradually became aware of the menace of fascism at home and in Europe. In 1933, desperate for work, Gold accepted the help of Thomas Black and went to work for him in Jersey City as chief chemist for the Holbrook Manufacturing Company. Black, a staunch communist, saw in Gold a potential convert. He worked hard to convince Gold that the only hope for defeating fascism lay in helping the Soviet Union since it had outlawed anti-Semitism. Though Gold never joined the Communist Party, he agreed to help it obtain industrial secrets from his employer. With that decision, there was no turning back. Gold eventually graduated to work as a courier for some of the NKVD's most important agents in the United States, including Klaus Fuchs, David Greenglass, and, indirectly, Greenglass's brother-in-law, Julius Rosenberg.

[14] John Wexley, *The Judgement of Julius and Ethel Rosenberg* (New York: Cameron & Kahn, 1955), 66, 73, 373, 384.

Hornblum describes Gold's "gradual seduction into industrial espionage" (45) and his often harsh on-the-job training administered by illegals who served the Soviets in the United States. After WW II began, Gold's assignments were redirected onto military targets. The most important agent he serviced was Klaus Fuchs. Although Hornblum writes that Moscow Centre approved Gold as a contact for David and Ruth Greenglass, who were part of another network, (145) John Haynes, Harvey Klehr, and Alexander Vassiliev in their book *Spies* revealed that Gold met with Greenglass as a last-minute substitution for another courier.[15] In any case, had this contact not occurred, the Rosenberg network might have escaped exposure.

The Invisible Harry Gold treats Gold's espionage assignments with the atom spies in considerable detail. According to Hornblum, FBI investigative work identified Gold as Fuchs's courier. This is contrary to a version reported by Robert Lamphere that Fuchs himself identified Gold as his courier from a picture.[16] The end result, however, was Gold's arrest, prompt confession, and his damning testimony at the Rosenbergs' trial.

Hornblum presents a well-documented, convincing picture of Harry Gold as an anti-fascist who only wanted to help an American ally. Caught up in Soviet espionage he had been unable to forsake, he was sentenced to 30 years in jail and served over half that time. The ultimate irony of this story is that while the American communist agents charged with espionage lied about their participation, Harry Gold, the noncommunist, is the only one who told the truth.

The Kremlin's Geordie Spy: The Man They Swapped for Gary Powers, by Vin Arthey. (New York: Dialogue, 2011), 242 pp., endnotes, bibliography, photos, index, 2nd edition revised.

The first edition of this book was published under the title, *Like Father Like Son: A Dynasty of Spies*. It told the life story of KGB illegal Col. Vilyam "Willie" Fisher, aka: "Col. Rudolf Abel, KGB."[17] The new title may puzzle American readers, but it makes immediate sense to a Brit. A *Geordie* is the common nickname for those from the Tyneside region of North East England, the region in which Willie Fisher was born on 18 April 1902, in Newcastle upon Tyne.

Author Vin Arthey explains Fisher's connections to the USSR—his father had been active in revolutionary activities in Russia and in 1901 fled to the UK, where he was involved in clandestine shipping of arms and literature back to Russia. The family returned to the Soviet Union when the younger Fisher was 17. He subsequently served in the Red Army as a radioman. In 1927 he joined the NKVD. His first overseas assignment was to England in 1935. There he worked for Alexander Orlov and Arnold Deutsch of Cambridge Five fame. Dismissed from the service during the Great Purge of 1938, Fisher was recalled in September, when there was a need for trained radio operators. After WW II, he was trained as an illegal and in 1948 was sent to the United States, where the Soviet networks were in disarray thanks to defectors and the Venona decrypts.

Arthey reviews Fisher's many assignments, including the handling of Soviet agents Morris and Leona Cohen and atom spy Theodore "Ted" Hall. Fisher used a number of codenames—the best known was Emil Goldfus—and his cover was as a commercial artist. Things began to go bad with the arrival of his future replacement, Reino Hayhanen, who proved to be an irresponsible drunk. Fisher had him recalled, but on the way home Hayhanen defected to the CIA in Paris and revealed that he knew a KGB illegal in New York. When the FBI arrested Fisher he gave his name as Col. Rudolf Abel, a prearranged signal to the KGB that he was in trouble. (The real Col. Abel was dead.) Fisher was serv-

[15] Haynes, Klehr, and Vassiliev, *Spies*, pp. 102–3.
[16] Robert Lamphere and Tom Shachtman, *The FBI-KGB War: A Special Agent's Story* (New York: Random House, 1986).
[17] Vin Arthey, *Like Father Like Son: A Dynasty of Spies* (London: St. Ermin's Press, 2004). (In the Bookshelf review of the book in *Studies in Intelligence* 49, no. 3 (2005) Fisher's first name was incorrectly rendered as "Willi.")

ing a 30-year sentence when he was traded for U-2 pilot Gary Powers. Fisher returned to limited duty for a while but soon retired. He never revealed what he did in England or the United States. He died on 15 November 1971 at age 59.

While there are no major changes in this edition, a number of corrections have been made and new details added. These include Fisher's date of birth, the name of his imprisoned brother—Ivan not Boris—and spelling errors. There is also some new material on Fisher's trial, the negotiation that led to his return to the Soviet Union, and "the Forbidden City"—the location of the KGB headquarters in Potsdam.

The Kremlin's Geordie Spy is the only biography of Willie Fisher in English that includes details of his KGB career. Arthey examined new materials from Russia, Britain, and the United States to piece together Fisher's extraordinary career. The result is a welcome contribution to the intelligence literature.

Radio Free Europe's "Crusade for Freedom": Rallying Americans Behind Cold War Broadcasting, 1950–1960. Richard H. Cummings (Jefferson, NC: McFarland & Company, Inc., Publishers, 2010), 257 pp., endnotes, appendices, bibliography, photos, index.

The Crusade for Freedom (CFF) was an early Cold War domestic propaganda campaign aimed at arousing the "average American against the Communist threat." (1) Intensely popular at the time, citizens contributed funds, attended rallies, marched in parades, participated in essay contests, and read the *Crusade for Freedom Newsletter*, which described the nature of the threat and advocated means to counter it. A principal component of the public program was Radio Free Europe (RFE), a broadcast service that sent the 'truth about communism' to countries behind the Iron Curtain. What was kept from the public at the time was that both CFF and RFE were covertly sponsored by the CIA. The CIA role was officially revealed in 1976, but *Radio Free Europe's "Crusade for Freedom"* adds details not made public at the time.

Author and former RFE officer Richard Cummings admits that some might consider CFF and its radio operations as a fraud on Americans. But his view is that if they were a fraud at all, they were benign and probably contributed to a Cold War anti-communist consensus. His book is devoted to documenting that position.

Cummings focuses on CFF and RFE from their planning stages in 1949 until CFF was terminated in 1962. RFE continued to function under CIA sponsorship until 1967, when RFE came under independent management, an arrangement that exists to this day. Cummings first describes the program's origin and goes on to review the bureaucratic and financial conflicts that persisted throughout its existence. Finally he looks at the program's clandestine elements.

The book treats the public side of CFF in some detail. This includes discussion of an extensive publicity campaign involving Hollywood celebrities, the news media, and political, industrial, and military figures. Here we read about the support of Eleanor Roosevelt, Bing Crosby, Ronald Reagan, General Eisenhower, President Truman, Walter Cronkite, President Kennedy, and the Boston Symphony Orchestra, to name a few. Defectors from the Soviet bloc were pressed into service. Col. Joseph Swiatlo of the Polish secret service is a case in point. In RFE broadcasts he informed those behind the Iron Curtain how the KGB dominated the security services of the bloc countries. The CIA role in CFF and RFE was exposed by journalist Drew Pearson in March 1953 (95). Fulton Lewis Jr. added critical remarks in 1957, noting "Dulles doesn't want it known." (171) Cummings explains how these events were dealt with and how they led to the demise of CFF in 1962.

Radio Free Europe's "Crusade for Freedom" is well documented and contains a useful chronology of major events. Cummings does not comment on the overall value of CFF, but judging from this history, it is unlikely that anything like it could be attempted successfully today.

Secrets of the Cold War: US Army Europe's Intelligence and Counterintelligence Activities against the Soviets, by Leland C. McCaslin. (Solihull, England: Helion and Company Limited, 2010), 200 pp., glossary photos, no index.

There are no secrets in this book. Most of the 19 chapters contain reminiscences written by the more than 50 contributors listed on pages 12–14. Curiously, "Special Comments by Francis Gary Powers, Jr.," though listed in the contents, are nowhere to be found. Author and retired military intelligence officer Leland McCaslin adds brief introductory comments to most chapters and contributes two himself, one on the annual military intelligence (MI) ball, the other on travel in Cold War Europe.

The topics covered are not without interest. They include the Soviet and Allied military missions that collected intelligence in occupied zones in Germany, the US-Russian hotline, defectors, counterintelligence, the Berlin duty train, and several case studies. The latter are illustrative and contain no specifics—first names only. No sources are provided.

Secrets of the Cold War with its many photographs does deliver a glimpse of military intelligence activities in Europe during the Cold War, but its content does not live up to the promise of its title.

Through Hitler's Back Door: SOE Operations in Hungary, Slovakia, Romania and Bulgaria 1939–1945, by Alan Ogden (Barnsley, South Yorkshire, UK: Pen & Sword, 2010), 284 pp., end of chapter notes, bibliography, photos, index.

The British Special Operations Executive (SOE) was established early in WW II to run sabotage and support resistance groups in German-occupied territory. By 1943 the SOE was also involved in political subversion—regime change—in Hungary, Slovakia, Romania, and Bulgaria, each one a German ally. Teams of the "wonderfully amateurish" (vi) businessmen, bankers, engineers and academics that staffed the SOE were dropped into each country to do the job. All operations failed to accomplish their primary objectives. *Through Hitler's Back Door* explains why.

The book is divided into three parts. The first deals with Hungary and Slovakia, the second with Bulgaria, and the third with Romania. Author Alan Ogden begins each part with a historical summary of the country and then turns to SOE efforts to bring it under Allied control. "From early on, SOE encountered difficulties in setting up subversive networks in Hungary," writes Ogden. (23) The same would prove true in the other countries. The difficulties included political opposition from the British Foreign Office, competition with the Secret Intelligence Service, and a lack of any established partisan networks. Logistical problems—air support, communications, and resupply—and the shifting loyalties of those contacted in the local governments also were problematic. But in the end, the uncompromising role of a Soviet Union on its own subversion mission was the dominant road block.

Ogden describes in considerable detail more than 30 missions, with emphasis on the persistent operational glitches encountered and their often herculean efforts to overcome them. He pays particular attention to the personnel involved—those that didn't survive and the few that did.

Though they fell short of their primary objective, the operations were not entirely in vain. Ogden tells how some tied up German forces that could have been deployed elsewhere and destabilized the planning of the Wehrmacht high command. He also records the considerable number of Allied aircrews the teams helped escape the enemy, often with partisan and OSS assistance.

This book is reasonably well documented, often with primary sources, though in some cases lengthy operational descriptions are not refer-

enced to sources—the efforts of the AUTONOMOUS team are an example. (249–52)

Through Hitler's Back Door concludes "there were few military or political laurels to emerge from Hungary, Romania, or Bulgaria. Scantily resourced and diplomatically constrained by the need to defer to and to consult with the USSR," they succumbed to "the pull of insuperable political forces." The brave efforts of the SOE teams are a tribute to their courage.

Wild Bill Donovan: The Spymaster Who Created the OSS and Modern American Espionage, by Douglas Waller. (New York: Free Press, 2011), 466 pp., endnotes, bibliography, photos, index.

Donovan of OSS was the first of four biographies of 'Wild Bill' Donovan.[18] It claimed to be the full story, and few in the public knew otherwise. The second and third made similar assertions, adding new details about OSS operations and bureaucratic battles.[19] Was there anything new left to say? The existence of a fourth biography suggests an affirmative answer, and author Douglas Waller calmly and carefully documents this position. The principal difference, however, is one of focus. Waller is concerned more with Donovan the man than with OSS operations. The result depicts an ambitious, brave, hard-charging Donovan, who almost by accident created America's first foreign intelligence service. It was only after completing two fact-finding trips to Europe for President Roosevelt that the idea occurred to him. With the encouragement of the British, Waller writes, Donovan convinced the president to establish the Office of the Coordinator of Information (COI), which became the OSS after the United States entered WW II.

The book concentrates on five aspects of Donovan's life. The first concerns his military career, his success as a Wall Street lawyer, and his political ambitions prior to serving Roosevelt. The second deals with the bureaucratic battles he fought and the egos he ruffled as he struggled to establish COI (later, OSS), and then to maintain its existence in the face of vigorous opposition from elements in the War Department and the FBI. Here we learn that the Army never accepted the OSS role and formed its own foreign intelligence service—nicknamed "The Pond"—under the control of Major John 'Frenchy' Grombach, a man Donovan had once fired. Donovan's other biographers do not mention the Grombach episode, which was treated in this journal in 2004.[20] Donovan's battles with Hoover and the FBI are also described in detail. On the operational side, Waller mentions Operation Kangaroo, a collection effort that defied an agreement with Hoover not to operate in Latin America, a topic covered in this book for the first time.

The third aspect of Donovan's life treated in this book, and for the first time, dealt with his many dalliances with women, something Waller did not try to hide. Their impact on Donovan's marriage did not do him credit.

The fourth part of the Donovan story concerns his frustrated attempts to create and head a postwar intelligence service after President Truman abolished the controversial OSS. Here, Hoover again enters the picture, and Waller leaves little doubt that it was Hoover who spread the rumor to the press that such a service would result in a domestic Gestapo, a charge that applied more to Hoover's own ambitions to direct an all-encompassing, postwar intelligence operation. Donovan's hopes were dashed forever when neither Truman nor his successor appointed him to head the new CIA.

[18] Corey Ford, *Donovan of OSS* (Boston: Little, Brown, 1970).
[19] Richard Dunlop interviewed Donovan for his book, *Donovan: America's Master Spy* (Chicago: Rand McNally, 1982). The other was *The Last Hero: Wild Bill Donovan* (New York: Times Books, 1982), by British journalist Anthony Cave Brown, who claimed "access to all Donovan's papers and his wife's diaries."
[20] See Mark Stout, "The Pond: Running Agents for State, War, and the CIA—The Hazards of Private Spy Operations," *Studies in Intelligence* 48, No. 3 (September 2004).

The final phase of Donovan's career that Waller covers is his service as ambassador to Thailand. Although in his late 60s, Donovan was still difficult to control. The concluding chapter ?overs Donovan's debilitating sickness that led to his death in 1959.

Wild Bill Donovan is absorbing reading. It is documented with primary sources, though the format used makes it impossible to tell what fact a particular document supports. In all other respects, it is a major contribution to the intelligence literature.

Memoirs

All Them Cornfields and Ballet in the Evening, by John Miller. (Kingston upon Thames, Surrey, UK: Hodgson Press, 2010), 324 pp., photos, index.

British journalist John Miller selected the title for this memoir from a line in the 1957 film, *I'm All Right Jack*, wherein a "leftish" shop steward played by Peter Sellers proclaims his desire to visit the Soviet workers' paradise with "all them cornfields and ballet in the evening." Beginning in 1960, Miller spent 40 years as a newspaper correspondent in the Soviet Union and Russia. His splendidly humorous reminiscences compare Soviet reality with the shop steward's fantasy.

While any firsthand account of life in the Soviet Union during the Cold War has inherent value, Miller's story is worthy of attention in an intelligence journal because of his encounters with several subjects of intelligence interest—Donald Maclean, Guy Burgess, and Kim Philby. He tracked down an uncooperative Maclean after acquiring a scarce copy of the Soviet phone book and going to his flat, though Miller was denied an interview four times. Burgess, always happy to talk to fellow Brits, gave Miller several interviews, and we learn some new details of Burgess's unhappy life in the Soviet Union. Miller carried a wreath at Burgess's funeral in 1963 and again met Maclean, who was more civil that time. Philby did not attend, but Miller later met him serendipitously in a Moscow restaurant where Philby was dining with his wife Eleanor and Maclean's wife (and Philby's mistress), Melinda. With a curse, Philby told him to "bugger" off, though Miller did acquire of photo of the elusive defector.

Like most correspondents, Miller got to know the MI6 head of station in Moscow at the time, Rory Chisholm, who was handling the British end of the Penkovsky case. Miller met Penkovsky once at a social function and later covered his show trial. Miller gives two accounts of Penkovsky's execution—a shot in the back of the head, and being burned alive in a crematorium furnace. The latter version has been reported before, and although Miller names a firsthand witness, the evidence is hearsay and the Soviet denials must be considered.

A variety of other vignettes include the Soviet reaction to their shooting down of the U-2 flown by Francis Gary Powers in 1960, Miller's encounter with Alexander Solzhenitsyn, and a KGB "honey trap" that caught the British ambassador in an affair with the sister of Captain Eugene Ivanov, a key player in the Profumo affair, which contributed to the resignation of British Prime Minister Harold Macmillan in 1963. Miller recalls frequent "chats" with the KGB without ending up in Lubyanka, even though he reported the joke about Brezhnev's last words: "Comrade Andropov, please stop fiddling with the life support machine."

All Them Cornfields broadens one's understanding of Soviet society, adds colorful details to some well-known Cold War espionage cases, and is an unqualified pleasure to read.

The C.I. Desk: FBI and CIA Counterintelligence As Seen from My Cubicle, by Christopher Lynch. (Indianapolis, IN: Dog Ear Publishing, 2009), 433 pp., index.

After graduating from Michigan State University, Christopher Lynch found a job in an FBI mailroom as a GS-2 clerk. It was all uphill from there. After 10 years with the Bureau he joined the CIA. Twenty years later, he retired as a GS-14 and wrote his memoir. Like all dutiful intelligence officers before him, he submitted the manuscript for clearance, twice: once to the CIA and once to the FBI. In an author's note, Lynch writes that the "successes in which I participated often seemed to get excised from the text.…As a result operations that fizzled out or otherwise went nowhere get an unwanted emphasis." (vii) He is right about that! *The C.I. Desk* reads like the story of a serial misfit whose cockroach persistence gets him through a 30-year career. Though he advanced from the FBI mailroom to become a counterintelligence (CI) analyst at the FBI and the CIA, something dissatisfies him in each job, and he is soon looking for another position. At the FBI he cut his teeth on the Boris Yushin case and learned how to do CI case reviews, a task he apparently performed skillfully. He later worked for two years for Robert Hanssen, with whom he got on well, he writes. His description of Hanssen as a "nice fellow" challenges those offered by other contemporaries who cast him as an eccentric computer nerd with few social skills.

In 1986, Lynch moved to the CIA where the pattern of job-hopping continued. He tells about his 20 years there, describing the CI cases he analyzed in most of the major divisions in the clandestine service. Many of the assignments were initially interesting, others quickly frustrating. His work on the Ames case and his tours in the new Counterintelligence Center are examples of the former. His assignment to the Office of Security is an example of the latter. Either way, after a year, or at the most two, he would declare that his "frustrations in the Branch kept growing" (320–21), or words to that effect, and move on. Lynch spent most of his final years at the CIA reviewing files for declassification and doing CI case reviews in an unspecified office where he "drifted from desk to desk." (424)

Despite his career turbulence, Lynch writes that he loved CI work and the challenges it presented. It is difficult to pin down the message he wants to convey in this book or to explain his candor in conveying it. But he does seem to be emphasizing the importance of doing one's work well. A most unusual contribution to the intelligence literature.

Holding Hands with Heroes, by Jack Kassinger. (Pittsburgh, PA: Dorrance Publishing Co. Inc., 2010), 242 pp., photos, glossary, no index.

It takes unusual qualifications to begin a CIA career as a GS-4 and retire as a supergrade. In *Holding Hands with Heroes* Jack Kassinger tells how he did it: no college degree, service in the Marine Corps, a recommendation from Dave Phillips (a senior CIA officer stationed in Latin America), and an impressive track record as a clandestine service support officer. In one respect, Kassinger's memoir is a typical account of worldwide assignments and service at CIA Headquarters while raising a family—his wife, Cherie, was a career officer too. But it is also atypical in that unlike the memoirs of clandestine service officers such as Phillips and Milton Bearden that tell of espionage cases in which they were involved,[21] Kassinger explains the critical services a support officer provides to espionage and covert action operations. His vivid descriptions of CIA support operations in Somalia and other African nations make the point. In

[21] After retiring, David Atlee Phillips, wrote a memoir of his career, *The Night Watch: 25 Years of Peculiar Service* (New York: Atheneum, 1977); Milton Bearden and James Risen, *The Main Enemy: The CIA in Battle with the Soviet Union* (New York: Random House, 2003)

the early 2000s, Kassinger was assigned to the Central Eurasia Division, and from that vantage point he describes the impact of the Ames case, the efforts to rebuild a new, secure embassy in Moscow, support operations in the Balkans and Albania, and the turmoil that followed the appointment of John Deutch as Director of Central Intelligence.

The book's title refers to the many officers with whom Kassinger served, some of whom will be familiar to those who worked in the CIA after the Vietnam War. In *Holding Hands with Heroes* Kassinger offers himself as an exemplar for those considering a CIA career.

Intelligence Abroad

The New Nobility: The Restoration of Russia's Security State and the Enduring Legacy of the KGB, by Andrei Soldatov and Irina Borogan. (New York: PublicAffairs, 2010), 301 pp., endnotes, index.

In the foreword to this book, British investigative journalist Nick Fielding warns that the Russian intelligence services "have little tolerance for criticism…since 2000 seventeen journalists have been murdered." (vii) That same year Andrei Soldatov and Irina Borogan created Agentura.ru (in Russian and English), "a journalism-based website for monitoring the Russian services." (7) Though they have been careful to base their often critical articles on open sources and have been interrogated more than once by the Federal Security Service (FSB),[22] the principal successor to the KGB, so far they have managed to survive. *The New Nobility* summarizes their work to date, with emphasis on the sudden breakup of the KGB, the struggle for power among the surviving elements, and the ascendancy of the FSB. It was Nikolai Patrushev, the successor to Vladimir Putin as FSB director in 1999, who called the FSB the "new nobility" with the mission of "stability and order." The authors take care to point out that the FSB should not be "mistaken for a revival of the Soviet KGB," though some journalists have made this error. With all its power, the KGB was subordinate to the Communist Party; the FSB is free of party and parliamentary control, reporting only to the president or prime minister. (4–5)

After the chaos of the Yeltsin era, the FSB moved rapidly to consolidate its power. The authors tell how it worked to "ferret out foreign spies," (36) to bring human rights organizations under control, and to deal with the oligarchs (giving them the choice of leaving the country or going to a jail in Siberia). A program to plant informants in "liberal organizations" was also established. New counterintelligence regulations were created that allowed access to private correspondence and communications through wiretapping. Restrictions on surveillance were removed and the right to search all premises was granted. (114ff) As incentive, FSB officers were given special benefits, including new brick dachas on land confiscated from the oligarchs.

There are several chapters on the FSB response to terrorism, the one area in which the organization has not been very successful. It was while the authors were preparing articles critical of Russian counterterrorism operations that they were summoned to the notorious Lefortovo prison; they don't provide any details of the ensuing interrogation. They do assert that FSB assassination teams have been sent abroad to deal with Chechen terrorists. And while they note the stories that claim the FSB poisoned Alexander Litvinenko using polonium-210 in London, they conclude that "there is no information about whether his death was ordered by the Russian leadership" or by mercenaries. (208)

[22] Federalnaya Sluzhba Bezopasnosti.

The final chapters deal with two interesting issues. The first looks at rumors that the FSB would absorb the foreign intelligence missions of the SVR (foreign intelligence service) and the GRU (military intelligence service). That hasn't happened yet, and for the time being Russia has three foreign intelligence services, with the FSB empowered to deal with the former Soviet republics. The second issue concerns the FSB program for cyberwarfare that uses its own cadre of experts and from time to time employs independent hackers.

The New Nobility presents a persuasive, well-documented view of the FSB that only dedicated, risk-taking Russians could provide.

❖ ❖ ❖

This Page Is Intentionally Left Blank

AFRL-RH-WP-TR-2013-0114

ADVANCED ANALYSIS COGNITION: IMPROVING THE COGNITION OF INTELLIGENCE ANALYSIS

Christina M. Kampman
Charles A. Mangio
Shim Enterprise, Inc.
7681 Tyler's Place Blvd. Suite 4
West Chester, OH 45069

Melinda Marsh
Acorn Consulting
3129 Baker Road
Springfield, OH 45504

SEPTEMBER 2013
Final Report

Distribution A. Approved for public release; distribution unlimited.

AIR FORCE RESEARCH LABORATORY
711TH HUMAN PERFORMANCE WING,
HUMAN EFFECTIVENESS DIRECTORATE,
WRIGHT-PATTERSON AIR FORCE BASE, OH 45433
AIR FORCE MATERIEL COMMAND
UNITED STATES AIR FORCE

NOTICE AND SIGNATURE PAGE

Using Government drawings, specifications, or other data included in this document for any purpose other than Government procurement does not in any way obligate the U.S. Government. The fact that the Government formulated or supplied the drawings, specifications, or other data does not license the holder or any other person or corporation; or convey any rights or permission to manufacture, use, or sell any patented invention that may relate to them.

This report was cleared for public release by the 88th Air Base Wing Public Affairs Office and is available to the general public, including foreign nationals. Copies may be obtained from the Defense Technical Information Center (DTIC) (http://www.dtic.mil).

AFRL-RH-WP-TR-2013-0114 HAS BEEN REVIEWED AND IS APPROVED FOR PUBLICATION IN ACCORDANCE WITH ASSIGNED DISTRIBUTION STATEMENT.

//signature//	//signature//
ROBERT EGGLESTON, Work Unit Manager Human Analyst Augmentation Branch	LOUISE CARTER, PhD. Chief, Human-Centered ISR Division Human Effectiveness Directorate 711th Human Performance Wing Air Force Research Laboratory

This report is published in the interest of scientific and technical information exchange, and its publication does not constitute the Government's approval or disapproval of its ideas or findings.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From - To)*
01 SEP 2013	Final	09/20/2009 – 09/20/2013

4. TITLE AND SUBTITLE
Advanced Analysis Cognition: Improving the Cognition of Intelligence Analysis

5a. CONTRACT NUMBER
FA8650-09-C-6038

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
*Christina M. Kampman
**Melinda Marsh
*Charles A. Mangio

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER
H06Q (7184X19W)

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) AND ADDRESS(ES)
*Shim Enterprise Inc.
7681 Tyler's Place Blvd., Suite 4
West Chester, OH 45069
**Acorn Consulting
3129 Baker Road
Springfield, OH 45504

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Air Force Research Laboratory
711 Human Performance Wing
Human Effectiveness Directorate
Human-Centered ISR Division
Human Analyst Augmentation Branch
Wright-Patterson AFB OH 45433

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
AFRL-RH-WP-TP-2013-0114

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
88ABW-2013-5245; Cleared 12 December 2013.

14. ABSTRACT A prior effort, *State of Knowledge Relative to Intelligence Analysis,* was initially motivated by the fact that seemingly little change had resulted from numerous studies of the intelligence community. Starting with Pearl Harbor, the U.S. intelligence community has often faced criticism for failing to predict or warn of future events. Though the criticisms have come from different groups, a certain commonality exists among the proposals for change in the intelligence community. The other noteworthy feature of these proposals is how little their content has changed over time. A thorough analysis of the intelligence literature was accomplished. This analysis provided an answer to the question of whether the existing literature on intelligence analysis contains the requisite knowledge to inform the development and application of both the mechanistic and cognitive activities to support doing intelligence analysis. A dominant finding was how little the practice of intelligence analysis had been informed by the findings in related scientific disciplines. The primary objective of this research effort was to understand the research findings in relevant scientific disciplines and to relate these findings to the practice of intelligence analysis. This research effort was based on the full text of over 5,800 documents consisting of nearly 172,000 pages. Our analysis of the current intelligence literature showed a continuation of previously observed trends. The number of publications dealing with intelligence analysis has decreased since 2007; in 2012 publication was at the level observed in 1996-1997. Also, we observed that the literature places less emphasis on the improvement of the quality of intelligence analysis. During the effort described in this report we conducted research syntheses for the topics of critical thinking, thinking dispositions, epistemological beliefs, practice based training, and various facets of cognition. Based on the findings of these syntheses, we provide recommendations for improvements to quality assurance practices, analyst selection, analyst training, and improving the content of the Framework for Analytic Cognition.

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			19b. TELEPHONE NUMBER *(include area code)*
U	U	U	SAR	408	Robert Eggleston

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

THIS PAGE INTENTIONALLY LEFT BLANK.

TABLE OF CONTENTS

Section ..... **Page**
List of Figures iv
List of Tables iv
Preface v
Note For The Reader vi
1.0 IMPROVING THE COGNITION OF INTELLIGENCE ANALYSIS 1
2.0 APPROACHES AND METHODS 2
3.0 STATE OF THE INTELLIGENCE LITERATURE 4
4.0 RELEVANT SCIENTIFIC RESEARCH 7
5.0 CRITICAL THINKING 8
6.0 THINKING DISPOSITIONS 15
7.0 PRACTICE-BASED LEARNING 21
8.0 EPISTEMOLOGICAL BELIEFS 24
8.1 Introduction 24
8.2 What are Epistemological Beliefs? 24
8.3 Findings 25
8.4 Recommendations 26
9.0 COGNITION 27
9.1 Introduction 27
9.2 Words as Concepts 24
9.3 Cognitive Behavior 31
9.3.1 Individual Need for Explanations 31
9.3.2 Individual Need for Certainty 33
9.3.3 Input to Thinking 33
9.3.4 Judgment of Thinking 35
9.3.5 Ramifications 37
10.0 FRAMEWORK FOR ANALYTICAL COGNITION 40
11.0 RECOMMENDATIONS 41
11.1 Quality Assurance 41
11.2 Analysis Selection 41
11.3 Analyst Training 41

11.4 FAC Enhancement 41
12.0 REFERENCES 42
13.0 BIBLIOGRAPHY 47
LIST OF ACRONYMS 392

LIST OF FIGURES

Figure **Page**

1 Volume of Intelligence Literature 1990 -2012……..……..4

LIST OF TABLES

Table **Page**

1 Recommended Critical Thinking Skills and Dispositions for Intelligence Analyst 11

PREFACE

This effort is a follow on to the analysis we reported in the reports AFRL-RH-WP-TR-2011-0049, AFRL-RH-WP-TR-2011-0051, AFRL-RH-WP-TR-2011-0052, and AFRL-RH-WP-TR-2011-0053. Our primary objective was not only to verify the findings of the previous effort but also to emphasize research synthesis of related scientific areas in order to better inform the practices of quality assurance, analyst selection and training. We have met our objectives and have recommendations on those topics. Unfortunately, our effort was terminated early so we were unable to complete all documentation supporting those recommendations.

This report was preceded by two interim reports: Marsh, M. *Advanced Analysis Cognition: Critical Thinking* and Marsh, M. *Advanced Analysis Cognition: Thinking Dispositions.* These reports were submitted to the Air Force Research Laboratory for review. At the time of this final report, both interim reports were still in press.

NOTE FOR THE READER

In order to communicate the quality and content of the documents found and to accurately portray the authors' different perspectives, this document contains many passages extracted from their original publications. These passages may contain references, footnotes, table and figure numbering, formatting, and errors that are part of the original document, not this report. We used the passages as they were, with no additional editing. We suggest that you refer to the References section to obtain the source document if you would like to see the extract in its original context.

1.0 IMPROVING THE COGNITION OF INTELLIGENCE ANALYSIS

1.1 Introduction

Our prior research effort for the Air Force Research Laboratory (AFRL), *State of Knowledge Relative to Intelligence Analysis*[1], was initially motivated by the fact that seemingly little change had resulted from numerous studies of the intelligence community. Starting with Pearl Harbor, the U.S. intelligence community has often faced criticism for failing to predict or warn of future events. As a result, numerous groups and commissions have been established during the past 30 years to study "what went wrong." All of these efforts have resulted in proposals to "fix" the intelligence community and thereby improve the quality of its products. While the proposals have come from different groups, a certain commonality exists among the proposals. The other noteworthy feature of these proposals is how little their content has changed over time.

The fact that the same solutions are proposed time and time again without any obvious implementation gave rise to a variety of questions. For example, do we know the cognitive and personality attributes (e.g., extrovert or introvert) of a "good analyst?" What does an analyst need to know in order to function effectively? What are the mechanistic as well as the cognitive processes associated with the acquisition, processing, and evaluating of data or information? What are the characteristics of the cognitive transformation of data or information into useable knowledge?

To answer these questions, we conducted a thorough analysis of the intelligence literature. Much was learned from this analysis, but the dominant discovery was how little the practice of intelligence analysis had been informed by the research that existed in related scientific disciplines. Mandel alluded to this discovery in a comment from 2009:

> It is telling, Mandel noted, that no one else has come along since Heuer to continue his work of translating cognitive psychology and other areas of behavioral science into tools for analysis. "In cognitive psychology alone there is at least a quarter century of new research since Heuer published *Psychology of Intelligence Analysis* that is waiting to be exploited by the intelligence community."[2]

The objective of this research effort was to understand the research findings in relevant scientific disciplines and to relate these findings to the practice of intelligence analysis. In addition, to accomplish this we also had to maintain our ongoing review and assessment of the current intelligence literature to insure the validity of our past evaluation of the content of such literature.

[1] Hereafter referred to as *State of Knowledge* for ease of discussion.
[2] Pool, R. *Field Evaluation in the Intelligence and Counterintelligence Context. Workshop Summary*. The National Academies Press, Washington, DC, 2010, p. 4.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

2.0 APPROACHES AND METHODS

2.1 Information Acquisition and Assessment – Approach

We used the same approach for acquiring information during the *Advanced Analysis Cognition* research projects as we used during the *State of Knowledge* research. We described our approach in the final report for *State of Knowledge*.[3] In addition, as part of the *Advanced Analysis Cognition* effort, we continued to acquire all literature related to intelligence analysis. We also expanded our effort to acquire information in subjects deemed potentially relevant to intelligence analysis.

We used a selective approach to acquire publications from various subject areas. We did not attempt to acquire all the available information in a given subject area. We made selections on an iterative basis. First, we acquired and reviewed a limited sample of information from a subject area. We then made a judgment about the potential relevance of the information for understanding the cognition of intelligence analysis. If the content of the information was judged as potentially relevant, we acquired literature for that subject using an approach comparable to that done for the intelligence literature.

Our overall information acquisition on all subject areas resulted in a large number of potentially relevant publications. We based the *Advanced Analysis Cognition* research on the full text of over 5,800 documents consisting of nearly 172,000 pages.

2.2 Information Assessment - Method

We used the methods associated with qualitative research synthesis[4] to evaluate the acquired literature, particularly those techniques elaborated by the Cochrane Collaboration.[5] The main phases for doing such research are:

- Problem formulation
- Literature search
- Data evaluation
- Analysis and interpretation
- Public presentation

This method is very similar to the analysis process as proposed by Kent.

1. The appearance of a problem requiring the attention of a strategic intelligence staff.
2. Analysis of this problem to discover which facets of it are of actual importance to the U.S. and which of several lines of approach are most likely to be useful to its governmental customers.

---

[3] Mangio, C.A. & Wilkinson, B.J. *State of Knowledge Relative to Intelligence Analysis. Volume 1: Cognitive Challenges for Intelligence Analysis - Past, Present, and Future,* AFRL-RH-WP-TR-2011-0049, 2011, p. 8.
[4] Cooper, H.M. *Synthesizing Research: A Guide for Literature Reviews,* 3rd ed., Sage Publications, Thousand Oaks, CA, 1998.
[5] Higgins, J.P.T. & Green, S. (eds) *Cochrane Handbook for Systematic Reviews of Interventions. 4.2.6 [Updated September 2006],* John Wiley & Sons, Ltd., Chichester, UK, 2006.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

3. Collection of data bearing upon the problem as formulated in Stage 2. This involves a survey of data already at hand and available in the libraries of documentary materials, and an endeavor to procure new data to fill in gaps.
4. Critical evaluation of the data thus assembled.
5. Study of the evaluated data with the intent of finding some inherent meaning. The moment of the discovery of such a meaning can be called the moment of hypotheses. In reality there is rarely such a thing as one moment of hypothesis though some students of method, largely as a convenience, speak as if there were. Nor can it be said categorically at what stage in the process hypotheses appear. One would be pleased to think that they appeared at this, the respectable Stage 5, but in actual practice they begin appearing when the first datum is collected. They have been known to appear even before that, and they may continue to appear until the project is closed out—or even after that.
6. More collecting of data along the lines indicated by the more promising hypotheses, to confirm or deny them.
7. Establishment of one or more hypotheses as truer than others and statement of these hypotheses as the best present approximation of truth. This stage is often referred to as the presentation state *[sic]*.[6]

Comparing the two descriptions illustrates the commonality of both approaches for assigning meaning and drawing conclusions from information. From a cognitive standpoint, doing qualitative research and intelligence analysis are the same. We found the use of the Cochrane Collaboration approach to be a natural complement to our previous intelligence analysis work.

[6] Kent, S. *Writing History,* 2d ed., Appleton-Century-Crofts, New York, NY, 1967, pp. 157-158.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

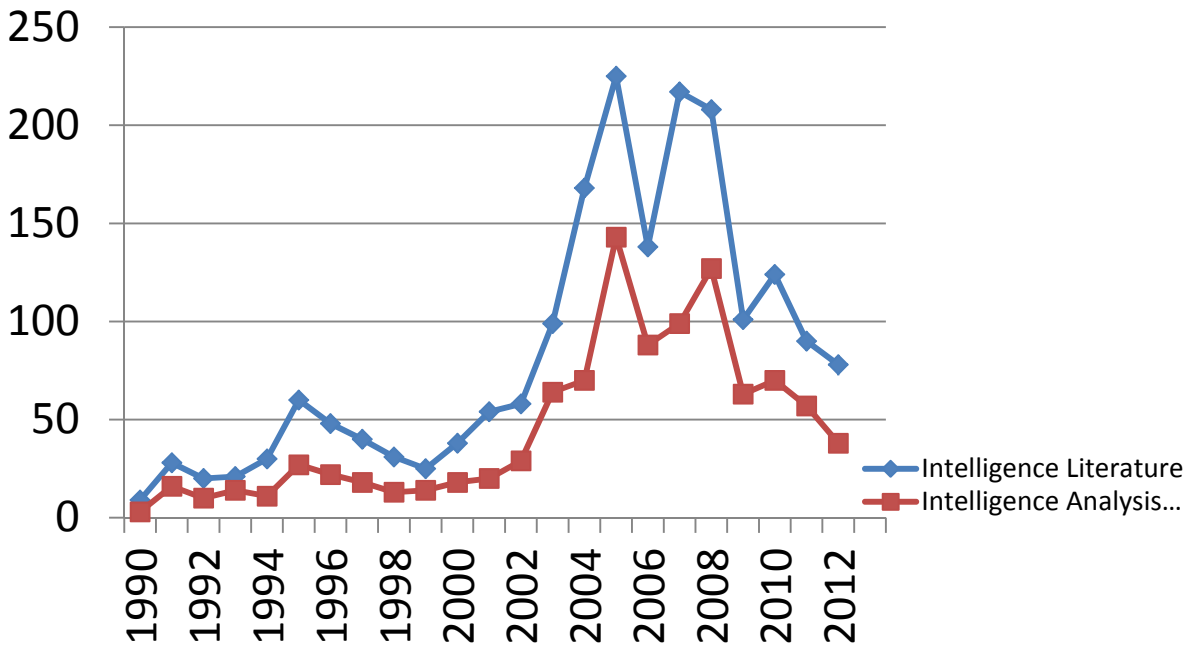
3.0 STATE OF THE INTELLIGENCE LITERATURE

In our ongoing review of the intelligence literature, we included as relevant any publications that contained information pertaining to the following topics:

- organization and management of the intelligence community
- analysis process and products
- intelligence failure
- analysts' characteristics
- training
- analytical work and management environment
- tools for augmenting analysis

Our intelligence literature reviews did not include searching for information on pre-WWII intelligence history, memoirs, and collection techniques. If an item seemed to be only marginally relevant, we made it a policy to include the item rather than to exclude it from our collection.

After collecting intelligence literature based on these selection criteria we were able to use data about our collection to plot trends in publishing for intelligence analysis. Figure 1 shows the results of analyzing our collection.



Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Figure 1: Volume of Intelligence Literature 1990 -2012[7]

We had initially performed this analysis in 2010 and noted in our final report for *State of Knowledge* that the publication volume was decreasing. Our current update of the same analysis shows an even greater decline in publication volume. We can offer no better explanation for the decrease in the amount of intelligence literature than we could two years ago:

> One can only speculate as to why the volume of intelligence literature has decreased in the last two years. One view is that intelligence failures spark an outpouring of publications dealing with why there was a failure and recommendations for preventing future failures. Certainly, the failures associated with 9-11 and the Iraqi Weapons of Mass Destruction (WMD) have been addressed in many publications. Perhaps without new failures, there may be a dearth of topics to write about that have not been extensively treated in the prior intelligence literature. Another possibility is that given the descriptive nature of the intelligence literature, the question is what can be said that hasn't already been said. For example, the first instance of the term *mirror imaging* that we found in the intelligence literature was in a 1960 publication.[8] The most recent instance of the term is in a 2010 publication.[9] The basic message has not changed over this 50-year period: mirror imaging is bad and an analyst shouldn't do it. The same is true for other concepts such as alternative analysis and Analysis of Competing Hypotheses (ACH). Both have been discussed for a long time, but there has been little change in the content of the discussion.[10]

Even in the context of the decrease in volume, fewer publications are dealing with the topic of improving the quality of intelligence analysis. The notable exception is the publication produced by the Committee on Behavioral and Social Science Research to Improve Intelligence Analysis for National Security; National Research Council.[11]

One topic that has gained more prominence in the last few years is field evaluation of intelligence analysis - "the testing of these methods and tools in the context in which they will be used in order to determine if they are effective in real-world settings."[12] A workshop addressing this issue was conducted by the Committee on Field Evaluation of Behavioral and Cognitive Sciences-Based Methods and Tools for Intelligence and Counterintelligence. The major findings of this workshop were that new tools and techniques were introduced without field evaluation. Others have also made this observation.

---

[7] The absolute value of the number of publications should be used with reservations since the numerical value is based on a series of subjective judgments. However, a constant framework was used for making these judgments so the relative value of numbers is considered valid. Thus, the trends depicted are real.

[8] Wasserman, B. "The Failure of Intelligence Prediction," *Political Studies,* Vol. 8, No. 2, 1960, pp. 156-169.

[9] Hall, W.M. & Citrenbaum, G.M. *Intelligence Analysis: How to Think in Complex Environments,* Praeger Security International, Santa Barbara, CA, 2010.

[10] Mangio, pp. 19.

[11] Fingar, T. "Analysis in the U.S. Intelligence Community: Missions, Masters, and Methods," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011.

[12] Pool, R. *Field Evaluation in the Intelligence and Counterintelligence Context Workshop Summary.* The National Academies Press, Washington, DC, 2010, p. 1.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

> Many methods used by or proposed to the Intelligence Community (IC) have not been formally evaluated using randomized controlled trials. For example, intelligence analysis tradecraft not evaluated adequately include alternative competing hypotheses, Preliminary Credibility Assessment Screening System (PCASS), and even recent communication innovations such as Intellipedia and A-Space.[13]

> Analysts who do not use structured analysis often justify their decision by claiming there is no hard evidence that these techniques improve analysis. It is true that little has been done to validate empirically the utility of these techniques as used in intelligence analysis, to formally assess the impact on the workload of analysts using these techniques or their supervisors, or to conduct systematic customer evaluation of products that have used structured techniques. This absence of proof of effectiveness makes it harder to "sell" analysts on the use of these techniques, especially analysts who claim they do not have enough time to use structured analytic techniques.[14]

The assessment we made of the content of intelligence publications in the *State of Knowledge* final report remains valid:

> …the content of the intelligence literature has not changed in meaningful ways over time. The focus has been on describing the shortcomings in the analysis process and discussing what the analyst should not do. Suggested improvements and reforms have been put forth repeatedly, but the analysis of why these reforms do not succeed is lacking. Very little of the writing has addressed improvement at the fundamental level where analysis is done, i.e., by the intelligence analyst, and addressed how analytic practices should be approached comprehensively to overcome the often identified shortfalls.[15]

What should be added to our original assessment as a result of more research is a note reflecting the lack of validation of the tools and techniques for doing intelligence analysis. Despite many claims and anecdotal information, whether any of these tools and techniques actually improves the results of intelligence analysis has yet to be proven.

[13] McClelland, G.H. "Use of Signal Detection Theory as a Tool for Enhancing Performance and Evaluating Tradecraft in Intelligence Analysis," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, p. 95.
[14] Heuer, R.J. & Pherson, R.H. *Structured Analytic Techniques for Intelligence Analysis*, CQ Press, Washington, DC, 201, p. 337.
[15] Mangio, p. 21.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

4.0 RELEVANT SCIENTIFIC RESEARCH

As we mentioned earlier, intelligence analysis is an intensely cognitive process involving information processing, information evaluation, and judgment making. Because of the broad nature of these cognitive processes, many areas of scientific research have the potential to inform the practice of intelligence analysis. Investigating these areas of research can shape the practice of intelligence analysis to be consistent with current scientific findings. The specific topics of interest that we pursued included:

Critical thinking	Thinking dispositions	Epistemological beliefs
Conceptual change	Information retrieval	Reasoning
Group behavior	Practice based learning	Persuasiveness
Self-efficacy	Rationality	Reception theory
Dual process mind	Thinking styles	Competence evaluation

The following sections of the final report discuss the major findings from the research synthesis work for critical thinking, thinking dispositions, epistemological beliefs, and practice-based learning. We completed research syntheses for critical thinking and thinking dispositions. We were able to partially complete research syntheses for epistemological beliefs and practice-based learning.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

5.0 CRITICAL THINKING

5.1 Introduction

Beginning in the late 1990s, the specific topic of *critical thinking* has been increasingly mentioned as one of the "fixes" to improve the quality of analysis. James Asker was one of the earliest authors to highlight critical thinking:

> Grumbling lawmakers say the intelligence failure to detect India's nuclear test preparations was rooted in defects flagged long ago, but continually sidestepped by both Congress and spy agencies. A quick review led by Admiral David Jeremiah, a former vice chairman of the Joint Chiefs of Staff, produced a litany of familiar flaws: lack of critical thinking and analytic rigor, weak internal coordination, botched collection priorities, and too much reliance on technical intelligence-gathering, too little on spies.[16]

Stephen Marrin, bringing critical thinking more explicitly to the attention of the intelligence community, included this quote in several of his articles published from 2002-2004[17] about improving intelligence analysis. Marrin was one of the first to emphasize the need for critical thinking.

Stephane Lefebvre also highlighted the importance of critical thinking in 2003:

> If we accept the cognitive model developed by Operating Systems, Inc. as valid, then it becomes clear why analysts must be trained and encouraged to develop the necessary skills to think critically and innovatively. Objectivity is, as Michael Herman argues, an 'elusive ideal.'58 This is important if intelligence analysts are to produce estimates that are as unbiased and free of logical fallacies as possible. To wit, if anything should be taken for granted it is the centrality of critical reflection, or boundary exploration and critique, to all forms of analysis. It is perhaps a poor reflection on the current analytical culture that critical thinking as an activity has to be made explicit.59 [18]

Major George E. Lewis III also wrote about how the lack of critical thinking contributed to intelligence failures in a document published in 2005:

> Short of a lack of information, failures in thinking are perhaps the number one reason behind intelligence failures. Failures or the inability to recognize bias, understand cultural deviations, and ignoring alternative premises are only a few of the traps that an intelligence analyst can fall prey to if he/she cannot think critically. Of the eight critical

---

[16] Anonymous. "Same Ol', Same Ol'," *Aviation Week and Space Technology*, Vol. 148, No. 23, 1998, pp. 21.

[17] See Marrin, S. "CIA's Kent School: A Step in the Right Direction," *International Studies Association Conference*, New Orleans, LA, March 18, 2002; Marrin, S. "Improving CIA Analysis by Overcoming Institutional Obstacles," in *Bringing Intelligence About: Practitioners Reflect on Best Practices*, ed. R.G. Swenson, Joint Military Intelligence College, Washington, D.C., 2003, pp. 41-59; and Marrin, S. "CIA's Kent School: Improving Training for New Analysts," *International Journal of Intelligence and Counterintelligence*, Vol. 16, No. 4, 2003-2004, pp. 609-637.

[18] Lefebvre, S.J. "Strategic Warning: If Surprise is Inevitable, what Role for Analysis? POSTER Presentation TC99," *International Studies Association (ISA) 44th Annual International Convention*, Portland, OR, February 25 - March 1, 2003, pp. 23-24.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

> skills within the core competencies of intelligence analysts, critical thinking is the most crucial and is often the least trained.[19]

In the years following the identification of the importance of *critical thinking*, it has appeared on lists of analyst competencies, is increasingly included in analyst training curricula, and is now mentioned explicitly in governing documents such as *The US Intelligence Community's Strategic Human Capital Plan*.[20] Yet it is not always clear what anyone means when the term *critical thinking* is used nor how to develop the competency in analysts in order to improve the analysis process and reduce failures caused by "a lack of critical thinking."

Noel Hendrickson noted the ongoing lack of understanding of critical thinking in intelligence analysis in 2008:

> Critical thinking appears on almost every list of the essential skills for intelligence analysts. But any corresponding attempt to define critical thinking more precisely is seldom encountered. And, on those rare occasions when definitions are offered, they inevitably (albeit quite understandably) amount to new applications of existing approaches. Yet, these existing approaches derive from more general academic attempts to create better thinkers and not from any specific concern for the problems of intelligence analysis. Thus, despite the undeniable importance of critical thinking in intelligence analysis, few if any attempts are made to define critical thinking specifically for intelligence.[21]

In support of Hendrickson's statement, we found a total of 21 intelligence analysis documents that contained definitions for critical thinking. Seventeen of the items had been published during or before 2008. Seven of the documents referenced existing scholarly definitions, 13 of the documents provided new, unique definitions, and some did both. No reports provided information on how critical thinking improves intelligence analysis nor gave any insight into which version of critical thinking might be the most useful for intelligence analysis.

Critical thinking's multiple definitions, the varied descriptions of how to apply critical thinking to intelligence analysis, and the lack of information demonstrating the benefit of critical thinking illustrate the need for a better understanding of critical thinking and how it might support effective intelligence analysis. While we can intuitively accept that improvements in cognitive processes described by the term *critical thinking* can improve analysis, it would be beneficial to reach agreement on specifically what leads to the desired cognitive improvements, including such topics as thinking skills, thinking dispositions, and effective training.

---

[19] Lewis, G.E. *Army Intelligence Analysis: Transforming Army Intelligence Analysis Training and Doctrine to Serve the Reasonable Expectations and Needs of Echelons Corps and Below Commanders, Consumers, and Customers,* ADA435988, United States Army Command and General Staff College, Ft. Leavenworth, KS, 2005, p. 32.

[20] Anonymous. *The US Intelligence Community's Strategic Human Capital Plan: An Annex to the US National Intelligence Strategy*, Office of the Director of National Intelligence, Washington, D.C., 2006.

[21] Hendrickson, N. "Critical Thinking in Intelligence Analysis," *International Journal of Intelligence and Counterintelligence,* Vol. 21, No. 4, 2008, p. 679.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

5.2 Purpose

The purpose of the research synthesis was to provide an understanding of the concept of critical thinking, how the concept is represented in the intelligence literature, and its potential applicability to intelligence analysis. We hoped to learn:

- What is critical thinking?
- What is the state of knowledge regarding critical thinking?
- Can we train someone to think critically?
- Can we assess someone's ability to think critically?
- How can this understanding of critical thinking be applied to improving intelligence analysis?

5.3 Findings

The answers to the basic questions that guided this research were:

1. *What is critical thinking?* We do not have a clear answer.
    a. Although critical thinking is generally recognized as important (and scholars in all disciplines in this study make this case emphatically), a formal agreement on what critical thinking is does not exist either within the intelligence community or within other disciplines. However, common themes do exist that clarify critical thinking and identify its potential usefulness in intelligence analysis.
    b. Critical thinking is a concept describing a quality of thinking. It refers to *how* one approaches the thinking task. Critical thinking is useful when exploring a situation, phenomenon, question, or problem to arrive at a hypothesis or conclusion about it that integrates all available information and that therefore can be convincingly justified.
    c. Skills and dispositions such as those listed in Table 1 are *hows* that might be especially useful in contributing to the quality of thinking called critical thinking. As a quality of thought, critical thinking can and potentially should be applied to every part of intelligence analysis.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Table 1: Recommended Critical Thinking Skills and Dispositions for Intelligence Analysts

Critical Thinking Skills	Critical Thinking Dispositions
Interpretation	Willingness to engage in intellectual effort
Analysis	Systematic
Evaluation	Persistent
Inference	Intellectual integrity
Synthesis	Open-minded
Explanation	Intellectual curiosity
Self-regulation	

2. *What is the state of knowledge of critical thinking?* The best description of the current state of knowledge was provided by Condon and Riley: "The current literature on critical thinking is rife with conflict and competing ideologies."[22]
    a. Examples supporting this statement include the many different definitions, lists of skills and kinds of skills, and models of critical thinking that I found in the literature.
    b. Little attention has been devoted to critical thinking performance – are individuals with strong critical thinking skills and dispositions as measured by assessments able to perform better in work that appears to require critical thinking? This shortcoming is as apparent in the intelligence literature as it is in the literature from other disciplines.
3. *Can we train someone to think critically?* Perhaps.
    a. Much of the education and training available to date in university courses, publicly available courses, and courses intended specifically for the intelligence community are based on simplistic descriptions of critical thinking, provide insufficient time for effective practice, use ineffective teaching strategies, and include few or ineffective methods of assessing what has been learned.
    b. Training that has been effective as demonstrated by performance on some sort of assessment was developed to teach a specific set of skills, dispositions, and operations in order to achieve a specific outcome.

[22] Condon, W. & Kelly-Riley, D. "Assessing and Teaching What We Value: The Relationship between College-Level Writing and Critical Thinking Abilities," *Assessing Writing*, Vol. 9, No. 1, 2004, p. 64.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Successful training has been focused, well-designed, and consistently delivered, with extensive opportunities for practice.

4. *Can we assess someone's ability to think critically?* Again, perhaps.
   a. A number of standardized assessments and examples of customized assessments exist that address different aspects of critical thinking. It is not clear whether any of the currently available standardized assessments are beneficial for the intelligence community. Few documents were found that described assessments designed for adults to be used in determining job readiness, suitability, or performance.[23] No documents were found describing how to assess whether someone uses critical thinking regularly in his or her job or life.
   b. Each publicly available assessment is somewhat different, focused on the critical thinking definition espoused by the assessment author.
   c. Publicly available assessments have primarily been used in assessing the impact that a class or an experience such as years in college has on the ability to think critically. That is, they assess an experience's impact at Level 2 in Breckenridge's schema.[24]
   d. Several documents provided guidelines for developing a custom assessment (i.e. rubrics) that could be designed for a unique environment such as the intelligence community. Those publications also provided examples of custom assessment tools.
5. *How can this understanding of critical thinking be applied to improving intelligence analysis?* The intelligence community needs to exert additional effort in order to benefit from investments in critical thinking.
   a. Critical thinking is widely recognized as an important competency for intelligence analysts. However, the intelligence community does not yet have a common understanding of what critical thinking is or how to apply it in intelligence analysis work. Without a common understanding of critical thinking, the claims regarding its ability to improve intelligence analysis, the investments in training for it, and documents such as strategic plans calling for critical thinking are built on a weak foundation. Which version of critical thinking is expected to improve analysis? What critical thinking competencies will result in better analysis? How would critical thinking be recognized if it were present?
   b. Current training in the intelligence community varies widely. Courses exist with different definitions of critical thinking, a variety of topics covered, and varying amounts of practice available, resulting in analysts who have

[23] One exception is a study of using the Watson Glaser Critical Thinking Assessment in hiring intelligence analysts completed in 1983.
[24] Breckenridge, J.G. "Designing Effective Teaching and Learning Environments for a New Generation of Analysts," *International Journal of Intelligence and Counterintelligence*, Vol. 23, No. 2, 2010, p. 308.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

differing levels of critical thinking knowledge and abilities. Many courses are primarily designed to introduce analysts to the *concept* of critical thinking. These courses do not provide sufficient depth or time for practice that would enable an analyst to become a skilled critical thinker. I found no reports of training evaluations that demonstrated that the courses actually improved analyst competencies or performance.

c. Although it is widely believed that critical thinking will improve intelligence analysis, we found no reports demonstrating the benefit of critical thinking to intelligence analysis.

5.4 Recommendations

These findings provide a roadmap for research and activities that will demonstrate the utility of critical thinking to the intelligence community. These activities will also identify the best way to integrate critical thinking into intelligence analysis to gain maximum benefit throughout the entire intelligence community.

1. Define a concept of critical thinking that makes sense for intelligence analysis and that can be accepted throughout the intelligence community. This definition should:
   a. Identify expected standards of critical thinking in intelligence analysis using techniques such as rubrics.
   b. Identify the appropriate skills, dispositions, and personal epistemology maturity level needed for effective intelligence analysis.
   c. Clearly articulate how to apply critical thinking in intelligence analysis.
2. Evaluate the various aspects of critical thinking prior to making major investments in fostering it throughout the intelligence community. Research projects might include:
   a. Investigating the impact that improved critical thinking skills and dispositions have on intelligence analysis.
   b. Determining an approach to training (including topics, teaching strategies, and practice mechanisms) that will provide the most improvement to the practitioners of intelligence analysis.
   c. Evaluating publicly available assessments and their usefulness for assessing an analyst's skills or dispositions and therefore predicting job performance or identifying training needs.
   d. Evaluating whether assessments of critical thinking skills, dispositions, and personal epistemology are useful in the hiring process.
3. Develop a consistent critical thinking training curriculum that includes topics that have been demonstrated to improve intelligence analysis and that uses best practices in skills training. Rigorously evaluate the effectiveness of the training and make appropriate improvements until the training meets the needs of the intelligence community.
   a. Successful experiments exist that provide models of effective instruction.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

b. The training used in nursing education provides a cautionary tale of training approaches to avoid.

4. Determine the best way to assess the thinking skills and dispositions of analysts and their ability to apply critical thinking to the analysis process. Develop an assessment methodology that measures not only the results of training, but the impact of that training on analytic results.

   a. For example, rubrics provide information that is not only useful for assessment, but also useful in identifying performance expectations in advance. An analyst could use a rubric to guide his or her work efforts and evaluate his or her own analytic products.[25]

[25] Marsh, M. *Advanced Analysis Cognition: Critical Thinking*, March, 2012 is the complete report of this research synthesis. It is in press at the time of the current final report for the Advanced Analysis Cognition effort.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

6.0 THINKING DISPOSITIONS

6.1 Introduction

Everyone agrees that intelligence analysis is an intensely cognitive process and that the quality of an analyst's cognition determines the quality of his or her analysis. However, less is understood about what elements combine to make productive, effective cognition.

Richards Heuer noted this challenge in *Psychology of Intelligence Analysis*:

> Of the diverse problems that impede accurate intelligence analysis, those inherent in human mental processes are surely among the most important and most difficult to deal with. Intelligence analysis is fundamentally a mental process, but understanding this process is hindered by the lack of conscious awareness of the workings of our own minds.[26]

Thinking dispositions are a theoretical construct intended to describe one aspect of cognition. They describe a person's *inclination* or *motivation* to make an effort to use one's mental skills to address tasks requiring thinking.

The *Framework for Analytic Cognition (FAC): A Guide for Doing All-Source Intelligence Analysis*[27] noted the contribution that thinking dispositions make to effective cognition:

> While there are many unknowns about how people think and various terms are used, the preceding discussion indicates the following factors are important.
>
> - Knowledge
> - Thinking dispositions
> - Cognitive skills
> - Motivation and engagement
> - Epistemological beliefs

Advanced Analysis Cognition: Critical Thinking.[28] Also highlighted the importance of thinking dispositions to effective thought:

> The ability to employ critical thinking skills is still not sufficient to ensure that an individual will bring a critical approach to thinking. A thinker must be willing to make the extra effort to think critically. The thinker must have the *disposition* to think critically

The earliest scholars interested in improving thinking highlighted the importance of attitude. For example, John Dewey noted that a thinker needs more than skills in *How We Think*.

> Knowledge of the methods alone will not suffice; there must be the desire, the will, to employ them. This desire is an affair of personal disposition. But on the other hand the

[26] Heuer, R.J.J. *Psychology of Intelligence Analysis*, Center for the Study of Intelligence, Washington, D.C., 1999, p. 1.
[27] Kampman, C.M., Mangio, C.A., Parry, T.L. & Wilkinson, B.J. *Framework for Analytic Cognition (FAC): A Guide for Doing All-Source Intelligence Analysis*, AFRL-RH-WP-TR-2012-0109, 2011.
[28] Marsh, M. *Advanced Analysis Cognition: Critical Thinking*, in press.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

> disposition alone will not suffice. There must also be understanding of the forms and techniques that are the channels through which these attitudes operate to the best advantage.[29]

Edward Glaser described the importance of thinking dispositions in his 1938 experiment regarding teaching critical thinking:

> The development of ability to think critically, it should be noted, is not limited to cultivation of better methods for finding and testing evidence and meanings, and arriving at well-founded conclusions. Knowledge of the methods of logical inquiry is important. Even more important for the everyday practice of democracy, however, are the *attitudes* involved in critical thinking. Persons who have acquired a disposition to *want* evidence for beliefs, and who have acquired an attitude of reasonableness have also acquired something of a way of life which makes for more considerate and humane relationships among men.[30]

Our understanding of the contribution of thinking dispositions toward effective thinking led us to explore further what has been researched about thinking dispositions. We hoped to determine if improving positive thinking dispositions could benefit the intelligence analysis process.

6.2 Purpose

Our primary research questions were:

> What is the value and feasibility of evaluating a candidate's thinking dispositions as one component of intelligence analyst selection? What is the feasibility of training individuals in order to strengthen their positive thinking dispositions?

To answer these questions, we explored the following topics:

- What are thinking dispositions?
  - How are they described? Do different professional disciplines have different perspectives on thinking dispositions?
  - How are they related to various descriptions of thinking such as critical thinking, reflective thinking, or rational thinking?
  - Are related concepts that describe the affective or motivational aspects of human cognition present in their literature?
  - How have thinking dispositions been understood over time?
- How do thinking dispositions affect cognitive performance?
  - How do individuals use their thinking dispositions while performing cognitive tasks?
  - Does the use and influence of thinking dispositions vary depending on the nature of the cognitive task?

[29] Dewey, J. *How We Think: A Restatement of the Relation of Reflective Thinking to the Educative Process*, 2nd ed., Regnery, Chicago, IL, 1933, p. 30.
[30] Glaser, E.M. *An Experiment in the Development of Critical Thinking*, AMS Press Inc., New York, NY, 1941, p. 6.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

- Can thinking dispositions be assessed? Do reliable and valid assessment methods exist? What evidence exists that supports the value of thinking disposition assessments?
- How do thinking dispositions relate to the characteristics, attributes, and traits of intelligence analysts?
- How are an individual's thinking dispositions established or subsequently changed?
  - What factors influence the development of various thinking dispositions?
  - Can thinking dispositions be improved with training and education or other factors such as life experience or maturity? What evidence exists for this improvement?

6.3 Findings

The primary questions guiding this research were:

> What is the value and feasibility of evaluating a candidate's thinking dispositions as one component of intelligence analyst selection? What is the feasibility of training individuals in order to strengthen their positive thinking dispositions?

Based on the results of this research, we believe it is practical and valuable to use thinking dispositions as one component of intelligence analyst selection. The research also shows that training intelligence analysts to improve their thinking dispositions can have a positive impact on their cognitive activity.

The findings that contributed to these conclusions include:

1. What are thinking dispositions?
   a. Thinking dispositions represent an individual's inclination toward thinking. An individual's strength in positive or productive thinking dispositions identifies *whether someone is likely to notice when effortful thinking is required and the degree of inclination to make the effort when thinking is required*. This description is accepted across academic disciplines and has remained consistent over time.
   b. Thinking dispositions that might be useful for intelligence analysts include:
      - Enjoyment of cognitive effort
      - Intellectual curiosity
      - Open-mindedness
      - Intellectual honesty
      - Tolerant of ambiguity
      - Focus on evidence
      - Persistent
      - Systematic
2. How do thinking dispositions affect cognitive performance?

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

a. It is clear that thinking dispositions are a trigger for cognitive activity. When an individual is *disposed* to think, he or she makes the effort to engage cognitively.

b. The specific thinking dispositions possessed by an individual and the relative strength of individual thinking dispositions influence the degree to which an individual makes an effort to:

- Engage cognitively at all
- Override personal beliefs and biases to ensure an open-minded approach to the task
- Thoroughly investigate a situation in order to find relevant information and to look at all sides of an issue
- Avoid premature closure of the thinking task and exhibit the willingness to tolerate lack of a clear answer (ambiguity) while investigation continues
- Reach a conclusion only after finding sufficient evidence to support the conclusion

c. Psychologists who have conducted experiments into cognitive performance have found that thinking dispositions can predict the outcome of cognitive performance after intellectual ability (IQ) has been considered.

3. Can thinking dispositions be assessed? Are there reliable and valid methods for assessment?

   a. Thinking dispositions can be assessed and a variety of different assessments exist.[31],[32],[33],[34]

4. How do thinking dispositions relate to the characteristics, attributes, and traits of intelligence analysts?

   a. Where scholars described disposition-like attributes of intelligence analysts, a significant overlap with thinking dispositions does exist. The thinking dispositions we have identified are recognized as important contributors to analytic success.

5. How are an individual's thinking dispositions established or subsequently changed?

   a. Thinking dispositions are believed to be developed by the environment and culture in which an individual lives. A family or school setting can foster positive or negative thinking dispositions and can strengthen or weaken

[31] See Facione, P.A. & Facione, N.C. *California Critical Thinking Disposition Inventory (CCTDI) Test Manual,* California Academic Press, Millbrae, CA, 2010.
[32] Sá, W., Kelley, C., Ho, C., Stanovich, K.E. & West, R.F. *Composite Actively Open-Minded Thinking Scale -- 11/6/03,* 2003, pp. 1-2.
[33] Cacioppo, J.T. & Petty, R.E. "The Need for Cognition," *Journal of Personality and Social Psychology,* Vol. 42, No. 1, 1982, p. 116.
[34] Frederick, S. "Cognitive Reflection and Decision Making," *Journal of Economic Perspectives,* Vol. 19, No. 4, 2005, p. 26.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

thinking dispositions by what is modeled, expected, and rewarded in the culture surrounding the thinker.

b. Positive thinking dispositions can be strengthened by instruction and practice. Both aspects of training, that is, creating a culture that expects effective thinking and explicitly teaching for positive thinking dispositions, appear to be valuable.[35]

c. One critical success factor appears to be ensuring sufficient practice for the positive thinking dispositions to become entrenched and habitual.

d. A workplace culture can encourage and strengthen positive thinking dispositions by expecting cognitive behaviors and outcomes that rely on positive thinking dispositions.

6.4 Recommendations

In order to gain maximum benefit from the use of a thinking dispositions assessment in the selection of analysts, the intelligence community should:

1. Conduct a comprehensive job analysis to identify the specific traits and characteristics needed by intelligence analysts. Using this job analysis, identify which specific thinking dispositions have the most positive impact on analytic performance.

   Numerous authors have described various traits and capabilities of the ideal intelligence analyst. These traits are, however, anecdotal. The intelligence community should use the existing intelligence literature as a starting point for developing what might be considered a definitive description of the needed competencies and traits of an intelligence analyst. This description should include thinking dispositions.

2. Purchase, adapt, or develop assessments that measure the strength of an individual's thinking dispositions.

   Once an understanding of analyst competencies, dispositions, and other traits exists, develop an assessment that addresses, at a minimum, the thinking dispositions a candidate has. The many assessments found in this study provide a starting point for the intelligence community. Although not all assessments identified in this study were found to be equally reliable and valid, they are a source of potentially useful questions and approaches that might be included in the selection process for intelligence analysts.

3. Validate that the assessment is useful in identifying individuals with thinking dispositions that have a positive impact on intelligence analysis.

   Because of the potential impact of using a thinking dispositions assessment in intelligence analyst selection, care must be taken to ensure that the assessment tool is valid and useful for selection. Although intelligence analysis does not lend itself to quantitative evaluation such as sales quota achievement, it is possible to

[35] Perkins, D.N., Jay, E. & Tishman, S. "Beyond Abilities: A Dispositional Theory of Thinking," *The Merrill-Palmer Quarterly,* Vol. 39, No. 1, 1993, pp. 16-17.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

experimentally assess the impact of thinking dispositions on an individual's analytic results. The experiments conducted by Stanovich, for example, provide a model for how this might be done.[36] An essential ingredient of the experiment would be a standard repertoire of intelligence problems and databases tailored to the participants' specialties. The experiment would include a solution for each problem that represents the best analysis that can be accomplished given the information in the databases. Experiment facilitators would use these solutions to evaluate each participant's analysis and would be able to compare analytic results with thinking disposition assessment results.

4. Validate that the assessment is fair and does not inappropriately exclude any individual or classes of individuals.

   Ensure that the assessment will meet the "Uniform Guidelines on Employee Selection Procedures" as defined by the Equal Employment Opportunity Commission, the Civil Service Commission, the Department of Labor, and the Department of Justice. These can be found at http://www.uniformguidelines.com/uniformguidelines.html.

5. Strengthen the thinking dispositions of intelligence analysts already at work in the intelligence community by improving intelligence analyst training programs. The goals of these improvement efforts are to ensure that the training culture fosters positive thinking dispositions and includes specific training on thinking dispositions.
6. Ensure the work environment continues the enculturation process through its efforts to expect, strengthen, and reward strong positive thinking dispositions.[37]

[36] Stanovich, K.E. *What Intelligence Tests Miss: The Psychology of Rational Thought*, Yale University Press, New Haven, CT, 2009, p. 34.

[37] Marsh, M. *Advanced Analysis Cognition: Thinking Dispositions*, Final Report, May 2012 is the complete report of this research synthesis. It was in press at the time of the current final report for the Advanced Analysis Cognition effort.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

7.0 PRACTICE-BASED LEARNING

7.1 Introduction

One of the recommendations developed as a result of the *State of Knowledge* contract was:

> Establish a training course using the handbook proposed in Recommendation 4. This would include using the procedures taught for performing the complete analysis process. The approach to training would incorporate procedures and exercises designed to accommodate context sensitivity. Accordingly, an essential ingredient of the training is a standard repertoire of intelligence problems and databases tailored to the students' specialties. The course will provide a solution for each problem that represents the best analysis that can be accomplished given the information in the databases. Course facilitators will use these solutions to evaluate each student's analysis. Each student would also be able to compare his or her results with what an expert has accomplished.

This recommendation implied certain content in the training intervention: learning the content of the handbook (eventually developed as the *Framework for Analytic Cognition(FAC)* and putting what has been learned into practice. The issue researched further in the effort under review was how to best design and develop such a training course, with particular emphasis on the practice component.

Based on the nature of intelligence analysis, the FAC, research done during the *State of Knowledge* contract, and the philosophical outlook of the FAC team, a performance improvement intervention designed with a practice based learning approach seemed to be the most appropriate method for achieving the best training outcomes. The goal of the current study was to validate this approach.

7.2 Purpose

Our goal was to be able to make informed recommendations regarding how best to incorporate practice based learning into an educational experience for the FAC. We hope to be prepared to participate in various course development efforts such as course design, material development, instructor and student selection and coaching, course reviews, and pilot courses. We intended to be able to provide guidance to any organizations wishing to implement an educational program based on the FAC.

We designed this effort to concentrate on three broad areas:

1) What is practice based learning?
2) Is practice based learning the optimal approach for developing an intelligence analyst's ability to use the FAC? That is, was practice based learning, as recommended in the final report of the *State of Knowledge* effort, the correct recommendation?
3) If practice based learning is the optimal approach for the FAC in general, are there some aspects of the FAC that are especially amenable to being learned through practice based learning?

The effort was not intended to be an exhaustive review of practice based learning. Our work on this portion of the contract did not review classic training approaches such as lecture, online

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

learning, or workshops, except for suggestions about how they are best integrated into a practice based learning environment. This effort also did not review basic course development methodologies.

7.3 Findings

Practice based learning is a variation of *problem based learning*, adapted to a variety of occupations. Problem based learning has the following characteristics:

1. A student-centered approach that relies on the learner to identify and review knowledge needed to resolve a case
2. Use of an authentic problem introduced to the tutorial group prior to any preparation or study
3. Synchronous small group collaborative work supported by a faculty facilitator, combined with self-directed study to investigate learning issues that arise from problem discussion
4. Use of the problem and tutorial discussion of the problem as vehicles to identify the required knowledge (facts and concepts) as well as problem-solving skills to resolve it[38]

Billett provides a useful definition of practice based learning:

> Before proceeding further, it is important to capture what constitutes practice and then learning through practice. The definition taken here of practice is that which occurs through the usual or everyday exercise of the occupation. That is, practice comprises the enactment of the kinds of activities and interactions that constitutes the occupation. This is referred to as *praxis* in some traditions, and is used to distinguish between practice and theory. Here, however, it is assumed that practice is enacted through access to and the exercise of forms of conceptual, procedural, and dispositional knowledge that underpin competent practice. Moreover, learning through practice is seen as a process that arises through the exercise of the occupational practice, and there is no distinction between engaging in practice and learning. Certainly, the process of learning is now widely acknowledged as being a ubiquitous and ongoing activity that is a necessary part of everyday conscious thinking and acting. In essence, the process of humans' construal and construction of experience constitutes learning. There is also no privileging of particular settings as sites of learning, except through the qualities of activities and interactions (i.e., experiences), because it is what and how individuals construe and construct from their experiences that ultimately shapes what they learn, not necessarily what social settings intend them to learn or even press them to learn (Billett, 2009a).[39]

We first encountered the term practice based learning as it was associated with the medical profession. Practice based learning seemed to be a good model for intelligence analysis as many

[38] Clark, R.C. *Building Expertise: Cognitive Methods for Training and Performance Improvement*, 3rd ed., Pfeiffer, San Francisco, CA, 2008, p. 288.
[39] Billett, S. "Learning through Practice," in *Learning through Practice: Models, Traditions, Orientations, and Approaches*, ed. S. Billett, Springer, Dordrecht, 2010, p. 2.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

of the cognitive challenges faced by physicians are similar to those faced by intelligence analysts.

As with many of the other topics studied during *Advanced Analysis Cognition*, developing a definition for the subject of the study was the first research challenge. While *practice based learning* is not widely used in the literature, *problem based learning* is found frequently and used in many different contexts. We searched the literature for both of these terms and then expanded the search to include learning approaches such as action learning, active learning, experiential learning, project-based learning, inquiry-based learning, professional learning, problem-centered instruction, situated learning, self-directed learning, and cognitive apprenticeship.

The planned outcome for this research was to develop a concise characterization for each topic that includes a definition, a description of how it is typically used, and a list of each approach's strengths and weaknesses. The characterization for each approach was to help the team and others validate the recommendation of practice based learning for the FAC.

7.4 Recommendations

We obtained and reviewed over 50 publications in order to develop an issue statement, analysis plan, and acquisition plan for this research effort. Unfortunately, work was suspended on the contract before we could make any further progress on this task. Therefore, the chief recommendation arising from this effort would be to continue our research and assessment efforts in order to address all of the questions set forth in the "Purpose" section of this document.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

8.0 EPISTEMOLOGICAL BELIEFS

8.1 Introduction

General agreement exists that the cognitive domain as applied to decision making, problem solving or assigning meaning consists of knowledge, comprehension, application, analysis, synthesis, and evaluation.[40] However, this description of the cognitive domain does not discuss the precursor functions used to establish the knowledge used during cognition. Researchers have investigated many facets of what determines the ability of an individual to acquire knowledge. One of the results of this research is the identification of epistemological beliefs, i.e., beliefs about the nature of knowledge, and their critical role in knowledge acquisition.[41] [42]

8.2 What are Epistemological Beliefs?

What are epistemological beliefs? This is one description:

> …CERTAINTY of knowledge, ranging from knowledge is absolute to knowledge is tentative…
>
> …STRUCTURE of knowledge, ranging from knowledge is organized as isolated bits and pieces to knowledge are organized as highly interwoven concepts…
>
> …SOURCE of knowledge, ranging from knowledge is handed down by authority to knowledge is derived through reason…
>
> …CONTROL of knowledge acquisition, ranging from the ability to learn is fixed at birth to the ability to learn can be changed…
>
> …SPEED of the knowledge acquisition, ranging from knowledge is acquired quickly to not-at-all to knowledge is acquired gradually.[43]

Epistemological beliefs at the lower end of the continuum (e.g., knowledge is absolute, organized in isolated bits and pieces, handed down by authority, with the ability to learn fixed at birth) are characterized as naïve beliefs. Those beliefs at the upper end of the continuum (e.g., knowledge is tentative, organized as interwoven concepts, derived through reason, with an ability to learn that can change) are characterized as sophisticated beliefs.[44]

There are many variants in definitions of epistemological beliefs. However, at the core of all these definitions is the question of whether knowledge is absolute or tentative.

---

[40]Alexander, P.A., Dinsmore, D.L., Fox, E., Grossnickle, E.M., Loughlin, S.M., Maggioni, L., Parkinson, M.M. & Winters, F.I. *Higher-Order Thinking and Knowledge: Domain-General and Domain-Specific Trends and Future Directions.* Undated Manuscript, pp. 4.

[41]Schommer, M. & Walker, K. "Are Epistemological Beliefs Similar Across Domains?" *Journal of Educational Psychology*, Vol. 87, No. 3, 1995, pp. 424-432.

[42]Harteis, C., Gruber, H. & Lehner, F. "Epistemological Beliefs and their Impact on Work, Subjectivity, and Learning," in *Work, Subjectivity and Learning: Understanding Learning through Working Life*, eds. S. Billett, T.J. Fenwick & M. Somerville, Springer, Dordrecht, The Netherlands, 2006, pp. 123-140.

[43]Schommer, M. "An Emerging Conceptualization of Epistemological Beliefs and their Role in Learning," in *Beliefs about Texts and Instruction with Text*, eds. R. Garner & P.A. Alexander, L. Erlbaum, Hillsdale, NJ, 1994, p. 28.

[44]Schommer p. 29.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

8.3 Findings

The work of Perry published in 1970 is generally agreed to mark the beginning of research on epistemological beliefs.[45] Since then the amount of publication dealing with epistemological beliefs has steadily increased. The general attributes of the published research are:

- The preponderance of the research has been directed at relating epistemological beliefs to learning. Little disagreement exists that higher (more sophisticated) levels of epistemological beliefs lead to improved performance in learning.
- The most frequent research subjects are children and adolescents in K-12 settings. Less work has been done on college students and even less on graduate students. Almost no work has been done with adults who have completed their formal education.
- The epistemological beliefs of teachers, both in training and in practice, have been investigated. The major point of interest was how their beliefs shaped their practice of teaching. Of particular note is that conflicts often exist between the teacher and the educational system. The educational system often pushes a pedagogical program as if knowledge is certain, while teachers new to the profession have more sophisticated beliefs.
- Research on the effect of epistemological beliefs on problem solving showed an almost one-time spurt of interest. Only a couple of reports on epistemological beliefs and work related task have been reported. These meager data do suggest that performance improves with a more sophisticated epistemological belief structure.
- A frequent current topic is the effect of culture on epistemological beliefs. As might be expected, most of the authors of these publications are not US-based.
- A variety of techniques have been developed to measure epistemological beliefs. The techniques are either interviews or a paper and pencil test. The variation in the techniques and what is being measured is very dependent on the researcher's definition of epistemological beliefs. However, regardless of how defined or measured, the same general pattern is observed: performance improves with increasing sophistication of epistemological beliefs.
- General acceptance exists that epistemological beliefs can be changed. The conditions that foster these changes have not been thoroughly addressed other than the observation that change occurs with increasing amount of education.

Given the preponderance of research relating educational performance conducted by people who are part of the educational system, the lack of research outside of the educational environment is not surprising. Most surprising is the lack of research on the relationship between thinking dispositions and epistemological beliefs. Intuitively one would expect that a sophisticated level of epistemological beliefs would correlate with a high level of thinking dispositions or vice

[45] Perry, W.G. *Forms of Intellectual and Ethical Development in the College Years: A Scheme*, Holt, Rinehart and Winston, New York, NY, 1970.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

versa. For example, a person who believes knowledge is certain will have weaker evidence of thinking disposition characteristics such as keeping an open mind.

A second major omission in the research on epistemological beliefs was mentioned above: almost none has been done with adults who have completed their formal education. Anecdotal information from other areas suggests that epistemological beliefs become less sophisticated as people age.

8.4 Recommendations

In summary, epistemological beliefs are a critical component of analytical cognition and its effectiveness. Various measurement techniques are available to assess the level of epistemological beliefs and provide a consistent indication of a person's overall level of beliefs. Ample evidence shows that this is one attribute of cognition that can be changed and measured. Thus, a real potential exists that using epistemological beliefs to aid in the selection of personnel for analysis, and the training of such personal to improve their performance, will improve analytic cognition.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

9.0 COGNITION

9.1 Introduction

Universal agreement exists that intelligence analysis is a cognitive process. However, despite the treatment of intelligence analysis as if it were something special, cognitively it isn't. Conceptually, differences between the cognition in intelligence analysis and that in many other intellectual activities are non-existent. It follows then that all research on cognition is potentially applicable to understanding the cognition of intelligence analysis.

Because of the universality of cognition to human activities an enormous amount of attention by philosophers and scientists has been focused on this topic. In general, these efforts fit into three categories:

- A study of the brain hierarchical structure and neural networks
- The processes of cognition such as sensemaking, mental models, and the divided mind
- Human cognitive behavior and the input/output of cognition

While all of these activities are adding to our understanding of cognition, the findings on behavior and input/output most readily translates into information that informs the act of intelligence analysis. What follows is an attempt to relate our findings on cognition to the practice of intelligence analysis.

9.2 Words as Concepts

Based on our analysis of research findings related to intelligence analysis, our intention is to develop and communicate concepts of the cognition of intelligence analysis and the foundation upon which this cognition rests. The immediate challenge is the means by which these concepts will be communicated: words. Many people have commented on difficulty of relating words to concepts.

> Socrates said, "Wisdom begins with the definition of terms."[46]
>
> "A vague idea is not clarified by giving it a name"[47]
>
> In the world of human thought ... the most fruitful concepts are those to which it is impossible to attach a well-defined meaning. —Hunter Lewis, *A Question of Values*
>
> "Names are codes; we should not let familiarity with them masquerade as understanding" [48]
>
> In as much as words do not have intrinsic meanings, the best we can aspire to is to discover the various connotations that have been given to the word, perhaps to see

[46] Cited in Bascatow, T. & Bellafiore, D.J. "Redefining Geospatial Intelligence," *American Intelligence Journal*, Vol. 27, No. 1, 2009, p. 38.
[47] Columbia Associates in Philosophy, 1923, p. 292.
[48] Atkins, P.W. *Creation Revisited: The Origin of Space, Time, and the Universe*, Penguin Books, London, 1992, p. 2.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

if usage reflects a high degree of consensus regarding what it should be taken to mean.[49]

Arguably, like most words familiar from common parlance, it is used uncritically, more often than not, with the tacit assumption that everybody knows what it means.[50]

All words begin as servants, eager to oblige and assume whatever functions may be assigned them, but, that accomplished, they become masters, imposing the will of their predefined intention and dominating the essence of human discourse. It is for this reason that articulate conversation must demand not only clarity of thought and expression but also preciseness of word choice and meaning.[51]

When we find a promising perspective, we do not merely appropriate it but, by making an imaginative interpretation of it, construe it to make it our own. The resulting perspective never will be exactly the same as that originally expressed by the other, just as the full range of meaning that we attach to words or concepts always will vary to some extent from the connotations attributed to the same words or concepts by others. [52]

We find it easy to fool ourselves into believing that something has been explained when it has really only been labeled or described, especially if the label sounds scientific or the description is given in technical terms. We can convince ourselves that we have made progress in our understanding of nature when, in fact, all we have done is substitute in our descriptions currently acceptable words for currently unacceptable ones.[53]

Words which stand for complicated concepts cannot be defined by a dictionary. Words like "Iiberalism" and “democracy" require the equivalent of scores of dictionaries, or scores of shelves of dictionaries. You cannot define those as you define "paper" and "ink." So with our own words that stand for complicated concepts - such as “evaluation," "indicator/' "capability," "estimates," and so on. As of today we use these words easily and often - yet one wonders if they are always understood in exactly the *way* intended. [54]

A word, therefore, can not only indicate a fact, but can also suggest an emotional attitude towards it. Such suggestion of an emotional attitude does go beyond mere factual description because our approvals and disapprovals are individual - they belong to ourselves and not to the objects we approve or disapprove of. An

[49] Nickerson, R.S. *Aspects of Rationality: Reflections on What It Means to be Rational and Whether We Are,* Psychology Press, New York, NY, 2008, p. 2.
[50] Nickerson, p. 212.
[51] Pajares, M.F. "Teachers' Beliefs and Educational Research: Cleaning Up a Messy Construct," *Review of Educational Research,* Vol. 62, No. 3, 1992, p. 308.
[52] Mezirow, J. *Transformative Dimensions of Adult Learning,* Jossey-Bass, San Francisco, CA, 1991, p. 165.
[53] Nickerson, p. 239.
[54] Kent, S. "The Need for an Intelligence Literature," *Studies in Intelligence,* Vol. 45th Anniversary Special Edition, No. Fall, 2000, p. 6.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

> animal which to the mind of its master is a faithful and noble dog of mixed ancestry may be a 'mongrel' to his neighbour whose chickens are chased by it.[55]
>
> Thus an author can never literally transfer an idea. He can merely put down certain arbitrary symbols, which will serve to arouse a similar thought in his readers. How greatly the reader's thought differs from the author's it is difficult if not impossible to determine, for minds can only communicate by words. It is this difference in associated concept which often makes a reader fail to appreciate the profoundest thoughts of an author, and even, on the other hand, occasionally to see depth where it does not exist. [56]

The above is a sample of the commentary in the literature on the relationship between concepts and words. Agreement exists on the idea that words are not concepts but we have no other way to communicate concepts other than the use of words. Despite all of the cautionary commentary, the common practice of using a word without a precise definition to represent a concept persists. As a matter of practice we do not define our words in terms of the concepts represented and we assume that others have the same conceptual definition of the words as we do. The result is as predicted. Despite all external manifestation of agreement and understanding we cannot be confident that we have developed a common understanding of concepts.

The offset between words and concepts is particularly great in the literature on intelligence analysis and cognitive psychology. A variety of words are used in this literature to describe the act of input, modification, and output such as fact, data, information, knowledge, belief, hypothesis, evidence, assumptions judgment, opinion, and theories. However, a consistent or precise meaning of these words is not used in the intelligence literature, sometimes even by the same author. In many cases the words are used as if they were synonyms of one another. The net result is a lack of conceptual clarity as to what is postulated about the act of cognition or the conduct of intelligence analysis.

The issue of words and concepts is particularly acute to our endeavor. We present concepts about cognition that differ from others but the words we use to describe these concepts are similar to words used by others. The conceptual differences only become apparent by recognition of the different meanings attributed to the same words. To alleviate this problem the following is the relationship of words and concepts used in our description of cognition. We are not asking you to agree with our definition of the relationship but we are asking you to use our definition as you assess our conceptual description of cognition. Otherwise our description loses all meaning if other relationships are used.

- Information – content that is received by one's senses. An umbrella description of all and any content of the input to the cognitive function. Content can include fact, data, and output from cognitive functioning of others such as belief, opinions, or judgments.
- Fact – identical results from repeated measurements of the characteristics of various objects, behavior, or phenomena. For example, the characteristics of gravity, speed of light and atomic weights are all facts. A distinctive feature of a fact is that it has

[55] Thouless, R.H. *Straight and Crooked Thinking,* Pan Books Ltd., London, UK, 1953, p. 5.
[56] Hazlitt, H. *Thinking as a Science,* E. P. Dutton & Co., New York, NY, 1916, p. 202.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

a value or meaning which involves little or no human interpretation. Therefore, the meaning of facts does not vary between individuals. Also, facts are not time dependent. The same measurement results are obtained whatever the time interval between measurements exists. Comparatively, there are few facts. Contrary to many assertions, facts do speak for themselves. Common usage is the phrase "the facts are." In almost all incidents the statement does not relate to facts but rather to what the individual considers indisputable data.

- Data - results of measurement that are likely to change when the condition of measurement changes. Examples include the population of the U.S., the Dow Jones index, polling results, and the IQ of a group. The assertion that data do not speak for themselves is correct. As mentioned above, the oft-used phrase "the facts are" is more accurately expressed as "the data are."
- Known – The content of the memory of an individual. Part of what is known is identical to the information received; the content has not been changed by cognition of the individual. The other part of what is known is the result of internal thought and thinking. An individual does not know what they know. What they know is not the same as the content that they can consciously retrieve.
- Belief – An explanation of phenomena, events, or occurrence in life that an individual holds to be true. The existence of a belief or the degree it is considered true is independent of the amount of supporting evidence held by the individual.
- Knowledge – What is known.
- Evidence – Information to which a meaning has been assigned that supports or negates a belief. All information is evidence of some belief. The same information can have many meanings, so it can be evidence for many beliefs.
- Assumption – statements, descriptions, or explanation that are treated as if they were true; a provisional belief to be used in cognition.
- Hypothesis – a tentative explanation of phenomena, events, or occurrences; a conditional belief for the purpose of marshaling supporting evidence. If the evidence convinces one that the hypothesis is true, it is no longer a hypothesis but a belief.
- Opinion/Judgment – an external expression of a belief or combinations of beliefs.
- Theory - a belief or collection of beliefs that are held to be true by a substantial number of individuals.
- Cognition – a global word for all functioning of the mind.
- Thinking – A specific form of cognition. A goal directed activity based on what is known to create explanations. [57]
- Inner speech – A conversation with yourself that does not involve external vocalization.

[57] Holyoak, K.J. & Morrison, R.G. "Thinking and Reasoning: A Reader's Guide," in *Oxford Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, p. 1.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

- Thought – The content of inner speech
- Consciousness – Cognitive activity using inner speech
- Unconsciousness- Cognitive activity without the use of inner speech

Since at this stage you are not aware of the concepts that are driving these definitions, we do not necessarily expect agreement. If you are unable, as expected, to adopt these definitions, we ask that you use them as assumptions, as defined above.

9.3 Cognitive Behavior

9.3.1. Individual Need for Explanations

Whether one calls it sensemaking, mental models, mindsets, frames, or schemata, humans have an unrelenting need to develop beliefs about everything with which they interact. This need is the underlying motivation for cognitive activity.

> The human brain is a compulsive explainer. It's constantly churning out hypotheses based on current observations, prior experiences, and existing beliefs. It does that automatically, effortlessly. And quickly. [58]
>
> It isn't that we humans like to have explanations for things; we must have explanations. We are an explaining species. Explanations, by making sense of an uncertain world, apparently render the circumstances of life more predictable and thus diminish our anxieties about what the future may hold. Although these explanations have not always been valid, they have enabled us through the millennia to cope with a dangerous world and to survive as a species. The compulsion to explain everything drives our curiosity and thirst for knowledge of the world.[59]
>
> Why should we care a whit whether black holes really exist, or whether neutrinos have mass, or what makes pulsars pulse? Whatever the answer to why we care about such things there can be no question that we do care. Many of the best minds the species has produced have devoted themselves to trying to extend our understanding of the universe in which we find ourselves, arguably for no more compelling reason than that of extending our understanding of the universe in which we find ourselves. The urge itself is remarkable, but so, as Davies and others have noted, is the apparent ability to ask and answer questions that have little direct relevance to our survival as individuals or as a species. [60]
>
> Himsworth (1986) attributes this need for explanations to fear of the unknown: "Fear of the unknown is deeply ingrained in human beings. In consequence, faced by anything they do not understand, they cannot rest until they have given themselves an explanation of it" (p. 94). Whether or not fear is the motivating factor, we are explanation-generating entities.[61]

---

[58] Gardner, D. "Our Brains Want Certainty about the Montreal Shooting," *Ottawa Citizen*, September 6, 2012, p. A11.

[59] Jones, M.D. *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving*, Three Rivers Press, New York, NY, 1998, p. 34.

[60] Nickerson, p. 333.

[61] As quoted in Nickerson, p. 209.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

But we will have explanations. It is our nature to wish to know both how things are and why they are that way. The instrumental value of the kind of knowledge that many explanations represent is unquestionably great, but our desire for explanations is not limited to those that have obvious practical utility; we wish to understand for the sake of understanding, and this, in my view, is as much of a defining property of a rational being as we are likely to find.[62]

I find it easy to see explanation as a key aspect of rationality, and believe the continual search for explanations to be a defining characteristic of human nature. Explanations provide one with a sense of closure, the resolution of uncertainty, sometimes answers to vexing questions. They can facilitate thinking by permitting it to move on, as when the resolution of a specific question provides the basis for making headway on perhaps more interesting or more general ones. [63]

Man differs from animals in that he has a reasoning mind, and this mind...cannot tolerate a vacuum, it finds an explanation for everything.[64]

For at least a century, psychologists and philosophers have suggested that our urge to explain the world is analogous to our urge to populate it. Like making babies, they argue, making theories is so crucial to our survival that we have a natural drive to do so - what William James called a "theoretic instinct."[65]

Reasoning with causal information clearly is an important aspect of reasoning about evidence. Basically, it can take two forms. Using familiar AI terminology, in prediction, one observes or assumes a certain event and tries to predict what will happen as a consequence of this event, while in explanation, one observes an event or state of affairs and tries to explain how it could have been caused by other events. Both forms of reasoning are, of course, of prime importance in reasoning about evidence, whether story or argument based[66]

We define sensemaking as the deliberate effort to understand events. It is typically triggered by unexpected changes or other surprises that make us doubt our prior understanding. We also describe how these sensemaking activities can result in a faulty account of events.[67]

The domain practitioner's higher purpose is not to perceive stimuli, but is, simply put, *to make sense of things*.[68]

---

[62] Nickerson, p. 252.
[63] Nickerson, p. 251.
[64] Gabor, D. *The Mature Society,* Praeger, New York, NY, 1972.
[65] Schulz, K. *Being Wrong: Adventures in the Margin of Error,* HarperCollins, New York, NY, 2010, p. 96.
[66] Bex, F., van den Braak, S., van Oostendorp, H., Prakken, H., Verheij, B. & Vreeswuk, G. "Sense-Making Software for Crime Investigation: How to Combine Stories and Arguments?" *Law, Probability, & Risk,* Vol. 6, 2007, p. 148.
[67] Klein, G., Phillips, J.K., Rall, E.L. & Peluso, D.A. "A Data-Frame Theory of Sensemaking," in *Expertise Out of Context*, ed. R.R. Hoffman, 2007, p. 114.
[68] Klein, p. 114.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

9.3.2. Individual Need for Certainty

By definition, an explanation does not necessarily have the attribute of being true. An explanation can be tentative, such as a hypothesis, or can be believed to be true and has become a belief. However, just as humans have a need for explanation, they also have the need to believe that their explanations are true.

> The certainty they exploit is the certainty - or the longing for it - already present inside each of us.[69]

> It seems to be a common defect of human minds that they tend to crave for complete certainty of belief or disbelief in anything. Not only is this undesirable scientifically, but it must be recognized that no such state is obtainable in science. However successful and reliable a theory may be up to any point of time, further data may come along and show a need for adjustment of the theory, while at the other extreme, however little confidence one has in a hypothesis, new data may change the situation.[70]
>
> The quest for truth, it seems to me, is one thing - possibly the only thing - that different traditions of rationality have in common. We may not all agree on what the truth is, but the assumption that we are all seeking it is what gives us reason to hope that progress - that can be recognized as progress by all - can be made. [71]
>
> It seems more than remotely possible that our intolerance of uncertainty and the assumption that we appear to make that every event has an identifiable cause may contribute to overly simplistic cause-effect views of phenomena in general and of human behavior in particular.[72]

9.3.3. Input to Thinking

As we pointed out earlier, the cognitive behavior of an individual is motivated by a need for justifying certain explanations. These explanations are the result of thinking that is based on what one knows and the purpose of thinking. While information as received can be incorporated into memory, the as-received information is insufficient for use in developing an explanation. The thinker must interpret information and assign a meaning to it.

> There is a widespread myth that information is something in the world that does not depend on the point of view of the observers and that it is (or is often) independent of the context in which it occurs.[73]

As pointed out by many, the assignment of meaning to any piece of information is highly individualized.

---

[69] Schulz, p. 162.
[70] Lyttleton, R.A. "The Nature of Knowledge," In R. Duncan & M. Weston-Smith eds., *The encyclopedia of Ignorance*, Pocket Books, New York, NY, p14
[71] Nickerson, p. 387.
[72] Nickerson, p. 248.
[73] Woods, D.D., Patterson, E.S. & Roth, E.M. *Can we Ever Escape from Data Overload? A Cognitive Systems Diagnosis*, AFRL-HE-WP-TR-1999-0195, Ohio State University and Roth Cognitive Engineering, Columbus, OH, 1998, p. 14.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

> One of the oldest and most reliable generalizations in psychology is that perception is not merely the passive receipt of information but is instead a process of active interpretation, selective attention, deduction, and inference. The "facts" never "speak for themselves."[74]
>
> There are no facts of fixed significance. … A particular datum gains significance or meaning only from its relationship to the context in which it occurs or could occur including the perspective of observers. As a result, informativeness is not a property of the data field alone, but is a relationship between observers and the data field.[75]
>
> There is no such thing as a definite piece of indisputable knowledge about the world whose meaning is not in some way colored by preexisting belief about the world.[76]
>
> …information cannot speak for itself. The significance of information is always a joint function of the nature of the information and the context in which it is interpreted. The context is provided by the analyst in the form of a set of assumptions and expectations concerning human and organizational behavior. These preconceptions are critical determinants of which information is considered relevant and how it is interpreted.[77]
>
> Information does in this view not include any inherent level of validity, truth or certainty in order to qualify as information . Quite on the contrary, information is the propositional content towards which an agent actively can entertain different attitudes. Hence, of significance are the propositional attitude of the agent, the processes and methods of justifying the different attitudes. [78]
>
> But evidence must be interpreted; and it is probably very infrequently the case that the evidence on any complex issue admits of only one interpretation or is overwhelmingly indicative of only one answer. What is made of any bit of evidence - indeed the extent to which any bit of data can function as evidence - must depend, to no small degree, on what else the one who interprets it already knows or believes.[79]

The source of this variability is described below.

> Most of this resonates well with the postmodern view that no determination of a single truth is possible. The complexity sciences confirm that the observer and the observed cannot be detached from each other …. This is supported by the postmodernist

---

[74] Stech, F.J. *Estimates of Peacetime Soviet Naval Intentions: An Assessment of Methods*, Office of Naval Research, Dept. of the Navy 1981, p. 56.
[75] Woods, D.D., Patterson, E.S. & Roth, E.M. *Can We Ever Escape from Data Overload? A Cognitive Systems Diagnosis,* AFRL-HE-WP-TR-1999-0195, Ohio State University and Roth Cognitive Engineering, Columbus, OH, 1998, p. 14.
[76] Cited in Nickerson, p. 81.
[77] Heuer, R.J.J. *Psychology of Intelligence Analysis,* Center for the Study of Intelligence, Washington, D.C., 1999, p. 41.
[78] Ronn, K.V. & Hoffding, S. "The Epistemic Status of Intelligence: An Epistemological Contribution to the Understanding of Intelligence, " *Intelligence and National Security,* Available as: http://dx.doi.org/10.1080/02684527.2012.701438, 2012, p. 13.
[79] Nickerson, p. 144.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

understanding that no matter how we assess information, knowledge or intelligence, we can never achieve anything other than a mirror of how we see the 'facts. [80]

Conflicting representations of the same event come to be understood as legitimate products of individuals' unique meaning-making efforts because interpretive mental processes vary across individuals, their products may also differ. It is at this point that the multiplist level of epistemological understanding begins to take hold: Perhaps all knowing is only opinion.[81]

Of more direct concern to the present chapter is the finding that content and context profoundly affects reasoning even when logical structure is held constant. So pervasive are the effects of prior knowledge and belief on reasoning, that Stanovich (1999) has recently described the tendency to contextualize all information given as the fundamental computational bias in human cognition. [82]

Behavior that is irrational for one person may be rational from the perspective of another whose knowledge, beliefs or values differ. [83]

The fact that the same observational evidence can be extrapolated to give two diametrically opposite predictions according to which explanation one adopts, and cannot justify either of them, is not some accidental limitation of the farmyard environment: it is true of all observational evidence under all circumstances. [84]

The fact that top-down knowledge affects interpretation means (among other things) that two people with the same information - be it a low-resolution satellite photograph or the incomplete facts surrounding a death - can logically interpret it differently given different prior knowledge. [85]

9.3.4. Judgment of Thinking

Because of the acknowledged variance in assignment of meaning between individuals, the difficulty in judging the validity of the thinking of an individual has been acknowledged by many.

Wherever we look, we see indications of the wisdom of Polya's (1954b) admonition to not neglect the obvious fact that two people presented with the same evidence may honestly disagree.[86]

When A reads something that B has written, A's task is to understand not what B says, but what B means. The task is complicated by the fact that B himself may not understand

---

[80] Rolington, A. "Objective Intelligence or Plausible Denial: An Open Source Review of Intelligence Method and Process since 9/11," *Intelligence and National Security*, Vol. 21, No. 5, 2006, p. 749.
[81] Kuhn, D., Cheney, R. & Weinstock, M. "The Development of Epistemological Understanding," *Cognitive Development*, Vol. 15, No. 3, 2000, p. 313.
[82] Evans, Jonathan St. B. T. "The Influence of Prior Belief on Scientific Thinking," in *The Cognitive Basis of Science*, eds. P. Carruthers, S.P. Stich & M. Siegal, Cambridge University Press, Cambridge, UK, 2002, p. 194.
[83] Nickerson, p. 402.
[84] Goodman, M.S. & Omand, D. "Teaching Intelligence Analysts in the UK: What Analysts Need to Understand: The King's Intelligence Studies Program," *Studies in Intelligence*, Vol. 52, No. 4, 2008, [p. 7 in original document].
[85] Spellman, B.A. "Individual Reasoning," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, p. 128.
[86] Nickerson, p. 144.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

clearly what he means. It is easy to imagine conversations between two parties in which one participant claims, in all sincerity, to understand what the other has said but really does not. [87]

In the Agency, and in other intelligence agencies, only ‘‘one organizational view’’ of an issue can prevail. Such conformity defies both human nature and logic. Within any organization, individual analysts frequently reach different judgments about the quality of information, the correct interpretation of data, and the likely implications of any foreign development.[88]

Hannes Alven (1988) provides a particularly interesting illustration, not only that experts in the same problem area can interpret the same evidence differently from each other, but that they can each interpret the evidence in different ways at different times.[89]

Thus even if we were willing to assume that two individuals had precisely the same knowledge with respect to some issue, we should not find it difficult to believe that they could come to different conclusions about the issue.[90]

Also, it is doubtful that, in complicated situations, two individuals ever have precisely the same evidence with which to work. If there is a large amount of information that is germane to the issue, chances are that different individuals will have acquired different aspects of that information at different times under different conditions and to different degrees, so that their knowledge, as it relates to the issue at any given time, is unlikely to be exactly the same.[91]

Finally, it must be acknowledged that justification is a very subjective matter. What I consider to be strong justification of a particular belief, you may see as inadequate; and I may fail to see the merit in the argument you advance in support of a belief that you hold and I do not. [92]

It is much easier to think that other people are biased or closed-minded than to understand that if everyone else sees the world through his own construction of it, then you yourself must be doing the same. What beliefs and assumptions do you bring to your consideration of the issues?[93]

Our earlier knowledge structure influence the way we receive and understand new information. The same piece of information is consequently received differently dependent on the person's pre-understanding of the topic.[94]

---

[87] Nickerson, p. 325.
[88] George, R.Z. "Beyond Analytic Tradecraft," *International Journal of Intelligence and Counterintelligence*, Vol. 23, No. 2, 2010, p. 300.
[89] Nickerson, p. 145.
[90] Nickerson, p. 145.
[91] Nickerson, p. 144.
[92] Nickerson, p. 140.
[93] Williams, J.P. "The Importance of Examining Beliefs about Text," in *Beliefs about Texts and Instruction with Text*, eds. R. Garner & P.A. Alexander, L. Erlbaum Associates, Hillsdale, NJ, 1994, p. xiv.
[94] Henstroem, J. "Five Personality Dimensions and Their Influence on Information Behaviour," *Information Research*, [Online], vol. 9, no. 1, October 5, 2010. Available as: http://informationr.net/ir/9-1/paper165.html, 2003, [p. 3 in original document].

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

> On one pole has been the view that only propositions verified by observed phenomena should be called knowledge. On the other pole has been the view that the world is always interpreted through different lenses of concepts and beliefs, and that there exists no independent criterion for deciding if one lens is more valid than another.[95]
>
> We do know that when a case is tried twice, as is possible in most civil law systems, different courts may reach different decisions in the same case and on the same evidence. It is not always clear what the origins of such disagreements are, but they definitely do not support the basic belief that the reasoning power of human beings will always lead to the one and only correct verdict[96]

9.3.5. Ramifications

The body of thought represented by the sampling of writings above lead to three conclusions

- Information does not have a single value of meaning. Information's value and meaning depend on the knowledge of the individual making the assignment plus the purpose that motivate the assignment.
- Differences in assignment of meaning can occur between individuals and even within a single individual as changes occur in what they know or believe, or changes in purpose.
- When the output of an individual's thinking is based on their assignment of meaning, the judgment of the validity of such thinking by another individual requires knowing what the other individual knows.

These conclusions seem to directly follow from the cited writing and as such are uncontroversial, but they are controversial when contrasted with common practice in research on cognition. Much of this research consists of measuring and comparing the output of the test subject to what the researchers believe is the correct answer. The subject is considered objective and rational when the cognitive output agrees with the output expected by the researcher.

Most research on thinking biases are so structured. One illustration is the so called confirmation bias. The normal mode for most individuals is to evaluate new information relative to their existing beliefs. As a result, the thinking purpose is not to answer the question of what does newly received information mean but rather it is to answer the question of whether the information supports an existing explanation. It is a common response that if the information does not support an existing explanation, the receiver of the information ceases to think about it.

The rejection of information that conflicts with existing beliefs is treated as if it is a flaw in thinking. However, such thinking is not flawed but rational in the context of the individual and the purpose of their thinking.

---

[95] Fitzgerald, J. & Cunningham, J.W. "Mapping Basic Issues for Identifying Epistemological Outlooks," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing*, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, p. 2.

[96] Wagenaar, W.A., van Koppen, P.J. & Crombag, H.F.M. *Anchored Narratives: The Psychology of Criminal Evidence*, Harvester Wheatsheaf, Hemel Hempstead, Hertfordshire, UK, 1993, p. 2.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

This example underscores what is apparent in the above comments on meaning. The thoughts and resultant thinking is the product of an individual. The results are likely to be as varied as the variability of knowledge, beliefs, and goals between individuals. One might disagree with the results of another individual's thinking, but that does not mean the thinking was any less rational than that used by the disagreeing party.

Despite all that has been written on natural differences in interpretation of information, the normal mode of interaction between individuals is to judge such differences. One only has to read the commentary on the internet to see the acrimonious attacks on others who have a differing opinion. The situation is not different when so-called experts are involved in such disagreements. Disagreements in scientific literature are legion. The participants are exhibiting individualized anthropocentrism, that is, a steadfast adherence to the belief that their interpretation is the correct one.

Also in contradiction to what has been written, the premise that information can be explained by a "single correct answer" is central to the quality assurance practices of many organizations involved in the interpretation of information.

> In the Agency, and in other intelligence agencies, only ''one organizational view'' of an issue can prevail. Such conformity defies both human nature and logic. Within any organization, individual analysts frequently reach different judgments about the quality of information, the correct interpretation of data, and the likely implications of any foreign development.[97]

One well known example of this condition was the claims made during his confirmation hearings by his subordinates that Gates politicized intelligence on the Soviet Union. An alternate explanation is that Gates had a more negative view of the motives and goals of the Soviet Union than his subordinates so he interpreted their actions as more threatening. In this case neither group at that time was correct since they didn't anticipate the breakup of the Soviet Union.

This example also illustrates a characteristic common to most instances of evaluating interpretation after the fact: a focus on the end product rather than the cognitive process used to arrive at the content of the end product. An alternate basis for judging the merits of the thinking can be gained by an examination of the process: How exhaustively was information acquired, the reasoning used in assigning meaning, and the amount of evidence supporting the explanation? The use of process evaluation does not resolve, however, the issue of judging which answer is "correct" since different results can be achieved by two equally thorough processes

Does one conclude that there are no "right" answers and, as stated above, "Is all knowing just a matter of opinion?" For answers that are based on human interpretation, yes, they are all opinions, some of which may be proven correct by subsequent events. However, not all opinions are of equal merit.

[97] George, R.Z. "Beyond Analytic Tradecraft," *International Journal of Intelligence and Counterintelligence*, Vol. 23, No. 2, 2010, p. 300.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

> One can therefore understand our ideological prisms as a kind of human shelter – the result of our individual experiences and collective histories. These prisms make it inherently difficult to believe that anyone who actually thinks truly can arrive at conclusions that differ from our own. Corroboration leading one person to believe in a hypothesis does not necessarily mean that another person believing in the hypothesis based on the same corroborative reason actually perceives the conclusion of the hypothesis the same way as we do. In other words, two people can believe the same hypothesis, but they can believe it differently, which entails that critical rationalism only ensures self-corrective criticisms of the thought process, and not self-criticism of our perception of the conclusion. [98]

The idea that one should strive for self-corrective criticism of the thought process rather than self-criticism of the conclusion is a foundation for a quality assurance program that is consistent with all of the research cited above. A wealth of literature exists on conceptual change, persuasion, and changing the mind of others, but is not directly applicable to the desired quality assurance program. The overall thrust of this literature is how to get people to change their opinions and adapt yours. This is contrary to the idea of judging the merit of an opinion based on the process used to form the opinion. However, a limited amount of research suggests that an act of self-corrective criticism of the process can lead to a self-corrective change in the conclusions. These processes are not to be confused with such structural analytic techniques as devil's advocacy, Team A/Team B or Red Team Analysis since these techniques involved comparison of results rather than processes.

The FAC provides the procedures and process of the entire analysis process from formulating the intelligence issue to be answered to the representation of the answer. In addition, the use of FAC results in all the information needed for a quality assurance program for the practice of intelligence analysis.

[98] Hatlebrekke, K.A. & Smith, M.L.R. "Towards a New Theory of Intelligence Failure? The Impact of Cognitive Closure and Discourse Failure," *Intelligence and National Security*, Vol. 25, No. 2, 2010, p. 157.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

10.0 FRAMEWORK FOR ANALYTIC COGNITION

The preparation of a handbook that encompasses the entire analysis process, which became known as the *Framework for Analytic Cognition (FAC)*, began in 2008. Two and a half years later we completed the FAC and published it in its entirety. We wrote each section, which represented a segment of the analysis process, in the same sequence as the topics occur in the analysis process. We made few modifications to prior sections as we completed subsequent sections of the FAC.

As we mention in the FAC itself, at the completion of analysis one is cognitively a different person than the one that embarked on the analysis effort. This is equally true for us at the completion of the writing of the FAC. In addition, we gained much more knowledge from our research synthesis of findings in scientific areas applicable to analysis. Thus, we recognize that the FAC can be improved, not to change its basic content but to provide more evidence supporting the practices we recommend. We could also improve the communication of the ideas embedded in the FAC.

Unfortunately, when work on the contract was suspended, we were not able to accomplish the updates and expansions that would improve the FAC. We were able, however, to create two condensed versions of the FAC designed to stimulate interest in its use:

- *Framework for Analytic Cognition (FAC): Essential Elements of the Intelligence Analysis Process* is approximately 14 pages long and provides, for each of the eight components of the FAC, a brief discussion of the purpose of the component, the benefits it provides to the intelligence analyst, a concise description of the activities needed to accomplish the goals of the component, and a review of the output of those activities.
- *Master the Cognitive Challenges of Intelligence Analysis Using the Framework for Analytic Cognition (FAC)* is approximately 80 pages long and contains highlights of the eight components that make up the FAC. For each component we provide an introduction, a review of the steps needed to accomplish the task, tips, a checklist, and a description of the outcome of each component of the FAC. Some components also have supplemental worksheets or questionnaires to help readers with the tasks described in that component.

These documents can be used as an introduction to the full FAC or as quick reference guides for use after learning the full FAC. Both of these publications were designed to communicate that the FAC is oriented to helping the individual intelligence analyst by providing concrete, practical assistance for doing a complex and essential job. In addition, we hoped to demonstrate that the FAC is systematic, but flexible enough to accommodate the way analysts think and the unstructured and highly iterative nature of intelligence analysis.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

11.0 RECOMMENDATIONS

11.1 Quality Assurance

Develop a quality assurance approach. The basic concepts to be used are cooperation rather than challenge with the focus on the execution of the process for formulating an analytical conclusion rather than the content of the conclusion. The review should occur at the end of each stage of the analysis process rather than at the end of process. This will result in early detection and correction of execution issues. This approach will not necessarily result in single answer to an intelligence issue but will provide the information and interpretation resulting in different answers. FAC provides the structure of this quality assurance program.

11.2 Analysis Selection

Assessments for thinking dispositions and epistemological beliefs should be added to existing criteria for the selection of personnel for the intelligence analysis function. A variety of validated assessment tools exist that can measure the characteristics of a person's thinking dispositions and epistemological beliefs.

11.3 Analyst Training

If the performance of an analyst is to be measured based on the execution of the analysis process, then the analyst has to be trained on how to execute. We recommend that a training course based on the FAC be developed. This course would include using the procedures taught for performing the complete analysis process. The approach to training would incorporate procedures and exercises designed to accommodate context sensitivity. Accordingly, an essential ingredient of the training would be a standard repertoire of intelligence problems and databases tailored to the students' specialties. The course would provide a solution for each problem that represents the best analysis that can be accomplished given the information in the databases. Course facilitators would use these solutions to evaluate each student's analysis. Each student would also be able to compare his or her results with what an expert has accomplished.

In addition, a training course to improve the thinking dispositions and epistemological beliefs of analysts should be established. Various techniques for such training already exist and should be incorporated into the professional development activities of intelligence analysts.

11.4 FAC Enhancement

Our efforts to survey the scientific literature for useful additions to the practice of intelligence analysis validate our original problem statement. However, we have not covered the available literature exhaustively so the potential that more information exists that can improve the analytical process is still large. Research synthesis of relevant topics should continue so a more complete understanding of cognition during analysis is acquired. The goal of such syntheses would be modifications of analytic practice that both facilitates the adoption of new techniques and information by analysts and the improvement of cognitive results.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

12.0 REFERENCES

Anonymous. "Same Ol', Same Ol'," *Aviation Week and Space Technology,* Vol. 148, No. 23, 1998, pp. 21.

Anonymous. *The US Intelligence Community's Strategic Human Capital Plan: An Annex to the US National Intelligence Strategy*, Office of the Director of National Intelligence, Washington, D.C., 2006.

Alexander, P.A., Dinsmore, D.L., Fox, E., Grossnickle, E.M., Loughlin, S.M., Maggioni, L., Parkinson, M.M. & Winters, F.I. *Higher-Order Thinking and Knowledge: Domain-General and Domain-Specific Trends and Future Directions* [undated].

Atkins, P.W. *Creation Revisited,* W.H. Freeman, Oxford, UK, 1992.

Bascatow, T. & Bellafiore, D.J. "Redefining Geospatial Intelligence," *American Intelligence Journal,* Vol. 27, No. 1, 2009, pp. 38-40.

Bex, F., van den Braak, S., van Oostendorp, H., Prakken, H., Verheij, B. & Vreeswuk, G. "Sense-Making Software for Crime Investigation: How to Combine Stories and Arguments?" *Law, Probability, & Risk,* Vol. 6, 2007, pp. 145-168.

Billett, S. "Learning through Practice," in *Learning Through Practice: Models, Traditions, Orientations, and Approaches*, ed. S. Billett, Springer, Dordrecht, 2010, pp. 1-20.

Breckenridge, J.G. "Designing Effective Teaching and Learning Environments for a New Generation of Analysts," *International Journal of Intelligence and Counterintelligence,* Vol. 23, No. 2, 2010, pp. 307-323.

Cacioppo, J.T. & Petty, R.E. "The Need for Cognition," *Journal of Personality and Social Psychology,* Vol. 42, No. 1, 1982, pp. 116-131.

Clark, R.C. *Building Expertise: Cognitive Methods for Training and Performance Improvement,* 3rd ed., Pfeiffer, San Francisco, CA, 2008.

Condon, W. & Kelly-Riley, D. "Assessing and Teaching What We Value: The Relationship between College-Level Writing and Critical Thinking Abilities," *Assessing Writing,* Vol. 9, No. 1, 2004, pp. 56-75.

Cooper, H.M. *Synthesizing Research: A Guide for Literature Reviews,* 3rd ed., Sage Publications, Thousand Oaks, CA, 1998.

Dewey, J. *How We Think: A Restatement of the Relation of Reflective Thinking to the Educative Process,* 2nd ed., Regnery, Chicago, IL, 1933.

Evans, Jonathan St. B. T. "The Influence of Prior Belief on Scientific Thinking," in *The Cognitive Basis of Science*, eds. P. Carruthers, S.P. Stich & M. Siegal, Cambridge University Press, Cambridge, UK, 2002, pp. 193-210.

Facione, P.A. & Facione, N.C. *California Critical Thinking Disposition Inventory (CCTDI) Test Manual,* California Academic Press, Millbrae, CA, 2010.

Fingar, T. "Analysis in the U.S. Intelligence Community: Missions, Masters, and Methods," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, D.C., 2011, pp. 3-27.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Fitzgerald, J. & Cunningham, J.W. "Mapping Basic Issues for Identifying Epistemological Outlooks," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing*, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, N.J., 2002, pp. 209-228.

Frederick, S. "Cognitive Reflection and Decision Making," *Journal of Economic Perspectives*, Vol. 19, No. 4, 2005, pp. 25-42.

Gabor, D. *The Mature Society*, Praeger, New York, NY, 1972.

Gardner, D. "Our Brains Want Certainty about the Montreal Shooting," *Ottawa Citizen*, September 6, 2012, p. A11.

George, R.Z. "Beyond Analytic Tradecraft," *International Journal of Intelligence and Counterintelligence*, Vol. 23, No. 2, 2010, pp. 296-306.

Glaser, E.M. *An Experiment in the Development of Critical Thinking*, AMS Press Inc., New York, NY, 1941.

Goodman, M.S. & Omand, D. "Teaching Intelligence Analysts in the UK: What Analysts Need to Understand: The King's Intelligence Studies Program," *Studies in Intelligence*, Vol. 52, No. 4, 2008, pp. 1-12.

Hall, W.M. & Citrenbaum, G.M. *Intelligence Analysis: How to Think in Complex Environments*, Praeger Security International, Santa Barbara, CA, 2010.

Harteis, C., Gruber, H. & Lehner, F. "Epistemological Beliefs and their Impact on Work, Subjectivity, and Learning," in *Work, Subjectivity and Learning: Understanding Learning through Working Life*, eds. S. Billett, T.J. Fenwick & M. Somerville, Springer, Dordrecht, The Netherlands, 2006, pp. 123-140.

Hatlebrekke, K.A. & Smith, M.L.R. "Towards a New Theory of Intelligence Failure? The Impact of Cognitive Closure and Discourse Failure," *Intelligence and National Security*, Vol. 25, No. 2, 2010, pp. 147-182.

Hazlitt, H. *Thinking as a Science*, E. P. Dutton & Co., New York, NY, 1916.

Hendrickson, N. "Critical Thinking in Intelligence Analysis," *International Journal of Intelligence and Counterintelligence*, Vol. 21, No. 4, 2008, pp. 679-693.

Henstroem, J. "Five Personality Dimensions and Their Influence on Information Behaviour", *Information Research*, [Online], vol. 9, no. 1, pp. October 5, 2010. Available as: http://informationr.net/ir/9-1/paper165.html, 2003.

Heuer, R.J.J. *Psychology of Intelligence Analysis*, Center for the Study of Intelligence, Washington, D.C., 1999.

Heuer, R.J. & Pherson, R.H. *Structured Analytic Techniques for Intelligence Analysis*, CQ Press, Washington, D.C., 2011.

Higgins, J.P.T. & Green, S. (eds) *Cochrane Handbook for Systematic Reviews of Interventions. 4.2.6 [Updated September 2006]*, John Wiley & Sons, Ltd., Chichester, UK, 2006.

Himsworth, H. *Scientific Knowledge & Philosophic Thought*, Johns Hopkins University Press, Baltimore, MD, 1986.

Holyoak, K.J. & Morrison, R.G. "Thinking and Reasoning: A Reader's Guide," in *Oxford Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 1-7.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Jones, M.D. *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving,* Three Rivers Press, New York, NY, 1998.

Kampman, C.M., Mangio, C.A., Parry, T.L. & Wilkinson, B.J. *Framework for Analytic Cognition (FAC): A Guide for Doing All-Source Intelligence Analysis,* AFRL-RH-WP-TR-2012-0109, 2011.

Kent, S. *Writing History,* 2d ed., Appleton-Century-Crofts, New York, NY, 1967.

Kent, S. "The Need for an Intelligence Literature," *Studies in Intelligence,* Vol. 45th Anniversary Special Edition, No. Fall, 2000, pp. 1-11.

Klein, G., Phillips, J.K., Rall, E.L. & Peluso, D.A. "A Data-Frame Theory of Sensemaking," in *Expertise Out of Context,* ed. R.R. Hoffman, 2007, pp. 113-155.

Kuhn, D., Cheney, R. & Weinstock, M. "The Development of Epistemological Understanding," *Cognitive Development,* Vol. 15, No. 3, 2000, pp. 309-328.

Lefebvre, S.J. "Strategic Warning: If Surprise is Inevitable, What Role for Analysis? POSTER Presentation TC99," *International Studies Association (ISA) 44th Annual International Convention,* Portland, OR, February 25 - March 1, 2003.

Lewis, G.E. *Army Intelligence Analysis: Transforming Army Intelligence Analysis Training and Doctrine to Serve the Reasonable Expectations and Needs of Echelons Corps and Below Commanders, Consumers, and Customers,* ADA435988, United States Army Command and General Staff College, Ft. Leavenworth, KS, 2005.

Lyttleton, R.A. "The Nature of Knowledge," in *The Encyclopedia of Ignorance,* eds. R. Duncan & M. Weston-Smith, Pocket Books, New York, NY, 1978, pp. 9-18.

Mangio, C.A. & Wilkinson, B.J. *State of Knowledge Relative to Intelligence Analysis. Volume 1: Cognitive Challenges for Intelligence Analysis - Past, Present, and Future,* AFRL-RH-WP-TR-2011-0049, 2011.

Marrin, S. "CIA's Kent School: A Step in the Right Direction," *International Studies Association (ISA) 43rd Annual International Convention,* New Orleans, LA, March 24-27, 2002.

Marrin, S. "Improving CIA Analysis by Overcoming Institutional Obstacles," in *Bringing Intelligence About: Practitioners Reflect on Best Practices,* ed. R.G. Swenson, Joint Military Intelligence College, Washington, D.C., 2003, pp. 41-59.

Marrin, S. "CIA's Kent School: Improving Training for New Analysts," *International Journal of Intelligence and Counterintelligence,* Vol. 16, No. 4, 2003-2004, pp. 609-637.

Marsh, M. *Advanced Analysis Cognition: Critical Thinking,* March, 2012. [in press]

Marsh, M. *Advanced Analysis Cognition: Thinking Dispositions,* May, 2012 [in press]

McClelland, G.H. "Use of Signal Detection Theory as a Tool for Enhancing Performance and Evaluating Tradecraft in Intelligence Analysis," in *Intelligence Analysis: Behavioral and Social Scientific Foundations,* eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, D.C., 2011, pp. 83-99.

Mezirow, J. *Transformative Dimensions of Adult Learning,* Jossey-Bass, San Francisco, CA, 1991.

Nickerson, R.S. *Aspects of Rationality: Reflections on What It Means to be Rational and Whether We Are,* Psychology Press, New York, NY, 2008.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Pajares, M.F. "Teachers' Beliefs and Educational Research: Cleaning Up a Messy Construct," *Review of Educational Research,* Vol. 62, No. 3, 1992, pp. 307-332.

Perkins, D.N., Jay, E. & Tishman, S. "Beyond Abilities: A Dispositional Theory of Thinking," *The Merrill-Palmer Quarterly,* Vol. 39, No. 1, 1993, pp. 1-21.

Perry, W.G. *Forms of Intellectual and Ethical Development in the College Years: A Scheme,* Holt, Rinehart and Winston, New York, NY, 1970.

Pool, R. *Field Evaluation in the Intelligence and Counterintelligence Context Workshop Summary.* The National Academies Press, Washington, D.C., 2010.

Rolington, A. "Objective Intelligence or Plausible Denial: An Open Source Review of Intelligence Method and Process since 9/11," *Intelligence and National Security,* Vol. 21, No. 5, 2006, pp. 738-759.

Ronn, K.V. & Hoffding, S. "The Epistemic Status of Intelligence: An Epistemological Contribution to the Understanding of Intelligence," *Intelligence and National Security,* Available as: http://dx.doi.org/10.1080/02684527.2012.701438, 2012.

Sá, W., Kelley, C., Ho, C., Stanovich, K.E. & West, R.F. *Composite Actively Open-Minded Thinking Scale -- 11/6/03* 2003.

Schommer, M. "An Emerging Conceptualization of Epistemological Beliefs and their Role in Learning," in *Beliefs about Texts and Instruction with Text,* eds. R. Garner & P.A. Alexander, L. Erlbaum Associates, Hillsdale, NJ, 1994, pp. 25-40.

Schommer, M. & Walker, K. "Are Epistemological Beliefs Similar Across Domains?" *Journal of Educational Psychology,* Vol. 87, No. 3, 1995, pp. 424-432.

Schulz, K. *Being Wrong: Adventures in the Margin of Error,* HarperCollins, New York, NY, 2010.

Spellman, B.A. "Individual Reasoning," in *Intelligence Analysis: Behavioral and Social Scientific Foundations,* eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, D.C., 2011, pp. 117-141.

Stanovich, K.E. *What Intelligence Tests Miss: The Psychology of Rational Thought,* Yale University Press, New Haven, CT, 2009.

Stech, F.J. *Estimates of Peacetime Soviet Naval Intentions: An Assessment of Methods,* Office of Naval Research, Dept. of the Navy 1981.

Thouless, R.H. *Straight and Crooked Thinking,* Pan Books Ltd., London, UK, 1953.

Wagenaar, W.A., van Koppen, P.J. & Crombag, H.F.M. *Anchored Narratives: The Psychology of Criminal Evidence,* Harvester Wheatsheaf, Hemel Hempstead, Hertfordshire, 1993.

Wasserman, B. "The Failure of Intelligence Prediction," *Political Studies,* Vol. 8, No. 2, 1960, pp. 156-169.

Williams, J.P. "The Importance of Examining Beliefs about Text," in *Beliefs about Texts and Instruction with Text,* eds. R. Garner & P.A. Alexander, L. Erlbaum Associates, Hillsdale, N.J., 1994, pp. xi-xv.

Woods, D.D., Patterson, E.S. & Roth, E.M. *Can We Ever Escape from Data Overload? A Cognitive Systems Diagnosis,* AFRL-HE-WP-TR-1999-0195, Ohio State University and Roth Cognitive Engineering, Columbus, OH, 1998.

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

13.0 BIBLIOGRAPHY

Anonymous. *About Specialized Search Engines* (RW 1415)

Anonymous. *About Specialized Search Engines* (RW 1436)

Anonymous. *Acquisition and Logistics Intelligence* (RW 1426)

Anonymous. *Advanced Technical Intelligence Center for Human Capital Development*, Advanced Technical Intelligence Center. Available: http://www.atichcd.org/, Viewed: November 2, 2009. (RW 4057)

Anonymous. *Battlefield Critical Thinking Skills*. Available: http://www.cog-tech.com/projects/TrainingBattlefieldCriticalThinking/BeginTraining.html, Viewed: February 19, 2010. (RW 4096)

Anonymous. *Brain 'Irrelevance Filter' Found* (RW 2902)

Anonymous. *Cognitive Technologies, Inc*. Available: http://www.cog-tech.com/index.html, Viewed: February 4, 2010. (RW 4058)

Anonymous. *Creatures of Habit: The Persistent Problem of Instincts*. Available: http://www.science.usyd.edu.au/research/sydney_science/instincts.shtml, (RW 3886)

Anonymous. *Critical Thinking Skills Workshop*, Pherson Associates. Available: http://www.pherson.org/CriticalThink.html, Viewed: August 3, 2010. (RW 4258)

Anonymous. *Critical Thinking: Distinguishing between Inferences and Assumptions*. Available: http://www.criticalthinking.org/articles/ct-distinguishing-inferencs.cfm, Viewed: April 30, 2007. (RW 2365)

Anonymous. *CS276 [Powerpoint Presentation]* (RW 1558)

Anonymous. *Defense Intelligence Agency, National Defense Intelligence College, Master of Science of Strategic Intelligence*, National Defense Intelligence College. Available: http://www.dia.mil/college/corecourses.htm, Viewed: November 30, 2009. (RW 4059)

Anonymous. *Disciple LTA - Analyst's Cognitive Assistant* (RW 3009)

Anonymous. *Google Books Ngram Viewer*, Google Inc. Available: http://ngrams.googlelabs.com/graph?content=straight+thinking,reflective+t..., Viewed: January 10, 2011. (RW 4659)

Anonymous. *Grey Literature [Powerpoint Presentation]* (RW 1446)

Anonymous. *Habits of Mind*. Available: www.habits-of-mind.net, Viewed: July 6, 2009. (RW 3512)

Anonymous. *The IC Advanced Analyst Program (ICAAP)* (RW 2852)

Anonymous. *Information and Intelligence*. Available: http://www.iom.int/jahia/Jahia/about-migration/managing-migration/migration-intelligence-systems/information-and-intelligence/cache/offonce;jsessionid=D5B6C508608F28A810BE4ECE814AA240.worker02, Viewed: June 24, 2010. (RW 4158)

Anonymous. *Intelligence Failure: From Pearl Harbor to 9/11 and Iraq. Transcript of an America Abroad Broadcast.* (RW 497)

Anonymous. *International Association for Intelligence Education*. Available: http://www.iafie.org/, Viewed: November 30, 2009. (RW 4061)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Anonymous. *The Invisible Web [Powerpoint Presentation]* (RW 1410)

Anonymous. *Jury Behavior* (RW 2056)

Anonymous. *Key Assumptions Check* (RW 4239)

Anonymous. *Largest Deep-Web Sites* (RW 1578)

Anonymous. *List of Cognitive Biases. Wikipedia.* (RW 3461)

Anonymous. *Measuring Search Effectiveness* (RW 1559)

Anonymous. *Mercyhurst College: Department of Intelligence Studies*. Available: http://intel.mercyhurst.edu/, Viewed: November 30, 2009. (RW 4063)

Anonymous. *Michael Handel, 1942-2001* (RW 633)

Anonymous. *Observational Science. Wikipedia Article.* (RW 1777)

Anonymous. *On Search: Precision and Recall* (RW 1560)

Anonymous. *The Pre-Mortem Assessment* (RW 4240)

Anonymous. *The Pre-Mortem Assessment Workshop: Theory and Practice* (RW 4238)

Anonymous. *Qualitative Or Quantitative Research.* (RW 1773)

Anonymous. *Report of the Advisory Committee on the Future of the U.S. Space Program. Appendix I Biographies of Members* (RW 454)

Anonymous. *Revolution in Intelligence Affairs: Transforming Intelligence for Emerging Challenges. Synopsis. Seminar #1- Survey Intelligence Opportunities and Shortfalls: An Agenda for Transformation*, The Potomac Institute for Policy Studies, Arlington, VA. (RW 452)

Anonymous. *Solving Unstructured Problems* (RW 2614)

Anonymous. *Support System for Research Synthesis (SSRS)* (RW 2202)

Anonymous. *Systems to Rate the Strength of Scientific Evidence* (RW 2219)

Anonymous. *Tackling the Big Stuff* (RW 2608)

Anonymous. *What is the Invisible Web? UC Berkeley Tutorial* (RW 1417)

Anonymous. *What is, was, & Will be. PS483 [Powerpoint Presentation]* (RW 2095)

Anonymous. *Why do Handsearching?* Available: http://www.cochrane.org/resources/hsearch.htm, (RW 2275)

Anonymous. *WWW: Information Retrieval and ...* (RW 1445)

Anonymous. "Introduction," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, CENTRA Technology, Burlington, MA, [in press], pp. viii-xxii. (RW 3673)

Anonymous. *Applied Critical Thinking: Skills for Rapid Problem Resolution and Effective Action*, Action Management Associates, Plano, TX, [undated]. (RW 3757)

Anonymous. *Competitive Intelligence Gathering Techniques from the Art of War. Course Description.*, Clearbridge Publishing, Shoreline, WA, [undated]. (RW 428)

Anonymous. *Critical Thinking for Problem Solving, Decision Making and Creativity [Workshop Brochure]*, Headscratchers LLC, Greenwood Village, CO, [undated]. (RW 4796)

Anonymous. *Edwin C. Allison Center for Historical Science*. Available: http://www.geology.sdsu.edu/facilities/allisonctr/, Viewed: October 10, 2011. (RW 5158)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Anonymous. *General Education Critical Thinking Rubric*, Northeastern Illinois University, Chicago, IL, [undated]. (RW 4037)

Anonymous. *NAIC Analyst Development Briefing [Powerpoint Presentation]* [undated]. (RW 615)

Anonymous. *National Defense Intelligence College. Academic Year 2008-2009*, National Defense Intelligence College, Washington, DC, [undated]. (RW 3563)

Anonymous. *National Defense Intelligence College. Academic Year 2009-2010*, National Defense Intelligence College, Washington, DC, [undated]. (RW 3895)

Anonymous. *Strategic Plan 2007-2012. Leading the Defense Intelligence Enterprise*, Defense Intelligence Agency, Washington, DC, [undated]. (RW 3057)

Anonymous. "Surprise," [undated] (RW 398)

Anonymous. *Trinity (Washington) University. IC CAE Syllabi* [undated]. (RW 1701)

Anonymous. "Cornell Plans Test of Pupil-Thinking," *New York Times*, 1939, No. September 17, p. 57. (RW 4508)

Anonymous. *Intelligence and Foreign Policy: The CIA's Global Strategy: The Complete Text of a Document Never Intended for Publication*, Africa Research Group, Council on Foreign Relations, Cambridge, MA, 1971. (RW 1094)

Anonymous. *A Review of the Intelligence Community* 1971. (RW 329)

Anonymous. *An Historical Review of Studies of the Intelligence Community for the Commission on the Organization of the Government for the Conduct of Foreign Policy* 1974. (RW 1058)

Anonymous. *Commission on the Organization of the Government for the Conduct of Foreign Policy. Chapter 7: The Organization of Intelligence.* 1975. (RW 1055)

Anonymous. *CIA Views on the Future Management of the Intelligence Community*, 1977. (RW 1057)

Anonymous. *Presidential Directive NSC-17. Reorganization of the Intelligence Community*, 1977. (RW 423)

Anonymous. *Presidential Review Memorandum NSC-11. Intelligence Structure and Mission*, 1977. (RW 424)

Anonymous. *United States Foreign Intelligence Activities. Executive Order 12036*, 1978. (RW 434)

Anonymous. *United States Intelligence Activities. Executive Order 12333*, 1981. (RW 435)

Anonymous. "Forum: Intelligence and Crisis Forecasting," *Orbis*, Vol. 26, No. 4, 1983, pp. 817-847. (RW 1191)

Anonymous. *Handbook for Strategic Intelligence Analysis*, Logicon, Inc., Operating Systems Division, Woodland Hills, CA, 1983. (RW 1120)

Anonymous. "Introduction," in *Developments in Design Methodology*, ed. N. Cross, Wiley, Chichester; New York, 1984, pp. vii. (RW 2593)

Anonymous. *Mindware*, International Data Corporation, 1984. (RW 5684)

Anonymous. "Part I. the Management of Design Process. Introduction." in *Developments in Design Methodology*, ed. N. Cross, Wiley, Chichester; New York, 1984, pp. 1. (RW 2734)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Anonymous. *International Review of Industrial and Organizational Psychology*, Wiley, Chichester; New York, 1986. (RW 3047)

Anonymous. "Conversation with Arthur Whimbey," in *Thinking Skills Instruction: Concepts and Techniques*, eds. M. Heiman & J. Slomianko, National Education Association, Washington, DC, 1987, pp. 160-166. (RW 5084)

Anonymous. *A Handbook of Intelligence Analysis*, School of Professional Studies, Defense Intelligence College, Washington, DC, 1989. (RW 744)

Anonymous. "Recommendations for Improving National Estimating and Enhancing its Impact on Policymaking Consumers," in *Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating*, eds. H.P. Ford & Defense Intelligence College (U.S.), Defense Intelligence College, Washington, D.C, 1989, pp. 164. (RW 1527)

Anonymous. *National Security Review 29. Intelligence Capabilities 1992-2005*, 1991. (RW 422)

Anonymous. "The Writer's Audience, Part 1," *Word Works*, 76, 1995 (RW 4488)

Anonymous. "The Writer's Audience, Part 2," *Word Works*, 77, 1995 (RW 4489)

Anonymous. "A Critique of Three Recent Commission Reports Exonerating the CIA", *The Failure of Intelligence Review*, April 22, 1996 (RW 4736)

Anonymous. *Improving Intelligence Analysis*, 1996. (RW 322)

Anonymous. *Improving Intelligence Analysis*, Viewed: September 9, 2005. (RW 665)

Anonymous. *Intelligence Analysis on the Long-Range Missile Threat to North America. Statement for the Record. Hearings of the Senate Select Committee on Intelligence. Opening Statement* 1996. (RW 442)

Anonymous. *Intelligence Community Reforms. Presidential Decision Directive.* 1996. (RW 450)

Anonymous. "References," in *The Science of Writing: Theories, Methods, Individual Differences, and Applications*, eds. C.M. Levy & S.E. Ransdell, 1996, pp. 383. (RW 1829)

Anonymous. *Coping with the End of Context: Intelligence Community Conference on Strategic Intelligence Analysis Held July 9, 1997. Summary Notes*, Intelligence Futures Project, Washington, DC, 1997. (RW 239)

Anonymous. *Some Definitions of Terms*. Available: http://www.bcholmes.org/definitions.html, Viewed: June 19, 2009. (RW 3506)

Anonymous. *Jeremiah News Conference* 1998. (RW 3320)

Anonymous. *Open Source Intelligence: Private Sector Capabilities to Support DoD Policy, Acquisitions, and Operations*, 1998. (RW 3349)

Anonymous. "Same Ol', Same Ol'," *Aviation Week and Space Technology*, Vol. 148, No. 23, 1998, pp. 21. (RW 4446)

Anonymous. *Combating Proliferation of Weapons of Mass Destruction*, Commission to Assess the Organization of the Federal Government to Combat the Proliferation of Weapons of Mass Destruction, Washington, DC, 1999. (RW 429)

Anonymous. "References," in *Doing Qualitative Research*, eds. B.F. Crabtree & W.L. Miller, 2nd ed., Sage Publications, Thousand Oaks, Calif, 1999, pp. 363. (RW 2510)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Anonymous. "Report of the Commission to Assess the Ballistic Missile Threat to the United States: Executive Summary, Pursuant to Public Law 201, 104th Congress, July 15,1998," *Comparative Strategy*, Vol. 18, No. 1, 1999, pp. 87-100. (RW 383)

Anonymous. *Intelligence Community Officer Training. Curriculum Guide.* 2000. (RW 5)

Anonymous. "Intelligence Gathering: Evaluating Sources for Objective Analysis," *Online*, Vol. 24, No. 1, 2000, pp. 47. (RW 1672)

Anonymous. *The NPEC Sourcebook on Assessment, Volume 1: Definitions and Assessment Methods for Critical Thinking, Problem Solving, and Writing*, U. S. Dept. of Education, National Center for Education Statistics, Washington D.C., 2000. (RW 4047)

Anonymous. *Strategic Investment Plan for Intelligence Community Analysis*, ADCI/AP 2000-01, National Intelligence Production Board, Washington, DC, 2000. (RW 394)

Anonymous. *Symposium on the Psychology of Intelligence Analysis*, 2000. (RW 745)

Anonymous. *Finding Answers Amidst Uncertainty: Cognitive Challenges of Counter-Terrorist Analysts*, Klein Associates Inc., Fairborn, OH, 2001. (RW 5648)

Anonymous. *Foreign Missile Developments and the Ballistic Missile Threat through 2015. Unclassified Summary of a National Intelligence Estimate*, National Intelligence Council, Washington, DC, 2001. (RW 357)

Anonymous. *Baker University Center for Critical Thinking*. Available: http://www.bakeru.edu/crit/index.html, Viewed: March 21, 2010. (RW 4073)

Anonymous. "Metacognitive Awareness," in *Better Thinking, Better Learning: An Introduction to Cognitive Awareness* 2002, (RW 3520)

Anonymous. "References," in *The Cognitive Basis of Science*, eds. P. Carruthers, S.P. Stich & M. Siegal, Cambridge University Press, Cambridge, UK, 2002, pp. 363. (RW 1951)

Anonymous. "Searching for Answers," *Harvard International Review*, Vol. 24, No. 3, 2002, pp. 40-43. (RW 384)

Anonymous. *U.S. Assessments of the Soviet and Post-Soviet Russian Economy: Lessons Learned and Not Learned. Proceedings of a Conference Held March 27-28, 2002.* Kennan Institute Occasional Paper No. 238, Woodrow Wilson International Center for Scholars, Washington, DC, 2002. (RW 517)

Anonymous. *The Deep Web* 2002 (?). (RW 1394)

Anonymous. *Cambridge Thinking Skills Assessment (TSA)*, University of Cambridge Local Examinations Syndicate, Cambridge, UK, 2003. (RW 4069)

Anonymous. "Intelligence Reform in the Wake of the 9/11 Commission Report. Session Transcript." Brookings Institution, September 23, 2004 (RW 243)

Anonymous. *Joint Intelligence Doctrine. Joint Doctrine Manual*, B-GJ-005-200/FP-000, Government of Canada. National Defence, Ottawa, Canada, 2003. (RW 591)

Anonymous. *What Makes a Search Engine Good? (Chart)* 2003. (RW 1409)

Anonymous. *Where is the Red Line? Actionable Intelligence Vs. Policy Advocacy*, Center for the Study of Intelligence, Washington, DC, 2003. (RW 905)

Anonymous. *DDI's State of Analysis Speech. all-Hands Meeting. CIA Auditorium*, 2004. (RW 96)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Anonymous. *Factiva iWorks. Data Sheet.* 2004. (RW 1443)

Anonymous. *A Guide to the Project Management Body of Knowledge: PMBOK Guide*, 3rd ed., Project Management Institute, Newtown Square, PA, 2004. (RW 1716)

Anonymous. *Guiding Principles for Intelligence Reform*, Center for Strategic and International Studies, Washington, DC, 2004. (RW 246)

Anonymous. *Handbook of Critical Thinking Resources*, Prince George's Community College, Largo, MD, 2004. (RW 4043)

Anonymous. *Intelligence Failures in the USA, UK and Russia: Lessons for India. Observer Research Foundation Seminar.* 2004. (RW 492)

Anonymous. *Intelligence Reform and Terrorism Prevention Act of 2004*, 2004. (RW 1423)

Anonymous. *New Threats! New Intelligence?* Inteligx.com 2004. (RW 493)

Anonymous. *Politics of US Intelligence. Course Syllabus. University of San Diego*, 2004. (RW 437)

Anonymous. *Better Spies, Better Intelligence: A Progressive Strategy for Creating a Professional Intelligence Corps*, Center for American Progress, Washington, DC, 2005. (RW 275)

Anonymous. "Cloak and Classroom," *Chronicle of Higher Education*, March 25, 2005, pp. 14. (RW 632)

Anonymous. *Commentary: Transforming Analysis* 2005. (RW 280)

Anonymous. *Expert Panel Addresses National Intelligence Analysis Capabilities: Content Analyst Company Opens Dialogue between Intelligence Community, Industry*, Content Analyst Company, 2005. (RW 464)

Anonymous. *Intelligence Community Centers of Academic Excellence. Guidance and Procedures. Program Plan for Fiscal Years 2005-2015*, Washington, DC, 2005. (RW 1700)

Anonymous. *Lockheed Martin Opens Knowledge Creation Lab in Herndon*, 2005. (RW 1582)

Anonymous. "The March of the Robo-Traders," *The Economist*, Vol. 376, No. 8444, 2005, pp. 25-26. (RW 939)

Anonymous. *Mental Models and the Mind. Current Developments in Cognitive Psychology, Neuroscience, and Philosophy of Mind*, 2005. (RW 1783)

Anonymous. *2006 Intelligence Community Centers of Academic Excellence Program. Office of the Director of National Intelligence. NGA Broad Agency Announcement.* 2006. (RW 1703)

Anonymous. "As Others See Us," *Economist*, December 19, 2006 (RW 1900)

Anonymous. "Bad Ideas," *C4ISR - The Journal of Net-Centric Warfare*, November 1, 2006 (RW 2271)

Anonymous. "Bayes Rules," *Economist.com*, 2006 (RW 1295)

Anonymous. "Captain Kirk's Revenge," *Economist*, December 19, 2006 (RW 1898)

Anonymous. "Collective Intelligence Training," *C4ISR - The Journal of Net-Centric Warfare*, 2006, pp. 38. (RW 1430)

Anonymous. *Cracking the LSAT. 2007 Edition.* 2006. (RW 2004)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Anonymous. "Digging for Hidden Meanings," *C4ISR - The Journal of Net-Centric Warfare,* 2006 (RW 1431)

Anonymous. "Dreamweavers," *Economist,* December 19, 2006 (RW 1899)

Anonymous. "Fight for Knowledge," *C4ISR - The Journal of Net-Centric Warfare,* 2006, pp. 40. (RW 1432)

Anonymous. "Free to Choose?" *Economist,* December 19, 2006 (RW 1902)

Anonymous. "The HumInt Touch," *C4ISR - The Journal of Net-Centric Warfare,* August 1, 2006 (RW 2270)

Anonymous. "Info-Centric Operations," *C4ISR - The Journal of Net-Centric Warfare,* 2006, pp. 14. (RW 1433)

Anonymous. "Joining Intelligence and Operations," *C4ISR - The Journal of Net-Centric Warfare,* 2006, pp. 16. (RW 1435)

Anonymous. *Kent's Imperative. Blog Entries. December 2006.* 2006. (RW 2601)

Anonymous. *Kent's Imperative. Blog Entries. February 2006.* 2006. (RW 2596)

Anonymous. *Kent's Imperative. Blog Entries. January 2006.* 2006. (RW 2595)

Anonymous. *Kent's Imperative. Blog Entries. March 2006.* 2006. (RW 2597)

Anonymous. *Kent's Imperative. Blog Entries. November 2006.* 2006. (RW 2600)

Anonymous. *Kent's Imperative. Blog Entries. October 2006.* 2006. (RW 2599)

Anonymous. *Kent's Imperative. Blog Entries. September 2006.* 2006. (RW 2598)

Anonymous. "Layered GeoInt," *C4ISR - The Journal of Net-Centric Warfare,* August 1, 2006 (RW 2269)

Anonymous. "Learning without Learning," *Economist,* 2006 (RW 1715)

Anonymous. *LexisNexis Symposium on Government Information Sharing and Data Usage: Policy and Implications for Open Source Intelligence. Highlights.* 2006. (RW 1782)

Anonymous. "A Man Who's Not Getting Much Sleep. Interview with John Negroponte," *US News and World Report,* Vol. 141, No. 18, 2006, pp. 49. (RW 1726)

Anonymous. *Misreading Intentions: Iraq's Reaction to Inspections Created Picture of Deception,* Central Intelligence Agency, Langley, VA, 2006. (RW 5805)

Anonymous. "The most Complex Thing in the Universe," *Economist,* December 19, 2006 (RW 1903)

Anonymous. *A Multi-Dimensional Framework for Academic Support: A Final Report,* University of Minnesota Libraries, Minneapolis, MN, 2006. (RW 4811)

Anonymous. "New Approaches to Air Force ISR," *C4ISR - The Journal of Net-Centric Warfare,* November 1, 2006 (RW 2268)

Anonymous. "Playing Defense," *US News and World Report,* Vol. 141, No. 17, 2006, pp. 47. (RW 1704)

Anonymous. "References," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 158. (RW 3671)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Anonymous. *The Schum Challenge: 7th June 2005* 2006. (RW 2982)

Anonymous. "Striking it Rich," *C4ISR - The Journal of Net-Centric Warfare,* 2006, pp. 16. (RW 1434)

Anonymous. "I Think, therefore I Am, I Think," *Economist,* December 19, 2006 (RW 1901)

Anonymous. "Transforming through Advanced Technology. an Interview with General Crawford," *C4ISR - The Journal of Net-Centric Warfare,* 2006 (RW 1429)

Anonymous. "TSU Receiving $750,000 Grant for Intelligence Analysis Program," *Nashville Business Journal,* 2006 (RW 1310)

Anonymous. *The US Intelligence Community's Strategic Human Capital Plan: An Annex to the US National Intelligence Strategy,* Office of the Director of National Intelligence, Washington, DC, 2006. (RW 1698)

Anonymous. "Who do You Think You are?" *Economist,* December 19, 2006 (RW 1897)

Anonymous. *Content Analysis Technique* 2007. (RW 2495)

Anonymous. *Critical Thinking Research*, University of New Mexico, Albuquerque, NM, 2007. (RW 4055)

Anonymous. *Foundation for Critical Thinking Sample Assessment*, Foundation for Critical Thinking, Dillon Beach, CA, 2007. (RW 4086)

Anonymous. "Getting Smarter about Intelligence," *C4ISR - The Journal of Net-Centric Warfare,* March 1, 2007, 2007 (RW 2267)

Anonymous. "Improving Intelligence Analysis: What Works? How can we Tell? Lessons from Outside the Intelligence Community. Summary of the Conference Sponsored by Office of Analytical Integrity and Standards. Director of National Intelligence." Chantilly, VA, January 9-10, 2007 (RW 2795)

Anonymous. *Information Sharing Environment Administrative Memoranda (ISE-AM). Common Terrorism Information Sharing Standards (CTISS) Program.* 2007. (RW 2956)

Anonymous. *Intelligence Center Launched at California State University, San Bernardino*. Available: http://newswire.ascribe.org/cgi-bin/behold.pl?ascribe...20070413.165046&time=17%2006%20PDT&year=2007&public=0, Viewed: April 15, 2007. (RW 2282)

Anonymous. "Introduction. Mental Processes in the Human Brain." *Phil. Trans. R. Soc. B,* 2007 (RW 2258)

Anonymous. "Introduction. Social Intelligence: From Brain to Culture," *Phil. Trans. R. Soc. B,* Vol. 362, 2007, pp. 485. (RW 2257)

Anonymous. *Kent's Imperative. Blog Entries.* 2007. (RW 2369)

Anonymous. *Kent's Imperative. Blog Entries. April 2007.* 2007. (RW 2604)

Anonymous. *Kent's Imperative. Blog Entries. August 2007.* 2007. (RW 2797)

Anonymous. *Kent's Imperative. Blog Entries. December 2007.* 2007. (RW 2908)

Anonymous. *Kent's Imperative. Blog Entries. January 2007.* 2007. (RW 2602)

Anonymous. *Kent's Imperative. Blog Entries. July 2007.* 2007. (RW 2607)

Anonymous. *Kent's Imperative. Blog Entries. June 2007.* 2007. (RW 2606)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Anonymous. *Kent's Imperative. Blog Entries. March 2007.* 2007. (RW 2603)

Anonymous. *Kent's Imperative. Blog Entries. May 2007.* 2007. (RW 2605)

Anonymous. *Kent's Imperative. Blog Entries. November 2007.* 2007. (RW 2884)

Anonymous. *Kent's Imperative. Blog Entries. October 2007.* 2007. (RW 2869)

Anonymous. *Kent's Imperative. Blog Entries. September 2007.* 2007. (RW 2821)

Anonymous. *Kent's Imperative. Designing for the Intelligence Professional*, 2007. (RW 2402)

Anonymous. *The Monash Critical Thinking Study,* Monash University. Available: http://arts.monash.edu.au/philosophy/research/thinking/07aomt.php, Viewed: April 12, 2010. (RW 4103)

Anonymous. *The New Noise from DNI* 2007. (RW 1979)

Anonymous. *Scan shows how Brains Plot Future* 2007. (RW 1904)

Anonymous. "While You Slumber, Your Brain Puts the World in Order," *New Scientist*, 2007 (RW 2102)

Anonymous. "Active Products: Composition and Dissemination of Smart Analytic Reports," *VAC Views*, May, 2008, pp. 10. (RW 3383)

Anonymous. *Analysis 101. Participant Guide* 2008. (RW 3151)

Anonymous. "Appendix: References to Supplementary Reading," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 438. (RW 3675)

Anonymous. *Executive Order 13470. further Amendments to Executive Order 12333, United States Intelligence Activities* 2008. (RW 3196)

Anonymous. "Glossary," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 431. (RW 3674)

Anonymous. "Jigsaw: Visualization for Investigative Analysis," *VAC Views*, May, 2008, pp. 18. (RW 3384)

Anonymous. *Kent's Imperative. Blog Entries. August 2008.* 2008. (RW 3239)

Anonymous. *Kent's Imperative. Blog Entries. February 2008.* 2008. (RW 2968)

Anonymous. *Kent's Imperative. Blog Entries. January 2008.* 2008. (RW 2927)

Anonymous. *Kent's Imperative. Blog Entries. March 2008.* 2008. (RW 3008)

Anonymous. *Kent's Imperative. Blog Entries. October 2008.* 2008. (RW 3302)

Anonymous. *Kent's Imperative. Blog Entries. September 2008.* 2008. (RW 3282)

Anonymous. *Our Unconscious Brain Makes the Best Decisions Possible* 2008. (RW 3479)

Anonymous. *Pentagon Shakes Up Intelligence Directorate's Organization* 2008. (RW 3195)

Anonymous. *A Pre-Mortem Assessment: The Case of Iraq's Aluminum Tubes* 2008. (RW 4237)

Anonymous. *Project Looking Glass. Analytic Collaboration Exercise. Course Summary* 2008. (RW 3032)

Anonymous. "Publish and be Wrong," *The Economist*, 2008 (RW 3283)

Anonymous. "Spies for Hire," *Foreign Policy*, 165, 2008, pp. 23-23. (RW 4361)

Anonymous. "Sugaring the Decision," *Economist*, Vol. 386, No. 8573, 2008, pp. 104-106. (RW 4545)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Anonymous. *UW to Lead $6.25 Million Project Creating Electronic Sherlock Holmes* 2008. (RW 4514)

Anonymous. *Why we are, as we are* 2008. (RW 3376)

Anonymous. *Action Management Associates, Inc.* Available: http://www.actionm.com/products.aspx, Viewed: December 5, 2009. (RW 3759)

Anonymous. *Analyst Boot Camp*, Advanced Technical Intelligence Center, Beavercreek, OH, 2009. (RW 4070)

Anonymous. *California Critical Thinking Disposition Inventory: Scale Descriptions*, Insight Assessment. Available: http://www.insightassessment.com/Scales%20CCTDI.html, Viewed: October 9, 2009. (RW 3761)

Anonymous. *California Critical Thinking Skills Tests*, Insight Assessment. Available: http://www.insightassessment.com/, Viewed: April 29, 2010. (RW 4098)

Anonymous. *Cambridge Assessment Admissions Tests.* Available: http://www.admissionstests.cambridgeassessment.org.uk/adt/, Viewed: November 2, (RW 3764)

Anonymous. *The Certificate in Teaching Critical Thinking*. Available: http://www.csuchico.edu/catalog/cat09/phil/TCRTNONEUC.html, Viewed: March 20, 2010. (RW 4077)

Anonymous. *Critical Thinking Boot Camp [Course Brochure]*, Pearson Education Inc. 2009. (RW 4084)

Anonymous. *The Critical Thinking Community*, Foundation for Critical Thinking. Available: http://www.criticalthinking.org/starting/index.cfm, Viewed: April 19, 2010. (RW 4097)

Anonymous. *Habits of Mind*. Available: http://en.wikipedia.org/wiki/Habits_of_mind, Viewed: July 6, 2009. (RW 3510)

Anonymous. *I2 Analyst's Notebook 8* 2009. (RW 3600)

Anonymous. *Introduction to General Intelligence Analysis (IGIA). Course Syllabus.* 2009. (RW 4051)

Anonymous. "Research in Organizational Behavior," Vol. 29, 2009 (RW 5581)

Anonymous. *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* 2009. (RW 3486)

Anonymous. *What People do and do Not Believe in*, Harris Interactive, Inc., New York, NY, 2009. (RW 5862)

Anonymous. *Analytic Thinking and Presentation. Course Syllabus.* 2010. (RW 4050)

Anonymous. *Belief in Climate Change Hinges on Worldview* 2010. (RW 3893)

Anonymous. *Case Studies, Articles & Books - Harvard Business Review*, Harvard Business School Publishing. Available: http://hbr.org/search/critical%2520thinking/, Viewed: February 22, 2010. (RW 4099)

Anonymous. *Course Description - Training: Critical Thinking Skills*, Advanced Technical Intelligence Center, Beavercreek, OH, 2010. (RW 4251)

Anonymous. *Critical Thinking. Course Syllabus*, National Air and Space Intelligence Center, Wright-Patterson AFB, OH, 2010. (RW 4048)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Anonymous. *Denial and Deception Awareness. Course Syllabus.* 2010. (RW 4052)

Anonymous. *Google NGram - Thinking Words* 2010. (RW 5274)

Anonymous. *MA in National Security Studies Course Requirements*, California State University, San Bernardino, San Bernardino, CA, 2010. (RW 4253)

Anonymous. *The National Center for Teaching Thinking*. Available: www.nctt.net, Viewed: January 18, 2010. (RW 4064)

Anonymous. "A Pre-Mortem Assessment: The Case of Iraq's Aluminum Tubes [Powerpoint Presentation]" *Global Intelligence Forum 2010*, Dungarvan, Ireland, July 11-13, 2010 (RW 4233)

Anonymous. *Sinclair Community College Advanced Technical Intelligence Certificate Overview*, Sinclair Community College. Available: http://www.sinclair.edu/components/bulletin/bulletin.cfc?method=displa, Viewed: March 22, 2010. (RW 4091)

Anonymous. *Sinclair Community College Advanced Technical Intelligence Degree*, Sinclair Community College. Available: http://www.sinclair.edu/components/bulletin/bulletin.cfc?method=displa, Viewed: March 22, 2010. (RW 4092)

Anonymous. *The Thinker's Workshop. Course Syllabus.* 2010. (RW 4053)

Anonymous. *Become a Better Thinker in just One Hour a Week*, ThinkWatson.com. Available: http://www.thinkwatson.com/training/critical-thinking-university, Viewed: April 28, 2011. (RW 4797)

Anonymous. *CIA's 'Vengeful Librarians' Monitor Twitter, Facebook*, Viewed: November 7, 2011. (RW 5244)

Anonymous. *Cognitive Learning Styles*, LearningRx Franchise Corp. Available: http://www.learningrx.com/cognitive-learning-styles.htm, Viewed: July 27, 2011. (RW 5022)

Anonymous. *Critical Thinking and the Art of Making Intelligent Decisions [Course Brochure]*, Foundation for Critical Thinking, Tomales, CA, 2011. (RW 5338)

Anonymous. *Sirius Program Proposers' Day* 2011. (RW 4525)

Anonymous. *We See into the Future*. Available: http://blog.bitly.com/post/11414840082/we-see-into-the-future?4c815e80, Viewed: January 19, 2012. (RW 5407)

Anonymous. "Special Issue: Re-Thinking Creativity," *Tropos: Journal of hermeneutics and philosophical criticism*, 2011? (RW 5263)

Anonymous. *Future Shock: IARPA, CIA Looks to Forecast Future Major World Events*. Available: http://stratrisks.com/geostrat/7712, Viewed: August 22, 2012. (RW 5785)

Anonymous. *Intelligence Analysts Taking Over Leading Role in Spy Game*. Available: http://stratrisks.com/geostrat/6653, Viewed: August 22, 2012. (RW 5784)

Anonymous. *Origin of Intelligence and Mental Illness Linked to Ancient Genetic Accident*. Available: http://www.sciencecodex.com/origin_of_intelligence_and_mental_illness_linked_to_ancient_genetic_accident-103065, Viewed: December 6, 2012. (RW 5879)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Anonymous. "Probing the Implications of Changing the Outputs of Intelligence: A Report of the 2011 Analyst-IC Associate Teams Program," *Studies in Intelligence,* Vol. 56, No. 1, 2012, pp. 1-11. (RW 5899)

Anonymous. *The Q&A: Samuel Arbesman: The Half-Life of Facts*. Available: http://www.economist.com/blogs/babbage/2012/11/qa-samuel-arbesman, Viewed: December 6, 2012. (RW 5878)

Anonymous. *Time's Arrows*. Available: http://www.economist.com/news/science-and-technology/21565921-some-pieces-ancient-weapons-may-illuminate-modern-mans-evolution-times-arrows, Viewed: November 14, 2012. (RW 5848)

Anonymous. "Special Issue: 20 Years of Argument Based Inference," *Journal of Logic and Computation,* 2012? (RW 5262)

Anonymous. *Intelligence Analysts Need Not Fear 'Watson,' Study shows*. Available: http://www.physorg.com/news/2011-03-intelligence-analysts-watson.html, (RW 4582)

Anonymous. *Comments on "A Review of the Intelligence Community"*, [undated]. (RW 765)

Aaronson, M.N. & Krieger, S.H. "Teaching Problem-Solving Lawyering: An Exchange of Ideas," *Clinical Law Review,* Vol. 112005, pp. 485. (RW 2647)

Abbott, S. "The Outsourcing of U.S. Intelligence Analysis: Will it make Us More Or Less Safe?" *Naval Intelligence Professionals Quarterly,* Vol. 23, No. 4, 2007, pp. 12-15. (RW 4164)

Abegglen, J. & Conger, C.O. "Critical Thinking in Nursing: Classroom Tactics that Work," *Journal of Nursing Education,* Vol. 36, No. 10, 1997, pp. 452-458. (RW 3954)

Abelson, R.P. "Beliefs are Like Possessions," *Journal for the Theory of Social Behaviour,* Vol. 16, No. 3, 1986, pp. 223-250. (RW 3504)

Abramson, D. "Blurring the Boundaries between Anthropology and Intelligence Analysis," in *Anthropologists in the SecurityScape: Ethics, Practice, and Professional Identity*, eds. R. Albro, G. Marcus, L.A. McNamara & M. Schoch-Spana, Left Coast Press, Walnut Creek, CA, 2011, pp. 57-70. (RW 5466)

Acar, W. *Toward a Theory of Problem Formulation and the Planning of Change: Causal Mapping and Dialectical Debate in Situation Formulation,* 1983. (RW 2524)

Ackerman, G. "The Application of Social Bookmarking Technology to the National Intelligence Domain," *International Journal of Intelligence and Counterintelligence,* Vol. 20, No. 4, 2007, pp. 678. (RW 2759)

Ackerman, P.L. "A Theory of Adult Intellectual Development: Process, Personality, Interest, and Knowledge," *Intelligence,* Vol. 221996, pp. 227. (RW 3466)

Ackerman, R.K. "Information Age Poses New Challenges to Intelligence," *Signal,* October, 1998, pp. 23-25. (RW 1073)

Ackerman, R.K. "Intelligence: Horizontal Integration Challenges Intelligence Planner," *Signal,* October, 2003, pp. 29. (RW 1659)

Ackerman, R.K. "Transforming Military Intelligence," *Signal,* July, 2003, pp. 41-43. (RW 228)

Ackerman, R.K. "Cultural Changes Drive Intelligence Analysis," *Signal,* May, 2007 (RW 2321)

Ackerman, R.K. "Defense Intelligence Assumes More Diverse Missions," *Signal,* April, 2007 (RW 2226)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Ackerman, R.K. "Intellipedia Seeks Ultimate Information Sharing," *Signal,* October, 2007 (RW 3158)

Ackerman, S. "Our Myopic Spooks. Under Analysis." *The New Republic Online,* May 29, 2006, 2006 (RW 2319)

Ackerman, S. & Judis, J.B. "The Operator: George Tenet Undermines the CIA," *New Republic,* Vol. 229, No. 12, 2003, pp. 18-29. (RW 899)

Ackerson, L.G. *Literature Search Strategies for Interdisciplinary Research: A Sourcebook for Scientists and Engineers,* Scarecrow Press, Lanham, Md., 2007. (RW 3116)

Ackoff, R.L. "From Data to Wisdom," *Journal of Applied Systems Analysis,* Vol. 16, 1989, pp. 3. (RW 2535)

Ackoff, R.L. *The Art of Problem Solving: Accompanied by Ackoff's Fables,* Wiley, New York, 1978. (RW 2580)

Adams, M.J. "Thinking Skills Curricula: Their Promise and Progress," *Educational Psychologist,* Vol. 24, No. 1, 1989, pp. 25-53. (RW 3873)

Adams, S. *War of Numbers: An Intelligence Memoir,* Steerforth Press, South Royalton, VT, 1994. (RW 683)

Addison, R.B. "A Grounded Hermeneutic Editing Approach," in *Doing Qualitative Research,* eds. B.F. Crabtree & W.L. Miller, 2nd ed., Sage Publications, Thousand Oaks, Calif, 1999, pp. 145. (RW 2504)

Adelman, L., Gualtieri, J. & Stanford, S. "Examining the Effect of Causal Focus on the Option Generation Process," *Organizational Behavior and Human Decision Processes,* Vol. 61, 1995, pp. 54. (RW 1611)

Adibi, J., Chalupsky, H., Melz, E. & Valente, A. "The KOJAK Group Finder: Connecting the Dots Via Integrated Knowledge-Based and Statistical Reasoning", *Proceedings of the 16th Conference on Innovative Applications of Artificial Intelligence,* San Jose, CA, July 27-29, 2004, pp.800-807. (RW 1239)

Adibi, J. & Chalupsky, H. "Scalable Group Detection Via a Mutual Information Model," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 868)

Adler, J.E. & Rips, L.J. *Reasoning: Studies of Human Inference and its Foundations,* Cambridge University Press, Cambridge; New York, 2008. (RW 3436)

Adsit, D.J. & London, M. "Effects of Hypothesis Generation on Hypothesis Testing in Rule-Discovery Tasks," *Journal of General Psychology,* Vol. 124, No. 1, 1997, pp. 19. (RW 2324)

AFCEA Intelligence Committee. *Intelligence and the New National Security Environment,* Armed Forces Communications and Electronics Association, Fairfax, VA, 2004. (RW 419)

AFCEA Intelligence Committee. *Intelligence: The Way Forward,* Armed Forces Communications and Electronics Association, Fairfax, VA, 2005. (RW 4893)

AFCEA Intelligence Committee. *Making Analysis Relevant: It's More than Connecting the Dots,* Armed Forces Communications and Electronics Association, Fairfax, VA, 2005. (RW 2)

AFCEA Intelligence Committee. *Enabling a Responsive and Agile Intelligence Enterprise,* Armed Forces Communications and Electronics Association, Fairfax, VA, 2008. (RW 4895)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

AFCEA Intelligence Committee. *The Intelligence Community: New Challenges, Sources, and Methods,* Armed Forces Communications and Electronics Association, Fairfax, VA, 2009. (RW 4894)

Agam, G., Argamon, S., Frieder, O., Grossman, D. & Lewis, D. "Complex Document Information Processing: Towards Software and Test Collections," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 830)

Agar, M. *The Professional Stranger: An Informal Introduction to Ethnography,* 2nd ed., Academic Press, San Diego, 1996. (RW 3529)

Agrell, W. "Intelligence in an Age of Transition - the Case of Sweden," *National Security and the Future,* Vol. 2, No. 1, 2000, pp. 15-24. (RW 4623)

Agrell, W. "When Everything is Intelligence - Nothing is Intelligence," *The Sherman Kent Center for Intelligence Analysis Occasional Papers,* Vol. 1, No. 4, 2002 (RW 347)

Agrell, W. "Intelligence Analysis After the Cold War - New Paradigm Or Old Anomalies?" in *National Intelligence Systems: Current Research and Future Prospects,* eds. G.F. Treverton & W. Agrell, Cambridge University Press, New York, 2009, pp. 93. (RW 3547)

Agrell, W. "The Next 100 Years? Reflections on the Future of Intelligence," *Intelligence and National Security,* Vol. 27, No. 1, 2012, pp. 118-132. (RW 5610)

Agrell, W. & Treverton, G.F. "The Science of Intelligence: Reflections on a Field that Never was," in *National Intelligence Systems: Current Research and Future Prospects,* eds. G.F. Treverton & W. Agrell, Cambridge University Press, New York, 2009, pp. 265. (RW 3548)

A'Hearn, F. *Northeast Power Failure and Lyndon B. Johnson,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1983. (RW 972)

Ahern, C.R. "The Yo-Yo Story: An Electronics Analysis Case History," *Studies in Intelligence,* Vol. 5, No. 1, 1961, pp. 11-23. (RW 572)

Aid, M.M. "Time of Troubles: The US National Security Agency in the Twenty-First Century," *Intelligence and National Security,* Vol. 15, No. 3, 2000, pp. 5-32. (RW 1072)

Aid, M.M. "Prometheus Embattled: A Post-9/11 Report Card on the National Security Agency," *Intelligence and National Security,* Vol. 21, No. 6, 2006, pp. 980. (RW 2082)

Aid, M.M. "Sins of Omission and Commission: Strategic Cultural Factors and U.S. Intelligence Failures during the Cold War," *Intelligence and National Security,* Vol. 26, No. 4, 2011, pp. 478-494. (RW 5394)

Aid, M.M. *Intel Wars: The Secret History of the Fight Against Terror,* Bloomsbury Press, New York, NY, 2012. (RW 5470)

Ainslie, F.M., Atwood, N.A., Burnstein, D.D. & Hopson, J.A. *A Methodological Study: A Semiotic Approach to Analyzing the Content of Information,* ARL-TR-1168, US Army Research Laboratory, Aberdeen Proving Ground, MD, 1996. (RW 1182)

Ainslie, G. *Breakdown of Will,* Cambridge University Press, Cambridge. UK, 2001. (RW 5743)

Ajzen, I. *Attitudes, Personality, and Behavior,* 2nd ed., Open University Press, Maidenhead, UK, 2005. (RW 5529)

Akhavi, N., Hengst, B. & Hales, S. "Foreword," *SAIS Review,* Vol. 24, No. 1, 2004, pp. vii. (RW 1304)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Alberti, R. "Benchmarking," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 6-20. (RW 3589)

Alcorta, M. "The Role of Rough Drafts in Written Text Production: The Transition from a "Self-Directed" Text to a Text "Geared to Others"," in *Theories, Models and Methodology in Writing Research*, eds. G. Rijlaarsdam, H. van den Bergh & M. Couzijn, Amsterdam University Press, Amsterdam, 1996, pp. 339. (RW 2137)

Aldrich, R.J. "Intelligence Test," *Foreign Policy*, Vol. 134, 2003, pp. 98. (RW 1660)

Aldrich, R.J. "Global Intelligence Cooperation Versus Accountability: New Facets to an Old Problem," *Intelligence and National Security*, Vol. 24, No. 1, 2009, pp. 26. (RW 3450)

Aldrich, R.J. "Intelligence and International Security," in *The International Studies Encyclopedia*, ed. R.A. Denemark, 2010, (RW 3922)

Aldrich, R.J. ""A Profoundly Disruptive Force": The CIA, Historiography and the Perils of Globalization," *Intelligence and National Security*, Vol. 26, No. 2-3, 2011, pp. 139-158. (RW 4846)

Alexander, P.A. "The Interplay between Domain and General Strategy Knowledge: Exploring the Influence of Motivation and Situation," in *Beyond Prior Knowledge*, ed. A.J. Pace, (RW 3714)

Alexander, P.A. "The Past, Present, and Future of Knowledge Research: A Reexamination of the Role of Knowledge in Learning and Instruction. Editor's Notes." *Educational Psychologist*, Vol. 31, 1996, pp. 89. (RW 2848)

Alexander, P.A. "The Development of Expertise: The Journey from Acclimation to Proficiency," *Educational Researcher*, Vol. 32, No. 8, 2003, pp. 10. (RW 3802)

Alexander, P.A. "Why this and Why Now? Introduction to the Special Issue on Metacognition, Self-Regulation, and Self-Regulated Learning," *Educational Psychology Review*, Vol. 20, 2008, pp. 369-372. (RW 5069)

Alexander, P.A. & Dochy, F. J. R. C. "Conceptions of Knowledge and Beliefs: A Comparison Across Varying Cultural and Educational Communities," *American Educational Research Journal*, Vol. 32, No. 2, 1995, pp. 413-442. (RW 2847)

Alexander, P.A. & Murphy, P.K. "The Research Base for APA's Learner-Centered Principles," in *How Students Learn: Reforming Schools through Learner-Centered Education*, eds. N.M. Lambert & B.L. McCombs, American Psychological Association, Washington, DC, 1998, pp. 25-60. (RW 4988)

Alexander, P.A., Schallert, D.L. & Hare, V.C. "Coming to Terms: How Researchers in Learning and Literacy Talk about Knowledge," *Review of Educational Research*, Vol. 61, 1991, pp. 315. (RW 3820)

Alexander, P.A. "Adults' Views about Knowing and Believing," in *Beliefs about Texts and Instruction with Text*, eds. R. Garner & P.A. Alexander, L. Erlbaum Associates, Hillsdale, NJ, 1994, pp. 223. (RW 2774)

Alexander, P.A. "The Path to Competence: A Lifespan Developmental Perspective on Reading," *Journal of Literacy Research*, Vol. 37, No. 4, 2005, pp. 413-436. (RW 4526)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Alexander, P.A. *The Path to Competence: A Lifespan Developmental Perspective on Reading* 2006. (RW 3786)

Alexander, P.A., Dinsmore, D.L., Fox, E., Grossnickle, E.M., Loughlin, S.M., Maggioni, L., Parkinson, M.M. & Winters, F.I. *Higher-Order Thinking and Knowledge: Domain-General and Domain-Specific Trends and Future Directions* [undated]. (RW 3832)

Alexander, P.A. & Fives, H. "Achieving Expertise in Teaching Reading," in *Engaging Young Readers: Promoting Achievement and Motivation*, eds. L. Baker, M.J. Dreher & J.T. Guthrie, Guilford Press, New York, 2000, pp. 285. (RW 3723)

Alexander, P.A. & Fox, E. *Adolescents as Readers* (RW 3831)

Alexander, P.A., Garner, R., Sperl, C.T. & Hare, V.C. "Fostering Reading Competence in Students with Learning Disabilities," in *Learning about Learning Disabilities*, ed. B.Y.L. Wong, 2nd ed., Academic Press, San Diego, CA, 1998, pp. 343-349. (RW 3724)

Alexander, P.A. & Jetton, T.L. "Learning from Text: A Multidimensional and Developmental Perspective," in *Handbook of Reading Research: Volume III*, ed. M.L. Kamil, L. Erlbaum Associates, Mahwah, NJ, 2000, pp. 285. (RW 3845)

Alexander, P.A. & Jetton, T.L. "Learning from Traditional and Alternative Texts: New Conceptualizations for the Information Age," in *Handbook of Discourse Processes*, eds. A.C. Graesser, M.A. Gernsbacher & S.R. Goldman, L. Erlbaum Associates, Mahwah, NJ, 2003, pp. 199. (RW 3722)

Alexander, P.A., Murphy, P.K., Buehl, M.M. & Sperl, C.T. "The Influence of Prior Knowledge, Beliefs, and Interest on Learning from Persuasive Text," in *National Reading Conference Yearbook*, eds. T. Shanahan & F.V. Rodriguez-Brown, Texas Christian University Press, Fort Worth, Tex., 1998, pp. 167. (RW 2843)

Alexander, P.A. & Sinatra, G.M. "First Steps: Scholars' Promising Movements into a Nascent Field of Inquiry," in *Re-Framing the Conceptual Change Approach in Learning and Instruction*, eds. S. Vosniadou, A. Baltas & X. Vamvakoussi, Elsevier, Amsterdam, 2007, pp. 221-238. (RW 5522)

Alexseev, M.A. *Without Warning: Threat Assessment, Intelligence, and Global Struggle*, St. Martin's Press, New York, NY, 1997. (RW 1107)

Alhenshiri, A., Shepherd, M. & Watters, C. "VISTO for Web Information Gathering and Organization", *HCIR 2010: Proceedings of the Fourth Workshop on Human-Computer Interaction and Information Retrieval,* New Brunswick, NJ, August 22, 2010, pp.77. (RW 4315)

Alicke, M.D. & Govorun, O. "The Better-than-Average Effect," in *The Self in Social Judgment*, eds. M.D. Alicke, D. Dunning & J.I. Krueger, Psychology Press, New York, 2005, pp. 85. (RW 2893)

Allan, J. "HARD Track Overview in TREC 2004 High Accuracy Retrieval from Documents", *Thirteenth Text Retrieval Conference (TREC 2004),* Gaithersburg, MD, November 16-19, 2004, pp.11-11. (RW 943)

Allan, J. "HARD Track Overview in TREC 2003 High Accuracy Retrieval from Documents", *Twelfth Text Retrieval Conference (TREC 2003),* Gaithersburg, MD, November 18-21, 2003, pp.2424-37. (RW 942)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Allard, C.K. *Business Intelligence: Open Sources and Methods,* Center for Information Policy Research. Harvard University, Cambridge, MA, 2002. (RW 1144)

Allard, C.K., Curuby, G.N., Freeman, K., Highsmith, N., Leney, T., McGaffey, D.C. & Millot, M.D. *Seminar on Command, Control, Communications, and Intelligence. Student Papers,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1980. (RW 1047)

Allard, K. *Information Warfare: Hierarchies Or Networks?* Center for Information Policy Research. Harvard University, Cambridge, MA, 1998. (RW 1045)

Allee, V. *The Knowledge Evolution: Expanding Organizational Intelligence,* Butterworth-Heinemann, Boston, MA, 1997. (RW 657)

Allen, C.D. & Gerras, S.J. "Developing Creative and Critical Thinkers," *Military Review,* November-December, 2009, pp. 77-83. (RW 4041)

Allen, C.E. *Intelligence: Cult, Craft, Or Business?* Center for Information Policy Research, Harvard University, Cambridge, MA, 2001. (RW 169)

Allen, G. "Complexity Management for Decision Making. Tutorial Notes. [Powerpoint Presentation]," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 831)

Allison, G.T. *Essence of Decision: Explaining the Cuban Missile Crisis,* 1971. (RW 1607)

Allwein, K. *Multidimensional Analysis [Powerpoint Presentation]* [undated]. (RW 3027)

Allwood, C.M. & Johansson, M. "Actor-Observer Differences in Realism in Confidence and Frequency Judgments," *Acta Psychologica,* Vol. 117, No. 3, 2004, pp. 251. (RW 2353)

Alonso, O., Berberich, K., Bedathur, S. & Weikim, G. "Time-Based Exploration of News Archives", *HCIR 2010: Proceedings of the Fourth Workshop on Human-Computer Interaction and Information Retrieval,* New Brunswick, NJ, August 22, 2010, pp.1212. (RW 4314)

Alonso, R. & Li, H. "Combating Cognitive Biases in Information Retrieval," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 829)

Alotaibi, Y.B. *Revitalizing the CIA: Intelligence Reform in the Post-Cold War World,* University of Tennessee, Knoxville, TN, 2010. (RW 5605)

Altier, W.J. *The Thinking Manager's Toolbox: Effective Processes for Problem Solving and Decision Making,* Oxford University Press, New York, 1999. (RW 2777)

Amabile, T.M., Mueller, J.S., Simpson, W.B., Hadley, C.N., Kramer, S.J. & Fleming, L. *Time Pressure and Creativity in Organization: A Longitudinal Field Study,* Harvard Business School Working Paper No. 02-073, 2002. (RW 4587)

Amernic, J.H. & Beechy, T.H. "Accounting Students' Performance and Cognitive Complexity: Some Empirical Evidence," *The Accounting Review,* Vol. 59, No. 2, 1984, pp. 300. (RW 4271)

Amidon, M. "Groupthink, Politics, and the Decision to Attempt the Son Tay Rescue," *Parameters,* Vol. 35, No. 3, 2005, pp. 119-131. (RW 767)

Amir, O. "Tough choices: how making decisions tires your brain", *Scientific American: Mind Matters,* [Online], 2008, (RW 3314)

Amodio, D.M., Jost, J.T., Master, S.L. & Yee, C.M. "Neurocognitive Correlates of Liberalism and Conservatism," *Nature Neuroscience,* 2007 (RW 2791)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Amsel, E. & Brock, S. "The Development of Evidence Evaluation Skills," *Cognitive Development,* Vol. 11, No. 4, 1996, pp. 523. (RW 2323)

Anastas, J.W. *Research Design for Social Work and the Human Services,* 2nd ed., Columbia University Press, New York, 1999. (RW 2558)

Andersen, L.J. "A Sense of Audience Or Conventional Wisdom?" *Journal of Advanced Composition,* Vol. 7, No. 1-2, 1987, pp. 112-120. (RW 4498)

Anderson, C. "The End of Theory," *Wired Magazine,* Vol. 16, No. 7, 2008, pp. 108. (RW 3180)

Anderson, C. *The Long Tail: Why the Future of Business is Selling Less of More,* Hyperion, New York, 2008. (RW 3417)

Anderson, D. "Yesterday's Weapons Tomorrow," *Studies in Intelligence,* Vol. 9, No. 4, 1965, pp. 13-17. (RW 4175)

Anderson, D.S. "What Makes a Good Intelligence Analyst?" *Intelligencer,* Vol. 13, No. 2, 2003, pp. 74-75. (RW 4455)

Anderson, E.R., Yoder, C.Y., Herrmann, D.J., Johnson, T.J. & Gennaro, R.J. "Inferring the Mental Processes of Other Minds," *Journal of Social Psychology,* Vol. 143, No. 3, 2003, pp. 355. (RW 2355)

Anderson, H.C., Marcham, F.G. & Dunn, S.B. "An Experiment in Teaching Certain Skills of Critical Thinking," *Journal of Educational Research,* Vol. 38, No. 4, 1944, pp. 241-251. (RW 4485)

Anderson, J.R. "Acquisition of Cognitive Skill," *Psychological Review,* Vol. 891982, pp. 369. (RW 3489)

Anderson, J.R. *The Architecture of Cognition,* Harvard University Press, Cambridge, MA, 1983. (RW 3488)

Anderson, M.G. *Personality Assessment in Personnel Selection,* CPP Inc., Mountain View, CA, 2007. (RW 5339)

Anderson, T. "On Generalizations I: A Preliminary Exploration," *South Texas Law Review,* Vol. 40, No. 2, 1999, pp. 455. (RW 4183)

Anderson, T., Schum, D.A. & Twining, W.L. *Analysis of Evidence,* 2nd ed., Cambridge University Press, Cambridge, UK, 2005. (RW 962)

Anderson, T., Twining, W.L. & Wigmore, J.H. *Analysis of Evidence: How to do Things with Facts Based on Wigmore's Science of Judicial Proof,* Northwestern University Press ed., Northwestern University Press, Evanston, Ill, 1998. (RW 4181)

Andre, L.E. "Intelligence Production: Towards a Knowledge-Based Future," *Defense Intelligence Journal,* Vol. 6, No. 2, pp. 35-45. (RW 1276)

Andre, T. & Windschitl, M. "Interest, Epistemological Belief and Intentional Conceptual Change " in *Intentional Conceptual Change* L. Erlbaum Associates, Mahwah, NJ, 2003, pp. 173-198. (RW 5517)

Andre, T. & Windschitl, M. "Interest, Epistemological Belief, and Intentional Conceptual Change," in *Intentional Conceptual Change,* eds. G.M. Sinatra & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2003, pp. 173. (RW 4435)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Andre, T. & Windschitl, M. "Interest, Epistemological Belief, and Intentional Conceptual Change," in *Intentional Conceptual Change*, eds. G.M. Sinatra & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2003, pp. 173-197. (RW 5040)

Andregg, M. *The Primary Value of Restoring a Healthy Relationship between Intelligence Agencies and the Academic World is a Revolution in Intelligence Affairs* 2002. (RW 2108)

Andregg, M. "How "Wisdom" Differs from Intelligence and Knowledge", *International Studies Association (ISA) 44th Annual International Convention,* Portland, OR, February 25 - March 1, 2003 (RW 340)

Andregg, M. "Why the Intelligence Community (IC) System Drives You Crazy, and how to Come in from the Cold", *OSS-04 Annual Meeting,* April 12-17, 2004 (RW 516)

Andregg, M. "Intelligence Ethics: Laying a Foundation for the Second Oldest Profession," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 52. (RW 2457)

Andregg, M. "Ethics and Professional Responsibility," in *Oxford Handbook of National Security Intelligence*, ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 735-756. (RW 4719)

Andregg, M.M. "The Birth of Professional Ethos: Some Comparisons among Medicine, Law, and Intelligence Communities," *American Intelligence Journal,* Vol. 28, No. 1, 2010, pp. 82-92. (RW 4474)

Andrew, C. "Conclusion: An Agenda for Future Research," in *Eternal Vigilance? 50 Years of the CIA*, eds. R. Jeffreys-Jones & C. Andrew, F. Cass, London, UK, 1997, pp. 224-233. (RW 39)

Andrew, C. *Intelligence Analysis Needs to Look Backwards before Looking Forwards: Why Lessons of the Past can Help Fight Terror of the Future*, Centre for Counterterrorism Studies 2004. (RW 332)

Andrew, C. "Intelligence, International Relations and Under-Theorisation," *Intelligence and National Security,* Vol. 19, No. 2, 2004, pp. 170-184. (RW 445)

Andrew, C. "Historical Attention Span Deficit Disorder: Why Intelligence Analysis Needs to Look Back before Looking Forward", *New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities,* Rome, Italy, 31 March - 2 April, 2004, pp.6363-80. (RW 1529)

Andrew, C. *Secret Intelligence: A Reader,* 2008. (RW 3401)

Andrews, D. *The I. R. G. Solution: Hierarchical Incompetence and how to Overcome it,* 1984. (RW 4029)

Andrews, P.P., Jr. & Peterson, M.B. *Criminal Intelligence Analysis,* Palmer Enterprises, Loomis, CA, 1990. (RW 1091)

Andriani, M.R. "The Impact of Transformation on National Intelligence Support Planning," *Defense Intelligence Journal,* Vol. 14, No. 1, 2005, pp. 115-120. (RW 4590)

Andriessen, J., Coirier, P., Roos, L., Passerault, J. & Bert-Erboul, A. "Thematic and Structural - Planning in Constrained Argumentative Text Production," in *Theories, Models and Methodology in Writing Research*, eds. G. Rijlaarsdam, H. van den Bergh & M. Couzijn, Amsterdam University Press, Amsterdam, 1996, pp. 237. (RW 2134)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Andriole, S.J. *Handbook of Problem Solving: An Analytical Methodology,* Petrocelli Books, Princeton, NJ, 1983. (RW 2698)

Andrus, C., DeAngelis, S. & Moran, M. *Can New Technology and Tradecraft Enhance Intelligence Sharing and National Security?* 2007. (RW 3017)

Andrus, D.C. "Toward a Complex Adaptive Intelligence Community," *Studies in Intelligence,* Vol. 49, No. 3, 2005, pp. 63. (RW 1497)

Angel, B.F., Duffey, M. & Belyea, M. "An Evidence-Based Project for Evaluating Strategies to Improve Knowledge Acquisition and Critical-Thinking Performance in Nursing Students," *Journal of Nursing Education,* Vol. 39, No. 5, 2000, pp. 219-228. (RW 3955)

Angeli, C. & Valanides, N. "Epistemological Beliefs and Ill-Structured Problem-Solving in Solo and Paired Contexts," *Educational Technology & Society,* Vol. 15, No. 1, 2012, pp. 2-14. (RW 5553)

Anglin, J.M., Bruner, J.S. & Olson, D.R. *The Social Foundations of Language and Thought: Essays in Honor of Jerome S. Bruner*, Norton, New York, 1980. (RW 3254)

Anglin, J.M., Bruner, J.S. & Olson, D.R. *The Social Foundations of Language and Thought: Essays in Honor of Jerome S. Bruner*, Norton, New York, 1980. (RW 3274)

Annett, J. "Theoretical and Pragmatic Influences on Task Analysis Methods," in *Cognitive Task Analysis*, eds. J.M. Schraagen, S.F. Chipman & V. Shalin, L. Erlbaum Associates, Mahwah, NJ, 2000, pp. 25. (RW 3487)

Annibale, P. "Decision Trees," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 71-79. (RW 3612)

Annibale, P. "When Will Machines Replace Analysts?" *SCIP.online,* 2003 (RW 588)

Anthes, E. "Dressed for Distress: Clothing's Effects on the Mind," *Scientific American,* 2008 (RW 3295)

Anton, P.S., Happel, M.D. & Mericsko, R.J. *Analyst of the Future (AoF) Advanced Research Program* 2004. (RW 1991)

Archer, L.B. "Systematic Method for Designers," in *Developments in Design Methodology*, ed. N. Cross, Wiley, Chichester; New York, 1984, pp. 57. (RW 2736)

Archer, L.B. "Whatever Became of Design Methodology?" in *Developments in Design Methodology*, ed. N. Cross, Wiley, Chichester; New York, 1984, pp. 347. (RW 2739)

Arfe, B., Dockrell, J. & Berninger, V. *Writing Development and Instruction in Children with Hearing, Speech, and Language Disorders,* Oxford University Press not yet published. (RW 5858)

Argamon, S., Chase, P. & Dodick, J. "The Languages of Science: A Corpus-Based Study of Experimental and Historical Science Articles", *27th Annual Conference of the Cognitive Science Society,* Stresa, Italy, July 21-23, 2005, pp.157157-162. (RW 5180)

Argamon, S. & Dodick, J. "Linking Rhetoric and Methodology in Formal Scientific Writing", *26th Annual Conference of the Cognitive Science Society,* Chicago, IL, August 5-7, 2004, pp.[unpaged][unpaged]. (RW 5186)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Argamon, S. & Dodick, J. "Linking Rhetorick and Methodology in Formal Scientific Writing", *Proceedings of the Twenty-Sixth Annual Conference of the Cognitive Science Society,* Chicago IL, Aug 5-7, 2004, pp.6161-66. (RW 5355)

Argamon, S. & Olsen, M. "Toward Meaningful Computing," *Communications of the ACM,* Vol. 49, No. 4, 2006, pp. 33. (RW 1515)

Argyris, C. *Overcoming Organizational Defenses: Facilitating Organizational Learning,* 1990. (RW 1730)

Argyris, C. "Teaching Smart People how to Learn," *Harvard Business Review,* May-June, 1991, pp. 99. (RW 1767)

Ariely, D. *Predictably Irrational: The Hidden Forces that Shape our Decisions,* Harper, New York, NY, 2008. (RW 3075)

Ariely, D. *The Upside of Irrationality: The Unexpected Benefits of Defying Logic at Work and at Home,* 2010. (RW 4128)

Ariely, D., Loewenstein, G. & Prelec, D. "Tom Sawyer and the Construction of Value," *Journal of Economic Behavior and Organization,* Vol. 602006, pp. 1. (RW 3315)

Arkes, H.R. "The Non-use of Psychological Research at Two Federal Agencies," *Psychological Science,* Vol. 142003, pp. 1. (RW 1967)

Arkes, H.R. *Judgment/decision Making Principles Pertinent to Intelligence Analysis: Lessons from Medicine[Powerpoint Presentation]* 2006. (RW 1993)

Arkes, H.R. & Kajdasz, J. "Intuitive Theories of Behavior," in *Intelligence Analysis: Behavioral and Social Scientific Foundations,* eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, pp. 143-168. (RW 4776)

Arkes, H.R. & Mellers, B.A. "Do Juries Meet our Expectations?" *Law & Human Behavior,* Vol. 26, No. 6, 2002, pp. 625. (RW 1968)

Arkes, H.R., Shaffer, V.A. & Dawes, R.M. "Comparing Holistic and Disaggregated Ratings in the Evaluation of Scientific Presentations," *Journal of Behavioral Decision Making,* Vol. 192006, pp. 429. (RW 1966)

Arms, W.Y. "Automated Digital Libraries: How Effectively can Computers be used for the Skilled Tasks of Professional Librarianship?" *D-Lib Magazine,* Vol. 6, No. 7/8, 2000 (RW 3418)

Armstrong, F.T. "Ways to make Analysis Relevant but Not Prescriptive," *Studies in Intelligence,* Vol. 46, No. 3, 2002, pp. 37-43. (RW 936)

Armstrong, J.S. "Unintelligible Management Research and Academic Prestige," *Interfaces,* Vol. 10, No. 2, 1980, pp. 80. (RW 2076)

Armstrong, S., B., M., Kirkpatrick, S., Khalsa, S., P., J. & Rieber, S. "How can Predictive Accuracy be Improved?", McLean, Virginia, May 2-6, 2005 (RW 3061)

Armstrong, W.C., Leonhart, W., McCaffrey, W.J. & Rothenberg, H.C. "The Hazards of Single Outcome Forecasting," in *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992*, ed. H.B. Westerfield, Yale University Press, New Haven, CT, 1995, pp. 238-254. (RW 887)

Arner, D.G. *Perception, Reason and Knowledge: An Introduction to Epistemology,* Scott, Foresman, Glenview, IL, 1972. (RW 4267)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Arnold, J.C. "Omens and Oracles (Past Intelligence Failures)," *Proceedings of the U.S. Naval Institute,* 1980, pp. 47-53. (RW 4448)

Arnold, V., Collier, P.A., Leech, S.A. & Sutton, S.G. "Impact of Intelligent Decision Aids on Expert and Novice Decision-Makers' Judgments," *Accounting and Finance,* Vol. 44, No. 1, 2004, pp. 1-26. (RW 207)

Arroyo, N. *What is the Invisible Web? A Crawler Perspective [Powerpoint Presentation]* (RW 1398)

Arter, J.A. & Salmon, J.R. *Assessing Higher Order Thinking Skills. A Consumer's Guide*, Northwest Regional Educational Laboratory, Portland, OR, 1987. (RW 3708)

Arum, R. & Roksa, J. *Academically Adrift: Limited Learning on College Campuses,* University of Chicago Press, Chicago, IL, 2011. (RW 4658)

Ashworth, E.D. "The Variety of Qualitative Research. Part One: Introduction to the Problem," *Nurse Education Today,* Vol. 171997, pp. 215. (RW 2691)

Ashworth, E.D. "The Variety of Qualitative Research. Part Two: Non-Positivist Approaches," *Nurse Education Today,* Vol. 171997, pp. 219. (RW 2692)

Ashworth, P.D. "Presuppose Nothing! the Suspension of Assumptions in Phenomenological Psychological Methodology," *Journal of Phenomenological Psychology*, Vol. 271996, pp. 1. (RW 2719)

Association of College and Research Libraries *Information Literacy Competency Standards for Higher Education,* ACRL, Chicago, IL, 2000. (RW 1619)

Atran, S. "A Failure of Imagination (Intelligence, WMDs, and "Virtual Jihad")," *Studies in Conflict and Terrorism,* Vol. 29, No. 3, 2006, pp. 285-300. (RW 5618)

Attfield, S. *Perspectives on Sensemaking [Powerpoint Presentation]* 2010. (RW 5606)

Audi, R. *Epistemology: A Contemporary Introduction to the Theory of Knowledge,* 2nd ed., Routledge, New York, 2003. (RW 2291)

Auger, A. "Applying Natural Language Processing Techniques to Domain Knowledge Capture," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 821)

Aunger, R. *Darwinizing Culture: The Status of Memetics as a Science*, Oxford University Press, Oxford, UK, 2000. (RW 5745)

Aunger, R. *The Electric Meme: A New Theory of how we Think*, Free Press, New York, 2002. (RW 3482)

Austin, J.A. "The Psychological Dimension of Intelligence Activities," in *Strategic Intelligence: Theory and Application*, eds. D.H. Dearth, Army War College & Joint Military Intelligence Training Center, 1991, pp. 181. (RW 3808)

Auyeung, P.K., Dagwell, R., Ng, C. & Sands, J. "Educators' Epistemological Beliefs of Accounting Ethics Teaching: A Cross-Cultural Study," *Accounting Research Journal*, Vol. 19, No. 2, 2006, pp. 122-138. (RW 5014)

Avison, D.E. & Taylor, V. "Information Systems Development Methodologies: A Classification According to Problem Situation," *Journal of Information Technology,* Vol. 121997, pp. 73. (RW 2627)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Axelrod, R.M. *Structure of Decision: The Cognitive Maps of Political Elites,* Princeton University Press, Princeton, NJ, 1976. (RW 2520)

Axelsson, R., Dahlgren, M.A. & Dahlgren, L.O. "Conceptualising Professional Identification as Flexibility, Stability, and Ambivalence," in *Learning through Practice: Models, Traditions, Orientations, and Approaches*, ed. S. Billett, Springer, Dordrecht, 2010, pp. 120-138. (RW 4959)

Ayer, A.J. *The Problem of Knowledge,* Macmillan, London, 1965. (RW 3186)

Ayoub, P.J., Petrick, I.J. & McNeese, M.D. "Weather Systems: A New Metaphor for Intelligence Analysis", *Human Factors and Ergonomics Society 51st Annual Meeting*, October 1.5, 2007 (RW 3266)

Ayres, I. *Super Crunchers: Why Thinking-by-Numbers is the New Way to be Smart,* Bantam Books, New York, 2007. (RW 2827)

Baar, D. "Questions of Focus: Advances in Lens-Based Visualizations for Intelligence Analysis," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 865)

Badalamente, R.V. & Greitzer, F.L. "Top Ten Needs for Intelligence Analysis Tool Development," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2-6 May 2005 (RW 597)

Badia, A. & Kantardzic, M. "Link Analysis Tools for Intelligence and Counterterrorism," *Lecture Notes in Computer Science,* Vol. 34952005, pp. 49-59. (RW 5650)

Badia, A. "Personal Information Management for Intelligence Tasks," in *Intelligence and Security Applications: Techniques and Applications*, eds. H. Chen & C.C. Yang, Springer, 2008, pp. 215-225. (RW 5778)

Bahrami, B., Olsten, K., Latham, P.E., Roepstorff, A., Rees, G. & Frith, C.D. "Optimally Interacting Minds," *Science,* Vol. 329, No. 5995, 2010, pp. 1081. (RW 4304)

Bailey, C.D., Daily, C.M. & Phillips, M.J.J. *A Study of Kruglanski's Need for Closure Construct and its Implications for Judgment and Decision Making in Accounting and Auditing* 2005. (RW 5174)

Bailey, S. *Managing the Crowd: Rethinking Records Management for the Web 2.0 World,* Facet Publishing, London, UK, 2008. (RW 4683)

Bailin, S. *A Conception of Critical Thinking for Curriculum, Instruction and Assessment,* British Columbia Ministry of Education and Ministry Responsible for Multi-Cultural and Human Rights, Victoria, B.C., Canada, 1993. (RW 3703)

Bailin, S. "The Problem with Percy: Epistemology, Understanding and Critical Thinking," *Informal Logic,* Vol. 19, No. 2-3, 1999, pp. 161-170. (RW 3707)

Bailin, S., Case, R. & Coombs, J.R. "Common Misconceptions of Critical Thinking," *Journal of Curriculum Studies,* Vol. 31, No. 3, 1999, pp. 269-283. (RW 4017)

Bailyn, L. "Research as a Cognitive Process: Implications for Data Analysis," *Quality and Quantity,* Vol. 11, 1977, pp. 97. (RW 3531)

Bain, A.M., Bailet, L.L. & Moats, L.C. *Written Language Disorders: Theory into Practice,* 2nd ed., Pro-Ed, Austin, Tex., 2001. (RW 2016)

Bain, B. *Intellipedia's Next Act.* 2008. (RW 3139)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Baker, B. *Newsthinking: The Secret of Making Your Facts Fall into Place,* Allyn and Bacon, Boston, MA, 2002. (RW 1858)

Baker, C.R. "Reflective Learning: A Teaching Strategy for Critical Thinking," *Journal of Nursing Education,* Vol. 35, No. 1, 1996, pp. 19-22. (RW 4114)

Baker, E.L. "The Influence of Learning Research on the Design and use of Assessment," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 333-355. (RW 5148)

Baker, L. & Brown, A.L. "Metagognitive Skills and Reading," in *Handbook of Reading Research,* ed. P.D. Pearson, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 353-394. (RW 5219)

Baker, L.M. & Dunbar, K. "Experimental Design Heuristics for Scientific Discovery: The use of "Baseline" and "Known Standard" Controls," *International Journal of Human-Computer Studies,* Vol. 53, No. 3, 2000, pp. 335. (RW 1816)

Baker, R. C. M. (Mark) *The Globalization of Telecommunications,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1996. (RW 974)

Baker, S. *Final Jeopardy: Man Vs. Machine and the Quest to Know Everything,* Houghton Mifflin Harcourt, Boston, MA, 2011. (RW 4548)

Baker, V.E. *Reexamining the Principle of Surprise in 21st Century Warfare,* Naval War College, Newport, RI, 1996. (RW 264)

Baker, W.R. "The Easter Offensive of 1972: A Failure to use Intelligence," *Military Intelligence Professional Bulletin,* Vol. 24, No. 1, 1998, pp. 40-42. (RW 462)

Baker, W.O. *The Convergence of C3I Techniques and Technology,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1981. (RW 973)

Balakrishna, M. & Srikanth, M. "Automatic Ontology Creation from Text for National Intelligence Priorities Framework (NIPF)", *Proceedings of the Third International Ontology for the Intelligence Community Conference OIC-2008,* Fairfax, VA, December 3-4, 2008, pp.88-12. (RW 4824)

Balatsoukas, P. & Ruthven, I. "What Eyes can Tell about the use of Relevance Criteria during Predictive Relevance Judgment?" *Iiix 2010,* New Brunswick, NJ, August 18-21, 2010 (RW 4864)

Baldwin, H. "The Future of Intelligence," *Strategic Review,* Vol. 9, No. 3, 1976, pp. 6. (RW 1257)

Ball, A.F. "To Know is Not enough: Knowledge, Power, and the Zone of Generativity," *Educational Researcher,* Vol. 41, No. 8, 2012, pp. 283-293. (RW 5871)

Ball, L.J. "The Dynamics of Reasoning: Chronometric Analysis and Dual-Process Theories," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans,* eds. K.I. Manktelow, D.E. Over & S. Elqayam, Psychology Press, Hove, East Sussex, UK, 2011, pp. 283-307. (RW 5711)

Baltas, A. "The Philosophical Foundations of the Conceptual Change Approach: An Introduction," in *Re-Framing the Conceptual Change Approach in Learning and Instruction,* eds. S. Vosniadou, A. Baltas & X. Vamvakoussi, Elsevier, Amsterdam, 2007, pp. 19-23. (RW 5125)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Balter, L. & Tamis-LeMonda, C. *Child Psychology: A Handbook of Contemporary Issues,* Psychology Press, Philadelphia, PA, 1999. (RW 4670)

Banaji, M.R. & Greenwald, A.G. *Blind Spot: Hidden Biases of Good People,* 2013. (RW 5902)

Banisar, D. *Freedom of Information Around the World Update 2002.* 2002. (RW 1448)

Bansal, P., Bertels, S., Ewart, T., MacConnachie, P. & O'Brien, J. "Bridging the Research-Practice Gap," *Academy of Management Perspectives,* Vol. 26, No. 1, 2012, pp. 73-92. (RW 5864)

Bansemer, J.D. *Intelligence Reform: A Question of Balance*, Center for Information Policy Research, Harvard University, Cambridge, MA, 2005. (RW 504)

Bao, L., Cai, T., Koenig, K., Fang, K., Han, J., Wang, J., Liu, Q., Ding, L., Cui, L., Luo, Y., Wang, Y., Li, L. & Wu, N. "Physics: Learning and Scientific Reasoning," *Science,* Vol. 323, No. 5914, 2009, pp. 586. (RW 3822)

Barabasi, A. *Bursts: The Hidden Pattern Behind Everything we do,* 2010. (RW 4026)

Barbera-Tomas, D., Schachter, M.E.E. & de los Reyes-Lopez, E. "Improving Organizational Learning with Concept Maps: A Business Case Study," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge*, eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 253-276. (RW 4975)

Bardwell, L.V. "Problem-Framing: A Perspective on Environmental Problem-Solving," *Environmental Management,* Vol. 15, No. 5, 1991, pp. 603. (RW 2637)

Barger, D.G. "It is Time to Transform, Not Reform, US Intelligence," *SAIS Review,* Vol. 24, No. 1, 2004, pp. 23-31. (RW 143)

Barger, D.G. *Toward a Revolution in Intelligence Affairs*, TR-242, RAND Corporation, Santa Monica, CA, 2005. (RW 376)

Baril, C.P., Cunningham, B.M., Fordham, D.R., Gardner, R.L. & Wolcott, S.K. "Critical Thinking in the Public Accounting Professions: Aptitudes and Attitudes," *Journal of Accounting Education,* Vol. 16, No. 3/4, 1998, pp. 381-406. (RW 4289)

Bar-Joseph, U. *Intelligence Intervention in the Politics of Democratic States: The United States, Israel, and Britain,* Pennsylvania State University Press, University Park, PA, 1995. (RW 701)

Bar-Joseph, U. "Israel Caught Unawares: Egypt's Sinai Surprise of 1960," *International Journal of Intelligence and Counterintelligence,* Vol. 8, No. 2, 1995, pp. 203-219. (RW 724)

Bar-Joseph, U. "Israel's Intelligence Failure of 1973: New Evidence, a New Interpretation, and Theoretical Implications," *Security Studies,* Vol. 4, No. 3, 1995, pp. 584-609. (RW 728)

Bar-Joseph, U. "The Wealth of Information and the Poverty of Comprehension: Israel's Intelligence Failure of 1973 Revisited," *Intelligence and National Security,* Vol. 10, No. 4, 1995, pp. 229-240. (RW 725)

Bar-Joseph, U. "State-Intelligence Relations in Israel: 1948-1996," *Journal of Conflict Studies,* Vol. 17, No. 2, 1997, pp. 133-156. (RW 726)

Bar-Joseph, U. "A Bull in a China Shop: Netanyahu and Israel's Intelligence Community," *International Journal of Intelligence and Counterintelligence,* Vol. 11, No. 2, 1998, pp. 154-174. (RW 723)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Bar-Joseph, U. "Surprise and its Causes in Business Administration and Strategic Studies," *International Journal of Intelligence and Counterintelligence*, Vol. 11, No. 3, 1998, pp. 331-349. (RW 727)

Bar-Joseph, U. "Israel's 1973 Intelligence Failure," *Israel Affairs*, Vol. 6, No. 1, 1999, pp. 11-35. (RW 158)

Bar-Joseph, U. "Intelligence Failure and the Need for Cognitive Closure: The Case of Yom Kippur", *Handel International Strategy Conference*, Naval War College, Newport, RI, 13-14 November 2001 (RW 334)

Bar-Joseph, U. "Israel's Military Intelligence Performance in the Second Lebanon War," *International Journal of Intelligence and Counterintelligence*, Vol. 20, No. 4, 2007, pp. 583. (RW 2758)

Bar-Joseph, U. *Military Intelligence as the National Intelligence Estimator: The Case of Israel* 2010. (RW 4493)

Bar-Joseph, U. "The Professional Ethics of Intelligence Analysis," *International Journal of Intelligence and Counterintelligence*, Vol. 24, No. 1, 2011, pp. 22-43. (RW 4576)

Bar-Joseph, U. & Kruglanski, A.W. "Intelligence Failure and Need for Cognitive Closure: On the Psychology of the Yom Kippur Surprise," *Political Psychology*, Vol. 24, No. 1, 2003, pp. 75-99. (RW 494)

Bar-Joseph, U. & McDermott, R. "Change the Analyst and Not the System: A Different Approach to Intelligence Reform," *Foreign Policy Analysis*, Vol. 4, No. 2, 2008, pp. 127. (RW 3784)

Bar-Joseph, U. & McDermott, R. "The Intelligence Analysis Crisis," in *Oxford Handbook of National Security Intelligence*, ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 359-374. (RW 4708)

Barlow, J.P. "Why Spy?" *Forbes*, 2002 (RW 4153)

Barnard-Brak, L. & Lan, W. "Epistemological Beliefs Across Faculty Experts and Student Non-Experts," *Journal of Further and Higher Education*, Vol. 33, No. 3, 2009, pp. 289-300. (RW 5233)

Barnett, T.P.M. *Mr. President, here's how to make Sense of our Iraq Strategy*, Available: www.leighbureau.com, (RW 509)

Baron, J. "Beliefs about Thinking," in *Informal Reasoning and Education*, eds. J.F. Voss, D.N. Perkins & J.W. Segal, L. Erlbaum Associates, Hillsdale, NJ, 1991, pp. 169-186. (RW 4937)

Baron, J. "Why Teach Thinking? an Essay," *Applied Psychology*, Vol. 42, No. 3, 1993, pp. 191-237. (RW 2413)

Baron, J. *Myside Bias in Thinking about Abortion* 2003. (RW 2410)

Baron, J.B. *Being Disposed to Think: A Typology of Attitudes and Dispositions Related to Acquiring and using Thinking Skills* 1987. (RW 5200)

Baron, J.B. "Evaluating Thinking Skills in the Classroom," in *Teaching Thinking Skills: Theory and Practice*, eds. J.B. Baron & R.J. Sternberg, Freeman, New York, NY, 1987, pp. 221-248. (RW 3743)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Baron, J. *Rationality and Intelligence*, Cambridge University Press, New York, NY, 1985. (RW 4943)

Baron, J. "What Kinds of Intelligence Components are Fundamental," in *Thinking and Learning Skills*, eds. S.F. Chipman, J.W. Segal & R. Glaser, L. Erlbaum Associates, Hillsdale, NJ, 1985, pp. 365-390. (RW 4951)

Baron, J. *Thinking and Deciding*, 3rd ed., Cambridge University Press, Cambridge, UK; New York, 2000. (RW 2411)

Barrass, G.S. *Getting Inside their Mind*, Available: http://www.unc.edu/depts/diplomat/item/2009/0103/comm/barrass_gettinginside.html, (RW 3890)

Barrett, A. *Politics and the Military - the Climate for Reform*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1986. (RW 975)

Barrol, L.W. *A Memoir of the Late Washington Platt: October 6, 1890 to May 19, 1965, Brigadier General, United States Army*, E.P. Erisman, Peterborough, NH, 1967. (RW 995)

Barrouillet, P. & Gauffroy, C. "Dual Processes in the Development of the Understanding of Conditionals," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans*, eds. K.I. Manktelow, D.E. Over & S. Elqayam, Psychology Press, Hove, East Sussex, UK, 2011, pp. 191-215. (RW 5707)

Barrows, H.S. *Practice-Based Learning: Problem-Based Learning Applied to Medical Education*, Southern Illinois University School of Medicine, Springfield, IL, 1994. (RW 5326)

Barry, J.A., Davis, J., Gries, D.D. & Sullivan, J. "Bridging the Intelligence-Policy Divide," *Studies in Intelligence*, Vol. 37, No. 5, 1994, pp. 1-8. (RW 4166)

Barry, T. *The Neocon Philosophy of Intelligence*, Available: http://www.lewrockwell.com/orig4/barry-tom1.html, (RW 403)

Barstow, D. "The Nuclear Card: The Aluminum Tube Story--A Special Report: How the White House Embraced Disputed Arms Intelligence," *New York Times*, 2004, October 3, 2004, p. 1. (RW 489)

Bartels, L.M. "The Irrational Electorate," *The Wilson Quarterly*, August, 2008 (RW 3317)

Bartlett, J.C. *A Task-Based and User-Centered Protocol for Bioinformatics Information Search and Retrieval* (RW 1780)

Bar-Yam, Y., Ramalingam, C., Burlingame, L. & Ogata, C. *Making Things Work: Solving Complex Problems in a Complex World*, NECSI, Knowledge Press, Cambridge, MA, 2004. (RW 5572)

Bascatow, T. & Bellafiore, D.J. "Redefining Geospatial Intelligence," *American Intelligence Journal*, Vol. 27, No. 1, 2009, pp. 38-40. (RW 3988)

Bassham, G., Irwin, W., Nardone, H. & Wallace, J.M. *Critical Thinking: A Student's Introduction*, McGraw-Hill, Boston, MA, 2008. (RW 4147)

Bassok, M. & Novick, L.R. "Problem Solving," in *Oxford Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 413-432. (RW 5501)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Basu, C., Cheng, H. & Fellbaum, C. "Creating a Geospatial and Visual Information Ontology for Analysts", *Proceedings of the Second International Ontology for the Intelligence Community Conference OIC-2007,* Columbia, MD, November 28-29, 2007, pp. 23-26. (RW 4817)

Bates, M.J. "The Design of Browsing and Berrypicking Techniques for the Online Search Interface," *Online Review,* Vol. 13, 1989, pp. 407. (RW 1350)

Bates, M.J. "Where should the Person Stop and the Information Search Interface Start?" *Information Processing and Management,* Vol. 26, 1990, pp. 575. (RW 1351)

Bath, D.M. & Smith, C.D. "The Relationship between Epistemological Beliefs and the Propensity for Lifelong Learning," *Studies in Continuing Education,* Vol. 31, No. 2, 2009, pp. 173-189. (RW 5563)

Bathurst, R.B. *Intelligence and the Mirror: On Creating an Enemy,* SAGE Publications, London, UK, 1993. (RW 98)

Bauer, J., Festner, D., Gruber, H., Harteis, C. & Heid, H. "The Effects of Epistemological Beliefs on Workplace Learning," *Journal for Workplace Learning,* Vol. 16, 2004, pp. 284. (RW 3774)

Baumard, P. "From Noticing to Making Sense: The use of Intelligence in Strategizing," *International Journal of Intelligence and Counterintelligence,* Vol. 7, No. 1, 1994, pp. 29-73. (RW 676)

Bawden, D. "Information Systems and the Stimulation of Creativity," *Journal of Information Science,* Vol. 12, 1986, pp. 203. (RW 2361)

Baxter Magolda, M.B. *Knowing and Reasoning in College: Gender-Related Patterns in Students' Intellectual Development,* Jossey-Bass, San Francisco, CA, 1992. (RW 4991)

Baxter Magolda, M.B. "Future Directions," in *Development and Assessment of Self-Authorship: Exploring the Concept Across Cultures,* eds. M.B. Baxter Magolda, E.G. Creamer & P.S. Meszaros, Stylus Pub., Sterling, VA, 2010, pp. 267-284. (RW 4764)

Bazan, E.B. *The Foreign Intelligence Surveillance Act: An Overview of the Statutory Framework and US Foreign Intelligence Surveillance Court and US Foreign Surveillance Court of Review Decisions* 2007. (RW 2170)

Bazerman, M.H. *Judgment in Managerial Decision Making,* 4th ed., John Wiley & Sons, New York, NY, 1998. (RW 775)

Bean, H. "The DNI's Open Source Center: An Organizational Communication Perspective," *International Journal of Intelligence and Counterintelligence,* Vol. 20, No. 2, 2007, pp. 240. (RW 3247)

Bean, H. "Foucault's Rhetorical Theory and U.S. Intelligence Affairs," *Poroi,* Vol. 6, No. 2, 2009, pp. 15-32. (RW 5601)

Bean, H. "United States Intelligence Cultures," in *The International Studies Encyclopedia,* ed. R.A. Denemark, 2010, (RW 3932)

Bean, H. *No More Secrets: Open Source Information and the Reshaping of U. S. Intelligence,* Praeger, Santa Barbara, CA, 2011. (RW 5589)

Beardsley, M.C. *Practical Logic,* Prentice-Hall, New York, NY, 1950. (RW 4451)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Beasley, R. "Collective Interpretations: How Problem Representations Aggregate in Foreign Policy Groups," in *Problem Representation in Foreign Policy Decision Making*, eds. D.A. Sylvan & J.F. Voss, 1998, pp. 80-115. (RW 1612)

Beauregard, M. *Re-Thinking Intelligence Analysis Training,* Available: http://www.vanguardcanada.com/intelligenceanalysttrainingbeauregard, Viewed: August 22, 2012. (RW 5782)

Becker, A.C. "Intelligence Fiasco Or Reasoned Accounting? CIA Estimates of Soviet GNP," *Post-Soviet Affairs,* Vol. 10, No. 4, 1994, pp. 291-329. (RW 85)

Becker, A.H. *Knowledge Discovery & Dissemination: Enabling Analysts to Quickly Produce Actionable Intelligence from Multiple Sources of Information[Powerpoint Presentation]* 2009. (RW 4519)

Becks, D., Goertz, M. & Womser-Hacker, C. "Understanding Information Seeking in the Patent Domain and its Impact on the Interface Design of IR Systems", *HCIR 2010: Proceedings of the Fourth Workshop on Human-Computer Interaction and Information Retrieval,* New Brunswick, NJ, August 22, 2010, pp.8787. (RW 4317)

Bedard, J.C. & Biggs, S.F. "Pattern Recognition, Hypotheses Generation, and Auditor Performance in an Analytical Task," *The Accounting Review,* Vol. 66, No. 3, 1991, pp. 622. (RW 4273)

Bedford, D. "Agnotology as a Teaching Tool: Learning Climate Science by Studying Misinformation," Vol. 109, No. 4, 2010, pp. 159-165. (RW 5091)

Beebe, S.M. & Beebe, G.S. "Understanding the Non-Linear Event: A Framework for Complex Systems Analysis," *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 3, 2012, pp. 508-528. (RW 5730)

Beebe, S.M. & Pherson, R.H. *Cases in Intelligence Analysis: Structured Analytic Techniques in Action,* CQ Press College 2011. (RW 4952)

Beekman, C.S. & Baden, W.W. "Continuing the Revolution," in *Nonlinear Models for Archaeology and Anthropology: Continuing the Revolution*, eds. C.S. Beekman & W.W. Baden, Ashgate, Aldershot, England, 2005, pp. 1-12. (RW 5190)

Beersma, B. & De Dreu, Carsten K. W. "Conflict's Consequences: Effects of Social Motives on Postnegotiation Creative and Convergent Group Functioning and Performance," *Journal of Personality and Social Psychology*, Vol. 89, No. 3, 2005, pp. 358. (RW 1935)

Begbie, F. *Critical Thinking Disposition - Counts and Matters in Post-Registration SCPH Nurse Education*, The Higher Education Academy, York, UK, 2007. (RW 5034)

Begley, S. "I can't think!" *Newsweek,* [Online], Available from: http://www.newsweek.com/2011/02/27/i-can-t-think.html. February 27, 2011, (RW 4585)

Belenky, M.F. *Women's Ways of Knowing: The Development of Self, Voice, and Mind,* Basic Books, New York, 1986. (RW 4992)

Belkin, N.J. "The Cognitive Viewpoint in Information Science," *Journal of Information Science,* Vol. 16, No. 1, 1990, pp. 11. (RW 4399)

Belkin, N.J., Brooks, H.M. & Oddy, R.N. "ASK for Information Retrieval - Part I: Background and Theory," *Journal of Documentation,* Vol. 38, 1982, pp. 61. (RW 3414)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Belkin, N.J., Brooks, H.M. & Oddy, R.N. "ASK for Information Retrieval - Part II: Results of a Design Study," *Journal of Documentation,* Vol. 38, 1982, pp. 145. (RW 3415)

Belkin, N.J. & Croft, W.B. "Information Filtering and Information Retrieval: Two Sides of the Same Coin?" *Communications of the ACM,* Vol. 35, No. 12, 1992, pp. 29. (RW 1478)

Bell, B.S., Kozlowski, S.W.J. & Blawath, S. "Team Learning: A Theoretical Integration and Review," in *Oxford Handbook of Organizational Psychology*, ed. W.J. Kozlowski, Oxford University Press, New York, NY, 2012, (RW 5766)

Bell, C.G. & Gemmell, J. *Total Recall: How the E-Memory Revolution Will Change Everything,* Dutton, New York, NY, 2009. (RW 4124)

Bell, P. & Coyne, J.W. "The Role of Strategic Intelligence in Anticipating Transnational Organised Crime: A Literary Review " *International Journal of Law, Crime and Justice,* Vol. 39, 2011, pp. 60-78. (RW 5820)

Bell, P. & Linn, M.C. "Beliefs about Science: How does Science Instruction Contribute," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing*, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 321. (RW 4392)

Bendixen, L.D., Dunkle, M.E. & Schraw, G. "Epistemological Beliefs and Reflective Judgment," *Psychological Reports,* Vol. 75, 1994, pp. 1595. (RW 3718)

Bendixen, L.D. "A Process Model of Epistemic Belief Change," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing*, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 191. (RW 3983)

Bendixen, L.D. & Feucht, F.C. "Personal Epistemology in the Classroom: What does Research and Theory Tell Us and Where do we Need to Go Next?" in *Personal Epistemology in the Classroom: Theory, Research, and Implications for Practice*, eds. L.D. Bendixen & F.C. Feucht, Cambridge University Press, Cambridge, UK, 2010, pp. 555-586. (RW 5132)

Bendixen, L.D. & Rule, D.C. "An Integrative Approach to Personal Epistemology: A Guiding Model," *Educational Psychologist,* Vol. 39, No. 1, 2004, pp. 69. (RW 2857)

Bendor, J. & Hammond, T.H. "Choice-Theoretic Approaches to Bureaucratic Structure," in *Oxford Handbook of American Bureaucracy*, ed. R.F. Durant, Oxford University Press, New York, NY, 2010, pp. 638-665. (RW 4684)

Ben-Israel, I. "The Philosophy and Methodology of Intelligence: The Logic of the Estimate Process," *Intelligence and National Security,* Vol. 4, No. 4, 1989, pp. 660-718. (RW 1277)

Benjafield, J. "Evidence that "Thinking Aloud" Constitutes an Externalization of Inner Speech," *Psychonomic Science,* Vol. 15, No. 2, 1969, pp. 83-84. (RW 5842)

Benjamin, A.J., Riggio, R.E. & Mayes, B.T. "Reliability and Factor Structure of Budner's Tolerance for Ambiguity Scale," *Journal of Social Behavior and Personality,* Vol. 11, No. 3, 1996, pp. 625-632. (RW 5363)

Bennett, B. "DIA's Analytic Competency-Based Training," *American Intelligence Journal,* Vol. 26, No. 2, 2008/2009, pp. 25-29. (RW 3627)

Bennett, D.B. & Williams, P. "Name Authority Challenges for Indexing and Abstracting Databases," *Evidence Based Library and Information Practice,* Vol. 1, No. 1, 2006, pp. 37-57. (RW 4802)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Bennett, D. "How Impostors Like Clark Rockefeller Capture our Trust Instantly - and Why We're so Eager to Give it to them," *Boston Globe*, 2008, August 17, 2008. (RW 3238)

Bensley, A., Doyle, R., Lyon, L. & Robinson, S. *Basic Proficiencies in Critical Thinking*, Frostburg State University, Frostburg, MD, 2006. (RW 4036)

Benson, P.G., Curley, S.P. & Smith, G.F. "Belief Assessment: An Underdeveloped Phase of Probability Elicitation," *Management Science*, Vol. 41, No. 10, 1995, pp. 1639-1653. (RW 5291)

Bensoussan, B.E. & Fleisher, C.S. *Analysis without Paralysis: 10 Tools to make Better Strategic Decisions*, FT Press, Upper Saddle River, NJ, 2008. (RW 5852)

Ben-Zvi, A. *Surprise - a Comparative Study of Failures on Intelligence Prediction* 1975. (RW 1279)

Ben-Zvi, A. *Hindsight and Foresight: A Conceptual Framework for the Analysis of Surprise Attacks* 1976. (RW 1278)

Ben-Zvi, A. "The Dynamics of Surprise: The Defender's Perspective," *Intelligence and National Security*, Vol. 12, No. 4, 1997, pp. 113-144. (RW 102)

Bereiter, C. "Development in Writing," in *Cognitive Processes in Writing*, eds. L.W. Gregg & E.R. Steinberg, L. Erlbaum Associates, Hillsdale, NJ, 1980, pp. 73-93. (RW 1500)

Bereiter, C. & Scardamalia, M. *The Psychology of Written Composition*, L. Erlbaum Associates, Hillsdale, NJ, 1987. (RW 2013)

Berelson, B. *Content Analysis in Communication Research*, Hafner, New York, 1971; 1952. (RW 3879)

Bergen, B.K. *Louder than Words: The New Science of how the Mind Makes Meaning*, Basic Books, New York, NY, 2012. (RW 5905)

Berger, P.L. & Luckmann, T. *The Social Construction of Reality: A Treatise in the Sociology of Knowledge*, Anchor Books, New York, 1990. (RW 3880)

Bergman, M.K. *The Deep Web: Surfacing Hidden Value.* 2001. (RW 1400)

Berkenkotter, C. "Understanding a Writer's Awareness of Audience," *College Composition and Communication*, Vol. 32, No. 4, 1981, pp. 388-399. (RW 4480)

Berkowitz, B. "The R&D Future of Intelligence," *Issues in Science and Technology*, Vol. 24, No. 3, 2008, pp. 37-46. (RW 5619)

Berkowitz, B. "Reform of the Intelligence Community," *Orbis*, Vol. 40, No. 4, 1996, pp. 653-663. (RW 441)

Berkowitz, B. "The Big Difference between Intelligence and Evidence," *Washington Post*, February 2, 2003, p. 3. (RW 4535)

Berkowitz, B. "The DI and IT. Failing to Keep Up with the Information Revolution," *Studies in Intelligence*, Vol. 47, No. 1, 2003 (RW 4305)

Berkowitz, B. "Failing to Keep Up with the Information Revolution," *Studies in Intelligence*, Vol. 47, No. 1, 2003 (RW 1661)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Berkowitz, B. "Intelligence for the Homeland," *SAIS Review,* Vol. 24, No. 1, 2004, pp. 1-6. (RW 201)

Berkowitz, B. "We Collected a Little, and Assumed a Lot," *Washington Post,* February 1, 2004, pp. B01. (RW 1662)

Berkowitz, B. "U.S. Intelligence Estimates of Soviet Collapse: Reality and Perception," in *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics*, ed. F. Fukuyama, Brookings Institution Press, Washington, DC, 2007, pp. 29-41. (RW 4698)

Berkowitz, B. "Homeland Security Intelligence: Rationale, Requirements, and Current Status," in *Analyzing Intelligence: Origins, Obstacles, and Innovations*, eds. R.Z. George & J.B. Bruce, 2008, pp. 281. (RW 3110)

Berkowitz, B.D. "Intelligence in the Organizational Context: Coordination and Error in National Estimates." *Orbis,* Vol. 29, No. Fall, 1985, pp. 571-596. (RW 4430)

Berkowitz, B.D. "Information Age Intelligence," *Foreign Policy,* 103, 1996, pp. 35-50. (RW 31)

Berkowitz, B.D. "Information Technology and Intelligence Reform," *Orbis,* Vol. 41, No. 1, 1997, pp. 107-118. (RW 75)

Berkowitz, B.D. "The Secret Sharers," *Orbis,* Vol. 43, No. 3, 1999, pp. 511-519. (RW 73)

Berkowitz, B.D. *An Alternative View on the Future of U.S. Intelligence,* 2000. (RW 1438)

Berkowitz, B.D. "Better Ways to Fix US Intelligence," *Orbis,* Vol. 45, No. 4, 2001, pp. 609-619. (RW 72)

Berkowitz, B.D. "Intelligence Reform, the Third Act," *Orbis,* Vol. 45, No. 1, 2001, pp. 152-161. (RW 71)

Berkowitz, B.D. "US Intelligence Estimates of the Soviet Collapse: Reality and Perception," *International Journal of Intelligence and Counterintelligence,* Vol. 21, No. 2, 2008, pp. 237. (RW 2969)

Berkowitz, B.D. & Goodman, A.E. *Strategic Intelligence for American National Security,* Princeton University Press, Princeton, NJ, 1989. (RW 28)

Berkowitz, B.D. & Goodman, A.E. *Best Truth: Intelligence in the Information Age,* Yale University Press, New Haven, CT, 2000. (RW 658)

Berkowitz, P. *The Future of American Intelligence,* Hoover Institution Press, Stanford, CA, 2005. (RW 945)

Berlin, D.L. "Why Intelligence Estimates Won't Mislead Us Anymore," *Defense Intelligence Journal,* Vol. 3, No. 2, 1994, pp. 21-35. (RW 182)

Bernadette, B.M., Gadzella, M., Hogan, L., Masten, W., Stacks, J., Stevens, R. & Zascavage, V. "Reliability and Validity of Watson-Glaser Critical Thinking Appraisal - Forms for Different Academic Groups," *Journal of Instructional Psychology,* Vol. 33, No. 2, 2006, pp. 141-143. (RW 4090)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Bernard, R.M., Zhang, D., Abrami, P.C., Sicoly, F., Borokhovski, E. & Surkes, M.A. "Exploring the Structure of the Watson–Glaser Critical Thinking Appraisal: One Scale Or Many Subscales?" *Thinking Skills and Creativity,* Vol. 3, No. 1, 2008, pp. 15-22. (RW 3966)

Bernardo, A.B.I. "Exploring Epistemological Beliefs of Bilingual Filipino Preservice Teachers in the Filipino and English Languages," *Journal of Psychology*, Vol. 142, No. 2, 2008, pp. 193. (RW 5527)

Bernardo, A.B.I. "Exploring the Links between Social Axioms and the Epistemological Beliefs Held by Filipino Students." in *Psychological Aspects of Social Axioms: Understanding Global Belief Systems*, eds. K. Leung & M.H. Bond, Springer, New York, NY, 2009, pp. 163-176. (RW 5524)

Bernhardt, D.C. "'I Want it Fast, Factual, Actionable' - Tailoring Competitive Intelligence to Executives' Needs," *Long Range Planning,* Vol. 27, No. 1, 1994, pp. 12-24. (RW 101)

Bernhardt, W. *Bridging the Uncertainty Gap in Intelligence Analysis: A Framework for Systematic Risk and Threat Assessment,* DPhil dissertation, University of Pretoria, 2003. (RW 421)

Berninger, V.W., Fuller, F. & Whitaker, D. "A Process Model of Writing Development Across the Life Span," *Educational Psychology Review,* Vol. 8, No. 3, 1996, pp. 193. (RW 2078)

Berninger, V.W. & Swanson, H.L. "Modifying Hayes and Flower's Model of Skilled Writing to Explain Beginning and Developing Writing," in *Advances in Cognition and Educational Practice. Volume 2. Children's Writing: Toward a Process Theory of the Development of Skilled Writing*, ed. E.C. Butterfield, Jai, Greenwich, CT; London, 1994, pp. 57. (RW 2124)

Berninger, V.W. *Reading and Writing Acquisition: A Developmental Neuropsychological Perspective,* Brown & Benchmark Publishers, Madison, Wis., 1994. (RW 2158)

Berninger, V.W. *Past, Present, and Future Contributions of Cognitive Writing Research to Cognitive Psychology*, Psychology Press, New York, NY, 2012. (RW 5857)

Bernstein, R.R. "Gut Feelings and Intuition," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 145. (RW 3646)

Berryman, J.M. "Influences on the judgment of enough information: an analysis using the information use environment as a framework", *Information Research,* [Online], vol. 13, no. 4, paper 356. Available from: http://InformationR.net/ir/13-4/paper356.html. 2008. (RW 4786)

Besharov, G. *Second Best Considerations in Correcting Cognitive Biases*, Duke University Economics Working Paper No. 01-08, Duke University, Durham, NC, 2003. (RW 1946)

Besson, P.M. *The Goldwater-Nichols Act: A Ten Year Report Card*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1998. (RW 976)

Best, R.A. *Proposals for Intelligence Reorganization, 1949-1996. Appendix C.*, Congressional Research Service, Library of Congress, Washington, DC, 1996. (RW 289)

Best, R.A. *Intelligence Issues for Congress,* Congressional Research Service, Library of Congress, Washington, DC, 2003. (RW 288)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Best, R.A. *Intelligence Community Reorganization: Potential Effects on DOD Intelligence Agencies*, Congressional Research Service, Library of Congress, Washington, DC, 2004. (RW 285)

Best, R.A. *Intelligence Community Reorganization: Potential Effects on DOD Intelligence Agencies. Updated*, Congressional Research Service, Library of Congress, Washington, DC, 2004. (RW 290)

Best, R.A. *Intelligence Issues for Congress*, Congressional Research Service, Library of Congress, Washington, DC, 2004. (RW 287)

Best, R.A. *Proposals for Intelligence Reorganization, 1949-2004*, Congressional Research Service, Library of Congress, Washington, DC, 2004. (RW 286)

Best, R.A. *The Director of National Intelligence and Intelligence Analysis*, Congressional Research Service, Library of Congress, Washington, DC, 2005. (RW 284)

Best, R.A. *Intelligence Issues for Congress*, Congressional Research Service, Library of Congress, Washington, DC, 2005. (RW 1425)

Best, R.A. *Intelligence Estimates: How Useful to Congress?* Congressional Research Service, Library of Congress, Washington, DC, 2007. (RW 2906)

Best, R.A. *Intelligence Issues for Congress*, Congressional Research Service, Library of Congress, Washington, DC, 2007. (RW 2828)

Best, R.A. "What the Intelligence Community Got Right about Iraq," *Intelligence and National Security*, Vol. 23, No. 3, 2008, pp. 289. (RW 3169)

Best, R.A. "The Dilemma of Defense Intelligence," in *Oxford Handbook of National Security Intelligence*, ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 422-436. (RW 4712)

Best, R.A. *Intelligence Issues for Congress*, Congressional Research Service, Library of Congress, Washington, DC, 2010. (RW 4496)

Best, R.A. *The Intelligence Appropriations Process: Issues for Congress*, Congressional Research Service, Washington, DC, 2011. (RW 5242)

Best, R.A. & Bazan, E.B. *Intelligence Spending: Public Disclosure Issues*, Congressional Research Service, Library of Congress, Washington, DC, 2007. (RW 2171)

Best, R.A. & Cumming, A. *Open Source Intelligence (OSINT): Issues for Congress*, Congressional Research Service, Library of Congress, Washington, DC, 2007. (RW 2903)

Betts, R.K. *Soldiers, Statesmen, and Cold War Crises*, Harvard University Press, Cambridge, MA, 1977. (RW 705)

Betts, R.K. "Analysis, War, and Decision: Why Intelligence Failures are Inevitable," *World Politics*, Vol. 31, No. 2, 1978, pp. 61-89. (RW 157)

Betts, R.K. "Intelligence for Policymaking," *Washington Quarterly*, Vol. 3, No. 3, 1980, pp. 118-129. (RW 733)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Betts, R.K. "Strategic Intelligence Estimates: Let's make them Useful," *Parameters,* Vol. 10, No. 4, 1980, pp. 20-26. (RW 729)

Betts, R.K. "Surprise Despite Warning: Why Sudden Attacks Succeed," *Political Science Quarterly*, Vol. 95, No. 4, 1980-81, pp. 551-572. (RW 731)

Betts, R.K. "American Strategic Intelligence: Politics, Priorities and Direction," in *Intelligence Policy and National Security*, eds. R.L. Pfaltzgraff, U. Ra'anan & W. Milberg, Archon Books, Hamden, CT, 1981, pp. 245-267. (RW 912)

Betts, R.K. *Surprise Attack: Lessons for Defense Planning,* Brookings Institution, Washington, DC, 1982. (RW 20)

Betts, R.K. "Warning Dilemmas: Normal Theory Vs. Exceptional Theory," *Orbis,* Vol. 26, No. 4, 1983, pp. 828-833. (RW 732)

Betts, R.K. "Policymakers and Intelligence Analysts: Love, Hate Or Indifference?" *Intelligence and National Security,* Vol. 3, No. 1, 1988, pp. 184-189. (RW 730)

Betts, R.K. *Statement of Views on Senate 1003. Prepared for Testimony to the US Senate Select Committee on Intelligence, September 11, 1991* 1991. (RW 1225)

Betts, R.K. *Military Readiness: Concepts, Choices, Consequences,* Brookings Institution, Washington, DC, 1995. (RW 707)

Betts, R.K. "Intelligence Warning: Old Problems, New Agendas," *Parameters,* Vol. 28, No. 1, 1998, pp. 26-35. (RW 104)

Betts, R.K. "Intelligence Test: The Limits of Prevention," in *How did this Happen? Terrorism and the New War,* eds. J.F. Hoge & G. Rose, PublicAffairs, New York, 2001, pp. 145-161. (RW 780)

Betts, R.K. *The Next Intelligence Failure: The Limits of Prevention. Author's Final Draft.* 2001. (RW 1439)

Betts, R.K. "Fixing Intelligence," *Foreign Affairs,* Vol. 81, No. 1, 2002, pp. 43-59. (RW 1138)

Betts, R.K. "Politicization of Intelligence: Costs and Benefits," in *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel,* eds. M.I. Handel, R.K. Betts & T.G. Mahnken, Frank Cass, London, UK, 2003, pp. 59-79. (RW 216)

Betts, R.K. "The New Politics of Intelligence: Will Reforms Work this Time?" *Foreign Affairs,* Vol. 83, No. 3, 2004, pp. 2-8. (RW 195)

Betts, R.K. "How to Think about Terrorism," *Wilson Quarterly,* Winter, 2006, pp. 44. (RW 1256)

Betts, R.K. *Enemies of Intelligence: Knowledge and Power in American National Security,* Columbia University Press, New York, NY, 2007. (RW 2811)

Betts, R.K. "Analysis, War, and Decision: Why Intelligence Failures are Inevitable," in *Intelligence Theory: Key Questions and Debates,* eds. P. Gill, S. Marrin & M. Phythian, 2009, pp. 87. (RW 3407)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Bevan, P. *A Revolution in Intelligence Affairs? the Impact of the Internet on the British Intelligence Services*, University of Wales, Aberystwyth, Wales, 2001. (RW 320)

Bex, F., van den Braak, S., van Oostendorp, H., Prakken, H., Verheij, B. & Vreeswuk, G. "Sense-Making Software for Crime Investigation: How to Combine Stories and Arguments?" *Law, Probability, & Risk,* Vol. 6, 2007, pp. 145. (RW 4224)

Beyer, B.K. "Critical Thinking: What is it?" *Social Education,* Vol. 49, No. 4, 1985, pp. 270-276. (RW 4016)

Beyer, B.K. *Practical Strategies for the Teaching of Thinking,* Allyn and Bacon, Boston, MA, 1987. (RW 3697)

Beyer, B.K. "Practice is Not enough," in *Thinking Skills Instruction: Concepts and Techniques,* eds. M. Heiman & J. Slomianko, National Education Association, Washington, DC, 1987, pp. 77-86. (RW 5081)

Beyerstein, B.L. & Beyerstein, D.F. *The Write Stuff: Evaluations of Graphology, the Study of Handwriting Analysis,* Prometheus Books, Buffalo, N.Y, 1992. (RW 1874)

Bier, E.A., Card, S.K. & Bodnar, J.W. "Entity-Based Collaboration Tools for Intelligence Analysis", *IEEE Symposium on Visual Analytics Science and Technoloogy (IEEE VAST),* Columbus, OH, October 21 - 23, 2008, pp. 99-106. (RW 5689)

bier, E., Ishak, E. & Chi, E. "Entity Workspace: An Evidence File that Aids Memory, Inference, and Reading", *Proceedings of Intelligence and Security Informatics (ISI 2006),* May 23, 2006. (RW 5576)

Bieri, J. "Cognitive Complexity-Simplicity and Predictive Behavior," *Journal of Abnormal and Social Psychology,* Vol. 51, No. 2, 1955, pp. 263. (RW 4299)

Biernat, M. *Standards and Expectancies: Contrast and Assimilation in Judgments of Self and Others,* Psychology Press, New York, 2005. (RW 2022)

Bierstaker, J.L. & Wright, S. "A Research Note Concerning Practical Problem-Solving Ability as a Predictor of Performance in Auditing Tasks," *Behavioral Research in Accounting,* Vol. 13, 2001, pp. 49. (RW 4274)

Billett, S. "Learning through Practice," in *Learning through Practice: Models, Traditions, Orientations, and Approaches,* ed. S. Billett, Springer, Dordrecht, 2010, pp. 1-20. (RW 4953)

Billett, S. "The Practices of Learning through Occupations," in *Learning through Practice: Models, Traditions, Orientations, and Approaches,* ed. S. Billett, Springer, Dordrecht, 2010, pp. 59-81. (RW 4956)

Billett, S. "Learning Vocational Practice in Relative Social Isolation: The Epistemological and Pedagogic Practices of Small-Business Operators," in *Supporting Workplace Learning: Towards Evidence-Based Practice,* eds. R.F. Poell & M. van Woerkom, Springer, Dordrecht, 2011, pp. 147-164. (RW 4911)

Billett, S. & Henderson, A. "Promoting Professional Learning: Integrating Experiences in University and Practice Settings," in *Developing Learning Professionals,* eds. S. Billett & A. Henderson, Springer, Dordrecht, 2011, pp. 1-20. (RW 4902)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Bimfort, M.T. "A Definition of Intelligence," *Studies in Intelligence*, Vol. 2, No. 4, 1958, pp. 75-78. (RW 519)

Binder, D.A. & Bergman, P. *Fact Investigation: From Hypothesis to Proof,* West Pub., St. Paul, Minn., 1984. (RW 1324)

Birch, S. & Bloom, P. "The Curse of Knowledge in Reasoning about False Beliefs," *Psychological Science*, Vol. 18, No. 5, 2007, pp. 382. (RW 3551)

Birnbaum, L., Forbus, K.D., Wagner, E., Baker, J. & Witbrock, M. "Analogy, Intelligent IR, and Knowledge Integration for Intelligence Analysis," 2005 *AAAI Spring Symposium on AI Technologies for Homeland Security,* Stanford, CA, March 21-23, 2005 (RW 6)

Biros, D.P., George, J.F. & Zmud, R.W. "Inducing Sensitivity to Deception in Order to Improve Decision Making Performance: A Field Study," *MIS Quarterly*, Vol. 26, No. 2, 2002, pp. 119-144. (RW 323)

Bisantz, A.M. & Burns, C.M. *Applications of Cognitive Work Analysis,* CRC Press, Boca Raton, 2009. (RW 3621)

Bishop, J.E. "Stroke Patients Yield Clues to Brain's Ability to Create Language," *Wall Street Journal*, October 12, 1993, pp. A1. (RW 1358)

Bixler, D. & Moldovan, D. "SYNERGIST: An Analyst's Assistant," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 873)

Bixler, D., Moldovan, D. & Fowler, A. "Using Knowledge Extraction and Maintenance Techniques to Enhance Analytical Performance", 2-8 May 2005. (RW 4913)

Bjork, R.A. "Assessing our Own Competence: Heuristics and Illusions," in *Attention and Performance XVII: Cognitive Regulation of Performance: Interaction of Theory and Application*, eds. D. Gopher & A. Koriat, MIT Press, Cambridge, MA, 1999, pp. 435. (RW 2481)

Bjork, R.A. "Structuring the Conditions of Training to Achieve Elite Performance: Reflections on Elite Training Programs and Related Themes in Chapters 10-13," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 312-329. (RW 5147)

Bjorneborn, L. "Serendipity dimensions and users' information behaviour in the physical library interface", *Information Research*, [Online], vol. 13, no. 4, paper 370. Available from: http://InformationR.net/ir/13-4/paper370.html. 2008, (RW 4788)

Black, A.C. & McCoach, D.B. "Validity Study of the Thinking Styles Inventory," *Journal for the Education of the Gifted,* Vol. 32, No. 8, 2008, pp. 180-276. (RW 3511)

Black, J.B. & Bower, G.H. "Story Understanding as Problem-Solving," *Poetics,* Vol. 91980, pp. 223. (RW 2856)

Black, M. *Critical Thinking; an Introduction to Logic and Scientific Method,* Prentice-Hall, New York, 1946. (RW 3806)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Black, M. *Critical Thinking: An Introduction to Logic and Scientific Method*, 2nd ed., Prentice-Hall, New York, NY, 1952. (RW 3805)

Blackmore, S.J. *The Meme Machine,* Oxford University Press, Oxford, UK, 1999. (RW 5850)

Blackmore, S.J. *Consciousness: An Introduction,* 2nd ed., Oxford Univeristy Press, New York, NY, 2012. (RW 5888)

Blair, B.G. "The Logic of Intelligence Failure", *10th International Castiglioncello Conference "Unilateral Actions and Military Interventions: The Future of Non-Proliferation",* Castiglioncello, Italy, September 18-21, 2003 (RW 581)

Blair, B.G. "The Logic of Intelligence Hype and Blindness", *10th International Castiglioncello Conference "Unilateral Actions and Military Interventions: The Future of Non-Proliferation",* Castiglioncello, Italy, Sept. 18-21, 2003 (RW 580)

Blair, C. "How Similar are Fluid Cognition and General Intelligence? A Developmental Neuroscience Perspective on Fluid Cognition as an Aspect of Human Cognitive Ability," *Behavioral and Brain Sciences,* Vol. 29, 2006, pp. 109. (RW 3341)

Blair, D.C. "Full Text Retrieval: Evaluation and Implications," *International Journal of Classification,* Vol. 13, No. 1, 1986, pp. 18-23. (RW 956)

Blair, D.C. *Language and Representation in Information Retrieval,* Elsevier Science Publishers, Amsterdam, 1990. (RW 955)

Blair, D.C. "STAIRS Redux: Thoughts on the STAIRS Evaluation. Ten Years After," *Journal of the American Society for Information Science,* Vol. 47, No. 1, 1996, pp. 2-22. (RW 957)

Blair, D.C. & Maron, M.E. "An Evaluation of Retrieval Effectiveness for a Full-Text Document Retrieval System," *Communications of the ACM,* Vol. 28, No. 3, 1985, pp. 289-299. (RW 670)

Blair, D.C. & Maron, M.E. "Full Text Retrieval: Further Analysis and Clarification," *Information Processing and Management,* Vol. 26, No. 3, 1990, pp. 437-447. (RW 959)

Blair, D.C. *Strengthening our Nation's Front Line of Defense* 2009. (RW 3827)

Blair, D.C. *Annual Threat Assessment of the US Intelligence Community for the Senate Select Committee on Intelligence. Statement for the Record.* 2010. (RW 3874)

Blake, R.R. & Mouton, J.S. *Making Experience Work: The Grid® Approach to Critique,* McGraw-Hill, New York, 1978. (RW 2776)

Blakeslee, S. & Blakeslee, M. *The Body has a Mind of its Own,* 2007. (RW 1708)

Blanchette, I. & Dunbar, K. "How Analogies are Generated: The Roles of Structural and Superficial Similarity," *Memory & Cognition,* Vol. 28, No. 1, 2000, pp. 108. (RW 1817)

Blanchette, I. & Dunbar, K. "Analogy use in Naturalistic Settings: The Influence of Audience, Emotion, and Goals," *Memory & Cognition,* Vol. 29, No. 5, 2001, pp. 730. (RW 1818)

Blanchette, I. & Dunbar, K. "Representational Change and Analogy: How Analogical Inferences Alter Target Representations," *Journal of Experimental Psychology: Learning, Memory, & Cognition,* Vol. 28, No. 4, 2002, pp. 672. (RW 1799)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Blanck, P.D. "What Empirical Research Tells Us: Studying Judges' and Juries' Behavior," *American University Law Review,* Vol. 40, pp. 775. (RW 2041)

Bland, D.F., Camacho, E. & Moorhead, L.B. "Knowledge Development in the United States Africa Command," *American Intelligence Journal,* Vol. 27, No. 1, 2009, pp. 23. (RW 3986)

Blank, H., Musch, J. & Pohl, R.F. "Hindsight Bias: On being Wise After the Event," *Social Cognition,* Vol. 25, No. 1, 2007, pp. 1. (RW 2442)

Blank, H. & Nestler, S. "Cognitive Process Models of Hindsight Bias," *Social Cognition,* Vol. 25, No. 1, 2007, pp. 132. (RW 2449)

Blank, S. "Soldiers Pay in Blood," *Asia Times Online,* July 17, 2003. (RW 603)

Blanken, L. & Overbaugh, J. "Looking for Intel? ..Or Looking for Answers? Reforming Military Intelligence for a Counterinsurgency Environment," *Intelligence and National Security,* Vol. 27, No. 4, 2012, pp. 559-575. (RW 5813)

Blas, A.K. "Intelligence in Afghanistan: Why is it Hard," *American Intelligence Journal,* Vol. 27, No. 1, 2009, pp. 49. (RW 3989)

Bleicher, J. *Contemporary Hermeneutics: Hermeneutics as Method, Philosophy, and Critique,* Routledge & Kegan Paul, London; Boston, 1980. (RW 2670)

Bloch, M. *The Historian's Craft,* Vintage, New York, NY, 1964. (RW 5189)

Bloom, B.S. *Taxonomy of Educational Objectives: The Classification of Educational Goals,* D. McKay, New York, NY, 1956. (RW 3849)

Bloom, J.W. "Contexts of Meaning and Conceptual Integration: How Children Understand and Learn," in *Philosophy of Science, Cognitive Psychology, and Educational Theory and Practice,* eds. R.A. Duschl & R.J. Hamilton, State University of New York Press, Albany, 1992, pp. 177-194. (RW 5480)

Bloom, B.S., Anderson, L.W. & Krathwohl, D.R. *A Taxonomy for Learning, Teaching, and Assessing: A Revision of Bloom's Taxonomy of Educational Objectives,* Longman, New York, NY, 2001. (RW 5523)

Blossfeld, H. *Techniques of Event History Modeling: New Approaches to Causal Analysis*, 2nd ed., L. Erlbaum Associates, Mahwah, NJ, 2002. (RW 5373)

Blossfeld, H. & Rohwer, G. *Techniques of Event History Modeling: New Approaches to Causal Analysis,* 2nd ed., L. Erlbaum Associates, Mahwah, NJ, 2002. (RW 5184)

Blum, R.H. *Surveillance and Espionage in a Free Society: A Report by the Planning Group on Intelligence and Security to the Policy Council of the Democratic National Committee,* Praeger, New York, NY, 1972. (RW 1098)

Blume, M. "Automatic Entity Disambiguation: Benefits to NER, Relation Extraction, Link Analysis, and Inference," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 593)

Blute, M. & Armstrong, P. "The Reinvention of Grand Theories of the scientific/scholarly Process," *Perspectives on Science,* Vol. 19, No. 4, 2011, pp. 391-425. (RW 5191)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Boal, K.B. & Hooijberg, R. "Strategic Leadership Research: Moving on," *Leadership Quarterly*, Vol. 11, No. 4, 2000, pp. 515. (RW 3050)

Boba, R. *Problem Analysis in Policing*, Police Foundation, Washington, DC, 2003. (RW 2632)

Bobrow, D.G. & Collins, A. *Representation and Understanding: Studies in Cognitive Science*, Academic Press, New York, 1975. (RW 2963)

Bodnar, J.W. *Warning Analysis for the Information Age: Rethinking the Intelligence Process*, Joint Military Intelligence College, Washington, DC, 2003. (RW 772)

Boes, L.M., Baxter Magolda, M.B. & Buckley, J.A. "Foundational Assumptions and Constructive-Developmental Theory," in *Development and Assessment of Self-Authorship: Exploring the Concept Across Cultures*, eds. M.B. Baxter Magolda, E.G. Creamer & P.S. Meszaros, Stylus Pub., Sterling, VA, 2010, pp. 3-24. (RW 4676)

Boice, R. *Procrastination and Blocking: A Novel, Practical Approach*, Praeger, Westport, Conn, 1996. (RW 1863)

Boicu, M., Marcu, D., Tecuci, G. & Schum, D. "Cognitive Assistants for Evidence-Based Reasoning Tasks", *Advances in Cognitive Systems: 2011 AAAI Fall Symposium*, Arlington, VA, November 4-6, 2011 (RW 5546)

Boicu, M., Tecuci, G., Ayers, C., Marcu, D., Boicu, C., Barbulescu, M., Stanescu, B., Wagner, W., Le, V., Apostolova, D. & Ciubotariu, A. "A Learning and Reasoning System for Intelligence Analysis", *Proceedings of the Twentieth National Conference on Artificial Intelligence*, Pittsburgh, PA, 9-13 July, 2005 (RW 4755)

Boicu, M., Tecuci, G. & Schum, D. "Intelligence Analysis Ontology for Cognitive Assistants", *Proceedings of the Third International Ontology for the Intelligence Community Conference OIC-2008*, Fairfax, VA, December 3-4, 2008, pp.3131-35. (RW 4828)

Boisot, M. "Intelligent Learning", *New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities*, Rome, Italy, 31 March - 2 April, 2004, pp.153153-168. (RW 4668)

Boldareva, L., de Vries, A.P. & Hiemstra, D. *Monitoring User-System Performance in Interactive Retrieval Tasks* (RW 1502)

Bolhuis, J.J. & Wynne, C.D.L. "Can Evolution Explain how Minds Work?" *Nature*, Vol. 458, 2009, pp. 832. (RW 3454)

Bonnefon, J. "How do Individuals Solve the Doctrinal Paradox in Collective Decisions? an Empirical Investigation," *Psychological Science*, Vol. 18, No. 9, 2007, pp. 753. (RW 2812)

Bonner, S.E. & Pennington, N. "Cognitive Processes and Knowledge as Determinants of Auditor Expertise," *Journal of Accounting Literature*, Vol. 10, 1991, pp. 1-50. (RW 4618)

Bonner, S.E. & Sprinkle, G.B. "The Effects of Monetary Incentives on Effort and Task Performance: Theories, Evidence, and a Framework for Research," *Accounting, Organizations, and Society*, Vol. 27, No. 4-5, 2002, pp. 303-345. (RW 4662)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Bonner, S.E. "Judgment and Decision-Making Research in Accounting," *Accounting Horizons,* Vol. 13, No. 4, 1999, pp. 385. (RW 4272)

Bonthous, J. "Understanding Intelligence Across Cultures," *International Journal of Intelligence and Counterintelligence,* Vol. 7, No. 3, 1995, pp. 275-311. (RW 185)

Boonstra, O., Breure, L. & Doorn, P. *Past, Present, and Future of Historical Information Science,* Amsterdam, 2004. (RW 5179)

Booth, W.C. *The Craft of Research,* 3rd ed., University of Chicago Press, Chicago, 2008. (RW 3114)

Bootzin, R.R., Kihlstrom, J.F. & Schacter, D.L. *Sleep and Cognition,* American Psychological Association, Washington, DC, 1990. (RW 1953)

Bor, D. *The Ravenous Brain: How the New Science of Consciousness Explains our Insatiable Search for Meaning,* Basic Books, New York, 2012. (RW 5906)

Boraas, J. *Teaching to Think,* Macmillan, New York, NY, 1922. (RW 4462)

Borel, P.A. "On Processing Intelligence Information," *Studies in Intelligence,* Vol. 3, No. 1, 1959, pp. 25-35. (RW 546)

Boren, D. & Perkins, E.J. *Preparing America's Foreign Policy for the 21st Century,* University of Oklahoma Press, Norman, OK, 1999. (RW 30)

Borgman, C.L. "The User's Mental Model of an Information Retrieval System: An Experiment on a Prototype Online Catalog," *International Journal of Man Machine Studies,* Vol. 24, 1986, pp. 47. (RW 1354)

Borkan, J. "Immersion/crystallization," in *Doing Qualitative Research,* eds. B.F. Crabtree & W.L. Miller, 2nd ed., Sage Publications, Thousand Oaks, CA, 1999, pp. 179-194. (RW 2506)

Borman, W.C., Hanson, M.A. & Hedge, J.W. "Personnel Selection," *Annual Review of Psychology,* Vol. 48, 1997, pp. 299. (RW 1962)

Born, H. & Wetzling, T. "Intelligence Accountability: Challenges for Parliaments and Intelligence Services," in *Handbook of Intelligence Studies,* ed. L.K. Johnson, 2007, pp. 315. (RW 2477)

Bors, D.A. & Forrin, B. "Age, Speed of Information Processing, Recall, and Fluid Intelligence," *Intelligence,* Vol. 20, No. 3, 1995, pp. 229-248. (RW 903)

Boscarino, C., de Vries, A. & Alink, W. "Search for Journalists: New York Times Challenge Report", *HCIR 2010: Proceedings of the Fourth Workshop on Human-Computer Interaction and Information Retrieval,* New Brunswick, NJ, August 22, 2010, pp.3232. (RW 4322)

Boscarino, C., de Vries, A. & van Ossenbruggen, J. "Better Search Applications through Domain Specific Context Descriptions: A Position Paper", *HCIR 2010: Proceedings of the Fourth Workshop on Human-Computer Interaction and Information Retrieval,* New Brunswick, NJ, August 22, 2010, pp.9191. (RW 4324)

Boschee, E., Weischedel, R. & Zamanian, A. "Automatic Information Extraction," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 825)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Boscolo, P. "Change as a Process and a Disposition: A Commentary," in *Reconsidering Conceptual Change: Issues in Theory and Practice*, eds. M. Limón & L. Mason, Kluwer Academic, Dordrecht, 2002, pp. 415-419. (RW 5008)

Boshuizen, H.P.A. "Teaching for Expertise: Problem-Based Methods in Medicine and Other Professional Domains," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 379-404. (RW 5150)

Boslough, M. "A Distributed Dynamic Intelligence Aggregation Method," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 800)

Bosse, T., Hoogendoorn, M., Klein, M., van Lambalgen, R., van Maanen, P. & Treur, J. "Incorporating Human Aspects in Ambient Intelligence and Smart Environments," in *Handbook of Research on Ambient Intelligence and Smart Environments: Trends and Perspectives*, eds. N. Chong & F. Mastrogiovanni, IGIGlobal, Hershey, PA, 2011, pp. 128-164. (RW 5510)

Bost, A. *The Need for Cognition Scale*, Wabash College. Available: http://www.liberalarts.wabash.edu/ncs/, Viewed: July 12, 2011. (RW 5308)

Botluk, D. *Exposing the Invisible Web* 1999. (RW 1413)

BouJaoude, S. *Epistemology and Sociology of Science According to Lebanese Educators and Students*, 1996. (RW 5494)

Bourdin, B. & Fayol, M. "Is Written Language Production More Difficult than Oral Language Production? A Working Memory Approach," *International Journal of Psychology*, Vol. 29, No. 5, 1994, pp. 591. (RW 2075)

Bourdin, B. & Fayol, M. "Even in Adults, Written Production is Still More Costly than Oral Production," *International Journal of Psychology*, Vol. 37, No. 4, 2002, pp. 219. (RW 2074)

Bouyssou, D. *Evaluation and Decision Models with Multiple Criteria: Stepping Stones for the Analyst*, Springer Science+Business Media, New York, 2006. (RW 2556)

Bovens, M.A.P. & Hart, P. *Understanding Policy Fiascoes*, Transaction Publishers, New Brunswick, NJ, 1996. (RW 4409)

Bovey, R. "The Quality of Intelligence Analysis," *American Intelligence Journal*, Vol. 3, No. 4, 1980-81, pp. 6. (RW 1555)

Bowell, T. & Kemp, G. *Critical Thinking: A Concise Guide*, 2nd ed., Routledge, London, UK, 2005. (RW 3939)

Bowen, B.L. "Concept Maps: Tools to Enhance Executive and Team Effectiveness," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge*, eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 67-92. (RW 4967)

Bowen, W. "Open-Source Intel: A Valuable National Security Resource," *Jane's Intelligence Review*, Vol. 11, No. 11, 1999, pp. 50-54. (RW 206)

Bower, G.H. & Morrow, D.G. "Mental Models in Narrative Comprehension," *Science*, Vol. 247, No. 4938, 1990, pp. 44. (RW 1322)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Bowers, F. & Grier, P. "Major Work Left to Fix US Intelligence," *Christian Science Monitor*, Vol. 97, No. 89, 2005, pp. 1. (RW 354)

Bowman, J. "Is Stupid Making Us Google?" *The New Atlantis,* Summer, 2008 (RW 3270)

Boy, G.A. "Knowledge Management for Product Maturity", *K-Cap '05,* Banff, Alberta, Canada, October 2-5, 2005, pp.4343. (RW 1523)

Boyd, C.G. *Statement before the Senate Select Committee on Intelligence* 2004. (RW 314)

Boyes, M.C. & Chandler, M. "Cognitive Development, Epistemic Doubt, and Identity Formation in Adolescence," *Journal of Youth and Adolescence,* Vol. 21, No. 3, 1992, pp. 277-304. (RW 4942)

Boyles, S. *The Psychology of the Undecided Voter,* (RW 3231)

Bozeman, A.B. *Strategic Intelligence & Statecraft: Selected Essays*, Brassey's US, Washington, DC, 1992. (RW 211)

Bracken, P. *Intelligence and Risk Management* 2008. (RW 3378)

Bradford, R. *Why LSI? The Case for Latent Semantic Indexing in Government*, Agilex, Chantilly, VA, 2011. (RW 5565)

Bradley, P.G. *Market Garden: Was Intelligence Responsible for the Failure?*Air War College, Air University, Maxwell AFB, AL, 2001. (RW 475)

Brady, C. "Intelligence Failures: Plus Ca Change," *Intelligence and National Security,* Vol. 8, No. 4, 1993, pp. 86-96. (RW 4854)

Brady, H.E., Collier, D. & Seawright, J. "Refocusing the Discussion of Methodology." in *Rethinking Social Inquiry, Diverse Tools, Shared Standards*, eds. H.E. Brady & D. Collier, Rowman & Littlefield, Lanham, Md., 2004, pp. 3-20. (RW 5753)

Brady, H.E. *Rethinking Social Inquiry: Diverse Tools, Shared Standards,* Rowman & Littlefield, Lanham, 2004. (RW 3123)

Brady, H.E., Collier, D. & Seawright, J. "Refocusing the Discussion of Methodology," in *Rethinking Social Inquiry: Diverse Tools, Shared Standards*, eds. H.E. Brady & D. Collier, Rowman & Littlefield, Lanham, Md, 2004, pp. 3. (RW 2106)

Brafman, O. & Brafman, R. *Sway: The Irresistible Pull of Irrational Behavior,* Currency Books/Doubleday, New York, 2008. (RW 3141)

Brand, A.G. *The Psychology of Writing: The Affective Experience,* Greenwood Press, New York, 1989. (RW 1848)

Brand, A.G. & Graves, R.L. *Presence of Mind: Writing and the Domain Beyond the Cognitive,* Boynton/Cook Pub, Portsmouth, NH, 1994. (RW 1846)

Brandstein, A.G. & Horne, G.E. "Data Farming: A Meta-Technique for Research in the 21st Century," in *Maneuver Warfare Science 1998* 1998, pp. 93-99. (RW 432)

Branigan, E. *Narrative Comprehension and Film,* Routledge, London; New York, 1992. (RW 1365)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Brannon, R.B. *Human Intelligence,* Center for Information Policy Research. Harvard University, Cambridge, MA, 2002. (RW 1145)

Bransford, J.D. & Schwartz, D.L. "It Takes Expertise to make Expertise: Some Thoughts about Why and how and Reflections on the Themes in Chapters 15-18," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments,* ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 432-448. (RW 5152)

Bransford, J.D., Sherwood, R.D. & Sturdevant, T. "Teaching Thinking and Problem Solving," in *Teaching Thinking Skills: Theory and Practice,* eds. J.B. Baron & R.J. Sternberg, Freeman, New York, NY, 1987, pp. 162-181. (RW 3741)

Brase, G.L. & Shanteau, J. "The Unbearable Lightness of "Thinking": Moving Beyond Simple Concepts of Thinking, Rationality, and Hypothesis Testing," *Behavioral and Brain Sciences,* Vol. 34, No. 5, 2011, pp. 250-251. (RW 5485)

Brasfield, A.D. *Forecasting Accuracy and Cognitive Bias in the Analysis of Competing Hypotheses,* M. S. thesis, Mercyhurst College, 2009. (RW 4250)

Brassard, M. & Ritter, D. "Conducting Effective Meetings," in *A Handbook of the Psychology of Intelligence Analysis,* ed. R.L. Rees, 2008, pp. 423. (RW 3667)

Brassard, M. & Ritter, D. "Team Guidelines," in *A Handbook of the Psychology of Intelligence Analysis,* ed. R.L. Rees, 2008, pp. 419. (RW 3666)

Braten, I. & Strømsø, H.I. "Epistemological Beliefs and Implicit Theories of Intelligence as Predictors of Achievement Goals," *Contemporary Educational Psychology,* Vol. 29, No. 4, 2004, pp. 371. (RW 4280)

Braten, I., Strømsø, H.I. & Samuelstuen, M.S. "Are Sophisticated Students always Better? The Role of Topic-Specific Personal Epistemology in the Understanding of Multiple Expository Texts," *Contemporary Educational Psychology,* Vol. 33, 2008, pp. 814-840. (RW 5065)

Braten, I. "Personal Epistemology, Understanding of Multiple Texts, and Learning within Internet Technologies," in *Knowing, Knowledge and Beliefs: Epistemological Studies Across Diverse Cultures,* ed. M.S. Khine, Springer, Dordrecht, 2008, pp. 351-376. (RW 4356)

Braten, I. & Strømsø, H.I. "Constructing Meaning from Multiple Information Sources as a Function of Personal Epistemology: The Role of Text-Processing Strategies." *Information Design Journal,* Vol. 14, No. 1, 2006, pp. 56-67. (RW 5225)

Bråten, I. & Strømsø, H.I. "The Relationship between Epistemological Beliefs, Implicit Theories of Intelligence, and Self-Regulated Learning among Norwegian Postsecondary Students," *British Journal of Educational Psychology,* Vol. 75, No. 4, 2005, pp. 539-565. (RW 5197)

Bråten, I. & Strømsø, H.I. "Effects of Personal Epistemology on the Understanding of Multiple Texts," *Reading Psychology,* Vol. 27, No. 5, 2006, pp. 457-484. (RW 5198)

Bråten, I. & Strømsø, H.I. "Epistemological Beliefs, Interest, and Gender as Predictors of Internet-Based Learning Activities," *Computers in Human Behavior,* Vol. 22, No. 6, 2006, pp. 1027-1042. (RW 5203)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Braten, I., Strømsø, H.I. & Samuelstuen, M.S. "The Relationship between Internet-Specific Epistemological Beliefs and Learning within Internet Technologies," *Journal of Educational Computing Research,* Vol. 33, No. 2, 2005, pp. 141-171. (RW 5199)

Brauer, M., Chambres, P., Niedenthal, P.M. & Chatard-Pannetier, A. "The Relationship between Expertise and Evaluative Extremity: The Moderating Role of Experts' Task Characteristics," *Journal of Personality and Social Psychology,* Vol. 86, No. 1, 2004, pp. 5. (RW 1917)

Breckenridge, J.G. "Designing Effective Teaching and Learning Environments for a New Generation of Analysts," in *A Handbook of the Psychology of Intelligence Analysis,* ed. R.L. Rees, CENTRA Technology, Burlington, MA, [in press], pp. 322-341. (RW 3655)

Breckenridge, J.G. "Designing Effective Teaching and Learning Environments for a New Generation of Analysts," *International Journal of Intelligence and Counterintelligence,* Vol. 23, No. 2, 2010, pp. 307-323. (RW 3898)

Breeding, M. "How we Funneled Searchers from Google to our Collections by Catering to Web Crawlers," *Computers in Libraries,* Vol. 26, No. 4, 2006, pp. 22. (RW 1395)

Breetvelt, I., van den Bergh, H. & Rijlaarsdam, G. "Rereading and Generating and their Relation to Text Quality. an Application of Multilevel Analysis on Writing Process Data," in *Theories, Models and Methodology in Writing Research,* eds. G. Rijlaarsdam, H. van den Bergh & M. Couzijn, Amsterdam University Press, Amsterdam, 1996, pp. 10. (RW 2130)

Brei, W.S. *Getting Intelligence Right: The Power of Logical Procedure,* Joint Military Intelligence College, Washington, DC, 1996. (RW 661)

Breisach, E. *Historiography: Ancient, Medieval, & Modern,* University of Chicago Press, Chicago, 1983. (RW 3206)

Brenner, J.F. *Intelligence, Thinking, and Academia* 2007. (RW 2731)

Brenner, J. *America the Vulnerable: Inside the New Threat Matrix of Digital Espionage, Crime, and Warfare,* Penguin Press, New York, NY, 2011. (RW 5521)

Brettle, A. "Systematic Reviews and Evidence Based Library and Information Practice," *Evidence Based Library and Information Practice,* Vol. 4, No. 1, 2009, pp. 43-50. (RW 4799)

Breuning, M. "Configuring Issue Areas: Belgian and Dutch Representations of the Role of Foreign Assistance in Foreign Policy," in *Problem Representation in Foreign Policy Decision Making,* eds. D.A. Sylvan & J.F. Voss, 1998, pp. 303-332. (RW 1613)

Brewer, W.F. & Lambert, B.L. "The Theory-Ladenness of Observation and the Theory-Ladenness of the Rest of the Scientific Process," *Philosophy of Science,* Vol. 68, 2001, pp. S176. (RW 4307)

Brewer, W.F. & Schommer-Aikins, M. "Scientists are Not Deficient in Mental Imagery: Galton Revised," *Review of General Psychology,* Vol. 10, 2006, pp. 130. (RW 4296)

Brewer, W.F. & Nakamura, G.V. "The Nature and Function of Schemas," in *Handbook of Social Cognition,* eds. R.S. Wyer & T.K. Srull, L. Erlbaum Associates, Hillsdale, NJ, 1984, pp. 119. (RW 1840)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Briggs, C.A. *CIA Paths Toward the Information Highway*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1998. (RW 977)

Briggs, J.P. & Briggs, J.P.I. *Bush and the Psychology of Incompetent Decisions*. Available: http://www.truthout.org/docs_2006/011807J.shtml, (RW 2105)

Bright, J.R., Schoeman, M.E. & Industrial Management Center *A Guide to Practical Technological Forecasting*, Prentice-Hall, Englewood Cliffs, NJ, 1972. (RW 3212)

Britton, B.K. "Rewriting: The Arts and Sciences of Improving Expository Instructional Text," in *The Science of Writing: Theories, Methods, Individual Differences, and Applications*, eds. C.M. Levy & S.E. Ransdell, 1996, pp. 323. (RW 1826)

Brodie, R. *Virus of the Mind: The New Science of the Meme*, Integral Press, Seattle, WA, 1996. (RW 4512)

Brodzinsky, D.M. "On the Relationship between Cognitive Styles and Cognitive Structures," in *Moderators of Competence*, eds. E.D. Neimark, R. De Lisi & J.L. Newman, L. Erlbaum Associates, Hillsdale, NJ, 1985, pp. 147-174. (RW 5097)

Broessel, P., Eder, A., Huber, F. & Zinke, A. "Formal Epistemology Research Group at the University of Konstanz, Germany," *The Reasoner*, Vol. 2, No. 8, 2008, pp. [unpaged]. (RW 5264)

Bromme, R., Rambow, R. & Nueckles, M. "Expertise and Estimating what Other People Know: The Influence of Professional Experience and Type of Knowledge," *Journal of Experimental Psychology: Applied*, Vol. 7, No. 4, 2001, pp. 317. (RW 4284)

Bromme, R. "Thinking and Knowing about Knowledge," in *Activity and Sign: Grounding Mathematics Education*, eds. M. Hoffmann, J. Lenhard & F. Seeger, Springer, New York, 2005, pp. 191. (RW 2862)

Bromme, R., Kienhues, D. & Porsch, T. "Who Knows what and Who can we Believe? Epistemological Beliefs are Beliefs about Knowledge (mostly) to be Attained from Others," in *Personal Epistemology in the Classroom: Theory, Research, and Implications for Practice*, eds. L.D. Bendixen & F.C. Feucht, Cambridge University Press, Cambridge, UK, 2010, pp. 163-193. (RW 5127)

Bromme, R., Kienhues, D. & Stahl, E. "Knowledge and Epistemological Beliefs: An Intimate but Complicate Relationship," in *Knowing, Knowledge and Beliefs: Epistemological Studies Across Diverse Cultures*, ed. M.S. Khine, Springer, Dordrecht; London, 2008, pp. 423-441. (RW 4358)

Bromme, R., Pieschl, S. & Stahl, E. "Epistemological Beliefs are Standards for Adaptive Learning: A Functional Theory about Epistemological Beliefs and Metacognition," *Metacognition and Learning*, Vol. 5, No. 1, 2010, pp. 7-26. (RW 4834)

Bronson, P. *How Not to Talk to Your Kids. the Inverse Power of Praise.* Available: http://nymag.com/new/features/27840/. (RW 2103)

Brookfield, S. *Developing Critical Thinkers: Challenging Adults to Explore Alternative Ways of Thinking and Acting*, Jossey-Bass, San Francisco, CA, 1987. (RW 3814)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Brookings Institution *Prospects for the US Intelligence Community: The Hayden Nomination, Electronic Surveillance, and the Question of Reform. Includes Transcript of Question and Answer Session.* 2006. (RW 1505)

Brooks, D. "The CIA: Methods and Madness," *New York Times,* February 3, 2004. (RW 3233)

Brooks, D. "A Partnership of Minds," *New York Times,* 2007. (RW 2723)

Brooks, D. "The Behavioral Revolution," *The New York Times,* October 28, 2008. (RW 3342)

Brooks, D. "The Social Animal," *The New York Times,* September 12, 2008. (RW 3255)

Brooks, T.A. "Did Intelligence Fail Us?" *Proceedings of the United States Naval Institute,* Vol. 127, No. 10, 2001, pp. 54-55. (RW 295)

Brooks-Harris, J.E. & Stock-Ward, S.R. *Workshops: Designing and Facilitating Experiential Learning,* Sage Publications, Thousand Oaks, CA, 1999. (RW 4883)

Broome, R. & Gouveia, W. "Mind the Gap: National Security and Resilience - a Tough Balancing Act," *American Intelligence Journal,* Vol. 26, No. 2, 2008/2009, pp. 38. (RW 3629)

Broomfield, J. *Other Ways of Knowing: Recharting our Future with Ageless Wisdom,* Inner Traditions, Rochester, Vt., 1997. (RW 3262)

Brown, D.C. "Another View of S&T Analysis," *Studies in Intelligence,* Vol. 19, No. 2, 1975, pp. 25-28. (RW 523)

Brown, H. & Rudman, W.B. *Preparing for the 21st Century: An Appraisal of US Intelligence,* US GPO, Washington, DC, 1996. (RW 652)

Brown, J.S., Collins, A. & Duguid, P. "Situated Cognition and the Culture of Learning," *Educational Researcher,* Vol. 18, 1989, pp. 32. (RW 2429)

Brown, J.S. "Balancing Act: How to Capture Knowledge without Killing it," *Harvard Business Review,* May-June, 2000, pp. 73. (RW 1328)

Brown, S.I. & Walter, M.I. *The Art of Problem Posing,* 2nd ed., L. Erlbaum Associates, Hillsdale, NJ, 1990. (RW 2665)

Brown, S.I. & Walter, M.I. *The Art of Problem Posing,* 3rd ed., L. Erlbaum Associates, Mahwah, NJ, 2005. (RW 2581)

Brown, T.A. & Shuford, E.H. *Quantifying Uncertainty into Numerical Probabilities for the Reporting of Intelligence* 1973. (RW 2850)

Brown, V.R. & Paulus, P.B. "Making Group Brainstorming More Effective: Recommendations from an Associative Memory Perspective," *Current Directions in Psychological Science,* Vol. 11, 2002, pp. 208. (RW 2807)

Brownlee, J., Purdie, N. & Boulton-Lewis, G. "Changing Epistemological Beliefs in Pre-Service Teaching Education Students," *Teaching in Higher Education,* Vol. 6, No. 2, 2001, pp. 247-268. (RW 5349)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Brownlee, J. "Knowing and Learning in Teacher Education: A Theoretical Framework of Core and Peripheral Epistemological Beliefs," *Asia-Pacific Journal of Teacher Education & Development,* Vol. 4, No. 1, 2001, pp. 131-55. (RW 5428)

Bruce, J.B. *Dynamic Adaptation: A Twenty-First Century Intelligence Paradigm.* 2005. (RW 1221)

Bruce, J.B. "Making Analysis More Reliable: Why Epistemology Matters to Intelligence," in *Analyzing Intelligence: Origins, Obstacles, and Innovations,* eds. R.Z. George & J.B. Bruce, Georgetown University Press, Washington, DC, 2008, pp. 171-190. (RW 3103)

Bruce, J.B. "The Missing Link: The Analyst-Collector Relationship," in *Analyzing Intelligence: Origins, Obstacles, and Innovations,* eds. R.Z. George & J.B. Bruce, 2008, pp. 191. (RW 3104)

Bruce, J.B. & Bennett, M. "Foreign Denial and Deception: Analytical Imperatives," in *Analyzing Intelligence: Origins, Obstacles, and Innovations,* eds. R.Z. George & J.B. Bruce, 2008, pp. 122. (RW 3100)

Bruce, J.B. & George, R.Z. "Introduction: Intelligence Analysis - the Emergence of a Discipline," in *Analyzing Intelligence: Origins, Obstacles, and Innovations,* eds. R.Z. George & J.B. Bruce, Georgetown University Press, Washington, DC, 2008, pp. 1-15. (RW 2974)

Brueggemann, C.E. *Mitigating Information Overload: The Impact of "Context-Based Approach" to the Design of Tools for Intelligence Analysts,* M.S. thesis, Naval Postgraduate School, 2008. (RW 4873)

Bruine de Bruin, W., Parker, A.M. & Fischhoff, B. "Individual Differences in Adult Decision Making Competence," *Journal of Personality and Social Psychology,* Vol. 92, No. 5, 2007, pp. 938. (RW 2418)

Brunatti, A.D. "The Architecture of Community: Intelligence Community Management in Australia, Canada, and New Zealand," *Public Policy and Administration,* 2012 (RW 5887)

Bruneau, T.C. "Democracy and Effectiveness: Adapting Intelligence for the Fight Against Terrorism," *International Journal of Intelligence and Counterintelligence,* Vol. 21, No. 3, 2008, pp. 448. (RW 3137)

Bruner, J.S. *Acts of Meaning,* Harvard University Press, Cambridge, MA, 1990. (RW 3795)

Brunet, A., Orr, S.P., Tremblay, J., Robertson, K., Nader, K. & Pitman, R.K. "Effect of Post-Retrieval Propranolol on Psychophysiologic Responding during Subsequent Script-Driven Traumatic Imagery in Post-Traumatic Stress Disorder," *Journal of Psychiatric Research,* 2007 (RW 2570)

Budiansky, S. "The Right Kind of Second Guessing," *Washington Post,* May 26, 2002, p. B03. (RW 589)

Budiansky, S. "What's the use of Cryptologic History?" *Intelligence and National Security,* Vol. 25, No. 6, 2010, pp. 767-777. (RW 4574)

Budner, S. "Intolerance of Ambiguity as a Personality Variable," *Journal of Personality,* Vol. 30, No. 1, 1962, pp. 29-50. (RW 5664)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Budner, S. *Tolerance of Ambiguity Scale* 1962. (RW 5312)

Buede, D.M. & Sticha, P.J. "Dealing with Biases and Overconfidence," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 401. (RW 3659)

Buede, D.M. & Sticha, P.J. "Reducing Overconfidence: Keeping it Real," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 403. (RW 3660)

Buede, D.M. & Sticha, P.J. "Using Evidence: A Diversion for the Lunch Hour," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 404. (RW 3661)

Buede, D., Rees, R.L., Sticha, P. & Lewellyn, M. "Bayesian Networks: An Analytic Tool for Predicting Behavior," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 826)

Buede, D. & Tatman, J. *Probability-Based Predictive Analysis: Moving Towards Evidence Based Predictive Analysis[Powerpoint Presentation]* (RW 2175)

Buede, D. & Tatman, J. *Probability-Based Predictive Analysis: Moving Towards Evidence Based Predictive Analysis[Powerpoint Presentation]* 2007. (RW 2849)

Buehl, M.M. & Alexander, P.A. "Examining the Dual Nature of Epistemological Beliefs," *International Journal of Educational Research*, Vol. 45, No. 1-2, 2006, pp. 28. (RW 3687)

Buehl, M.M. & Alexander, P.A. "Beliefs about Academic Knowledge," *Educational Psychology Review*, Vol. 13, No. 4, 2001, pp. 385. (RW 4276)

Buehner, M.J. & Cheng, P.W. "Causal Learning," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 143-168. (RW 4002)

Buller, D.J. "Evolution of the Mind: 4 Fallacies of Psychology," *Scientific American*, 2008 (RW 3472)

Bunker, D.J. & Tuttle, R.F. "On the Feasibility of a Peer-Reviewed, Classified MASINT Journal," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 862)

Buonomano, D. *Brain Bugs: How the Brain's Flaws Shape our Lives*, W. W. Norton, New York, NY, 2011. (RW 4930)

Burchill, G., Brodie, C.H.*Voices into Choices: Acting on the Voice of the Customer*, Joiner Publication, Madison, WI, 1997. (RW 2740)

Burgess, C. *Predicting the Future with Social Media*. Available: http://www.business2community.com/social-media/predicting-the-future-with-social-media-0117502, Viewed: January 19, 2012. (RW 5408)

Burgin, R. "Variations in Relevance Judgments and the Evaluation of Retrieval Performance," *Information Processing and Management*, Vol. 28, No. 5, 1992, pp. 619. (RW 1479)

Burgoon, J.K., Jensen, M.L., Meservy, T.O., Kruse, J. & Nunamaker, J.F. "Augmenting Human Identification of Emotional States in Video," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 823)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Burke, C. *Freeing Knowledge, Telling Secrets: Open Source Intelligence and Development,* Research paper series: Centre for East-West Cultural and Economic Studies; number 13, 2007. (RW 3828)

Burns, B.D. & Vollmeyer, R. "Goal Specificity Effects on Hypothesis Testing in Problem Solving," *Quarterly Journal of Experimental Psychology Section A - Human,* Vol. 55, No. 1, 2002, pp. 241. (RW 1882)

Burns, K. "Mental Models and Normal Errors," in *How Professionals make Decisions,* eds. H. Montgomery, R. Lipshitz & B. Brehmer, L. Erlbaum Associates, Mahwah, NJ, 2005, pp. 15. (RW 1381)

Burns, T.L. *The Origins of the National Security Agency 1940-1952,* Center for Cryptologic History, National Security Agency 1990. (RW 370)

Burr, J.E. & Hofer, B.K. "Personal Epistemology and Theory of Mind: Deciphering Young Children's Beliefs about Knowledge and Knowing," *New Ideas in Psychology,* Vol. 20, No. 2-3, 2002, pp. 199-224. (RW 4637)

Burris, W.C. "The Uses of History in Intelligence Analysis," *International Journal of Intelligence and Counterintelligence,* Vol. 6, No. 3, 1993, pp. 297-301. (RW 53)

Burrows, M.J. "Intelligence Community Perspective on the Maturing URW Threat", *Unrestricted Warfare Symposium Proceedings,* Johns Hopkins University, March 20-21, 2007, pp.9797. (RW 2781)

Burrows, W.E. *Deep Black: Space Espionage and National Security,* Random House, New York, NY, 1986. (RW 22)

Burson, K.A., Larrick, R.P. & Klayman, J. "Skilled Or Unskilled, but Still Unaware of it: How Perceptions of Difficulty Drive Miscalibration in Relative Comparisons," *Journal of Personality and Social Psychology,* Vol. 90, No. 1, 2006, pp. 60. (RW 3298)

Burtis, P.J., Bereiter, C., Scardamalia, M. & Tetroe, J. "The Development of Planning in Writing," in *Explorations in the Development of Writing: Theory, Research, and Practice,* eds. B.M. Kroll & C.G. Wells, Wiley, Chichester Sussex; New York, 1983, pp. 153. (RW 2284)

Burton, B. *Top Secret: The Dictionary of Espionage and Intelligence,* 2005. (RW 3683)

Burton, M.S. "How the Web can Relieve our Information Glut and Get Us Talking to each Other," *Studies in Intelligence,* Vol. 49, No. 3, 2005, pp. 55. (RW 1498)

Burton, R.A. *On being Certain: Believing You are Right Even when You're Not,* St. Martin's Press, New York, NY, 2008. (RW 3313)

Burton, R. & Lehrer, J. "The Certainty Bias: A Potentially Dangerous Mental Flaw," *Scientific American,* 2008 (RW 3294)

Busbee, M., Drake, D., Gerogosian, D. & Pedtke, T. "21st Century Intelligence Production, Analysis, Access, and Delivery," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 595)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Busch, F. *When People Publish: Essays on Writers and Writing,* University of Iowa Press, Iowa City, 1986. (RW 1859)

Butchart, S., Forster, D., Gold, I., Bigelow, J., Korb, K., Oppy, G. & Serenti, A. "Improving Critical Thinking using Web Based Argument Mapping Exercises with Automated Feedback," *Australasian Journal of Educational Technology,* Vol. 25, No. 2, 2009, pp. 268-291. (RW 4044)

Butler, R., Chilcot, J., Inge, P., Mates, M. & Taylor, A. *Review of Intelligence on Weapons of Mass Destruction,* The Stationery Office, London, UK, 2004. (RW 4855)

Butterfield, A.P. *Accuracy of Intelligence Assessment: Bias, Perception, and Judgment in Analysis and Decision,* ADA266925/7, Naval War College, Newport, RI, 1993. (RW 1206)

Butterfield, E.C. *Children's Writing: Toward a Process Theory of the Development of Skilled Writing,* Jai, Greenwich, CT; London, 1994. (RW 2014)

Butterfield, E.C. "Diverse Data about Writing Processes and their Theoretical Implications," in *Advances in Cognition and Educational Practice. Volume 2. Children's Writing: Toward a Process Theory of the Development of Skilled Writing*, ed. E.C. Butterfield, Jai, Greenwich, CT; London, 1994, pp. 199. (RW 2127)

Butterfield, E.C., Hacker, D.J. & Albertson, L.R. "Environmental, Cognitive, and Metacognitive Influences on Text Revision: Assessing the Evidence," *Educational Psychology Review,* Vol. 8, No. 3, 1996, pp. 239. (RW 2077)

Butterfield, E.C., Hacker, D.J. & Plumb, C. "Topic Knowledge, Linguistic Knowledge, and Revision Processes as Determinants of Text Revision," in *Advances in Cognition and Educational Practice. Volume 2. Children's Writing: Toward a Process Theory of the Development of Skilled Writing*, ed. E.C. Butterfield, Jai, Greenwich, CT; London, 1994, pp. 83. (RW 2125)

Butterworth, R.M. *The Terrorist Threat Integration Center,* National Defense University, Washington, DC, [undated]. (RW 363)

Cacioppo, J.T. & Petty, R.E. "The Need for Cognition," *Journal of Personality and Social Psychology,* Vol. 42, No. 1, 1982, pp. 116-131. (RW 5311)

Cacioppo, J.T., Petty, R.E., Feinstein, J.A. & Jarvis, W.B.G. "Dispositional Differences in Cognitive Motivation: The Life and Times of Individuals Varying in Need for Cognition," *Psychological Bulletin,* Vol. 119, No. 2, 1996, pp. 197-253. (RW 4944)

Cacioppo, J.T., Petty, R.E. & Kao, C.F. "The Efficient Assessment of Need for Cognition," *Journal of Personality Assessment,* Vol. 48, No. 3, 1984, pp. 306-307. (RW 5019)

Cacioppo, J.T., Visser, P.S. & Pickett, C.L. *Social Neuroscience: People Thinking about Thinking People,* MIT Press, Cambridge, MA, 2006. (RW 2653)

Cahoy, D.R. & Ding, M. "Using Experimental Economics to Peek into the "Black Box" of Jury Behavior: A Proproals for Jury Research Reform," *Southern California Interdisciplinary Law Journal,* Vol. 14, No. 3, pp. 31. (RW 2035)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Cai, D., Mednick, S., Harrison, E., Kanady, J. & Mednick, S. "REM, Not Incubation, Improves Creativity by Priming Associative Networks," *Proceedings of the National Academy of Sciences*, Vol. 106, No. 25, 2009, pp. 10130-10134. (RW 3502)

Caldwell, G. *Political Analysis for Intelligence*, Center for the Study of Intelligence, Langley, Va., 1992. (RW 4188)

Calishain, T. *Web Search Garage*, Prentice Hall PTR, Upper Saddle River, NJ, 2004. (RW 3541)

Callahan, C.M. "Test Review of the California Critical Thinking Dispositions Inventory," in *The Twelfth Mental Measurements Yearbook*, eds. J.C. Conoley & J.C. Impara, Buros Institute, 1995. (RW 5518)

Callum, R. "The Case for Cultural Diversity in the Intelligence Community," *International Journal of Intelligence and Counterintelligence*, Vol. 14, No. 1, 2001, pp. 25-48. (RW 461)

Calpin, J.A. *Inherent Challenges in Conducting Sound and Objective Analysis. Presentation to the Mid-Atlantic Intergovernmental Audit Forum[Powerpoint Presentation]* 2004. (RW 277)

Calvillo, D.P. & Revlin, R. "Reasoning and Belief Revision with Deontic, Causal, and Arbitrary Conditionals", *Proceedings of the 25th Annual Conference of the Cognitive Science Society*, July 31-August 2, 2003, pp.1322. (RW 1983)

Cambone, S.A. *Statement for the Record before the Senate Armed Services Committee, Strategic Forces Subcommittee* 2004. (RW 604)

Cambridge, R.M. & Shreckengost, R.C. *Are You Sure?: The Subjective Probability Assessment Test*, Information Science Center, Office of Training, Central Intelligence Agency, Washington, 1978. (RW 3728)

Camerer, C. "Behavioral Economics: Reunifying Psychology and Economics," *Proceedings of the National Academy of Sciences*, Vol. 96, No. 19, 1999, pp. 10575-10577. (RW 1918)

Camerer, C.F. "Strategizing in the Brain," *Science*, Vol. 300, 2003, pp. 1673. (RW 2019)

Camerer, C.F. & Johnson, E.J. "The Process-Performance Paradox in Expert Judgment: How can Experts Know so Much and Predict so Badly?" in *Toward a General Theory of Expertise: Prospects and Limits*, eds. K.A. Ericsson & J. Smith, Cambridge University Press, Cambridge; New York, 1991, pp. 195. (RW 2780)

Cameron, C. *Flinging Open the Doors to Intelligence Gathering*. Available: http://www.ojr.org/ojr/workplace/1097814155.php, Viewed: February 21, 2011. (RW 230)

Campbell, A. & Sarat, A. *Forensic Science: Evidence, Clues, and Investigation*, Chelsea House Publishers, Philadelphia, 2000. (RW 3904)

Campbell, A. "Seven Deadly Sins and Seven Cardinal Virtues of Analytic Best Practices. Outline for Comments." *Global Intelligence Forum 2010*, Dungarvan, Ireland, July 11-13, 2010 (RW 4236)

Campbell, A. & Mandel, D.R. *Summary Record of the GFF Community of Interest on the Practice and Organization of Intelligence Ottawa Roundtable. what can the Cognitive and*

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Behavioural Sciences Contribute to Intelligence Analysis? Towards a Collaborative Agenda for the Future, DRDC Toronto CR 2010-012, Defence R&D, Toronto, ONT, 2010. (RW 4034)

Campbell, J.P. "Behavior, Performance, and Effectiveness in the 21st Century," in *Oxford Handbook of Organizational Psychology*, ed. W.J. Kozlowski, Oxford University Press, New York, NY, 2012, pp. 159-194. (RW 5764)

Campbell, S. "A Snapshot of the U.S. Market for Intelligence Education," *American Intelligence Journal,* Vol. 28, No. 1, 2010, pp. 121. (RW 4444)

Campbell, S.H. "A Survey of the U.S. Market for Intelligence Education," *International Journal of Intelligence and Counterintelligence,* Vol. 24, No. 2, 2011, pp. 307-337. (RW 4596)

Campitelli, G. & Gobet, F. "Deliberate Practice: Necessary but Not Sufficient," *Current Directions in Psychological Science,* Vol. 20, No. 5, 2011, pp. 280-285. (RW 5240)

Candib, L.M., Stange, K.C. & Levinson, W. "Qualitative Research: Perspectives on the Future," in *Doing Qualitative Research*, eds. B.F. Crabtree & W.L. Miller, 2nd ed., Sage Publications, Thousand Oaks, Calif, 1999, pp. 347. (RW 2509)

Canfield, J.L. "Gerbil Redux: What Course Ahead for Naval Intelligence?" *International Journal of Intelligence and Counterintelligence,* Vol. 6, No. 3, 1993, pp. 271-295. (RW 52)

Cannon, M.D. & Edmondson, A.C. "Confronting Failure: Antecedents and Consequences of Shared Beliefs about Failure in Organizational Work Groups," *Journal of Organizational Behavior,* Vol. 22, No. 2, 2001, pp. 161-177. (RW 1924)

Cano, F. "Epistemological Beliefs and Approaches to Learning: Their Change through Secondary School and their Influence on Academic Performance," *British Journal of Educational Psychology,* Vol. 75, 2005, pp. 203. (RW 2859)

Canton, B. "The Active Management of Uncertainty," *International Journal of Intelligence and Counterintelligence*, Vol. 21, No. 3, 2008, pp. 487-518. (RW 3138)

Cantor, J. *Conquer Cyberoverload: Get More done, Boost Your Creativity, and Reduce Stress,* Cyber Outlook Press, Madison, WI, 2009. (RW 4680)

Caplan, B. "Terrorism: The Relevance of the Rational Choice Model," *Public Choice,* Vol. 128, No. 1-2, 2006, pp. 91. (RW 3888)

Capps, R. *Langley Won't Tell Us: How I Fought the Intelligence Turf Wars - and Lost* 2010. (RW 3859)

Carbonell, J., Gazen, C., Jin, C., Hayes, P., Goldstein, A., Mathew, J. & Dietrich, D. "Finding Novel Information in Large, Constantly Incrementing Collections of Structured Data," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 845)

Card, S.K. "The Science of Analytical Reasoning," in *Illuminating the Path: The Research and Development Agenda for Visual Analytics*, eds. J.J. Thomas & K.A. Cook, IEEE, Los Alamitos, CA, 2005, pp. 33-68. (RW 4028)

Carenini, G., Ng, R.T. & Zwart, E. "Extracting Knowledge from Evaluative Text", *K-Cap '05,* Banff, Alberta, Canada, October 2-5, 2005, pp.1111. (RW 1522)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Carey, S. & Smith, C. "On Understanding the Nature of Scientific Knowledge," *Educational Psychologist,* Vol. 28, No. 3, 1993, pp. 235. (RW 4425)

Carl, L.D. *International Dictionary of Intelligence,* International Defense Consultant Services Inc., McLean, VA, 1990. (RW 1106)

Carley, K. & Palmquist, M. "Extracting, Representing, and Analyzing Mental Models," *Social Forces,* Vol. 70, No. 3, 1992, pp. 601. (RW 2514)

Carlile, P.R. "Transferring, Translating, and Transforming: An Integrative Framework for Managing Knowledge Across Boundaries," *Organization Science,* Vol. 15, No. 5, 2004, pp. 555. (RW 1658)

Carlisle, C. "Creatures of Habit: The Problem and the Practice of Liberation," *Continental Philosophy Review,* Vol. 38, 2006, pp. 19. (RW 3891)

Carlisle, R.P. *Encyclopedia of Intelligence and Counterintelligence,* Sharpe Reference, Armonk, NY, 2005. (RW 1214)

Carlson, J. "Lloyd B. Sharp: Trailblazer in Outdoor Education," in *Sourcebook of Experiential Education: Key Thinkers and their Contributions,* eds. T.E. Smith & C. Knapp, Routledge, New York, 2011, pp. 123-130. (RW 4926)

Carlson, K.A. & Russo, J.E. "Biased Interpretation of Evidence by Mock Jurors," *Journal of Experimental Psychology: Applied,* Vol. 7, No. 2, 2001, pp. 91. (RW 2094)

Carpenter, S. "Buried Prejudice," *Scientific American Mind,* Vol. 19, No. 2, 2008, pp. 32. (RW 3177)

Carr, N. "The Ignorance of Crowds," *Strategy + Business,* 47, 2007. (RW 3133)

Carr, N. "Is Google Making Us Stupid?" *Atlantic Magazine,* July/August, 2008. (RW 3269)

Carr, N.G. "Is Greatness a Network Effect?" *DigitAll Magazine,* Fall, 2006. (RW 3134)

Carr, S.C. "Assessing Learning Processes: Useful Information for Teachers and Students," *Intervention in School and Clinic,* Vol. 37, No. 3, 2002, pp. 156-162. (RW 5259)

Carroll, J.B. *Human Cognitive Abilities: A Survey of Factor-Analytic Studies,* Cambridge University Press, Cambridge; New York, 1993. (RW 3464)

Carroll, J.M. "Introduction," in *Scenario-Based Design: Envisioning Work and Technology in Systems Development,* ed. J.M. Carroll, Wiley, New York, 1995, pp. 1. (RW 3393)

Carroll, J.M. *Scenario-Based Design: Envisioning Work and Technology in Systems Development,* Wiley, New York, 1995. (RW 3387)

Carroll, J.M. *Making use: Scenario-Based Design of Human-Computer Interactions,* MIT Press, Cambridge, MA, 2000. (RW 3399)

Carroll, R.P. "Can Reasoning be Taught?" *Journal of Education,* Vol. 114, No. 16, 1931, pp. 370-371. (RW 4481)

Carroll, T.P. "The Case Against Intelligence Openness," *International Journal of Intelligence and Counterintelligence,* Vol. 14, No. 4, 2001, pp. 559-574. (RW 186)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Carruthers, P. *An Architecture for Dual Reasoning* [undated]. (RW 5859)

Carruthers, P. *The Architecture of the Mind: Massive Modularity and the Flexibility of Thought*, Clarendon Press, Oxford, UK, 2006. (RW 1720)

Carruthers, P. "How we Know our Own Minds: The Relationship between Mindreading and Metacognition," *Behavioral and Brain Sciences*, Vol. 32, No. 2, 2009, pp. 121-138. (RW 5843)

Carruthers, P., Stich, S.P. & Siegal, M. "Introduction: What Makes Science Possible?" in *The Cognitive Basis of Science*, eds. P. Carruthers, S.P. Stich & M. Siegal, Cambridge University Press, Cambridge; New York, 2002, pp. 1. (RW 3067)

Carter, D.L. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* 2004. (RW 2496)

Carver, R.H. *Students' Ambiguity Tolerance as a Success Factor in Learning to Reason Statistically [Powerpoint Presentation]*, Waltham, MA, 2007. (RW 5173)

Case, D.O. *Looking for Information: A Survey of Research on Information Seeking, Needs, and Behavior*, Academic Press, New York, NY, 2002. (RW 948)

Case, D.O. *Looking for Information: A Survey of Research on Information Seeking, Needs, and Behavior*, 2nd ed., Elsevier/Academic Press, Amsterdam ; Boston, 2007. (RW 3534)

Cassino, D., Taber, C.S. & Lodge, M. "Information Processing and Public Opinion," *Politische Vierteljahresschrift*, Vol. 48, No. 2, 2007, pp. 205-220. (RW 5458)

Cassino, D., Lodge, M. & Taber, C. *Implicit Political Attitudes: When, how, Why, with what Effects* [undated]. (RW 5726)

Cassino, D., Lodge, M. & Taber, C.S. "Political Attitudes: When, how, Why, with what Effects," in *The Oxford Handbook of Political Communication*, eds. K.H. Jamieson & K. Kenski, Oxford University Press, (RW 5461)

Cassity, J. *Restructuring Military Policy to Reflect Worldwide Political Changes*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1991. (RW 978)

Castro, J. *Your Scientific Reasoning is More Flawed than You Think*. Available: http://www.scientificamerican.com/article.cfm?id=your-scientific-reasoning-more-flawed-than-you-think, Viewed: September 4, 202. (RW 5800)

Catrambone, R. & Holyoak, K.J. "Overcoming Contextual Limitations on Problem Solving Transfer," *Journal of Experimental Psychology: Learning, Memory, & Cognition*, Vol. 15, No. 6, 1990, pp. 1147. (RW 2732)

Cattell, R.B. "Theory for Fluid and Crystallized Intelligence: A Critical Experiment," *Journal of Experimental Psychology*, Vol. 54, No. 1, 1963, pp. 1. (RW 3467)

Cattell, R.B. *Abilities: Their Structure, Growth, and Action*, Houghton Mifflin, Boston, 1971. (RW 3465)

Cavelty, M. & Mauer, V. "Postmodern Intelligence: Strategic Warning in an Age of Reflexive Intelligence," *Security Dialogue*, Vol. 40, No. 2, 2009, pp. 123-144. (RW 5659)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Cebrowski, A.K. *Command and Information Systems*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1997. (RW 979)

Cebrowski, A.K. *Control and Transformation*, 2004. (RW 1345)

Cebrowski, A.K. & Raymond, J.W. "Operationally Responsive Space: A New Defense Business Model," *Parameters,* Vol. 35, No. 2, 2005, pp. 67-77. (RW 787)

Center for the Study of Intelligence. *Symposium on Teaching Intelligence October 1-2, 1993. A Report.* 1994. (RW 907)

Center for the Study of Intelligence. "Intelligence for a New Era in American Foreign Policy. Conference Report," September 10-11, 2003 (RW 1301)

Center for the Study of Intelligence. "Intelligence Lessons Learned Conference. Conference Report," January 14, 2005 (RW 1347)

Central Intelligence Agency. *A Compendium of Analytic Tradecraft Notes* 1995. (RW 587)

Central Intelligence Agency. Directorate of Intelligence *A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis* 2005. (RW 3278)

Chabris, C. *Research Plan: Resistance to Cognitive Illusions and Biases: An Exploration of Individual Differences,* 2002. (RW 3727)

Chabris, C.F., Jerde, T.E., Woolley, A.W., Gerbasi, M.E., Schuldt, J.P., Bennett, S.L., Hackman, J.R. & Kosslyn, S.M. *Spatial and Object Visualization Cognitive Styles: Validation Studies in 3800 Individuals,* The Group Brain Project, technical report no. 2, 2006. (RW 3012)

Chacko, G.K. *Applied Operations Research: Systems Analysis in Hierarchical Decision-Making,* North-Holland, Amsterdam, 1976. (RW 2549)

Chai, C.S., Dung, F., Wong, B. & Qian, Y. "South China Education Majors' Epistemological Beliefs and their Conception of the Nature of Science," *Asia Pacific Education Researcher,* Vol. 19, 2010, pp. 111-125. (RW 5060)

Chai, C.S., Teo, T. & Lee, C.B. "Modelling the Relationships among Beliefs about Learning, Knowledge, and Teaching of Pre-Service Teachers in Singapore," *Asia Pacific Education Researcher,* Vol. 19, 2010, pp. 25-42. (RW 5061)

Chai, C.S., Teo, T. & Lee, C.B. "The Change in Epistemological Beliefs and Beliefs about Teaching and Learning: A Study among Pre-Service Teachers," *Asia-Pacific Journal of Teacher Education,* Vol. 37, No. 4, 2009, pp. 351-362. (RW 5231)

Chaiken, S. & Trope, Y. *Dual-Process Theories in Social Psychology,* Guilford Press, New York, 1999. (RW 4157)

Chainey, S. "Improving the explanatory content of analysis products using hypothesis testing" *Policing,* [Online] April 9, 2012. Available from: http://dx.doi.org/10.1093/police/pas007. 2012. (RW 5556)

Chait, R., Ryan, W.P. & Taylor, B.E. *Governance as Leadership: Reframing the Work of Nonprofit Boards,* John Wiley & Sons, Hoboken, NJ, 2005. (RW 3246)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Chalk, P. & Rosenau, W. *Confronting the "Enemy within": Security Intelligence, the Police and Counterterrorism in Four Democracies,* RAND Corp., Santa Monica CA, 2004. (RW 4554)

Chalmers, I. *Research Synthesis [Powerpoint Presentation]* 2004. (RW 2199)

Chalmers, I. & Altman, D.G. *Systematic Reviews,* BMJ Pub, London, 1995. (RW 2213)

Chalmers, I., Hedges, L.V. & Cooper, H. "A Brief History of Research Synthesis," *Evaluation and the Health Professions,* Vol. 25, No. 1, 2002, pp. 12. (RW 2239)

Chamberlin, T.C. "The Method of Multiple Working Hypotheses," *Journal of Geology,* Vol. 6, No. 5, 1897, pp. 837-848. (RW 5187)

Chamberlin, T.C. "The Method of Multiple Working Hypotheses," *Journal of Geology,* Vol. 102, No. 5, 1995, pp. 6. (RW 5356)

Chambers, D.I. "The Past and Present State of Chinese Intelligence Historiography," *Studies in Intelligence,* Vol. 56, No. 3, 2012, pp. 31-46. (RW 5896)

Chambers, J.R., Baron, R.S. & Inman, M.L. "Misperceptions in Intergroup Conflict - Disagreeing about what we Disagree about," *Psychological Science,* Vol. 17, No. 1, 2006, pp. 38. (RW 2352)

Chambliss, M.J. "Text Cues and Strategise Successful Readers use to Construct the Gist of Lengthy Written Arguments," *Reading Research Quarterly,* Vol. 30, No. 4, 1995, pp. 778. (RW 2805)

Chambliss, M.J. "Why do Readers Fail to Change their Beliefs After Reading Persuasive Text?" in *Beliefs about Texts and Instruction with Text,* eds. R. Garner & P.A. Alexander, L. Erlbaum Associates, Hillsdale, NJ, 1994, pp. 75. (RW 2814)

Chambliss, M.J. "Do Adults Change their Minds After Reading Persuasive Text?" *Written Communication,* Vol. 13, No. 3, 1996, pp. 291. (RW 2790)

Chambliss, S. "Re-Forming Intelligence," *The National Interest,* 79, 2005, pp. 79-83. (RW 409)

Chambliss, S. "We have Not Correctly Framed the Debate on Intelligence Reform," *Parameters,* Vol. 35, No. 1, 2005, pp. 5-13. (RW 747)

Chamovitz, D. *What a Plant Knows: A Field Guide to the Senses,* Scientific American/Farrar, Straus and Giroux, New York, 2012. (RW 5918)

Champion, D.J. *Research Methods for Criminal Justice and Criminology,* 3rd ed., Pearson/Prentice Hall, Upper Saddle River, NJ, 2006. (RW 2545)

Chan, K.W. "The Role of Epistemological Beliefs in Hong Kong Preservice Teachers' Learning," *Asia Pacific Education Researcher,* Vol. 19, 2010, pp. 7-24. (RW 5062)

Chan, K. & Elliott, R.G. "Exploratory Study of Hong Kong Teacher Education Students' Epistemological Beliefs: Cultural Perspectives and Implications," *Contemporary Educational Psychology,* Vol. 27, No. 3, 2002, pp. 292. (RW 4279)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Chan, K. "Epistemological Beliefs, Learning, and Teaching: The Hong Kong Cultural Context," in *Knowing, Knowledge and Beliefs: Epistemological Studies Across Diverse Cultures*, ed. M.S. Khine, Springer, Dordrecht, 2008, pp. 257-272. (RW 4353)

Chan, K. "Preservice Teacher Education Students' Epistemological Beliefs and Conceptions about Learning," *Instructional Science*, Vol. 39, No. 1, 2009, pp. 87-108. (RW 5227)

Chan, K. & Elliott, R.G. "Epistemological Beliefs Across Cultures: Critique and Analysis of Beliefs Structure Studies," *Educational Psychology*, Vol. 24, No. 2, 2004, pp. 123. (RW 2858)

Chan, S. "The Intelligence of Stupidity: Understanding Failures in Strategic Warning," *The American Political Science Review*, Vol. 73, No. 1, 1979, pp. 171-180. (RW 141)

Chandler, M.J., Hallett, D. & Sokol, B.W. "Competing Claims about Competing Knowledge Claims," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing*, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 145. (RW 4332)

Chandler, M.J. & Proulx, T. "Stalking Young Persons' Changing Beliefs about Belief," in *Personal Epistemology in the Classroom: Theory, Research, and Implications for Practice*, eds. L.D. Bendixen & F.C. Feucht, Cambridge University Press, Cambridge, UK, 2010, pp. 197-219. (RW 5128)

Chang, K.C., He, B., Li, C., Patel, M. & Zhang, Z. "Structured Databases on the Web: Observations and Implications," *SIGMOD Record*, Vol. 33, No. 3, 2004, pp. 61. (RW 1407)

Chant, S.N.F. "An Objective Experiment on Reasoning," *American Journal of Psychology*, Vol. 114, No. 2, 1931, pp. 282-291. (RW 4482)

Chao, C. & Salvendy, G. "Impact of Cognitive Abilities of Experts on the Effectiveness of Elicited Knowledge," *Behaviour & Information Technology*, Vol. 14, No. 3, 1995, pp. 174-182. (RW 927)

Chapman, B. *Researching National Security and Intelligence Policy*, CQ Press, Washington, DC, 2004. (RW 770)

Chapman, J., Edwards, C. & Hampson, S. *Connecting the Dots*, Demos, London, UK, 2009. (RW 3825)

Chapman, J. *The Development of the Assessment of Thinking Skills*, University of Cambridge Local Examinations Syndicate, Cambridge, UK, 2005. (RW 4068)

Chappell, A.R., Cowell, A.J., Thurman, D.A. & Thomson, J.R. "Supporting Mutual Understanding in a Visual Dialogue between Analyst and Computer", *HFES 2004: Proceedings of the Human Factors and Ergonomics Society. 48th Annual Meeting.* New Orleans, LA, September 20-24, 2004, pp. 376-380. (RW 2871)

Charlton, R.E. "The Direct Teaching of Analysis," in *Thinking Skills Instruction: Concepts and Techniques*, eds. M. Heiman & J. Slomianko, National Education Association, Washington, DC, 1987, pp. 152-159. (RW 5083)

Charness, G. & Levin, D. *Bayesian Updating Vs. Reinforcement and Affect: A Laboratory Study. Author's Working Paper,* 2003. (RW 1919)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Charness, G. & Levin, D. *When Optimal Choices Feel Wrong: A Laboratory Study of Bayesian Updating, Complexity, and Affect*, UC Santa Barbara, Santa Barbara, CA, 2004. (RW 1914)

Charters, D.A. "Canadian Military Intelligence in Afghanistan," *International Journal of Intelligence and Counterintelligence*, Vol. 25, No. 3, 2012, pp. 470-507. (RW 5732)

Charters, D., Farson, A.S. & Hastedt, G.P. *Intelligence Analysis and Assessment*, Frank Cass, London, UK, 1996. (RW 654)

Chaseling, J. *Statistics in Court: The Ultimate Communication Challenge* 2006. (RW 2059)

Chater, N. & Oaksford, M. "Normative Systems: Logic, Probability, and Rational Choice," in *Oxford Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 11-21. (RW 5496)

Chatham, R.E. "The 20th-Century Revolution in Military Training," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 27-60. (RW 5135)

Chatham, R.E. "Toward a Second Training Revolution: Promise and Pitfalls of Digital Experiential Learning," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 215-246. (RW 5143)

Cheikes, B.A., Brown, M.J., Lehner, P.E. & Adelman, L. *Confirmation Bias in Complex Analyses*, MITRE Corporation, Bedford, MA, 2004. (RW 2940)

Chelimsky, E. "Politics, Policy, and Research Synthesis," *Evaluation*, Vol. 1, No. 1, 1995, pp. 97. (RW 2247)

Chen, H., Wang, F.Y. & Zeng, G. "Intelligence and Security and Informatics for Homeland Security: Information, Communication, and Transportation," *IEEE Transactions on Intelligent Transportation Systems*, Vol. 5, No. 4, 2004, pp. 329-341. (RW 5734)

Chen, H. & Xu, J. "Intelligence and Security Informatics," *Annual Review of Information Science and Technology*, Vol. 40, No. 1, 2006, pp. 229-289. (RW 4454)

Chen, J.Q. "Semantic Filters in Intelligence Analysis", *2011 IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology (WI-IAT)*, Lyon, France, August 22-27, 2011, pp. 265-268. (RW 5464)

Chen, K.H. & Olson, S.K. "Measuring Cognitive Complexity in the Accounting Domain," *Behavioral Research in Accounting*, Vol. 11989, pp. 160. (RW 4301)

Chen, P. & Kuo, F. "An Information Retrieval System Based on a User Profile," *The Journal of Systems and Software*, Vol. 54, No. 1, 2000, pp. 3-8. (RW 762)

Cheng, J., Emami, R., Kerschberg, L. & et al. *OmniSeer: A Cognitive Framework for User Modeling, Reuse of Prior and Tacit Knowledge, and Collaborative Knowledge Services* (RW 1513)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Cheng, J. & Senator, T. "A Combinatorial Analysis of Link Discovery," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 796)

Cheng, P.W. & Holyoak, K.J. "Pragmatic Reasoning Schemas," *Cognitive Psychology*, Vol. 17, 1985, pp. 391. (RW 2123)

Chesbro, M. *Intel-Cyclopedia: A Guide to Sources of Information for the Intelligence Community* 2012. (RW 5736)

Cheuvront, M. *The Inconvenience of Change: We are Creatures of Habit [Grace Boyle]*. Available: http://www.lifewithoutpants.com/the-inconvenience-of-change/, (RW 3885)

Chi, E.H. "Information Seeking can be Social," *Computer*, Vol. 42, No. 3, 2009, pp. 42. (RW 3439)

Chi, M.T.H., Glaser, R. & Rees, E. "Expertise in Problem Solving," *Advances in the Psychology of Human Intelligence*, Vol. 1, 1982, pp. 7. (RW 2588)

Chi, M.T.H. & Ohlsson, S. "Complex Declarative Learning," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 371-400. (RW 4010)

Chi, M.T.H. & Roscoe, R.D. "The Processes and Challenges of Conceptual Change," in *Reconsidering Conceptual Change: Issues in Theory and Practice*, eds. M. Limón & L. Mason, Kluwer Academic, Dordrecht, 2002, pp. 3-28. (RW 4935)

Chido, D.E. *Civilian Skills for African Military Officers to Resolve the Infrastructure, Economic Development, and Stability Crisis in Sub-Saharan Africa*, US Army War College, Carlisle, PA, 2011. (RW 4584)

Chilukuri, M. & Doraiswamy, P.M. "Does Eating Fewer Calories Improve the Brain?" *Scientific American: Mind Matters*, 2009 (RW 3471)

Chin, G., Kuchar, O.A., Whitney, P.D., Powers, M.E. & Johnson, K.E. "Graph-Based Comparisons of Scenarios in Intelligence Analysis", *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics*, The Hague, Netherlands, October 10-13, 2004, pp. 3175-3180. (RW 5733)

Chin, G., Kuchar, O.A. & Wolf, K.E. "Exploring the Analytical Processes of Intelligence Analysts", *27th CHI Conference*, Boston, MA, April 4-9, 2009, pp.1111-20. (RW 5690)

Chinn, C.A. & Brewer, W.F. "The Role of Anomalous Data in Knowledge Acquisition: A Theoretical Framework and Implications for Science Instruction," *Review of Educational Research*, Vol. 63, 1993, pp. 1. (RW 2756)

Chinn, C.A. & Brewer, W.F. "Models of Data: A Theory of how People Evaluate Data," *Cognition and Instruction*, Vol. 19, No. 3, 2001, pp. 323-393. (RW 2519)

Chinn, C.A. & Samarapungavan, A. "Distinguishing between Understanding and Belief," *Theory into Practice*, Vol. 40, 2001, pp. 235. (RW 2518)

Chinn, C.A. & Brewer, W.F. "Mental Models in Data Interpretation," *Philosophy of Science (Proceedings)*, Vol. 63, 1996, pp. S211. (RW 2515)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Chinn, C.A. & Brewer, W.F. "Theories of Knowledge Acquisition," in *International Handbook of Science Education*, eds. B.J. Fraser & K.G. Tobin, Kluwer Academic, Dordrecht; Boston, 1998, pp. 97. (RW 2513)

Chinn, C.A. & Malhotra, B.A. "Epistemologically Authentic Scientific Reasoning," in *Designing for Science: Implications from Everyday, Classroom, and Professional Settings*, eds. K.D. Crowley, C.D. Schunn & T. Okada, 2001, pp. 351. (RW 3942)

Chinn, C.A. & Samarapungavan, A. "Distinguishing between Understanding and Belief," *Theory into Practice*, Vol. 40, No. 4, 2001, pp. 235-241. (RW 4852)

Chipman, S.E.F. "Expertise in the Management of People: A New Frontier for Research on Expert Performance," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 470-493. (RW 5154)

Chizek, J.G. *Military Transformation: Intelligence, Surveillance and Reconnaissance. Report for Congress*, Congressional Research Service, Library of Congress, Washington, DC, 2003. (RW 240)

Cho, K. & Schunn, C. "Does Writing Improve as a Function of Number of Reviewers?", *Proceedings of the 28th Annual Conference of the Cognitive Science Society*, July 26-29, 2006, pp. 1109. (RW 1988)

Cho, Y.H., Lee, J. & Jonassen, D.H. "The Role of Tasks and Epistemological Beliefs in Online Peer Questioning," *Computers & Education*, Vol. 56, No. 1, 2011, pp. 112-126. (RW 5070)

Choi, B.C.K. "Understanding the Basic Principles of Knowledge Translation," *Journal of Epidemiology and Community Health*, Vol. 59, No. 2, 2005, pp. 93. (RW 2228)

Chorev, M. *Surprise Attack: The Case of the Yom Kippur War*, National Defense University, Washington, DC, 1996. (RW 1184)

Chorvat, T., McCabe, K. & Smith, V. *Law and Neuroeconomics* (RW 2055)

Chowdhury, G.G. *Introduction to Modern Information Retrieval*, 2nd ed., Facet, London, 2004. (RW 1114)

Christiaans, H. *Creativity in Design*, 1992. (RW 2932)

Christoff, K., Ream, J.M. & Gabrieli, J.D. "Neural Basis of Spontaneous Thought Processes," *Cortex*, Vol. 40, No. 4-5, 2004, pp. 623. (RW 2020)

Christoffersen, K. & Woods, D. *Making Sense of Change: The Challenge of Events in Operations Environments*, Laboratory, Institute for Ergonomics, Ohio State University, Columbus, OH, 2003. (RW 1920)

Chu, H. *Information Representation and Retrieval in the Digital Age*, Information Today, Medford, NJ, 2003. (RW 1115)

Chun, S. & Kim, S.H. "Automated Generation of New Knowledge to Support Managerial Decisionmaking: Case Study in Forecasting a Stock Market," *Expert Systems*, Vol. 21, No. 4, 2004, pp. 192-207. (RW 687)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Chuter, D. "The Buddha as an Intelligence Analyst", *New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities,* Rome, Italy, 31 March - 2 April, 2004, pp. 111-126. (RW 2835)

CIA Study Group *American Intelligence: A Framework for the Future* 1975. (RW 1056)

Ciarelli, Maj. Gen. Peter W. & Michaelis, M.P.R. "Winning the Peace: The Requirement for Full-Spectrum Operations," *Military Review,* July-August, 2005, pp. 4-17. (RW 3810)

Cilluffo, F.J., Marks, R.A. & Salmoiraghi, G.C. "The use and Limits of US Intelligence," *The Washington Quarterly,* Vol. 106, No. 1, 2002, pp. 61-74. (RW 106)

Cirincione, J. "Assessing the Assessment: The 1999 National Intelligence Estimate of the Ballistic Missile Threat," *The Nonproliferation Review,* Vol. 7, No. 1, 2000, pp. 125-137. (RW 97)

Clapper, J.R. "Joint Military Intelligence," *Joint Forces Quarterly,* 4, 1994, pp. 92-99. (RW 100)

Clapper, J.R. *Proposed Restructuring of the Intelligence Community*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1997. (RW 980)

Clapper, J.R. *How 9/11 Transformed the Intelligence Community*. Available: http://online.wsj.com/article/SB10001424053111904537404576554430822300352.html?mod=asia_opinion, (RW 5092)

Clapper, J.R.J. "The Role of Defense in Shaping U.S. Intelligence Reform," in *Oxford Handbook of National Security Intelligence,* ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 629-639. (RW 4716)

Clarebout, G., Elen, J., Luyten, L. & Bamps, H. "Assessing Epistemological Beliefs: Schommer's Questionnaire Revisited," *Educational Research & Evaluation,* Vol. 7, No. 1, 2001, pp. 53-77. (RW 5302)

Clark State Community College. *Advanced Technical Intelligence,* Clark State Community College. Available: http://www.clarkstate.edu/programdetails.php?Program=4, Viewed: March 22, 2010. (RW 4075)

Clark State Community College. *Advanced Technical Intelligence Certificate,* Clark State Community College. Available: http://www.clarkstate.edu/programdetails.php?Program=120, Viewed: March 22, 2010. (RW 4074)

Clark, A. *Mindware: An Introduction to the Philosophy of Cognitive Science*, Oxford University Press, New York, NY, 2001. (RW 5656)

Clark, C. "Demographic Analysis," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 80-87. (RW 3613)

Clark, K. "On Warning," *Studies in Intelligence,* Vol. 9, No. 1, 1965, pp. 15-21. (RW 548)

Clark, K. "Notes on Estimating," *Studies in Intelligence,* Vol. 11, No. 3, 1967, pp. 55-64. (RW 543)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Clark, R.M. "Scientific and Technical Intelligence Analysis," *Studies in Intelligence,* Vol. 19, No. 1, 1975, pp. 39-48. (RW 552)

Clark, R.M. *Intelligence Analysis: Estimation and Prediction,* American Literary Press, Baltimore, MD, 1996. (RW 1209)

Clark, R.M. *Intelligence Analysis: A Target-Centric Approach,* CQ Press, Washington, DC, 2004. (RW 213)

Clark, R.M. *Intelligence Analysis: A Target-Centric Approach,* 2nd ed., CQ Press, Washington, DC, 2007. (RW 3077)

Clark, R.C. *Building Expertise: Cognitive Methods for Training and Performance Improvement,* 3rd ed., Pfeiffer, San Francisco, 2008. (RW 5105)

Clark, R.C., Nguyen, F. & Sweller, J. *Efficiency in Learning: Evidence-Based Guidelines to Manage Cognitive Load,* Pfeiffer, San Francisco, 2006. (RW 4881)

Clarke, E.L. *The Art of Straight Thinking,* D. Appleton and Company, New York, NY, 1929. (RW 4463)

Clarkson, A. *Toward Effective Strategic Analysis: New Applications of Information Technology,* Westview Press, Boulder, CO, 1981. (RW 700)

Clauser, J. *An Introduction to Intelligence Research and Analysis,* 2008. (RW 3679)

Clauser, J.K. *Propaganda Analysis: Techniques and Procedures for Analysts,* HRB-Singer, Inc, State College, PA, 1973. (RW 964)

Clauser, J.K. & Weir, S.M. *Intelligence Research Methodology: An Introduction to Techniques and Procedures for Conducting Research in Defense Intelligence,* HRB-Singer, State College, PA, 1976. (RW 946)

Clauser, J.K. & Carter, E.S. *The Design of an Intelligence Discipline: Assessment of Intelligence Educational and Training Requirements,* HRB-Singer, Inc, State College, PA, 1965. (RW 947)

Clausner, T.C. & Fox, J.R. "A Framework and Toolkit for Visualizing Tacit Knowledge," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 801)

Clawson, D.A. *What does (should) an Analyst do?* NSWCDD/MP-08/85, Naval Surface Warfare Center, Dahlgren, VA, 2008. (RW 4874)

Claxton, G. *Hare Brain, Tortoise Mind: Why Intelligence Increases when You Think Less,* Ecco Press, Hopewell, NJ, 1999. (RW 5643)

Cleland, C.E. "Methodological and Epistemic Differences between Historical Science and Experimental Science," *Philosophy of Science,* Vol. 69, No. 3, 2002, pp. 474. (RW 5306)

Clift, A.D. *"Catching Field Mice": Intelligence and Policy in the Twenty-First Century,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2003. (RW 1146)

Clift, A.D. *The Changing Landscape of Intelligence Accountability. Speech.* 2007. (RW 2427)

Clift, D.A. "Analysis in the New Era", *National Military Intelligence Association Seminar,* November 12, 2002 (RW 3)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Cline, R.S. "Is Intelligence Over-Coordinated?" *Studies in Intelligence,* Vol. 1, No. 4, 1957, pp. 11-18. (RW 540)

Cline, R.S. "Intelligence: The Problem of Accurate Assessment," in *Foreign Policy and U.S. National Security: Major Postelection Issues*, ed. W.W. Whitson, Praeger, New York, 1976, (RW 4189)

Cline, R.S. *Secrets, Spies, and Scholars: Blueprint of the Essential CIA,* Acropolis Books, Washington, DC, 1976. (RW 779)

Clontz, W.R. *C3I Issues from the United Nations Perspective - Revisited*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1999. (RW 981)

Cloud, J. *The Science of Experience* 2008. (RW 2995)

Clunchy, B. "Revisiting Women's Ways of Knowing," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing*, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 63-87. (RW 4999)

Cluxton, D., Eick, A., Eick, S.G. & Lopez, R. *Hypothesis Mapping and Visualization* (RW 1509)

Cluxton, D. & Eick, S.G. "DECIDE (Tm) Hypothesis Visualization Tool," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 837)

Cluxton, D., Eick, S.G. & Yun, J. *Hypothesis Visualization* (RW 1510)

Codevilla, A.M. *Informing Statecraft: Intelligence for a New Century,* Free Press, New York, NY, 1992. (RW 29)

Codevilla, A.M. "US Intelligence: A Losing Proposition," *The American Spectator,* Vol. 37, No. 7, 2004, pp. 10-16. (RW 234)

Codevilla, A.M. *Why US Intelligence is Inadequate, and how to Fix it,* The Center for Security Policy Occasional Papers No. 2, Center for Security Policy, Washington, DC, 2004. (RW 416)

Coffman, T., Greenblatt, S. & Marcus, S. "Graph-Based Technologies for Intelligence Analysis," *Communications of the ACM,* Vol. 47, No. 3, 2004, pp. 45. (RW 1663)

Cogan, C. "Hunters Not Gatherers: Intelligence in the Twenty-First Century," in *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows,* eds. L.V. Scott & P. Jackson, Routledge, London, UK, 2004, pp. 147-161. (RW 212)

Cogan, C.G. "Intelligence and Crisis Management: The Importance of the Pre-Crisis," *Intelligence and National Security,* Vol. 9, No. 4, 1994, pp. 633-650. (RW 135)

Cognitive Science Society. *Proceedings of the Fifteenth Annual Conference of the Cognitive Science Society: June 18 to 21, 1993, Institute of Cognitive Science, University of Colorado, Boulder,* L. Erlbaum Associates, Hillsdale, N.J, 1993. (RW 1791)

Cohen, E. "Analysis. Essay," in *Intelligence Requirements for the 1990s: Collection, Analysis, Counterintelligence, and Covert Action,* ed. R. Godson, Lexington Books, Lexington, MA, 1989, pp. 71-96. (RW 155)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Cohen, G.L. "Party Over Policy: The Dominating Impact of Group Influence on Political Beliefs," *Journal of Personality and Social Psychology*, Vol. 85, No. 5, 2003, pp. 808-822. (RW 4608)

Cohen, G.L., Aronson, J. & Steele, C.M. "When Beliefs Yield to Evidence: Reducing Biased Evaluation by Affirming the Self," *Personality and Social Psychology Bulletin*, Vol. 26, No. 9, 2000, pp. 1151-1164. (RW 4624)

Cohen, G.L., Bastardi, A., Sherman, D.K., Hsu, L., McGoey, M. & Ross, L. "Bridging the Partisan Divide: Self-Affirmation Reduces Ideological Closed-Mindedness and Inflexibility in Negotiation," *Journal of Personality and Social Psychology*, Vol. 93, No. 3, 2007, pp. 415-430. (RW 4607)

Cohen, H.J. "Policymaker: Know Thine (Intelligence) Analyst," *American Foreign Policy Interests*, Vol. 26, No. 5, 2004, pp. 385-390. (RW 279)

Cohen, J. & Medley, G. *Stop Working & Start Thinking: A Guide to Becoming a Scientist*, 2nd ed., Taylor & Francis Group, Abingdon, Oxon, UK, 2005. (RW 1857)

Cohen, J.D., McClure, S.M. & Yu, A.J. "Should I Stay Or should I Go? How the Human Brain Manages the Trade-Off between Exploitation and Exploration," *Phil. Trans. R. Soc. B: Biological Sciences*, 2007 (RW 2235)

Cohen, M.S. & Freeman, J.T. "Improving Critical Thinking," in *Decision Making Under Stress: Emerging Themes and Applications*, eds. R. Flin, E. Salas, M. Strub & L. Martin, Ashgate Publishing Co., Brookfield, VT, 1997, pp. 161-169. (RW 3791)

Cohen, M.Z. & Omery, A. "Schools of Phenomenology: Implications for Research," in *Critical Issues in Qualitative Research Methods*, ed. J.M. Morse, Sage Publications, Thousand Oaks, 1994, pp. 136. (RW 2746)

Cohen, M.S. *A Database Tool to Support Probabilistic Assumption-Based Reasoning in Intelligence Analysis*, Decision Science Consortium Inc., Reston, VA, [undated]. (RW 482)

Cohen, M.S., Adelman, L., Bresnick, T.A., Marvin, F.F., Salas, E. & Riedel, S. *Dialogue as Medium (and Message) for Training Critical Thinking*, 2004. (RW 4042)

Cohen, M.S., Freeman, J.T., Fallesen, J.J., Marvin, F.F. & Bresnick, T.A. *Training Critical Thinking Skills for Battlefield Situation Assessment: An Experimental Test*, Technical Report 1050, US Army Research Institute for Behavioral and Social Sciences, Alexandria, VA, 1996. (RW 4083)

Cohen, M.S., Freeman, J.T. & Thompson, B. "Critical Thinking Skills in Tactical Decision Making: A Model and A Training Strategy," in *Making Decisions Under Stress: Implications for Individual and Team Training*, eds. J.A. Cannon-Bowers & E. Salas, American Psychological Association, Washington D.C., 1998, pp. 155-190. (RW 4089)

Cohen, M.S. & Thompson, B.B. *Training Teams to Take Initiative: Critical Thinking in Novel Situations*, Arlington, VA, 1999. (RW 4106)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Cohen, M.S., Thompson, B.B., Adelman, L., Bresnick, T.A. & Riedel, S.L. *Training Battlefield Critical Thinking and Initiative,* ARI Research Note 2000-01, US Army Research Institute for the Behavioral and Social Sciences, Alexandria, VA, 1999. (RW 4095)

Cohen, M.S., Thompson, B.B., Adelman, L., Bresnick, T.A., Shastri, L. & Riedel, S.L. *Training Critical Thinking for the Battlefield: Volume I: Basis in Cognitive Theory and Research,* US Army Research Institute, Ft. Leavenworth, KS, 2000. (RW 3790)

Cohen, S. *States of Denial: Knowing about Atrocities and Suffering,* Polity, Cambridge, UK, 2001. (RW 4405)

Cohen, W.M. & Levinthal, D.A. "Absorptive Capacity: A New Perspective on Learning and Innovation," *Administrative Science Quarterly,* Vol. 35, No. 1, 1990, pp. 128-152. (RW 4808)

Coirier, P. "Composing Argumentative Texts: Cognitive and/or Textual Complexity," in *Theories, Models and Methodology in Writing Research,* eds. G. Rijlaarsdam, H. van den Bergh & M. Couzijn, Amsterdam University Press, Amsterdam, 1996, pp. 317. (RW 2136)

Colbaugh, R. & Glass, K. "Discovery and Analysis in Large, Incomplete Data: Proliferation Examples", *ITIC Knowledge Discovery and Dissemination Workshop,* Washington, DC, November (RW 5639)

Colbaugh, R., Glass, K. & Gosler, J. *Some Intelligence Analysis Problems and their Graph Formulations,* Sandia National Laboratories, Albuquerque, NM, 2010. (RW 5603)

Colby, E.A. "Making Intelligence Smart," *Policy Review,* August/September, 2007 (RW 2730)

Colby, W.E. *Memo to Ambassador Murphy* 1973. (RW 1233)

Colby, W.E. "Deception and Surprise: Problems of Analysts and Analysis," in *Intelligence Policy and National Security*, eds. R.L. Pfaltzgraff, U. Ra'anan & W. Milberg, Archon Books, Hamden, CT, 1981, pp. 91-97. (RW 911)

Colby, W.E. "Intelligence in the 1980s," *The Information Society,* Vol. 1, No. 1, 1981, pp. 53-69. (RW 140)

Cole, M. "The Analyst's Toolbox," *Journal of Counterterrorism and Homeland Security International,* Vol. 12, No. 1, 2006, pp. 34. (RW 2367)

Collier, M.W. "Intelligence Analysis: A 9/11 Case Study. " in *Homeland Security and Intelligence,* ed. K.G. Logan, Praeger Security International, Santa Barbara, CA, 2010, pp. 59-73. (RW 5754)

Collier, M.W. "A Pragmatic Approach to Developing Intelligence Analysis," *Defense Intelligence Journal,* Vol. 14, No. 2, 2005, pp. 17-35. (RW 2307)

Collins, A. & Gentner, D. "A Framework for a Cognitive Theory of Writing," in *Cognitive Processes in Writing*, eds. L.W. Gregg & E.R. Steinberg, L. Erlbaum Associates, Hillsdale, NJ, 1980, pp. 51-72. (RW 1499)

Commission on the Roles and Capabilities of the United States Intelligence Community *Scope of the Commission's Inquiry: Executive Summary* 1995. (RW 302)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Commission to Assess the Ballistic Missile Threat to the US *Executive Summary. Report of the Commission*, 1998. (RW 427)

Committee on Behavioral and Social Science Research to Improve Intelligence Analysis for National Security, National Research Council. *Intelligence Analysis for Tomorrow: Advances from the Behavioral and Social Sciences*, National Academies Press, Washington, DC, 2011. (RW 4639)

Committee on Forecasting Future Disruptive Technologies. National Research Council. *Persistent Forecasting of Disruptive Technologies*, 2010. (RW 4120)

Compaine, B.M. & McLaughlin, J.F. *Management Information: Back to Basics*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1986. (RW 982)

Conant, J.B. *On Understanding Science: An Historical Approach*, Yale University Press, New Haven, 1947. (RW 2916)

Condell, J., Wade, J., Galway, L., McBride, M., Gormley, P., Brennan, J. & Somasundram, T. "Problem Solving Techniques in Cognitive Science," *Artificial Intelligence Review*, Vol. 34, 2010, pp. 221. (RW 4370)

Condon, W. & Kelly-Riley, D. "Assessing and Teaching what we Value: The Relationship between College-Level Writing and Critical Thinking Abilities," *Assessing Writing*, Vol. 9, No. 1, 2004, pp. 56-75. (RW 1702)

Conetta, C. & Knight, C. "Inventing Threats," *Bulletin of the Atomic Scientists*, Vol. 54, No. 2, 1998, pp. 32-38. (RW 5669)

Conklin, E.J. *Dialogue Mapping: Building Shared Understanding of Wicked Problems*, Wiley, Chichester, England; Hoboken, NJ, 2006. (RW 4364)

Conley, A.M., Pintrich, P.R., Vekiri, I. & Harrison, D. "Changes in Epistemological Beliefs in Elementary Science Students," *Contemporary Educational Psychology*, Vol. 29, No. 2, 2004, pp. 186-204. (RW 5113)

Conley, R. *Data Security in the Information Age*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1987. (RW 983)

Connable, A.B. *Open Source Acquisition and Analysis: Leveraging the Future of Intelligence at the United States Central Command* 2001. (RW 1471)

Connell, M.W. "Cognitive Factors, Part I: Narrative Psychology," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 20. (RW 3641)

Connell, M.W. "Cognitive Factors, Part I: Narrative Psychology," in *A Handbook of the Psychology of Intelligence Analysis* Central Intelligence Agency, Washington, DC, in publication, pp. 20-52. (RW 2965)

Conradt, L. *When it Pays to Share Decisions*, MacMillan Publishers Ltd. 2011. (RW 4677)

Convertino, G., Billman, D., Pirolli, P., Massar, J.P. & Shrager, J. "The CACHE Study: Group Effects in Computer-Supported Collaborative Analysis," *Computer-Supported Cooperative Work*, Vol. 17, No. 4, 2008, pp. 353-393. (RW 5473)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Conway, L.G. & Schaller, M. "When Authorities' Commands Backfire: Attributions about Consensus and Effects on Deviant Decision Making," *Journal of Personality and Social Psychology,* Vol. 89, No. 3, 2005, pp. 311-326. (RW 1913)

Conway, P. "Red Team: How the Neoconservatives Helped Cause the Iraq Intelligence Failure," *Intelligence and National Security,* Vol. 27, No. 4, 2012, pp. 488-512. (RW 5747)

Cook, D.T. *Roy Godson and Richard Schultz.* Available: http://www.csmonitor.com/2005/0318/p20s01-usmb.html. (RW 624)

Cook, P., Johnson, R., Moore, P., Myers, P., Pauly, S., Pendarvis, F., Prus, J. & Ulmer-Sottong, L. *Critical Thinking Assessment: Measuring a Moving Target. Report & Recommendations of the South Carolina Higher Education Assessment Network Critical Thinking Task Force,* South Carolina Higher Education Assessment Network, Rock Hill, SC, 1996. (RW 3963)

Coombs, M.J., Hartley, R.T. & Pfeiffer, H.D. *Assessment of Model Generative Reasoning for use in the Intelligence Production Performance Model. - Final Rept.* ADA238834/6, New Mexico State University, Las Cruces, NM, 1991. (RW 1204)

Cooper, D.C. *Fundamentals of Search and Rescue,* Jones and Bartlett, Sudbury, MA, 2005. (RW 3903)

Cooper, H.M. *Synthesizing Research: A Guide for Literature Reviews,* 3rd ed., Sage Publications, Thousand Oaks, CA, 1998. (RW 2195)

Cooper, H. & Hedges, L.V. "Potentials and Limitations of Research Synthesis," in *The Handbook of Research Synthesis,* eds. H.M. Cooper & L.V. Hedges, Russell Sage Foundation, New York, 1994, pp. 521. (RW 2492)

Cooper, H. & Hedges, L.V. "Research Synthesis as a Scientific Enterprise," in *The Handbook of Research Synthesis,* eds. H.M. Cooper & L.V. Hedges, Russell Sage Foundation, New York, 1994, pp. 3. (RW 2246)

Cooper, J.R. *Sensemaking: Focusing on the Last Six Inches.* 2002. (RW 2926)

Cooper, J.R. *The Road to Intelligence Transformation: A Process Approach to Curing Analytic Pathologies* 2004?. (RW 3712)

Cooper, J.R. *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis,* Center for the Study of Intelligence, Washington, DC, 2005. (RW 1300)

Copeland, T.E. "Intelligence Failure Theory," in *The International Studies Encyclopedia,* ed. R.A. Denemark, 2010, (RW 3927)

Corbett, L.E. "Serials: Review of the Literature 2000-2003," *Library Resources and Technical Services,* Vol. 50, No. 1, 2006, pp. 16. (RW 1567)

Cordesman, A.H. *Intelligence Failures in the Iraq War,* Center for Strategic and International Studies, Washington, DC, 2003. (RW 481)

Cordesman, A.H. *Intelligence Reform as a Self-Inflicted Wound: Asking the Right Questions,* Center for Strategic and International Studies 2004. (RW 281)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Cornish, E. "How we can Anticipate Future Events," *Futurist*, Vol. 35, No. 4, 2001, pp. 26-33. (RW 236)

Corpora, C.A. "The Stone and the Quarry: Intelligence Studies in a Dynamic Global Environment," *American Intelligence Journal*, Vol. 25, No. 2, 2007/2008, pp. 12. (RW 3225)

Costa, A.L. & Kallick, B. *Describing 16 Habits of Mind*, The Institute for Habits of Mind [undated]. (RW 4544)

Costa, P.C.G., Barbara, D., Laskey, K.B., Wright, E.J., Alghamdi, G., Mirza, S., Revankar, M. & Shackelford, T. "DTB Project: A Behavioral Model for Detecting Insider Threats," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 838)

Couger, J.D. *Creative Problem Solving and Opportunity Finding*, Boyd & Fraser Pub. Co., Danvers, MA, 1995. (RW 2579)

Coulam, R.F. *Illusions of Choice: The F-111 and the Problem of Weapons Acquisition Reform*, Princeton University Press, Princeton, NJ, 1977. (RW 165)

Coulter, J. *'Science' in the Social Sciences*, Office of Behavioral and Social Science Research. Available: http://www.esourceresearch.org/eSourceBook/ScienceintheSocialSciences/1LearningObjectives/tabid/223/Default.aspx, Viewed: April 5, 2012. (RW 5548)

Council for Emerging National Security Affairs. *6th Annual Security Conference. Program and Biographies.* 2005. (RW 272)

Courtright, C. "Context in Information Behavior Research," *Annual Review of Information Science and Technology*, Vol. 41, No. 1, 2007, pp. 273-206. (RW 4453)

Cousins, D.B., Wishar, D.J. & Sharkey, J.B. "Intelligence Collection for Counter Terrorism in Massive Information Content", *Proceedings of the 2004 IEEE Aerospace Conference*, March 6-13, 2004, pp.3273. (RW 3311)

Cousins, N. "The Prisoners of Context," *Saturday Review*, June 1, 1963, pp. 14-49-50. (RW 894)

Coutinho, S.A. "The Relationship between the Need for Cognition, Metacognition and Intellectual Task Performance," *Educational Research and Reviews*, Vol. 1, No. 5, 2006, pp. 162-164. (RW 5309)

Couzin, I. "Connections - Collective Minds," *Nature*, Vol. 445, 2007, pp. 715. (RW 2100)

Cowan, D.A. "Developing a Process Model of Problem Recognition," *Academy of Management Review*, Vol. 11, 1986, pp. 764. (RW 2681)

Cowan, F. "A Review of Recent Intelligence Literature," *SAIS Review*, Vol. 28, No. 1, 2008, pp. 195. (RW 3332)

Cowell, A.J., Chappell, A.R. & Thurman, D.A. "Towards an Adaptive Question Answering System for Intelligence Analysts", *Proceedings of the Human Factors and Ergonomics Society 49th Meeting*, pp. 927. (RW 3569)

Cowell, A.J., McGuinness, D.L., Varley, C.F. & Thurman, D.A. "Knowledge-Worker Requirements for Next Generation Query Answering and Explanation Systems", *Proceedings of*

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

the International Conference on Intelligent User Interfaces, Sydney, Australia, January 29 - February 1, 2006, [unpaged]. (RW 5649)

Cowey, R. "The Future Market for Finished Intelligence," *Studies in Intelligence,* Vol. 20, No. 4, 1976, pp. 1-19. (RW 562)

Cowley, P., Haack, J. & Littlefield, R. "Glass Box: Capturing, Archiving, and Retrieving Workstation Activities", *Carpe'06,* October 28, 2006 (RW 3265)

Cowley, P., Nowell, L. & Scholtz, J. "Glass Box: An Instrumented Infrastructure for Supporting Human Interaction with Information", *Proceedings of the 38th Hawaii International Conference on System Sciences.* (RW 3264)

Coyne, J.W. & Bell, P. "The Role of Strategic Intelligence in Anticipating Transnational Organised Crime: A Literary Review," *International Journal of Law, Crime, and Justice,* Vol. 39, No. 1, 2011, pp. 60-78. (RW 5584)

Coyne, K.P. & Coyne, S.T. "Seven Steps to Better Brainstorming," *McKinsey Quarterly,* 2011, pp. 1-6. (RW 4612)

Coyne, R. "Wicked Problems Revisited," *Design Studies,* Vol. 26, No. 1, 2005, pp. 5. (RW 2571)

Crabtree, B.F. & Miller, W.L. "Primary Care Research: A Multimethod Typology and Qualitative Road Map," in *Doing Qualitative Research*, eds. B.F. Crabtree & W.L. Miller, Sage Publications, Thousand Oaks, Calif, 1992, pp. 3. (RW 2679)

Crabtree, B.F. & Miller, W.L. "Using Codes and Code Manuals: A Template Organizing Style of Interpretation," in *Doing Qualitative Research*, eds. B.F. Crabtree & W.L. Miller, 2nd ed., Sage Publications, Thousand Oaks, Calif, 1999, pp. 163. (RW 2505)

Craig, S. *A Tradecraft Primer: Alternative Analysis Techniques.* 2010. (RW 4476)

Cramer, J. & Thrall, A.T. "Introduction: Why did the United States Invade Iraq?" in *Why did the United States Invade Iraq?*, eds. J. Cramer & A.T. Thrall, Routledge, London, UK, 2011, pp. 1-24. (RW 5012)

Crandall, B., Klein, G.A. & Hoffman, R.R. *Working Minds: A Practitioner's Guide to Cognitive Task Analysis*, MIT Press, Cambridge, MA, 2006. (RW 3554)

Crawford, N.C. "The Passion of World Politics: Propositions on Emotion and Emotional Relationships," *International Security,* Vol. 24, No. 4, 2000, pp. 116. (RW 4413)

Crawford, T.W. "Intelligence Cooperation," in *The International Studies Encyclopedia*, ed. R.A. Denemark, 2010, (RW 3926)

Cremeans, C.D. "The Agency and the Future," *Studies in Intelligence,* Vol. 14, No. 1, 1970, pp. 77-87. (RW 558)

Cremeans, C.D. "Basic Psychology for Intelligence Analysts," *Studies in Intelligence,* Vol. 15, No. 1, 1971, pp. 109-114. (RW 524)

Cressley, C.A. "Predictive Markets," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 95-102. (RW 3615)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Creswell, J.W. *Research Design: Qualitative & Quantitative Approaches*, Sage Publications, Thousand Oaks, CA, 1994. (RW 4726)

Creswell, J.W. *Qualitative Inquiry & Research Design: Choosing among Five Approaches*, 2nd ed., Sage Publications, Thousand Oaks, 2007. (RW 2244)

Creswell, J.W. & Plano Clark, V.L. *Designing and Conducting Mixed Methods Research*, SAGE Publications, Thousand Oaks, CA, 2007. (RW 3091)

Cristobal, R. *How Best to Organize and Optimize the Analytical Effort within the US Intelligence Community*, Accenture, Reston, VA, 2010. (RW 5678)

Cristobal, R. *How Best to Organize and Optimize the Analytical Effort within the US Intelligence Community*, U. S. Army War College, Carlisle, PA, 2010. (RW 5798)

Cristol, A.J. *The Liberty Incident*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1996. (RW 984)

Cristol, A.J. *The USS Liberty and the Role of Intelligence.* 2004. (RW 514)

Croft, W.B. & Center for Intelligent Information Retrieval *Advances in Information Retrieval: Recent Research from the Center for Intelligent Information Retrieval*, Kluwer Academic, Boston, 2000. (RW 3538)

Cross, V. *The Practice-Based Educator: A Reflective Tool for CPD and Accreditation*, Wiley, Chichester, England; Hoboken, NJ, 2006. (RW 5318)

Crotty, M. *The Foundations of Social Research: Meaning and Perspective in the Research Process*, Sage Publications, London; Thousand Oaks, CA, 1998. (RW 3842)

Crystal, M.R. & Pine, C. "Automated Org-Chart Generation from Intelligence Message Traffic," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 596)

Cuban, L. "Policy and Research Dilemmas in the Teaching of Reasoning: Unplanned Designs," *Review of Educational Research*, Vol. 54, No. 4, 1984, pp. 655-81. (RW 5366)

Cuban, L. "Informal Reasoning and Instruction: A Commentary," in *Informal Reasoning and Education*, eds. J.F. Voss, D.N. Perkins & J.W. Segal, L. Erlbaum Associates, Hillsdale, NJ, 1991, pp. 473-484. (RW 5001)

Cubukcu, Z. "Critical Thinking Dispositions of the Turkish Teacher Candidates," *The Turkish Online Journal of Educational Technology*, Vol. 5, No. 4, 2006, pp. 22-36. (RW 5033)

Cumming, A. *The Position of Director of National Intelligence: Issues for Congress.* 2004. (RW 283)

Cumming, A. *Side-by-Side Comparison of Intelligence Community Reforms Proposed by 9/11 Commission, the Bush Administration, Senators Feinstein, Graham and Daschle, and Representatives Harman and Goss; and Current Statute.* 2004. (RW 291)

Cunha, F. & Heckman, J.J. *Investing in our Young People*, Working paper 16201, National Bureau of Economic Research, 2010. (RW 4365)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Cunningham, C.J. *Information Technology and Organizational Agility*, Center for Information Policy Research. Harvard University, Cambridge, MA, 2000. (RW 985)

Cunningham, J.W. & Fitzgerald, J. "Epistemology and Reading," *Reading Research Quarterly*, Vol. 31, No. 1, 1996, pp. 36-60. (RW 5350)

Cunningham, S.J., Witten, I.H. & Littin, J. "Cognitive Information Retrieval," *Annual Review of Information Science and Technology*, Vol. 34, 1999-2000, pp. 341. (RW 3979)

Cupp, S., Foreman, J., Gievska-Krliu, S. & Heller, R.S. *Learning to use Virtual Team Collaboration to Solve Wicked Problems*. Available: http://www.acm.org/crossroads/xrds10-1/wickedproblems.html, Viewed: June 1, 2009. (RW 3498)

Cushman, J.H. *C3I and the Commander: Responsibility and Accountability*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1981. (RW 986)

Cushman, J.H. *Command and Control of Theater Forces: The Future of Force Projection*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1995. (RW 987)

Cutler, R. "Intelligence as a Foundation for Policy," *Studies in Intelligence*, Vol. 3, No. 4, 1959, pp. 59-71. (RW 534)

Czaja, S.J., Sharit, J. & Nair, S.N. "What Factors Other than Age Predict Performance on an Information Search Task?", *Proceedings of the Human Factors and Ergonomics Society 50th Meeting*, pp. 195. (RW 3576)

Czarnecki, J.E. "The Limits of Information," in *Proteus Futures Digest: A Compilation of Selected Works Derived from the 2007 Proteus Workshop*, eds. J. Auger & W. Wimbish, 2nd ed., U.S. Army War College, Carlisle Barracks, PA, 2007, pp. 59-67. (RW 4812)

Daalder, I.H. & Lake, A. "Smart Choices about Intelligence Reform," *Boston Globe*, August 19, 2004 (RW 233)

Daguio, K. *Protecting the Financial and Payment System by Dispelling Myths*, Center for Information Policy Research. Harvard University, Cambridge, MA, 2000. (RW 988)

Dahl, E.J. *Warning of Terror: Explaining the Failure of Intelligence Against Terrorism*, M.A. thesis, Tufts University, 2004. (RW 485)

Dahl, E.J. “Warning of Terror: Explaining the Failure of Intelligence Against Terrorism,” *the Journal of Strategic Studies*, Vol. 28, No. 1, 2005, pp. 31-55. (RW 1302)

Dahl, E.J. "Intelligence and Terrorism," in *The International Studies Encyclopedia*, ed. R.A. Denemark, 2010. (RW 3925)

Dahl, E.J. "Missing the Wake-Up Call: Why Intelligence Failures Rarely Inspire Improved Performance," *Intelligence and National Security*, Vol. 25, No. 6, 2010, pp. 778-799. (RW 4575)

Dahl, E.J. "Why Won't they Listen? Comparing Receptivity Toward Intelligence at Pearl Harbor and Midway," *Intelligence and National Security*, Vol. 28, No. 1, 2013, pp. 68-90. (RW 5913)

Dahl, T.I., Bals, M. & Turi, A.L. "Are Students' Beliefs about Knowledge and Learning Associated with their Reported use of Learning Strategies?" *British Journal of Educational Psychology*, Vol. 75, No. 2, 2005, pp. 257-273. (RW 5429)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Dahlstrom, E.L. *From Reconnaissance to Surveillance: Intelligence Transformation in the New Millennium,* (RW 1254)

Dahn, M. "Spotlight on the Invisible Web," *Online Magazine,* July-August, 2000, pp. 57. (RW 1460)

Dai, D.Y. "Epilogue: Putting it all Together: Some Concluding Thoughts," in *Motivation, Emotion, and Cognition: Integrative Perspectives on Intellectual Functioning and Development,* eds. D.Y. Dai & R.J. Sternberg, L. Erlbaum Associates, Mahwah, NJ, 2004, pp. 419. (RW 3485)

Dalby, S. "Security, Intelligence, the National Interest and the Global Environment," *Intelligence and National Security,* Vol. 10, No. 4, 1995, pp. 175. (RW 1664)

Daley, B.J., Shaw, C.R., Balistrieri, T., Glasenapp, K. & Piacentine, L. "Concept Maps: A Strategy to Teach and Evaluate Critical Thinking," *Journal of Nursing Education,* Vol. 38, No. 1, 1999, pp. 42-47. (RW 3956)

Daley, B.J., Lovell, M.R., Perez, R.A. & Stern, N.E. "Using Concept Maps within the Product Design Process in Engineering: A Case Study," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge,* eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 229-252. (RW 4974)

Dall'Alba, G. & Sandberg, J. "Learning through and about Practice: A Lifeworld Perspective," in *Learning through Practice: Models, Traditions, Orientations, and Approaches,* ed. S. Billett, Springer, Dordrecht, 2010, pp. 104-119. (RW 4958)

Daly, P.H. *Critical Infrastructure Protection,* Center for Information Policy Research. Harvard University, Cambridge, MA, 2000. (RW 989)

Dama, M. & Dunbar, K. "Distributed Reasoning. an Analysis of Where Social and Cognitive Worlds Fuse." *Proceedings of the 18th Annual Conference of the Cognitive Science Society,* 1996, pp. 166. (RW 2225)

Damer, T.E. *Attacking Faulty Reasoning: A Practical Guide to Fallacy-Free Arguments,* 5th ed., Thomson/Wadsworth, Belmont, CA, 2005. (RW 4019)

Daneman, M. & Carpenter, P.A. "Individual Differences in Working Memory and Reading," *Journal of Verbal Learning and Verbal Behavior,* Vol. 19, No. 4, 1980, pp. 450-466. (RW 4920)

Danforth, L.W. *One Dog to Kick.* (RW 1255)

Daniel, B. "Alexander Von Humboldt: Expeditionary Scientist," in *Sourcebook of Experiential Education: Key Thinkers and their Contributions,* eds. T.E. Smith & C. Knapp, Routledge, New York, 2011, pp. 93-99. (RW 4925)

Daniels, H. *The Role of the National Security Agency in Command, Control, and Communications,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1987. (RW 990)

Dannefer, D. "Adult Development and Social Theory: A Paradigmatic Reappraisal," *American Sociological Review,* Vol. 49, No. 1, 1984, pp. 100. (RW 4424)

Darr, K. "Problem Solving Revisited," *Hospital Topics,* Vol. 76, No. 2, 1998 (RW 2612)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Das-Neves, F., Fox, E.A. & Yu, X. "Connecting Topics in Document Collections with Stepping Stones and Pathways", *Proceedings of the 14th ACM International Conference on Information and Knowledge Management,* Bremen, Germany, October 31 - November 05, 2005, pp. 91-98. (RW 5577)

Daugherty, W.J. "Behind the Intelligence Failure in Iran," *International Journal of Intelligence and Counterintelligence,* Vol. 14, No. 4, 2001, pp. 449-484. (RW 274)

Daugherty, W.J. "The Role of Covert Action," in *Handbook of Intelligence Studies,* ed. L.K. Johnson, 2007, pp. 279. (RW 2474)

Dave, C. & Wolfe, K.W. *On Confirmation Bias and Deviations Prom Bayesian Updating.* 2003. (RW 1943)

Davenport, T.H. *Thinking for a Living: How to Get Better Performance and Results from Knowledge Workers,* Harvard Business School Press, Boston, MA, 2005. (RW 971)

Davenport, T.H. "Rethinking Knowledge Work: A Strategic Approach," *McKinsey Quarterly,* February, 2011 (RW 4551)

Davenport, T.H. *Enterprise Analytics: Optimize Performance, Process, and Decisions through Big Data,* FT Press, Upper Saddle River, NJ, 2013. (RW 5854)

Davidson, R.A. "Cognitive Complexity and Performance in Professional Accounting Examinations," *Accounting Education,* Vol. 5, No. 3, 1996, pp. 219. (RW 4288)

Davidson, R.A. & Jones, S.H. *An Empirical Test of Three Measures of Problem-Solving Ability.* 2000. (RW 2613)

Davies, H.T.O. & Crombie, I.K. *What is a Systematic Review?* (RW 2218)

Davies, J. "Believing the Evidence," in *Evidence, Inference and Enquiry*, eds. P. Dawid, W. Twining & M. Vasilaki, 2011, pp. 395-434. (RW 5632)

Davies, P.C.W. *The Mind of God: The Scientific Basis for a Rational World,* Simon & Schuster, New York, NY, 1992. (RW 5826)

Davies, P. "The Relevance of Systematic Reviews to Educational Policy and Practice," *Oxford Review of Education,* Vol. 26, No. 3/4, 2000 (RW 2253)

Davies, P.H. "Intelligence Culture and Intelligence Failure in Britain and the United States," *Cambridge Review of International Affairs,* Vol. 17, No. 3, 2004, pp. 495-520. (RW 160)

Davies, P.H.J. "Intelligence, Information Technology, and Information Warfare," *Annual Review of Information Science and Technology,* Vol. 36, No. 1, 2002, pp. 312. (RW 1577)

Davies, P.H.J. "Assessment BASE: Simulating National Intelligence Assessment in a Graduate Course," *International Journal of Intelligence and Counterintelligence,* Vol. 19, No. 4, 2006, pp. 721. (RW 1753)

Davies, P.H.J. "Theory and Intelligence Reconsidered," in *Intelligence Theory: Key Questions and Debates,* eds. P. Gill, S. Marrin & M. Phythian, 2009, pp. 186. (RW 3412)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Davis, C.N. "The Flaws in Intelligence Reform (Analysis) (the Intelligence Reform Bill is Analysed)," *National Catholic Reporter,* Vol. 41, No. 9, 2004, pp. 6. (RW 790)

Davis, D.A. "How to Help Professionals Maintain and Improve their Knowledge and Skills: Triangulating Best Practices in Medicine," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 180-202. (RW 5141)

Davis, E.A. "Students' Epistemological Beliefs about Science and Learning", *Annual Meeting of the American Educational Research Association,* Chicago, IL, April, 1997 (RW 4841)

Davis, J. *The Challenge of Opportunity Analysis,* Center for Study of Intelligence Monograph Program, Reston VA, 1992. (RW 4190)

Davis, J. "Combating Mindset," *Studies in Intelligence,* Vol. 36, No. 5, 1992, pp. 13-18. (RW 66)

Davis, J. "Kent-Kendall Debate of 1949," *Studies in Intelligence,* Vol. 36, No. 5, 1992, pp. 91-103. (RW 4176)

Davis, J. "Defining the Analytic Mission: Facts, Findings, Forecasts, and Fortune-Telling," *Studies in Intelligence,* Fall, 1995, pp. 25. (RW 117)

Davis, J. "A Policymaker's Perspective on Intelligence Analysis," *Studies in Intelligence,* Vol. 38, No. 2, 1995, pp. 1-9. (RW 65)

Davis, J. "The Challenge of Managing Uncertainty: Paul Wolfowitz on Intelligence-Policy Relations," *Studies in Intelligence,* Vol. 39, No. 5, 1996, pp. 35-42. (RW 4167)

Davis, J. "Paul Wolfowitz on Intelligence Policy-Relations," *Studies in Intelligence,* Vol. 39, No. 5, 1996, pp. 35-42. (RW 115)

Davis, J. *Uncertainty, Surprise, and Warning,* 1996. (RW 197)

Davis, J. *Intelligence Analysis in a New Century: A Curmudgeon's View* 2000. (RW 1450)

Davis, J. "Improving CIA Analytic Performance: Analysts and the Policymaking Process," *The Sherman Kent Center for Intelligence Analysis Occasional Papers,* Vol. 1, No. 2, 2002 (RW 345)

Davis, J. "Improving CIA Analytic Performance: DI Analytic Priorities," *The Sherman Kent Center for Intelligence Analysis Occasional Papers,* Vol. 1, No. 3, 2002 (RW 346)

Davis, J. "Improving CIA Analytic Performance: Strategic Warning," *The Sherman Kent Center for Intelligence Analysis Occasional Papers,* Vol. 1, No. 1, 2002 (RW 344)

Davis, J. "Sherman Kent and the Profession of Intelligence Analyst," *The Sherman Kent Center for Intelligence Analysis Occasional Papers,* Vol. 1, No. 5, 2002 (RW 253)

Davis, J. *Analytic Paradoxes: Can Open Source Intelligence Help?* 2003. (RW 1449)

Davis, J. "Sherman Kent's Final Thoughts on Analyst-Policymaker Relations," *The Sherman Kent Center for Intelligence Analysis Occasional Papers,* Vol. 2, No. 3, 2003 (RW 349)

Davis, J. "Strategic Warning: If Surprise is Inevitable, what Role for Analysis?" *The Sherman Kent Center for Intelligence Analysis Occasional Papers,* Vol. 2, No. 1, 2003, pp. 1. (RW 93)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Davis, J. "Tensions in Analyst-Policymaker Relations: Opinions, Facts, and Evidence," *The Sherman Kent Center for Intelligence Analysis Occasional Papers,* Vol. 2, No. 2, 2003 (RW 348)

Davis, J. "Defining the Analytic Mission: Facts, Findings, Forecasts, and Fortunetelling," in *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, eds. R.Z. George & R.D. Kline, National Defense University Press, Washington, DC, 2004, pp. 295-301. (RW 694)

Davis, J. "Intelligence Analysts and Policymakers: Benefits and Dangers of Tensions in the Relationship," *Intelligence and National Security,* Vol. 21, No. 6, 2006, pp. 999. (RW 2083)

Davis, J. "Intelligence Analysts and Policy Makers: Benefits and Dangers of Tensions in the Relationship," in *Strategic Intelligence. Volume 2: The Intelligence Cycle: The Flow of Secret Information from Overseas to the Highest Councils of Government*, ed. L.K. Johnson, Praeger Security International, Westport, CT, 2007, pp. 143. (RW 2707)

Davis, J. "Strategic Warning: Intelligence Support in a World of Uncertainty and Surprise," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 173. (RW 2466)

Davis, J. "Why Bad Things Happen to Good Analysts," in *Analyzing Intelligence: Origins, Obstacles, and Innovations*, eds. R.Z. George & J.B. Bruce, 2008, pp. 157-170. (RW 3102)

Davis, J., Dutra, I., Page, D. & Costa, V.S. "Establishing Identity Equivalence in Multi-Relational Domains," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 840)

Davis, L.E., Treverton, G.F., Byman, D., Daly, S. & Rosenau, W. *Coordinating the War on Terrorism,* OP-110-RC, RAND Corporation, Santa Monica, CA, 2004. (RW 1084)

Davis, P.K. & Arquilla, J. *Thinking about Opponent Behavior in Crisis and Conflict: A Generic Model for Analysis and Group Discussion,* ADA253258, 1991. (RW 1135)

Davis, R. *Foreign Missile Threat. Analytic Soundness of National Intelligence Estimate 95-19. United States General Accounting Office Testimony before the Select Committee on Intelligence,* 1996. (RW 438)

Davis, R.M. "Introductory Remarks to the Information Systems for Intelligence Session," in *Information System Science and Technology. Papers Prepared for the Third Congress*, eds. D.E. Walker, United States & Mitre Corporation, Thompson Book Co, Washington, 1967, pp. 293. (RW 1474)

Dawes, R.M. "Prediction of the Future Versus an Understanding of the Past: A Basic Asymmetry," *American Journal of Psychology,* Vol. 106, No. 1, 1993, pp. 1. (RW 2334)

Dawid, P. "Introduction," in *Evidence, Inference and Enquiry*, eds. P. Dawid, W. Twining & M. Vasilaki, 2011, pp. 1-10. (RW 5261)

Dawid, P., Schum, D. & Hepler, A. "Inference Networks: Bayes and Wigmore," in *Evidence, Inference and Enquiry*, eds. P. Dawid, W. Twining & M. Vasilaki, 2011, pp. 119-150. (RW 5630)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Dawson, M. "Intelligence Work: The Mundane World of High-Consequence Analysis," in *Anthropologists in the SecurityScape: Ethics, Practice, and Professional Identity*, eds. R. Albro, G. Marcus, L.A. McNamara & M. Schoch-Spana, Left Coast Press, Walnut Creek, CA, 2011, pp. 71-86. (RW 5486)

Day, D.V. "Leadership," in *Oxford Handbook of Organizational Psychology*, ed. W.J. Kozlowski, Oxford University Press, New York, NY, 2012, pp. 696-729. (RW 4720)

Dayton, B.W. "Managing Crises in the Twenty-First Century," *International Studies Review*, Vol. 6, 2004, pp. 165. (RW 2622)

DCI Director of Central Intelligence. Scientific and Technical Intelligence Committee. *Preparing US Intelligence for the Information Age Part III: Analytical Tools Recommendations for Open Source Information* 1995. (RW 1200)

DCI Director of Central Intelligence. Scientific and Technical Intelligence Committee. *Preparing US Intelligence for the Information Age Part IV: Analyst Training Recommendations*, National Technical Information Service, Springfield, VA, 1995. (RW 1201)

de Blaaij, C. "Grey Literature from Invisibility to Visibility," *Publishing Research Quarterly*, Spring, 2004, pp. 70. (RW 1421)

de Borchgrave, A., Sanderson, T. & Harned, J. *Force Multiplier for Intelligence: Collaborative Open Source Networks*, 2007. (RW 2798)

de Borchgrave, A., Sanderson, T. & MacGaffin, J. *Open Source Information*, 2006. (RW 1627)

De Corte, E., Eynde, O.T. & Verschaffel, L. ""Knowing what to Believe": The Relevance of Students' Mathematical Beliefs for Mathematics Education," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing*, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 297-320. (RW 4989)

de Kwaadsteniet, L., Witteman, C. & Krol, N. *Capturing Psychodiagnostic Decision Making* (RW 2067)

de Mesquita, B.B. "Applications of Game Theory in Support of Intelligence Analysis," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, pp. 57-82. (RW 4772)

De Montfort University Library *Internet 4. Accessing the Invisible Web. Electronic Information Guides.* (RW 1397)

de Sousa *Reasoning and Emotion, in Light of the Dual Processing Model of Cognition* [undated]. (RW 5860)

de Valk, G.G. *Dutch Intelligence - Towards a Qualitative Framework for Analysis*, Ph.D. dissertation, Rijksuniversiteit Groningen, 2005. (RW 3122)

de Waal, F. B. M. *The Bonobo and the Atheist: In Search of Humanism among the Primates*, W.W. Norton, New York, 2013. (RW 5916)

Deacon, T.W. *The Symbolic Species: The Co-Evolution of Language and the Brain*, W.W. Norton, New York, 1997. (RW 5907)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Dean, D. & Webb, C. "Recovering from Information Overload," *McKinsey Quarterly*, January, 2011 (RW 4553)

Dearlove, R. "National Security and Public Anxiety: Our Changing Perceptions," in *Oxford Handbook of National Security Intelligence*, ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 33-42. (RW 4702)

Dearth, D.H. & Goodden, R.T. *Strategic Intelligence: Theory and Application,* 2nd ed., United States Army War College, Carlisle Barracks, PA, 1995. (RW 1121)

Dearth, D.H. & Shope, V.C. *Strategic Intelligence and National Security: A Selected Bibliography,* Updated ed., U.S. Army War College Library, Carlisle Barracks, PA, 1992. (RW 1092)

Deary, I. "Why do Intelligent People Live Longer?" *Nature,* Vol. 456, 2008, pp. 175. (RW 3355)

Deaton, C., Shepard, B., Klein, C., Mayans, C., Summers, B., Brusseau, A., Witbrock, M. & Lenat, D. "The Comprehensive Terrorism Knowledge Base in Cyc," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 875)

DeBacker, T.K., Crowson, H.M., Beesley, A.D., Thoma, S.J. & Hestevold, N. "The Challenges of Measuring Epistemic Beliefs: An Analysis of Three Self-Report Instruments," *Journal of Experimental Education*, Vol. 76, No. 3, 2008, pp. 281-312. (RW 5068)

DeBacker, T.K. & Crowson, H.M. "Influences on Cognitive Engagement: Epistemological Beliefs and Need for Closure," *British Journal of Educational Psychology*, Vol. 76, No. 3, 2006, pp. 535-551. (RW 5528)

Dedijer, S. & Jequier, N. *Intelligence for Economic Development: An Inquiry into the Role of the Knowledge Industry,* St. Martin's Press, New York; NY, 1987. (RW 656)

DeFalco, R.L. "Blind to the Sun: US Intelligence Failures before the War with Japan," *International Journal of Intelligence and Counterintelligence*, Vol. 16, No. 1, 2003, pp. 95-107. (RW 512)

Defense Intelligence Agency. *General Defense Intelligence Program. Information Technology Strategic Plan Fiscal Years 2008-2013* 2006. (RW 2904)

Defense Intelligence Agency. Directorate for Analysis. *A Tradecraft Primer: Basic Structured Analytic Techniques* 2008. (RW 3277)

Defense Intelligence Agency. Directorate for Analysis. *A Tradecraft Primer: Basic Structured Analytic Techniques. Second Edition* 2009. (RW 3503)

Degrace, P. & Stahl, L.H. *Wicked Problems, Righteous Solutions: A Catalogue of Modern Software Engineering Paradigms,* Yourdon Press, Englewood Cliffs, NJ, 1990. (RW 2532)

Delaney, H.D. *III. The Nature of Science*. Available: http://www.unm.edu/~hdelaney/natureofscience.html, Viewed: October 10, 2011. (RW 5163)

DeLauer, R.D. *A Major Contractor's View of C3I,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1981. (RW 991)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

DeLauer, R.D. *The View from the Hot Seat,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1982. (RW 993)

DeLauer, R.D. *A Consultant's View,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1986. (RW 992)

DeLisi, P. & Danielson, R. *"I Think I Am, therefore..." an Inquiry into the Thinking Styles of IT Executives and Professionals* (RW 2403)

Dellerman, P., Coirier, P. & Marchand, E. "Planning and Expertise in Argumentative Composition," in *Theories, Models and Methodology in Writing Research,* eds. G. Rijlaarsdam, H. van den Bergh & M. Couzijn, Amsterdam University Press, Amsterdam, 1996, pp. 182. (RW 2133)

DeLuca, J.B., Mullins, M.M., Lyles, C.M. & Crepaz, N. "Developing a Comprehensive Search Strategy for Evidence Based Systematic Reviews," *Evidence Based Library and Information Practice,* Vol. 3, No. 1, 2008, pp. 3-32. (RW 4801)

DeMarines, V.A. *FFRDC Business at MITRE,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1999. (RW 996)

Dempsey, J.A. *Intelligence and Homeland Security After 9/11,* Center for Information Policy Research. Harvard University, Cambridge, MA, 2004. (RW 619)

Dempsey, J.A. *The Limitations of Recent Intelligence Reforms.* 2006. (RW 1781)

Denyer, D. & Tranfield, D. "Using Qualitative Research Synthesis to Build an Actionable Knowledge Base," *Management Decision,* Vol. 44, No. 2, 2006, pp. 213. (RW 2292)

Denzin, N.K. & Lincoln, Y.S. *Handbook of Qualitative Research,* Sage Publications, Thousand Oaks, 1994. (RW 2671)

Department of Defense. *Directive 5105.21. Defense Intelligence Agency (DIA)* 2008. (RW 3024)

Department of Defense. *Instruction Number 1400.36. DoD Implementation of the Joint Intelligence Community Duty Assignment (JDA) Program* 2008. (RW 3166)

Department of Defense. *Instruction Number 3305.26. DoD Measurement and Signature Intelligence (MASINT) Training* 2008. (RW 3165)

Department of Defense. Department of the Army. *Production Requirements and Threat Intelligence Support to the U.S. Army. Army Regulation 381-11* 2000. (RW 420)

Department of Defense. Under Secretary of Defense for Intelligence *Defense Intelligence Strategy* 2008. (RW 3132)

Department of the Army. *Open Source Intelligence. Field Manual. Interim.* 2006. (RW 2054)

Department of the Navy. Office of the Chief of Naval Operations. *OPNAVINST 3811.1C. Threat Support to Weapons Systems Planning and Acquisition.* 1995. (RW 449)

Deptula, D. *USAF Intelligence Way Ahead [Powerpoint Presentation] v2.* 2007. (RW 1956)

Deptula, D. & Francisco, M. "Air Force ISR Operations: Hunting Versus Gathering," *Air & Space Power Journal,* Winter, 2010, pp. 13-17. (RW 4507)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Depue, B.E., Curran, T. & Banich, M. "Prefrontal Regions Orchestrate Suppression of Emotional Memories Via a Two-Phase Process," *Science,* Vol. 317, No. 13 July, 2007, pp. 215. (RW 2569)

Der Derian, J. *Antidiplomacy: Spies, Terror, Speed, and War,* Blackwell, Cambridge, MA, 1992. (RW 1194)

Derbentseva, N. & Mandel, D.R. "Using Concept Maps to Improve the Practice and Organization of Intelligence in Canada. Draft Version," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge*, eds. B. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, [undated], (RW 4745)

Derbentseva, N. & Mandel, D.R. "Using Concept Maps to Improve the Practice and Organization of Intelligence in Canada," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge*, eds. B. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 109-130. (RW 4742)

Derbentseva, N., McLellan, L. & Mandel, D.R. *Issues in Intelligence Production: Summary of Interviews with Canadian Managers of Intelligence Analysts,* TR 2010-144, Defence R&D Canada, Toronto, ONT, 2010. (RW 4849)

DeRosa, M. *Data Mining and Data Analysis for Counterterrorism,* CSIS Press, Washington, DC, 2004. (RW 1687)

Derrick, A.A. *The Availability and Viability of Open Source Operational Tradecraft,* M. S. thesis, Mercyhurst College, 2007. (RW 3422)

Dervin, B. & Nilan, M. "Information Needs and Uses," *Annual Review of Information Science and Technology,* Vol. 21,1986, pp. 3. (RW 1357)

Dervin, B. "What Methodology does to Theory: Sense-Making Methodology as Exemplar," in *Theories of Information Behavior,* eds. K.E. Fisher, S. Erdelez & L. McKechnie, Published for the American Society for Information Science and Technology by Information Today, Medford, N.J, 2005, pp. 25. (RW 3533)

Dervin, B., Foreman-Wernet, L. & Lauterbach, E. *Sense-Making Methodology Reader: Selected Writings of Brenda Dervin,* Hampton Press, Cresskill, NJ, 2003. (RW 3553)

Dery, D. *Problem Definition in Policy Analysis,* University Press of Kansas, Lawrence, Kan., 1984. (RW 2701)

Desforges, C. & McNamara, D. "Theory and Practice: Methodological Procedures for the Objectification of Craft Knowledge," *British Journal of Teacher Education,* Vol. 5, No. 2, 1979, pp. 145-152. (RW 4569)

Desimone, R. & Charles, D. *Towards an Ontology for Intelligence Analysis and Collection Management*, QinetiQ Ltd, Malvern, UK, [undated]. (RW 305)

Desnoyers, C.A. "Vying for the use of CmapTools in Corporate Training," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge*, eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 317-326. (RW 4978)

Detterman, D.K. & Sternberg, R.J. *Transfer on Trial: Intelligence, Cognition, and Instruction,* Ablex Pub. Corp., Norwood, NJ, 1993. (RW 2799)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Deutch, J. & Smith, J.H. "Smarter Intelligence," *Foreign Policy,* Vol. 232, January/February, 2002, pp. 64-69. (RW 232)

Deutsch, D. *The Fabric of Reality: The Science of Parallel Universes and its Implications,* Allen Lane, New York, NY, 1997. (RW 4565)

Devine, D.J. & Kozlowski, S.W.J. "Domain-Specific Knowledge and Task Characteristics in Decision Making," Vol. 64, No. 3, 1995, pp. 294. (RW 2766)

Devlin, K. *A Framework for Modeling Evidence-Based, Context-Influenced Reasoning,* [undated]. (RW 486)

Devlin, K. *Confronting Context Effects in Intelligence Analysis: How can Mathematics Help? July 15, 2005 Version,* 2005. (RW 1220)

Devlin, K. *Confronting the Context Effects in Intelligence Analysis: How can Mathematics Help?* 2005. (RW 4)

Devlin, K.J. *Infosense: Turning Information into Knowledge,* W.H. Freeman, New York, 1999. (RW 1538)

Dewey, J. *How we Think,* D. C. Heath & Co., Chicago, IL, 1910. (RW 4460)

Dewey, J. *How we Think: A Restatement of the Relation of Reflective Thinking to the Educative Process,* 2nd ed., Regnery, Chicago, IL, 1933. (RW 3935)

Dewey, J. & Bentley, A.F. *Knowing and the Known,* Beacon Press, Boston, 1960. (RW 4241)

Dexter, P., Applegate, M., Backer, J., Claytor, K., Keffer, J., Norton, B. & Ross, B. "A Proposed Framework for Teaching and Evaluating Critical Thinking in Nursing," *Journal of Professional Nursing,* Vol. 13, No. 3, 1997, pp. 160-167. (RW 3957)

Diamond, J. "Soft Sciences are often Harder than Hard Sciences," *Discover,* Vol. 8, No. 8, 1987, pp. 34-39. (RW 5134)

Diamond, J.M. *Guns, Germs, and Steel: The Fates of Human Societies,* W.W. Norton, New York, NY, 1997. (RW 5104)

Diamond, J.M. & Robinson, J.A. *Natural Experiments of History,* Belknap Press, Cambridge, MA, 2010. (RW 5103)

Diamond, J. *The CIA and the Culture of Failure: U.S. Intelligence from the End of the Cold War to the Invasion of Iraq,* Stanford Security Series, Stanford, CA, 2008. (RW 3271)

Diaz, G. *Methodological Approaches to the Concept of Intelligence Failure,* UNISCI, Madrid, Spain, 2005. (RW 499)

Dick, R.D. "An Empirical Taxonomy of Critical Thinking," *Journal of Instructional Psychology,* Vol. 18, No. 2, 1991, pp. 79-92. (RW 5236)

Dickinson, H. *Planning for Defense-Wide Command and Control,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1982. (RW 997)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Didsbury, K. "Teaching Precise Processing through Writing Instruction," in *Thinking Skills Instruction: Concepts and Techniques*, eds. M. Heiman & J. Slomianko, National Education Association, Washington, DC, 1987, pp. 167-173. (RW 5085)

Dieckmann, N.F. *Communicating Risk in Intelligence Forecasts: The Consumer's Perspective*, Ph.D. dissertation, University of Oregon, 2007. (RW 4542)

Diekema, A.R., Hannouche, J., Ingersoll, G., Oddy, R.N. & Liddy, E.D. "Analyst-Focused Arabic Information Retrieval," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 817)

Diesing, P. *Patterns of Discovery in the Social Sciences*, Aldine·Atherton, Chicago, 1971. (RW 3530)

Dietrich, F. & List, C. *A Model of Jury Decisions Where all Jurors have the Same Evidence.* 2002. (RW 2061)

Dilworth, R.L. & Boshyk, Y. *Action Learning and its Applications*, Palgrave Macmillan, Basingstoke, UK, 2010. (RW 5314)

Dimnet, E. *The Art of Thinking*, Simon and Schuster, New York, NY, 1928. (RW 4490)

Dinneen, G.P. *C3 Priorities*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1982. (RW 998)

Director of National Intelligence. *100 Day Integration and Collaboration Plan* 2007. (RW 2209)

Director of National Intelligence. *Vision 2015*, 2008? (RW 3187)

Director of National Intelligence. CIO, Intelligence Community Technology Governance *Intelligence Community Classification Guidance Findings and Recommendations Report* 2008. (RW 3060)

Diriye, A., Wilson, M.L., Blandford, A. & Tombros, A. "Revisiting Exploratory Search from the HCI Perspective", *HCIR 2010: Proceedings of the Fourth Workshop on Human-Computer Interaction and Information Retrieval*, New Brunswick, NJ, August 22, 2010, pp. 99. (RW 4320)

DiSalvo, D. *What Makes Your Brain Happy and Why You should do the Opposite*, Prometheus Books, Amherst, NY, 2011. (RW 5377)

diSessa, A.A., Elby, A. & Hammer, D. "J's Epistemological Stance and Strategies," in *Intentional Conceptual Change*, eds. G.M. Sinatra & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2003, pp. 237-290. (RW 5041)

Distin, K. *The Selfish Meme: A Critical Reassessment*, Cambridge University Press, Cambridge, UK, 2005. (RW 3483)

Dixon, D.S. & Reynolds, W.N. "Visualizing the Political Landscape," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 881)

Dixon, N. *The Three Eras of Knowledge Management - Summary*. Available: http://www.nancydixonblog.com, Viewed: August 13, 2010. (RW 4249)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Dixon, N. *How to make use of Your Organization's Collective Knowledge - Accessing the Knowledge of the Whole Organization - Part I*. Available: http://www.nancydixonblog.com/2011/01/how-to-make-use-of-your-organizations-collective-knowledge-accessing-the-knowledge-of-the-whole-orga.html, Viewed: January 11, 2011, 2011. (RW 4510)

Dixon, N. *Conversational Patterns that Support Speaking Truth to Power*. Available: www.nancydixonblog.com, Viewed: January 30, 2012. (RW 5416)

Dixon, N.M. *How A-Space is Shaping Analysts' Work*, 2009. (RW 3672)

Dixon, N.M. & McNamara, L.A. *Our Experience with Intellipedia: An Ethnographic Study at the Defense Intelligence Agency*, 2008. (RW 3350)

Djumovic, N. "Getting CIA History Right: The Informal Partnership between Agency Historians and Outside Scholars," *Intelligence and National Security*, Vol. 26, No. 2-3, 2011, pp. 228-245. (RW 4848)

Dobbins, J. "A Perilous Dialogue of Pessimists," *Financial Times*, February 4, 2004, p. 2. (RW 4558)

Dobbs, M. *One Minute to Midnight: Kennedy, Khrushchev, and Castro on the Brink of Nuclear War*, Alfred A. Knopf, New York, 2008. (RW 5229)

Dobrzykowski, T.M. "Teaching Strategies to Promote Critical Thinking Skills in Nursing Staff," *Journal of Continuing Education in Nursing*, Vol. 25, No. 6, 1994, pp. 272-276. (RW 3958)

Doel, R.E. & Needell, A.A. "Science, Scientists, and the CIA: Balancing International Ideals, National Needs, and Professional Opportunities," in *Eternal Vigilance? 50 Years of the CIA*, eds. R. Jeffreys-Jones & C. Andrew, F. Cass, London, UK, 1997, pp. 59-81. (RW 41)

Doherty, W.J. & Thadani, A.J. *The Economic Value of Rapid Response Time*. Available: www.vm.ibm.com/devpates/jelliott/evrrt.html, January 28, 2011. (RW 4516)

Dole, J.A. & Sinatra, G.M. "Reconceptualizing Change in the Cognitive Construction of Knowledge," *Educational Psychologist*, Vol. 33, No. 2-3, 1998, pp. 109-128. (RW 4643)

Dominguez, C., Cox, D., Long, W.G., Moon, B. & Klein, G. "Helping Analysts Deal with Data Overload: Profiling Profilers", *Proceedings of the Human Factors and Ergonomics Society 49th Meeting*, pp. 908. (RW 3566)

Dominowski, R. "Verbalization and Problem Solving," in *Metacognition in Educational Theory and Practice*, eds. D.J. Hacker, J. Dunlosky & A.C. Graesser, L. Erlbaum Associates, Mahwah, NJ, 1998, pp. 25-46. (RW 3792)

Donaldson, A., Heathwaite, L., Lane, S., Ward, N. & Whatmore, S. "Holistic Approaches to Understanding Diffuse Land Management Issues: A Framework for Interdisciplinary Working," *Centre for Rural Economy Discussion Paper Series*, 2, 2005. (RW 2626)

Donovan, S. & Bransford, J. *How Students Learn*, National Academies Press, Washington, DC, 2004. (RW 3803)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Doran, C. "Why Forecasts Fail: The Limits and Potential of Forecasting in International Relations and Economics," *International Studies Review,* Vol. 1, No. 2, 1999, pp. 11-41. (RW 1066)

Dorando, P.J. "For College Courses in Intelligence," *Studies in Intelligence,* Vol. 4, No. 3, 1960, pp. A15-A18. (RW 529)

Dorn, E., Blair, D.G., Disney, D.M., Faga, M.C., Hawley, K., Hazlewood, L., Lachance, J. & Massiah, M.G. *The Defense Civilian Intelligence Personnel System: An Independent Assessment of Design, Implementation, and Impact*, National Academy of Public Administration, Washington, DC, 2010. (RW 4731)

Doron, G. "The Vagaries of Intelligence Sharing: The Political Imbalance," *International Journal of Intelligence and Counterintelligence,* Vol. 6, No. 2, 1993, pp. 135-146. (RW 183)

Dorsey, D.W., Mueller-Hanson, R.A. & Pulakos, E.D. "Management and Leadership Effects on Employee Performance and Organizational Effectiveness," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, CENTRA Technology, Burlington, MA, [in press], pp. 147-175. (RW 3647)

Dorsey, D.W., Mueller-Hanson, R.A. & Pulakos, E.D. "Leadership Behavior Self-Assessment," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 413. (RW 3664)

Dorst, K.H. & Cross, N.G. "Creativity in the Design Process: Co-Evolution of Problem-Solution," *Design Studies,* Vol. 22, 2001, pp. 425. (RW 2686)

Dosenbach, N.U.F., Fair, D.A., Miezin, F.M. & et al. "Distinct Brain Networks for Adaptive and Stable Task Control in Humans," *Proceedings of the National Academy of Sciences,* Vol. 104, No. 26, 2007, pp. 11073. (RW 2563)

Douglas, N.L. "Enemies of Critical Thinking: Lessons from Social Psychology Research," *Reading Psychology,* Vol. 21, No. 2, 2000, pp. 129-144. (RW 2788)

Douville, J.A. *The Serials Librarian*, Vol. 4, No. 3, 1980, pp. 313. (RW 4245)

Dow, J.W. "The Evolution of Knowledge Systems: Narrative Knowledge Versus Scientific Knowledge", *Society for Anthropological Sciences,* February 22-26, 2006 (RW 3565)

Dowling, T. "Failures of Imagination: Thoughts on the 9/11 Commission Report," in *Learning with Professionals: Selected Works from the Joint Military Intelligence College*, eds. J.E. Lightfoot, J.S. Major, S.E. Brownfeld & Joint Military Intelligence College, 2005, pp. 131. (RW 1570)

Dreisbach, C. "The Challenges Facing an Intelligence Community Epistemologist-in-Residence," *International Journal of Intelligence and Counterintelligence,* Vol. 24, No. 4, 2011, pp. 757-792. (RW 5401)

Drell, B. "Intelligence Research: Some Suggested Approaches," *Studies in Intelligence,* Vol. 1, No. 4, 1957, pp. 79-95. (RW 539)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Dressel, P.L. & Lehmann, I.J. "The Impact of Higher Education on Student Attitudes, Values, and Critical Thinking Abilities," *Educational Record,* Vol. 46, No. 3, 1965, pp. 248-258. (RW 5371)

Dreyfus, H.L. "A Framework for Misrepresenting Knowledge," in *Philosophical Perspectives in Artificial Intelligence*, ed. M. Ringle, Humanities Press, Atlantic Highlands, NJ, 1979, pp. 124. (RW 2661)

Dreyfuss, R. "Dim Intelligence - what did we Get for all that Money?" *The American Prospect,* October 22, 2001, pp. 10-11. (RW 296)

Drezner, D.W. *What Kind of Intelligence Reform is Necessary?* Available: www.danieldrezner.com, (RW 293)

Driskell, J.E., Goodwin, G.F., Salas, E. & O'shea, P.G. "What Makes a Good Team Player? Personality and Team Effectiveness," *Group Dynamics - Theory and Practice,* Vol. 10, No. 4, 2006, pp. 249. (RW 2348)

Druckenmiller, D., Acar, W. & Troutt, M. *Agent-Based Modeling and Simulation of Strategic Scenarios with Repast 2.0.* 2004. (RW 2616)

Drucker, P. "The Future that has Already Happened," *The Futurist,* Vol. 32, No. 8, 1998, pp. 16-18. (RW 3391)

Druckman, J.N., Green, D.P., Kuklinski, J.H. & Lupia, A. *Cambridge Handbook of Experimental Political Science,* Cambridge University Press, New York, NY, 2011. (RW 5449)

Dube, C., Rotello, C.M. & Heit, E. "Assessing the Belief Bias Effect with ROCs: It's a Response Bias Effect," *Psychological Review,* Vol. 117, No. 3, 2010, pp. 831-863. (RW 5721)

Duggan, W.R. *Strategic Intuition: The Creative Spark in Human Achievement,* Columbia Business School Pub., New York, 2007. (RW 3635)

Dugosh, K.L. & Paulus, P.B. "Cognitive and Social Comparison Processes in Brainstorming," *Journal of Experimental Social Psychology,* Vol. 41, 2005, pp. 313. (RW 2808)

Dugosh, K.L., Paulus, P.B., Roland, E.J. & Yang, H. "Cognitive Stimulation in Brainstorming," *Journal of Personality and Social Psychology,* Vol. 79, 2000, pp. 722. (RW 2809)

Duhigg, C. *The Power of Habit: Why we do what we do in Life and Business,* Random House, New York, NY, 2012. (RW 5627)

Dujmovic, N. "Fifty Years of *Studies in Intelligence*," *Studies in Intelligence,* Vol. 49, No. 4, 2005, pp. 1-14. (RW 4225)

Dulles, A.W. "Valediction," *Studies in Intelligence,* Vol. 6, No. 1, 1962, pp. A1-A4. (RW 574)

Dunbar, K. "Concept Discovery in a Scientific Domain," *Cognitive Science,* Vol. 17, 1993, pp. 397. (RW 1801)

Dunbar, K. "How Scientists really Reason: Scientific Reasoning in Real-World Laboratories," in *The Nature of Insight,* eds. R.J. Sternberg & J.E. Davidson, MIT Press, Cambridge, Mass, 1995, pp. 365. (RW 1804)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Dunbar, K. "How Scientists Think: On-Line Creativity and Conceptual Change in Science," in *Creative Thought: An Investigation of Conceptual Structures and Processes*, eds. T.B. Ward, S.M. Smith & J. Vaid, 1997, pp. 461. (RW 1764)

Dunbar, K. "Problem Solving," in *A Companion to Cognitive Science*, eds. W. Bechtel, G. Graham & D.A. Balota, Blackwell, Malden, Mass, 1998, pp. 289. (RW 1803)

Dunbar, K. "How Scientists Build Models: In Vivo Science as a Window on the Scientific Mind," in *Model-Based Reasoning in Scientific Discovery*, eds. L. Magnani, N.J. Nersessian & P. Thagard, 1999, pp. 85. (RW 1814)

Dunbar, K. "How Scientists Think in the Real World: Implications for Science Education," *Journal of Applied Developmental Psychology*, Vol. 21, No. 1, 2000, pp. 49. (RW 1888)

Dunbar, K. "The Analogical Paradox: Why Analogy is so Easy in Naturalistic Settings, Yet so Difficult in the Psychological Laboratory," in *The Analogical Mind: Perspectives from Cognitive Science*, eds. D. Gentner, K.J. Holyoak & B.N. Kokinov, 2001, pp. 313. (RW 1815)

Dunbar, K. "What Scientific Thinking Reveals about the Nature of Cognition," in *Designing for Science: Implications from Everyday, Classroom, and Professional Settings*, eds. K.D. Crowley, C.D. Schunn & T. Okada, 2001, pp. 115. (RW 1813)

Dunbar, K. "Understanding the Role of Cognition in Science: The Science as Category Framework," in *The Cognitive Basis of Science*, eds. P. Carruthers, S.P. Stich & M. Siegal, Cambridge University Press, Cambridge, UK, 2002, pp. 154. (RW 1792)

Dunbar, K.N. & Fugelsang, J.A. "Causal Thinking in Science: How Scientists and Students Interpret the Unexpected," in *Scientific and Technological Thinking*, ed. M.E. Gorman, L. Erlbaum Associates, Mahwah, N.J, 2005, pp. 57. (RW 1794)

Dunbar, K.N., Fugelsang, J.A. & Stein, C. *Do Naive Theories Ever Go Away? Using Brain and Behavior to Understand Changes in Concepts* (RW 1812)

Dunbar, K.N. & Klahr, D. "Scientific Thinking and Reasoning," in *Oxford Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 701-718. (RW 5505)

Dunbar, K. & Blanchette, I. "The in vivo/in Vitro Approach to Cognition: The Case of Analogy," *Trends in Cognitive Sciences*, Vol. 5, No. 8, 2001, pp. 334. (RW 1819)

Dunbar, K. & Fugelsang, J. "Scientific Thinking and Reasoning," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, 2005, pp. 705-735. (RW 1805)

Dunbar, K. & Klahr, D. "Developmental Differences in Scientific Discovery Processes," in *Complex Information Processing: The Impact of Herbert A. Simon*, eds. H.A. Simon, D. Klahr & K. Kotovsky, L. Erlbaum Associates, Hillsdale, NJ, 1989, pp. 109. (RW 1947)

Duncker, K. *On Problem-Solving*, American Psychological Association, Washington, 1945. (RW 2742)

Dungan, M. *Interview of Dr. Donald M. Kerr, Principal Deputy Director of National Intelligence.* 2008. (RW 3160)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Dunkle, M.E., Schraw, G.J. & Bendixen, L. "The Relationship between Epistemological Beliefs, Causal Attributions, and Renective Judgment", *Annual Meeting of the American Educational Research Association*, (RW 3767)

Dunn, P.A. *Talking, Sketching, Moving: Multiple Literacies in the Teaching of Writing*, Boynton/Cook, Portsmouth, NH, 2001. (RW 3499)

Dunning, D. *Self-Insight: Roadblocks and Detours on the Path to Knowing Thyself*, Psychology Press, New York, 2005. (RW 2886)

Dunning, D. "Prediction: The Inside View," in *Social Psychology: Handbook of Basic Principles*, eds. E.T. Higgins & A.W. Kruglanski, Second ed., 2007, pp. 69. (RW 1574)

Dunning, D.A., Krueger, J.I. & Alicke, M.D. "The Self in Social Perception: Looking Back, Looking Ahead," in *The Self in Social Judgment*, eds. M.D. Alicke, D. Dunning & J.I. Krueger, Psychology Press, New York, 2005, pp. 269. (RW 2894)

Dunning, D., Heath, C. & Suls, J.M. "Flawed Self-Assessment: Implications for Health, Education, and the Workplace," *Psychological Science in the Public Interest*, Vol. 5, No. 3, 2004, pp. 69-106. (RW 1075)

Dunyak, J., Costa, P. & Mohtashemi, M. "A Model of Early Detection of Infectious Disease Outbreaks with Application to Biological Terrorism," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 804)

Dupont, A. "Intelligence for the Twenty-First Century," *Intelligence and National Security*, Vol. 18, No. 4, 2003, pp. 15-39. (RW 327)

Durbin, B. "Strategic Intelligence in a Changing World: Lessons from Organization Theory", *Annual Meeting of the American Political Science Association*, September 2 - 5 (RW 2920)

Duvenage, D. *Private/academic Partnership in Intelligence Analysis Training: The South African Experience* (RW 3297)

Duvenage, M.A. *Intelligence Analysis in the Knowledge Age*, Stellenbosch University. Available: http://www.opensourcesinfo.org/journal/2010/9/10/intelligence-analysis-in-the-knowledge-age-an-analysis-of-th.html, Viewed: September 23, 2010. (RW 4360)

Duyvesteyn, I. "Hearts and Minds, Cultural Awareness and Good Intelligence: The Blueprint for Successful Counter-Insurgency," *Intelligence and National Security*, Vol. 26, No. 4, 2011, pp. 445-459. (RW 5393)

Dweck, C.S. "Beliefs that make Smart People Dumb," in *Why Smart People can be so Stupid*, ed. R.J. Sternberg, Yale University Press, New Haven, CT, 2002, pp. 24-41. (RW 3456)

Dweck, C.S. *Mindset: The New Psychology of Success*, Ballantine Books, New York, NY, 2008. (RW 4216)

Dweck, C.S. & Leggett, E.L. "Social-Cognitive Approach to Motivation and Personality," *Psychological Review*, Vol. 95, No. 2, 1988, pp. 256-273. (RW 4901)

Dzbor, M. & Zdrahal, Z. *Design as Interactions of Problem Framing and Problem Solving* (RW 2636)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Dzbor, M. & Zdrahal, Z. *Modeling Design Interpretation as Interaction of Problem Framing and Problem Solving* (RW 2631)

Dziedzic, M.J. & Wood, W.B. *Information Technology as a Catalyst for Civil-Military Unity of Effort: The Kosovo Test Case* (RW 1453)

Dzindolet, M.T., Stover, A. & Pierce, L.G. "Predicting Group Decision Making with a Computerized Text Analysis Tool", *Proceedings of the Human Factors and Ergonomics Society 49th Meeting*, pp. 586. (RW 3571)

Eames, C. & Coll, R.K. "Cooperative Education: Integrating Classroom and Workplace Learning," in *Learning through Practice: Models, Traditions, Orientations, and Approaches*, ed. S. Billett, Springer, Dordrecht, 2010, pp. 180-196. (RW 4960)

Eberstadt, N. "Where did the CIA Go Wrong?" *National Review*, Vol. 43, No. 10, 1991, pp. 31-34. (RW 4214)

Ecker, U., Lewandowsky, S. & Tang, D. "Explicit Warnings Reduce but do Not Eliminate the Continued Influence of Misinformation," *Memory & Cognition*, Vol. 38, No. 8, 2010, pp. 1087-1100. (RW 4809)

Eckert, M. *Theories of Mind: An Introductory Reader*, Rowman & Littlefield Publishers, Lanham, Md., 2006. (RW 3429)

Eco, U. & Sebeok, T.A. *The Sign of Three: Dupin, Holmes, Peirce*, Indiana University Press, Bloomington, 1983. (RW 4032)

Ed *Intelligence Fusion: The Race Against Time* 2006. (RW 1731)

Eden, C., Jones, S. & Sims, D. *Messing about in Problems: An Informal Structured Approach to their Identification and Management*, Pergamon Press, Oxford Oxfordshire; New York, 1983. (RW 2660)

Eden, C. & Spender, J.C. *Managerial and Organizational Cognition: Theory, Methods and Research*, Sage, London; Thousand Oaks, CA, 1998. (RW 2521)

Ederer, M. "New and Emerging Challenges for Intelligence Analysis", *New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities*, Rome, Italy, 31 March - 2 April, 2004, pp.8181-86. (RW 2836)

Edmonds, A. *Integrated Information Systems for Warrior*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1996. (RW 999)

Edmonds, A.J. *Information Systems Support to DOD and Beyond*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1997. (RW 1046)

Edmonds, A.J. *Managing Your E-Business: Electrifying Reality*, Center for Information Policy Research. Harvard University, Cambridge, MA, 2001. (RW 1172)

Edmonds, S. *Letter to Thomas Kean, National Committee on Terrorist Attacks upon the US* 2004. (RW 488)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Edmondson, K.M. & Novak, J.D. "The Interplay of Scientific Epistemological Views, Learning Strategies, and Attitudes of College Students," *Journal of Research in Science Teaching,* Vol. 30, No. 6, 1993, pp. 547-559. (RW 4649)

Educational Policies Commission. *The Purposes of Education in American Democracy,* National Educational Association of the United States, Washington, DC, 1938. (RW 4513)

Edwards, A. "The Pyramid of Excellence for Intelligence Analysis and Production a Maturity Model," *Cryptologic Quarterly,* Vol. 20, No. 2, 2001, pp. 33-37. (RW 674)

Edwards, A. *Being an Expert Professional Practitioner: The Relational Turn in Expertise,* Springer, Dordrecht, 2010. (RW 4880)

Egger, M., Juni, P., Bartlett, C., Holenstein, F. & Sterne, J. "How Important are Comprehensive Literature Searches and the Assessment of Trial Quality in Systematic Reviews? Empirical Study." *Health Technology Assessment,* Vol. 7, No. 1, 2003, pp. 1. (RW 2221)

Eggleston, R.G., Bearavolu, R. & Mostashfi, A. "Sensemaking Support Environment: A Thinking Aid for all-Source Intelligence Analysis Work," 2005 *International Conference on Intelligence Analysis*, McLean, VA, May 2-6, 2005. (RW 250)

Eichhorn, R. *Developing Thinking Skills: Critical Thinking at the Army Management Staff College*, Army Management Staff College, Fort Belvoir, VA, 2010. (RW 4255)

Eilbert, J.L. "Prediction and Metacognition", *Fourth IEEE International Conference on Self-Adaptive and Self-Organizing Systems Workshop,* Budapest, Hungary, September 27-29, 2010, pp. 308-311. (RW 5674)

Einhorn, H. "Accepting Error to make Less Error," *Journal of Personality Assessment,* Vol. 50, No. 3, 1986, pp. 387-395. (RW 4688)

Eisendrath, C. "Needed: More Intelligent Intelligence," *Bulletin of the Atomic Scientists,* Vol. 55, No. 6, 1999, pp. 23-25. (RW 359)

Eisendrath, C.R. & Goodman, M.A. "Reforming US Intelligence After Terrorist Attack," *USA Today Magazine,* Vol. 130, No. 2678, 2001, pp. 10-13. (RW 377)

Eisenstadt, A.S. *The Craft of American History: Selected Essays,* Harper & Row, New York, 1966. (RW 3731)

Eisner, E. "Forms of Understanding and the Future of Educational Research," *Educational Researcher,* Vol. 22, No. 7, 1993, pp. 5. (RW 2395)

Elby, A. & Hammer, D. "On the Substance of a Sophisticated Epistemology," *Science Education,* Vol. 85, No. 5, 2001, pp. 554. (RW 5188)

Elder, A.D. "Characterizing Fifth Grade Students' Epistemological Beliefs in Science," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing,* eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 347. (RW 4393)

Elder, G. "Intelligence in War: It can be Decisive," *Studies in Intelligence,* Vol. 15, No. 2, 2006, pp. 13-25. (RW 4588)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Elder, L. & Paul, R. *The Miniature Guide to the Art of Asking Essential Questions,* 4th ed., Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3779)

Elder, L. & Paul, R. *The Thinker's Guide to Analytic Thinking,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3778)

Elen, J., Stahl, E., Clarebout, G. & Broom, R. *Links between Beliefs and Cognitive Flexibility: Lessons Learned,* Springer 2011. (RW 4297)

Elio, R. & Scharf, P.B. "Modeling Novice-to-Expert Shifts in Problem Solving Strategy and Knowledge Organization," *Cognitive Science,* Vol. 14, 1990, pp. 579. (RW 2733)

Ellis, D. "A Behavioural Approach to Information Retrieval System Design," *Journal of Documentation,* Vol. 45, 1989, pp. 171. (RW 1355)

Ellis, D. *Progress and Problems in Information Retrieval,* 2nd ed., Library Association Pub, London, 1996. (RW 1628)

Ellis, J.D. & Kiefer, G.D. *Combating Proliferation: Strategic Intelligence and Security Policy,* Johns Hopkins University Press, Baltimore, 2004. (RW 1321)

Ellis, R.H. *Strategic Connectivity*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1982. (RW 1000)

Elm, W.C., Cook, M.J., Greitzer, F.L., Hoffman, R., Moon, B. & Hutchins, S.G. "Designing Support for Intelligence Analysts. Panel Discussion." *HFES 2004: Proceedings of the Human Factors and Ergonomics Society. 48th Annual Meeting.* September 20-24, 2004, pp.406. (RW 2842)

Elm, W., Potter, S., Tittle, J., Grossman, J., Patterson, E. & Woods, D.D. *Finding Decision Support Requirements for Effective Intelligence Analysis Tools* 2007. (RW 2278)

Elm, W., Potter, S., Tittle, J., Woods, D., Grossman, J. & Patterson, E. "Finding Decision Support Requirements for Effective Intelligence Analysis Tools," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 844)

Elqayam, S. "Grounded Rationality: A Relativist Framework for Normative Rationality," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans,* eds. K.I. Manktelow, D.E. Over & S. Elqayam, Psychology Press, Hove, East Sussex, UK, 2011, pp. 397-419. (RW 5714)

Elqayam, S. & Evans, Jonathan St. B. T. "Subtracting "Ought" from "is": Descriptivism Versus Normativism in the Study of Human Thinking," *Behavioral and Brain Sciences,* Vol. 34, No. 5, 2011, pp. 233-290. (RW 5863)

Emergency Management Australia. *Manual 4. Land Search Operations,* 1997. (RW 3909)

Endert, A., Fox, S., Maiti, D., Leman, S. & North, C. "The Semantics of Clustering: Analysis of User-Generated Spatializations of Text Documents", *Proceedings of the International Working Group on Advanced Visualizations Interfaces,* Capri Island, Italy, May 21-25, 2012, pp. 555-562. (RW 5758)

Engel, A. *Problem-Solving Strategies,* Springer, New York, 1998. (RW 2662)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Engel, J.A. "Change is Hard...but Even Small Steps Matter," in *Rethinking Leadership and "Whole of Government" National Security Reform: Problems, Progress, and Prospects*, eds. J.R. Cerami & J.A. Engel, 2010, pp. 187. (RW 4193)

Engelmann, J.B., Capra, C.M., Noussair, C. & Berns, G.S. "Expert Financial Advice Neurobiologically "Offloads" Financial Decision-Making Under Risk," *PLos ONE,* Vol. 4, No. 3, 2009 (RW 3717)

Engels, F. *Anti-Duehring*. Available: http://www.marxists.org/archive/marx/works/1877/anti-duhring/ch13.htm, Viewed: October 10, 2011. (RW 5164)

Engle, R.W., Carullo, J.W. & Collins, K.W. "Individual Differences in Working Memory for Comprehension and Following Directions," *Journal of Educational Research,* Vol. 84, No. 5, 1991, pp. 253-262. (RW 4687)

Engle, R.W., Toholski, S.W., Laughlin, J.E. & Conway, R.A. "Working Memory, Short-Term Memory, and General Fluid Intelligence: A Latent-Variable Approach," *Journal of Experimental Psychology: General,* Vol. 128, No. 3, 1999, pp. 309-331. (RW 4692)

Engle, R.W., Kane, M.J. & Tuholski, S.W. "Models of Working Memory: Mechanisms of Active Maintenance and Executive Control," in *Models of Working Memory: Mechanisms of Active Maintenance and Executive Control*, eds. A. Miyake & P. Shah, Cambridge University Press, Cambridge, UK, 1999, pp. 102-134. (RW 4678)

Englert, C.S., Raphael, T.E., Anderson, L.M., Anthony, H.M. & Stevens, D.S. "Making Strategies and Self-Talk Visible: Writing Instruction in Regular and Special Education Classrooms," *American Educational Research Journal,* Vol. 28, No. 2, 1991, pp. 337-372. (RW 5844)

Ennis, R.H. "Critical Thinking: More on its Motivation," *Progressive Education,* May, 1956, pp. 75-78. (RW 4458)

Ennis, R.H. "An Appraisal of the Watson-Glaser Critical Thinking Appraisal," *Journal of Educational Research,* Vol. 52, No. 1, 1958, pp. 155-158. (RW 4457)

Ennis, R.H. "A Concept of Critical Thinking," *Harvard Educational Review,* Vol. 32, No. 1, 1962, pp. 81-111. (RW 4456)

Ennis, R.H. "Needed: Research in Critical Thinking," *Educational Leadership,* Vol. 21, No. 1, 1963, pp. 17-20. (RW 4452)

Ennis, R.H. "A Taxonomy of Critical Thinking Dispositions and Abilities," in *Teaching Thinking Skills: Theory and Practice*, eds. J.B. Baron & R.J. Sternberg, Freeman, New York, NY, 1987, pp. 9-26. (RW 3733)

Ennis, R.H. "Critical Thinking and Subject Specificity: Clarification and Needed Research," *Educational Researcher,* Vol. 18, No. 3, 1989, pp. 4-10. (RW 3704)

Ennis, R.H. "The Extent to which Critical Thinking is Subject-Specific: Further Clarification," *Educational Researcher,* Vol. 19, No. 4, 1990, pp. 13-16. (RW 3705)

Ennis, R.H. "Critical Thinking Assessment," *Theory into Practice,* Vol. 32, No. 3, 1993, pp. 179-186. (RW 4509)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Ennis, R.H. *Critical Thinking*, Prentice-Hall, Upper Saddle River, NJ, 1994. (RW 4020)

Ennis, R.H. "Critical Thinking Dispositions: Their Nature and Assessability," *Informal Logic*, Vol. 18, No. 2 & 3, 1996, pp. 165-182. (RW 5176)

Ennis, R.H. *An Outline of Goals for a Critical Thinking Curriculum and its Assessment*. Available: http://faculty.ed.uiuc.edu/rhennis/outlinegoalsctcurassess3.html, Viewed: January 25, 2010. (RW 3865)

Ennis, R.H. *An Annotated List of Critical Thinking Tests*. Available: http://faculty.ed.uiuc.edu/rhennis/testlistrevised606.htm;, Viewed: September 25, 2009. (RW 3763)

Ennis, R.H., Millman, J. & Tomko, T.N. *Cornell Critical Thinking Tests Level X & Level Z Manual*, 5th ed., The Critical Thinking Co., Seaside, CA, 2005. (RW 4022)

Ennis, R.H. & Weir, E. *The Ennis-Weir Critical Thinking Essay Test*, Midwest Publications, Pacific Grove CA, 1985. (RW 3971)

Entwistle, N. "Frameworks for Understanding as Experienced in Essay Writing and in Preparing for Examinations," *Educational Psychologist*, Vol. 30, No. 1, 1995, pp. 47. (RW 3516)

Epley, C.M. *The Relationship between Implicit Theories of Intelligence, Epistemological Beliefs, and the Teaching Practices of in-Service Teachers: A Mixed Methods Study*, Ph.D. dissertation, Virginia Institute of Technology, 2011. (RW 5076)

Epley, N. & Dunning, D. "The Mixed Blessings of Self-Knowledge in Behavioral Prediction: Enhanced Discrimination but Exacerbated Bias," *Personality and Social Psychology Bulletin*, Vol. 32, No. 5, 2006, pp. 641. (RW 2351)

Eppler, M.J. & Mengis, J. "A Framework for Information Overload Research in Organizations," 2003 (RW 3689)

Epstein, L.G. & Schneider, M. *Learning Under Ambiguity*, Rochester Center for Economic Research. Working Paper No. 497, University of Rochester, Rochester, NY, 2005. (RW 1934)

Epstein, S. & Meier, P. "Constructive Thinking: A Broad Coping Variable with Specific Components," *Journal of Personality and Social Psychology*, Vol. 57, No. 2, 1989, pp. 332-350. (RW 5283)

Eraut, M. "Knowledge, Working Practices, and Learning," in *Learning through Practice: Models, Traditions, Orientations, and Approaches*, ed. S. Billett, Springer, Dordrecht, 2010, pp. 37-58. (RW 4955)

Erb, H.P. & et al. "Searching for Commonalities in Human Judgment," *European Review of Social Psychology*, Vol. 14, No. 1, 2003, pp. 1. (RW 1539)

Erdfelder, E. & Brandt, M. "Recollection Biases in Hindsight Judgments," *Social Cognition*, Vol. 25, No. 1, 2007, pp. 114. (RW 2448)

Erdmann, D. & Mendonca, L. "Focused on Foresight: An Interview with the US's National Intelligence Officer for Warning," *McKinsey Quarterly*, September, 2009. (RW 3601)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Erdmann, J.B. "Test Review of the Law School Admission Test," in *The Thirteenth Mental Measurements Yearbook*, eds. J.C. Impara & B.S. Plake, Buros Institute, 1998. (RW 4102)

Erev, I., Wallsten, T.S. & Neal, M.M. "Vagueness, Ambiguity, and the Cost of Mutual Understanding," *Psychological Science*, Vol. 2, No. 5, 1991, pp. 321. (RW 1895)

Erickson, T. "Notes on Design Practice: Stories and Prototypes a Catalysts for Communication," in *Scenario-Based Design: Envisioning Work and Technology in Systems Development*, ed. J.M. Carroll, Wiley, New York, 1995, pp. 37. (RW 3395)

Ericsson, K.A. "Exceptional Memorizers: Made, Not Born," *Trends in Cognitive Sciences*, Vol. 7, No. 6, 2003, pp. 233. (RW 4132)

Ericsson, K.A. "Recent Advances in Expertise Research: A Commentary on the Contributions to the Special Issue," *Applied Cognitive Psychology*, Vol. 19, 2005, pp. 233. (RW 4129)

Ericsson, K.A. "The Influence of Experience and Deliberate Practice on the Development of Superior Expert Performance," in *The Cambridge Handbook of Expertise and Expert Performance*, ed. K.A. Ericsson, Cambridge University Press, Cambridge, UK, 2006, pp. 685. (RW 4143)

Ericsson, K.A. "Protocol Analysis and Expert Thought: Concurrent Verbalizations of Thinking during Experts' Performance on Representative Tasks," in *The Cambridge Handbook of Expertise and Expert Performance*, ed. K.A. Ericsson, Cambridge University Press, Cambridge, UK, 2006, pp. 223. (RW 4144)

Ericsson, K.A. "Deliberate Practice and the Modifiability of Body and Mind: Toward a Science of the Structure and Acquisition of Expert and Elite Performance," *International Journal of Sport Psychology*, Vol. 38, 2007, pp. 4. (RW 4131)

Ericsson, K.A. & Kintsch, W. "Long-Term Working Memory," *Psychological Review*, Vol. 102, 1995, pp. 211. (RW 4136)

Ericsson, K.A., Patel, V.L. & Kintsch, W. "How Experts' Adaptations to Representative Task Demands Account for the Expertise Effect in Memory Recall: Comment on Vicente and Wang (1998)," *Psychological Review*, Vol. 107, 2000, pp. 578. (RW 4133)

Ericsson, K.A. "Deliberate Practice and the Acquisition and Maintenance of Expert Performance in Medicine and Related Domains," *Academic Medicine*, Vol. 79, No. 10 Supplement, 2004, pp. S70. (RW 4141)

Ericsson, K.A. *The Cambridge Handbook of Expertise and Expert Performance*, Cambridge University Press, Cambridge, UK, 2006. (RW 1648)

Ericsson, K.A. "An Expert-Performance Perspective of Research on Medical Expertise: The Study of Clinical Performance," *Medical Education*, Vol. 41, 2007, pp. 1124. (RW 4139)

Ericsson, K.A. "Deliberate Practice and Acquisition of Expert Performance: A General Overview," *Academic Emergency Medicine*, Vol. 15, No. 11, 2008, pp. 988. (RW 4138)

Ericsson, K.A. "Enhancing the Development of Professional Performance: Implications from the Study of Deliberate Practice," in *Development of Professional Expertise: Toward Measurement*

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

of Expert Performance and Design of Optimal Learning Environments, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 405-431. (RW 5151)

Ericsson, K.A., Krampe, R.T. & Tesch-Roemer, C. "The Role of Deliberate Practice in the Acquisition of Expert Performance," *Psychological Review,* Vol. 100, No. 3, 1993, pp. 363. (RW 4121)

Ericsson, K.A., Perez, R.S., Eccles, D.W., Lang, L., Baker, E.L., Bransford, J.D., VanLehn, K. & Ward, P. "The Measurement and Development of Professional Performance: An Introduction to the Topic and a Background to the Design and Origin of this Book," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 1-24. (RW 4135)

Ericsson, K.A., Whyte, J. & Ward, P. "Expert Performance in Nursing: Reviewing Research on Expertise in Nursing within the Framework of the Expert-Performance Approach," *Advances in Nursing Science,* Vol. 30, No. 1, 2007, pp. E58. (RW 4140)

Ericsson, K.A. & Williams, A.M. "Capturing Naturally Occurring Superior Performance in the Laboratory: Translational Research on Expert Performance," *Journal of Experimental Psychology: Applied,* Vol. 13, No. 3, 2007, pp. 115. (RW 4137)

Erisen, C., Lodge, M. & Taber, C.S. "Affective Contagion in Effortful Political Thinking," *Political Psychology*, 2012 (RW 5451)

Erlandson, D.A. *Doing Naturalistic Inquiry: A Guide to Methods,* Sage, Newbury Park, CA, 1993. (RW 3211)

Ermarth, F. "The Role of Analysis," *Periscope,* Vol. 13, No. 4, 1988, pp. 7-11. (RW 4385)

Ermarth, F.W. "Intelligence in Recent Public Literature (Book Reviews)," *Studies in Intelligence,* Vol. 18, No. 1, 1974, pp. 61. (RW 1298)

Ermolayev, V., Moreno, C.R., Tilly, M., Jentzsch, E., Gomez-Perez, J.M. & Matzke, W. "A Context Model for Knowledge Workers", *Second International Workshop on Context Information and Ontologies,* Lisbon, October 11, 2010. (RW 4863)

Etherington, K. *Becoming a Reflexive Researcher: Using our Selves in Research,* Jessica Kingsley Publishers, London, UK, 2004. (RW 5686)

Eugene, S. "The Relationship between Learning Style and Cognitive Style," *Personality and Individual Differences,* Vol. 30, No. 4, 2001, pp. 609-616. (RW 5169)

Evans, D.A. "Issues of Cognitive Science in Medicine," in *Cognitive Science in Medicine: Biomedical Modeling,* eds. D.A. Evans & V.L. Patel, MIT Press, Cambridge, MA, 1989, pp. 1-19. (RW 5322)

Evans, E.M., Legare, C.H. & Rosengren, K.S. "Engaging Multiple Epistemologies: Implications for Science Education," in *Epistemology and Science Education: Understanding the Evolution Vs. Intelligent Design Controversy,* eds. R.S. Taylor & M. Ferrari, Routledge, New York, NY, 2011, pp. 111-140. (RW 4765)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Evans, Jonathan St. B. T. "Reasoning," in *Oxford Handbook of Cognitive Psychology*, ed. D. Reisberg, Oxford University Press, [in press], (RW 5727)

Evans, Jonathan St. B. T. "Deciding before You Think: Relevance and Reasoning in the Selection Task," *British Journal of Psychology*, Vol. 87, 1996, pp. 223. (RW 2435)

Evans, Jonathan St. B. T. "The Influence of Prior Belief on Scientific Thinking," in *The Cognitive Basis of Science*, eds. P. Carruthers, S.P. Stich & M. Siegal, Cambridge University Press, Cambridge, UK, 2002, pp. 193-210. (RW 1950)

Evans, Jonathan St. B. T. *Hypothetical Thinking: Dual Processes in Reasoning and Judgment*, Psychology Press, Hove, UK, 2007. (RW 5794)

Evans, Jonathan St. B. T. "Dual-Processing Accounts of Reasoning, Judgment and Social Cognition," *Annual Review of Psychology*, Vol. 59, 2008, pp. 255-278. (RW 5567)

Evans, Jonathan St. B. T. *Thinking Twice: Two Minds in One Brain*, Oxford University Press, New York, 2010. (RW 5410)

Evans, Jonathan St. B. T. "The Psychology of Reasoning: Reflections on Four Decades of Research," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans*, eds. K.I. Manktelow, D.E. Over & S. Elqayam, Psychology Press, Hove, East Sussex, UK, 2011, pp. 423-443. (RW 5715)

Evans, Jonathan St. B. T. "Dual-Process Theories of Deductive Reasoning: Facts and Fallacies," in *Oxford Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 115-133. (RW 5498)

Evans, Jonathan St. B. T. "Reflections on Rationality," *American Journal of Psychology*, Vol. 125, No. 1, 2012, pp. 113-116. (RW 5716)

Evans, Jonathan St. B. T., Clibbens, J. & Harris, A. "Prior Belief and Polarity in Multicue Learning," *Quarterly Journal of Experimental Psychology: Section A*, Vol. 58, No. 4, 2005, pp. 651-665. (RW 5698)

Evans, Jonathan St. B. T. & Feeney, A. "The Role of Prior Belief in Reasoning," in *The Nature of Reasoning*, eds. R.J. Sternberg & J.P. Leighton, Cambridge University Press, Cambridge, U.K.; New York, 2004, pp. 78. (RW 2312)

Evans, Jonathan St. B. T., Handley, S., Neilens, H., Bacon, A.M. & Over, D.E. "The Influence of Cognitive Ability and Instructional Set on Causal Conditional Inference," *Quarterly Journal of Experimental Psychology*, Vol. 63, No. 5, 2010, pp. 892-909. (RW 5722)

Evans, Jonathan St. B. T., Handley, S.J., Hadjchristidis, C., Thompson, V., Over, D.E. & Bennett, S. "On the Basis of Belief in Causal and Diagnostic Conditionals," *Quarterly Journal of Experimental Psychology*, Vol. 60, No. 5, 2007, pp. 635-643. (RW 5697)

Evans, Jonathan St. B. T., Handley, S.J. & Harper, C.N.J. "Necessity, Possibility and Belief: A Study of Syllogistic Reasoning," *Quarterly Journal of Experimental Psychology: Section A*, Vol. 54, No. 3, 2001, pp. 935-958. (RW 5700)

Evans, Jonathan St. B. T., Handley, S.J., Over, D.E. & Perham, N. "Background Beliefs in Bayesian Inference," *Memory & Cognition*, Vol. 30, No. 2, 2002, pp. 179. (RW 5696)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Evans, Jonathan St. B. T. & Stanovich, K.E. "Dual-Process Theories of Higher Cognition: Advancing the Debate," *Perspectives on Psychological Science,* [in press] (RW 5824)

Evans, J.C. "US Business Competitiveness and the Intelligence Community," *International Journal of Intelligence and Counterintelligence,* Vol. 7, No. 3, 1994, pp. 353-361. (RW 184)

Evans, R.M. "Cultural Paradigms and Change: A Model of Analysis," in *The Handbook of Intelligent Policing: Consilience, Crime Control, and Community Safety,* ed. C. Harfield, Oxford University Press, Oxford, UK, 2008, pp. 105-120. (RW 5773)

Evans, R.M. "Influencing Decision Makers with Intelligence and Analytical Products," in *Strategic Thinking in Criminal Intelligence,* ed. J. Ratcliffe, 2nd ed., Federation Press, Sydney, 2009, pp. 187-203. (RW 5769)

Eynde, P.O., De Corte, E. & Verschaffel, L. "Epistemic Dimensions of Students' Mathematics-Related Belief Systems," *International Journal of Educational Research,* Vol. 45, No. 1-2, 2006, pp. 57. (RW 3692)

Facione, N.C. & Facione, P.A. *Critical Thinking Assessment in Nursing Education Programs: An Aggregate Data Analysis,* California Academic Press, Millbrae, CA, 1997. (RW 3976)

Facione, P.A. "Toward a Theory of Critical Thinking," *Liberal Education,* Vol. 70, No. 3, 1984, pp. 253-261. (RW 5370)

Facione, P.A. *The California Critical Thinking Skills Test - College Level. Technical Report #1. Experimental Validation and Content Validity,* California Academic Press, Millbrae, CA, 1990. (RW 3636)

Facione, P.A. *The California Critical Thinking Skills Test - College Level. Technical Report #2. Factors Predictive of CT Skills,* California Academic Press, Millbrae, CA, 1990. (RW 3637)

Facione, P.A. *The California Critical Thinking Skills Test - College Level. Technical Report #3. Gender, Ethnicity, Major, CT Self-Esteem, and the CCTST,* California Academic Press, Millbrae, CA, 1990. (RW 3638)

Facione, P.A. *Critical Thinking: A Statement of Expert Consensus for Purposes of Educational Assessment and Instruction. Research Findings and Recommendations,* American Philosophical Association, Newark, DE, 1990. (RW 3633)

Facione, P.A. *Critical Thinking: What it is and Why it Counts. 2009 Update,* Insight Assessment, Millbrae, CA, 2009. (RW 3631)

Facione, P.A. & Facione, N.C. *California Critical Thinking Disposition Inventory (CCTDI) Test Manual,* California Academic Press, Millbrae, CA, 2010. (RW 5021)

Facione, P.A., Facione, N.C. & Giancarlo, C.A. "The Disposition Toward Critical Thinking: Its Character, Measurement, and Relationship to Critical Thinking Skill," *Informal Logic,* Vol. 20, No. 1, 2000, pp. 61-94. (RW 3694)

Facione, P.A., Facione, N.C. & Giancarlo, C.A.F. *Professional Judgment and the Disposition Toward Critical Thinking,* California Academic Press, Millbrae, CA, 1997. (RW 3758)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Facione, P.A., Sanchez, C.A. & Facione, N.C. *Are College Students Disposed to Think?* California Academic Press, Millbrae, CA, 1994. (RW 3947)

Facione, P.A., Sanchez, C. & Facione, N.C. "The Disposition Toward Critical Thinking," *The Journal of General Education,* Vol. 44, No. 1, 1995, pp. 1-25. (RW 3974)

Fagnant, A. & Crahay, M. "Theories of Mind and Personal Epistemology: Their Interrelation and Connection with the Concept of Metacognition," *European Journal of Psychology of Education,* Vol. 26, No. 2, 2011, pp. 257-271. (RW 5211)

Fahey, L. "Intelligence Analysis: The Business Context [Powerpoint Presentation]", *Global Intelligence Forum 2010,* Dungarvan, Ireland, July 11-13, 2010 (RW 4226)

Fahey, L. & Randall, R.M. *Learning from the Future: Competitive Foresight Scenarios,* Wiley, New York, 1998. (RW 3307)

Fain, T.G., Plant, K.C. & Milloy, R. *The Intelligence Community: History, Organization, and Issues,* R. R. Bowker Co., New York, NY, 1977. (RW 935)

Fallows, J. "What was I Thinking?" *Atlantic Monthly,* Vol. 299, No. 5, 2007, pp. 131-133. (RW 3143)

Farnsworth, W. *The Legal Analyst: A Toolkit for Thinking about the Law,* University of Chicago Press, Chicago, 2007. (RW 2761)

Farson, S. "Schools of Thought: National Perceptions of Intelligence," *Conflict Quarterly,* Vol. 9, No. 2, 1989, pp. 52-104. (RW 5660)

Farson, S. & Whitaker, R. "Accounting for the Future Or the Past?: Developing Accountability and Oversight Systems to Meet Future Intelligence Needs," in *Oxford Handbook of National Security Intelligence,* ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 673-698. (RW 4717)

Faul, K. *Intelligence and the Analytical Perspective*, Naval War College, Newport, RI, 1995. (RW 1175)

Feder, S.A. "Forecasting for Policy Making in the Post-Cold War Period," *Annual Review of Political Science,* Vol. 5, No. 1, 2002, pp. 111-125. (RW 4686)

Feder, S.A. "Factions and Policon: New Ways to Analyze Politics," in *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992*, ed. H.B. Westerfield, Yale University Press, New Haven, CT, 1995, pp. 274-292. (RW 889)

Feeney, A. & Crisp, A. "A Conjunction of Fallacies: What Different Types of Causal Conjunction Error Reveal about Dual Processes for Thinking," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans*, eds. K.I. Manktelow, D.E. Over & S. Elqayam, Psychology Press, Hove, East Sussex, UK, 2011, pp. 237-257. (RW 5709)

Feist, G.J. "Domain-Specific Creativity in the Physical Sciences," in *Creativity Across Domains: Faces of the Muse*, eds. J.C. Kaufman & J. Baer, L. Erlbaum Associates, Mahwah, NJ, 2005, pp. 123. (RW 4269)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Feist, G.J. *The Psychology of Science and the Origins of the Scientific Mind*, Yale University Press, New Haven, 2006. (RW 3004)

Felbrich, A., Müller, C. & Blömeke, S. "Epistemological Beliefs Concerning the Nature of Mathematics among Teacher Educators and Teacher Education Students in Mathematics " *ZDM*, Vol. 40, No. 5, 2008, pp. 763-776. (RW 5271)

Felder, R.M. & Brent, R. "The Intellectual Development of Science and Engineering Students. Part 1: Models and Challenges," *Journal of Engineering Education*, Vol. 93, No. 4, 2004, pp. 269-277. (RW 5557)

Felder, R.M. & Brent, R. "Understanding Student Differences," *Journal of Engineering Education*, Vol. 94, No. 1, 2005, pp. 57-72. (RW 5559)

Feldman, D.A. *Critical Thinking: Strategies for Decision Making*, Axzo Press, Rochester, NY, 2002. (RW 3870)

Fellman, P.V. "The Complexity of Intelligence Estimates", *Eighth International Conference on Complex Systems (ICCS 2011)*, Quincy, MA, June 26 - July 1, 2011, pp. 1444-1458. (RW 5512)

Feltovich, P.J., Hoffman, R.R., Woods, D. & Roesler, A. "Keeping it Too Simple: How the Reductive Tendency Affects Cognitive Engineering," *IEEE Intelligent Systems*, Vol. 19, No. 3, 2004, pp. 90. (RW 2050)

Fennema, E. & Franke, M.L. "Teachers' Beliefs and Conceptions: A Synthesis of the Research," in *Handbook of Research on Mathematics Teaching and Learning*, ed. D.A. Grouws, Macmillan, New York, 1992, pp. 147-164. (RW 5039)

Fenstermacher, G.D. "The Knower and the Known: The Nature of Knowledge in Research on Teaching," *Review of Research in Education*, Vol. 20,1994, pp. 3. (RW 4298)

Ferenstein, G. "How to make skeptics believe Obama's birth certificate is authentic", *Fastcompany.com*, [Online], Available from: http://www.fastcompany.com/1750214/how-to-make-skeptics-believe-obamas-birth-certificate-is-authentic. 2011. (RW 4806)

Fernandes, R. & Simon, H.A. "A Study of how Individuals Solve Complex and Ill-Structured Problems," *Policy Sciences*, Vol. 32, No. 3, 1999, pp. 225. (RW 2572)

Ferris, J. "Coming in from the Cold War: The Historiography of American Intelligence 1945-1990," *Diplomatic History*, Vol. 19, No. 1, 1995, pp. 87-115. (RW 82)

Ferris, J. "Intelligence in War," in *The International Studies Encyclopedia*, ed. R.A. Denemark, 2010. (RW 3930)

Ferris, J.R. *Intelligence and Strategy: Selected Essays*, Routledge, London, UK, 2005. (RW 923)

Ferris, J. & Handel, M.I. "Clausewitz, Intelligence, Uncertainty and the Art of Command in Military Operations," *Intelligence and National Security*, Vol. 10, No. 1, 1995, pp. 1-58. (RW 177)

Ferrucci, S. *Conceptual Modeling: Missing Link in the Analytic Process*, 2009. (RW 3478)

Ferrucci, S.L. *Explicit Conceptual Models: Synthesizing Divergent and Convergent Thinking*, M. S. thesis, Mercyhurst College, 2009. (RW 4117)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Feucht, F.C. & Bendixen, L.D. "Exploring Similarities and Differences in Personal Epistemologies of U.S. and German Elementary School Teachers," *Cognition and Instruction,* Vol. 28, 2010, pp. 39-69. (RW 5067)

Fikes, R., Ferrucci, D. & Thurman, D. "Knowledge Associates for Novel Intelligence (KANI)," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 852)

Fingar, T. "US Intelligence Reform and the Analytic Community: Challenges and Opportunities", *Proceedings of the IALEIA World Intelligence Training Conference,* Mexico City, MX, April 24-28 (RW 5634)

Fingar, T. *Statement to Senate Select Committee on Intelligence. Security Threats to the United States,* 2005. (RW 626)

Fingar, T. "Questionable Intelligence. Correspondence regarding Under Analysis." *The New Republic Online,* July 10, 2006. (RW 2320)

Fingar, T. *Remarks and Q&A by the Deputy Director of National Intelligence for Analysis & Chairman, National Intelligence Council. ODNI Open Source Conference.* 2007. (RW 2727)

Fingar, T. *Remarks and Q&A by the Deputy Director of National Intelligence for Analysis & Chairman, National Intelligence Council. Council on Foreign Relations.* 2008. (RW 3023)

Fingar, T. *Reducing Uncertainty: Intelligence and National Security Spies Collect Data, Analysts Provide Insight,* 2009. (RW 3597)

Fingar, T. *Reducing Uncertainty: Intelligence and National Security using Intelligence to Anticipate Opportunities and Shape the Future,* 2009. (RW 3695)

Fingar, T. "Analysis in the U.S. Intelligence Community: Missions, Masters, and Methods," in *Intelligence Analysis: Behavioral and Social Scientific Foundations,* eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, pp. 3-27. (RW 4640)

Fingar, T. *Reducing Uncertainty: Intelligence Analysis and National Security,* Stanford University Press, Stanford, CA, 2011. (RW 4721)

Fingar, T. "Intelligence and Grand Strategy," *Orbis,* Vol. 56, No. 1, 2012, pp. 118-134. (RW 5536)

Fingar, T. "Intelligence as a Service Industry," *The American Interest,* Vol. 7, No. 4, 2012, pp. 80-84. (RW 5633)

Fingar, T. *Mapping the Global Future,* 2008. (RW 3179)

Fink, A. *Conducting Research Literature Reviews: From the Internet to Paper,* 2nd ed., Sage Publications, Thousand Oaks, CA, 2005. (RW 2242)

Fink, A. *Practicing Research: Discovering Evidence that Matters,* Sage Publications, Los Angeles, 2008. (RW 3113)

Fink, E. *Changes of Problem Representation: Theory and Experiments,* Physica-Verlag, Heidelberg Germany; New York, 2003. (RW 2557)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Finkelstein, D. "The Social Psychology Revolution is Reaching its Tipping Point," *The Times,* July 16, 2008, (RW 3235)

Finkelstein, L., Gabrilovich, E., Matias, Y., Rivlin, E., Solan, Z., Wolfman, G. & Ruppin, E. "Placing Search in Context: The Concept Revisited, " *Proceedings of the Tenth International World Wide Web Conference (WWW10),* Hong Kong, May 2-4, 2001, pp. 406-414. (RW 4932)

Finley, J.P. "Nobody Likes to be Surprised: Intelligence Failures," *Military Intelligence Professional Bulletin,* Vol. 20, No. 1, 1994, pp. 15. (RW 4213)

Finnegan, M.J. *Evaluating SWOT's Value in Creating Actionable, Strategic Intelligence,* M. S. thesis, Mercyhurst College, 2010. (RW 4369)

Fiora, B. "Writing Intelligence Reports that Get Read," *Competitive Intelligence Magazine,* Vol. 5, No. 1, 2002, pp. 52. (RW 4104)

Fiore, S.M., Rosen, M.A., Smith-Jentsch, K.A., Salas, E., Letsky, M. & Warner, N. "Toward an Understanding of Macrocognition in Teams: Predicting Processes in Complex Collaborative Contexts," *Human Factors,* Vol. 52, No. 2, 2010, pp. 203-224. (RW 4689)

Fiore, S.M. "Cognition and Technology: Interdisciplinarity and the Impact of Cognitive Engineering Research on Organizational Productivity," in *Oxford Handbook of Organizational Psychology*, ed. W.J. Kozlowski, Oxford University Press, New York, NY, 2012. (RW 5767)

Firat, A.K., Woon, W.L. & Madnick, S. *Technological Forecasting: A Review,* CISL#2008-15, 2008. (RW 3853)

Firestein, S. *Ignorance: How it Drives Science,* Oxford University Press, New York, NY, 2012. (RW 5763)

Firestone, J.M. & McElroy, M.W. *Key Issues in the New Knowledge Management,* Knowledge Management Consortium International, Hartland Four Corners, Vt, 2003. (RW 4561)

Fischer, B.B. "Solidarity, the CIA, and Western Technology," *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 3, 2012, pp. 427-469. (RW 5731)

Fischer, D.H. *Historians' Fallacies: Toward a Logic of Historical Thought,* Harper & Row, New York, 1970. (RW 3508)

Fischer, F. *Reframing Public Policy: Discursive Politics and Deliberative Practices,* Oxford University Press, Oxford, 2003. (RW 2590)

Fischer, G. *Reflective Practitioners and Unselfconscious Cultures of Design* (RW 2642)

Fischer, K.W. & Pruyne, E. "Reflective Thinking in Adulthood: Emergence, Development, and Variation," in *Handbook of Adult Development,* eds. J. Demick & C. Andreoletti, Kluwer Academic/Plenum, New York, NY, 2003, pp. 169-198. (RW 4328)

Fischhoff, B. "An Early History of Hindsight Research," *Social Cognition,* Vol. 25, No. 1, 2007, pp. 10. (RW 2445)

Fischhoff, B. "Communicating about Analysis," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, pp. 227-248. (RW 4779)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Fischhoff, B. "Science & intelligence analysis", *Livebetter eMagazine*, [Online], no. 24, pp. September 10. Available from: http://livebettermagazine.com/eng/magazine/article_detail.lasso?id=356&-session=user_pref:42F9487313cd739475NXKWN2440B2012. [September 10] (RW 5804)

Fischl, M.A. & Gilbert, A.C.F. *Selection of Intelligence Analysts*, Army Research Institute for the Behavioral and Social Sciences, Alexandria, VA, 1983. (RW 1134)

Fishbein, W. & Treverton, G.F. "Making Sense of Transnational Threats," *The Sherman Kent Center for Intelligence Analysis Occasional Papers*, Vol. 3, No. 1, 2004 (RW 343)

Fishbein, W. & Treverton, G.F. "Rethinking "Alternative Analysis" to Address Transnational Threats," *The Sherman Kent Center for Intelligence Analysis Occasional Papers*, Vol. 3, No. 2, 2004 (RW 342)

Fisher, A. *Critical Thinking: An Introduction*, Cambridge University Press, Cambridge, UK, 2001. (RW 3813)

Fisher, A. & Scriven, M. *Critical Thinking: Its Definition and Assessment*, Edgepress, Point Reyes, CA, 1997. (RW 3864)

Fisher, C.M. *What Team Leaders See: Toward an Understanding of the Timing of Team Leader Coaching Interventions*, The Group Brain Project, technical report no. 6, 2007. (RW 3016)

Fisher, K.E. & Julien, H. "Information Behavior," in *Annual Review of Information Science and Technology*, ed. B. Cronin, Medford, NJ, 2009, pp. 317. (RW 4348)

Fisher, R. & Johnston, R. "Is Intelligence Analysis a Discipline?" in *Analyzing Intelligence: Origins, Obstacles, and Innovations*, eds. R.Z. George & J.B. Bruce, 2008, pp. 55. (RW 3095)

Fisk, C.E. "The Sino-Soviet Border Dispute: A Comparison of the Conventional and Bayesian Methods for Intelligence Warning," in *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992*, ed. H.B. Westerfield, Yale University Press, New Haven, CT, 1995, pp. 264-273. (RW 888)

Fiske, S.T. & Taylor, S.E. *Social Cognition*, 2nd ed., McGraw-Hill, New York, 1991. (RW 2212)

Fitzgerald, F. "Geographic Analysis and Crime Mapping," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 88-94. (RW 3614)

Fitzgerald, J. & Cunningham, J.W. "Balance in Teaching Reading: An Instructional Approach Based on a Particular Epistemological Outlook," *Reading & Writing Quarterly*, Vol. 18, No. 4, 2002, pp. 353-364. (RW 5353)

Fitzgerald, J. & Cunningham, J.W. "Mapping Basic Issues for Identifying Epistemological Outlooks," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing*, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 209. (RW 4390)

Fitzgerald, M. & Lebow, R.N. "Iraq: The Mother of all Intelligence Failures," *Intelligence and National Security*, Vol. 21, No. 5, 2006, pp. 884. (RW 2086)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

FitzSimonds, J.R. "Intelligence and the Revolution in Military Affairs," in *U.S. Intelligence at the Crossroads: Agendas for Reform*, eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 265-287. (RW 649)

Fives, H. & Buehl, M.M. "What do Teachers Believe? Developing a Framework for Examining Beliefs about Teachers' Knowledge and Ability," *Contemporary Educational Psychology*, Vol. 33, No. 2, 2008, pp. 134-176. (RW 5066)

Flaherty, A. *The Midnight Disease: The Drive to Write, Writer's Block, and the Creative Brain*, Houghton Mifflin, Boston, 2004. (RW 1835)

Flanagan, K., Marsh, J., Moore, K., Walker, E., Wheaton, K. & Williams, S. *Wikis and Intelligence Analysis*, Mercyhurst College, Erie, PA, 2012. (RW 5665)

Flank, S. "Measurably Better: Bringing ROI Assessments to Intelligence Tools," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 855)

Flavell, J.H. "Metacognition and Cognitive Monitoring: A New Area of Cognitive-Developmental Inquiry," *American Psychologist*, Vol. 34, No. 10, 1979, pp. 906-911. (RW 4655)

Fleisher, C.S. "Competitive Intelligence Education: Competencies, Sources, and Trends," *The Information Management Journal*, Vol. 38, No. 2, 2004, pp. 56-62. (RW 3944)

Fleisher, C.S. & Bensoussan, B.E. *Business and Competitive Analysis: Effective Application of New and Classic Methods*, Financial Times Press, Upper Saddle River, NJ, 2007. (RW 5853)

Fletcher, J.D. "The Value of Expertise and Expert Performance: A Review of Evidence from the Military," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 449-469. (RW 5153)

Flood, R.L. & Senge, P.M. *Rethinking the Fifth Discipline: Learning within the Unknowable*, Routledge, London, UK, 1999. (RW 4564)

Florence, M.K. & Yore, L.D. "Learning to Write Like a Scientist: Coauthoring as an Enculturation Task," *Journal of Research in Science Teaching*, Vol. 41, No. 6, 2004, pp. 637-668. (RW 2328)

Flower, L. "Taking Thought: The Role of Conscious Processing in the Making of Meaning," in *Thinking, Reasoning, and Writing*, eds. E.P. Maimon, B.F. Nodine & F.W. O'Connor, Longman, New York, 1989, pp. 185. (RW 4351)

Flower, L. & Hayes, J.R. "The Cognition of Discovery: Defining a Rhetorical Problem," in *Landmark Essays on Writing Process*, ed. S. Perl, 1994, pp. 63. (RW 1831)

Flower, L., *The Role of Task Representation in Reading to Write*, Center for the Study of Writing, Berkeley, CA, 1987. (RW 1860)

Flynn, M.T., Pottinger, M. & Batchelor, P.D. *Fixing Intel: A Blueprint for Making Intelligence Relevant in Afghanistan*, Center for a New American Security, Washington, DC, 2010. (RW 4892)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Flyvbjerg, B. "Five Misunderstandings about Case-Study Research," *Qualitative Inquiry*, Vol. 12, No. 2, 2006, pp. 219. (RW 3304)

FMJ *Red Team: How Aluminum Tubes were Fixed Around Policy* (RW 2060)

Foley, R. "Beliefs, Degrees of Belief, and the Lockean Thesis," in *Degrees of Belief*, eds. F. Huber & C. Schmidt-Petri, Springer, Dordrecht, 2009, pp. 37-47. (RW 5277)

Folker, R.D. *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods,* Joint Military Intelligence College, Washington, D.C, 2000. (RW 1223)

Folker, R.D. & Bressette, K.B. "A Culminating Point for Air Force Intelligence, Surveillance, and Reconnaissance," *Air & Space Power Journal*, Vol. 26, No. 6, 2012, pp. 130-136. (RW 5882)

Foo, C. & Foo, C. "Forecastability, Chaos, and Foresight," *Foresight*, Vol. 5, No. 5, 2003, pp. 22-33. (RW 218)

Forbus, K.D. "Knowledge Capture for Bootstrapping Intelligent Systems", pp.22. (RW 1492)

Forbus, K.D., Birnbaum, L., Wagner, E., Baker, J. & Witbrock, M. "Analogy, Intelligent IR, and Knowledge Integration for Intelligence Analysis: Situation Tracking and the Whodunit Problem," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 815)

Forbus, K.D. & Feltovich, P.J. *Smart Machines in Education: The Coming Revolution in Educational Technology*, AAAI Press, Menlo Park, Calif, 2001. (RW 2018)

Ford, C. *Frontline: The Dark Side: Interviews.* 2006. (RW 1775)

Ford, C.W. *Senate Democratic Policy Committee Hearing. An Oversight Hearing on Pre-War Intelligence Relating to Iraq.* 2006. (RW 1772)

Ford, H.P. "A Tribute to Sherman Kent," *Studies in Intelligence*, Vol. 24, No. 3, 1980 (RW 388)

Ford, H.P. *Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating*, Defense Intelligence College, Washington, DC, 1989. (RW 1078)

Ford, H.P. "The Primary Purpose of National Estimating," *Studies in Intelligence*, Vol. 35, No. Fall, 1991, pp. 69-79. (RW 341)

Ford, H.P. *Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating*, University Press of America, Lanham, MD, 1993. (RW 1079)

Ford, H.P. *Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating*, University Press of America, Lanham, MD, 1993. (RW 1081)

Ford, H.P. "The US Government's Experience with Intelligence Analysis: Pluses and Minuses," *Intelligence and National Security*, Vol. 10, No. 4, 1995, pp. 34-53. (RW 131)

Ford, H.P. *CIA and the Vietnam Policymakers: Three Episodes 1962-1968*, Center for the Study of Intelligence, Langley, VA, 1998. (RW 1080)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Ford, N. "Modeling Processes in Information Seeking: From Popper to Pask," *Journal of the American Society for Information Science & Technology*, Vol. 55, No. 9, 2004, pp. 769. (RW 2855)

Ford, N. "New Cognitive Directions," in *New Directions in Cognitive Information Retrieval*, eds. A. Spink & C. Cole, Springer, Dordrecht, 2005, pp. 81. (RW 3591)

Fort, R.M. "Economic Espionage," in *U.S. Intelligence at the Crossroads: Agendas for Reform*, eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 181-196. (RW 646)

Fort, R.M. *Whither the Elephant? Public-Private Sector Dynamics in the Information Realm*, Center for Information Policy Research. Harvard University, Cambridge, MA, 2000. (RW 1001)

Foryst, C.A. "Missing from US Intelligence Analysis: The Concept of "Total US"," *International Journal of Intelligence and Counterintelligence*, Vol. 22, No. 3, 2009, pp. 396. (RW 3585)

Foryst, C.A. "Rethinking National Security Strategy Priorities," *International Journal of Intelligence and Counterintelligence*, Vol. 23, No. 3, 2010, pp. 399. (RW 4154)

Foryst, C.A. "TechNet: To Improve the Intelligence Community's Science and Technology Pursuits," *International Journal of Intelligence and Counterintelligence*, Vol. 24, No. 3, 2011, pp. 510-533. (RW 5402)

Foss, J. "Just the Facts, and Only the Facts, about Human Rationality?" *Behavioral and Brain Sciences*, Vol. 34, No. 5, 2011, pp. 254-255. (RW 5488)

Foster, G.D. "Research, Writing, and the Mind of the Strategist," *Joint Forces Quarterly*, 11, 1996, pp. 111-115. (RW 1070)

Foundation for Critical Thinking. *The Critical Thinking Community*, Foundation for Critical Thinking. Available: http://www.criticalthinking.org/professionalDev/business.cfm, Viewed: April 28, 2011. (RW 4798)

Fox, D. "The Limits of Intelligence," *Scientific American*, Vol. 305, No. 1, 2011, pp. 36-43. (RW 4923)

Fox, E. "The Role of Reader Characteristics in Processing and Learning from Informational Text," *Review of Educational Research*, Vol. 79, 2009, pp. 197. (RW 3800)

Fox, E. & Alexander, P.A. "Text Comprehension: A Retrospective, Perspective, and Prospective," in *Handbook of Research on Reading Comprehension*, eds. S.E. Israel & G.G. Duffy, Routledge, New York, NY, 2009, pp. 227-239. (RW 3719)

Fox, E., Dinsmore, D.L., Maggioni, L. & Alexander, P.A. "Factors Associated with Undergraduates' Success in Reading and Learning from Course Texts", *2009 Annual Meeting of the American Educational Research Association*, San Diego, CA, April 13-17, 2009. (RW 3829)

Fox, E., Maggioni, L., Dinsmore, D.L. & Alexander, P.A. "The Multi-Layered Reading Goals of Expert Readers: Bridging between Knowledge, Interest, and Strategy use", *2008 Annual Meeting of the American Educational Research Association*, New York, NY, March 24-28, 2008. (RW 3830)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Fox, J.M. *Crisis Management at the FBI*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1990. (RW 1002)

Fox, W.M. *Effective Group Problem Solving: How to Broaden Participation, Improve Decision Making, and Increase Commitment to Action*, Jossey-Bass, San Francisco, 1987. (RW 2667)

Frame, M.T. "Information Discovery and Retrieval Tools," *Information Services & Use*, Vol. 24, 2004, pp. 187. (RW 2752)

Frank, J. & Deveraux, P.J. *Scientific Research Synthesis (Systematic Reviews and Meta-Analyses): What, Why, and How*, 2003. (RW 2201)

Frankel, R.M. "Standards of Qualitative Research," in *Doing Qualitative Research*, eds. B.F. Crabtree & W.L. Miller, 2nd ed., Sage Publications, Thousand Oaks, Calif, 1999, pp. 333. (RW 2508)

Frankish, K. & Evans, Jonathan St. B. T. "The Duality of Mind: An Historical Perspective," in *In Two Minds: Dual Processes and Beyond*, eds. Evans, Jonathan St. B. T. & K. Frankish, Oxford University Press, Oxford, UK, 2009, pp. 1. (RW 3435)

Frankish, K. & Kasmirli, M. "Scalar Implicature: Inference, Convention, and Dual Processes," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans*, eds. K.I. Manktelow, D.E. Over & S. Elqayam, Psychology Press, Hove, East Sussex, UK, 2011, pp. 259-281. (RW 5710)

Franklin, J. *The Science of Conjecture: Evidence and Probability before Pascal*, Johns Hopkins University Press, Baltimore, 2001. (RW 3362)

Frants, V.I., Shapiro, J., Taksa, I. & Voiskunskii, V.G. "Boolean Search: Current State and Perspectives," *Journal of the American Society for Information Science*, Vol. 50, No. 1, 1999, pp. 86-95. (RW 898)

Fratila, O. & Solomon, I. "Strategic Intelligence - EU Security Resource," *The International Scientific Conference: Strategies XXI. The Complex and Dynamic Nature of the Security Environment*, Bucharest, Romania, November 22-23, 2012, pp. 485-493. (RW 5876)

Frawley, W.J., Piatetsky-Shapiro, G. & Matheus, C.J. "Knowledge Discovery in Databases: An Overview," *AI Magazine*, Vol. 13, No. 3, 1992, pp. 57-70. (RW 470)

Frederick, S. "Cognitive Reflection and Decision Making," *Journal of Economic Perspectives*, Vol. 19, No. 4, 2005, pp. 25-42. (RW 5273)

Freedman, L. "The CIA and the Soviet Threat: The Politicization of Estimates, 1966-1977," in *Eternal Vigilance? 50 Years of the CIA*, eds. R. Jeffreys-Jones & C. Andrew, F. Cass, London, UK, 1997, pp. 122-142. (RW 40)

Freitag, D., Blume, M., Byrnes, J., Calmbach, R. & Rohwer, R. "A Workbench for Rapid Development of Extraction Capabilities," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 807)

French, J.C., Powell, A.L., Gey, F. & Perelman, N. "Exploiting Manual Indexing to Improve Collection Selection and Retrieval Effectiveness," *Information Retrieval*, Vol. 5, No. 4, 2002, pp. 323-351. (RW 952)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Frensch, P.A. & Sternberg, R.J. "Expertise and Intelligent Thinking: When is it Worse to Know?" *Advances in the Psychology of Human Intelligence,* Vol. 5, 1989, pp. 161. (RW 2763)

Frerichs, R.L. & DiRienzo, S.R. "Establishing a Framework for Intelligence Education and Training," *Joint Forces Quarterly*, 62, 2011, pp. 68-73. (RW 5538)

Frey, B.S. & Stutzer, A. *Economics and Psychology: A Promising New Cross- Disciplinary Field,* MIT Press, Cambridge, MA, 2007. (RW 4078)

Frey, F.E. & Tropp, L.R. "Being seen as Individuals Versus as Group Members: Extending Research on Metaperception to Intergroup Contexts," *Personality and Social Psychology Review,* Vol. 10, No. 3, 2006, pp. 265. (RW 2349)

Friedman, B. *Web Search Savvy: Strategies and Shortcuts for Online Research,* L. Erlbaum Associates, Mahwah, NJ, 2005. (RW 3542)

Friedman, B. *Writing Past Dark: Envy, Fear, Distraction, and Other Dilemmas in the Writer's Life,* HarperCollins Publishers, New York, 1993. (RW 1868)

Friedman, G. *The Problem of Intelligence Reform* [undated]. (RW 404)

Friedman, G. "For Better Intel, Add Courage," *New York Post Online*, 2005 (RW 609)

Friedman, J.A. *Assessing Uncertainty in Intelligence*, 2011. (RW 5250)

Friedman, J.A. & Zeckhauser, R. *Assessing Uncertainty in Intelligence,* Harvard University, Cambridge, MA, 2011. (RW 5543)

Friedman, J.A. & Zeckhauser, R. *Assessing Uncertainty in Intelligence,* Harvard University, Cambridge, MA, 2012. (RW 5799)

Friedman, R.S. "US Intelligence at the Crossroads?" *Parameters,* Vol. 27, No. 2, 1997, pp. 131-136. (RW 203)

Friedman, R.S. "Open Source Intelligence," *Parameters,* Vol. 28, No. 2, 1998, pp. 159-165. (RW 1049)

Friedman, S.L., Scholnick, E.K. & Cocking, R.R. *Blueprints for Thinking: The Role of Planning in Cognitive Development,* Cambridge University Press, Cambridge Cambridgeshire; New York, 1987. (RW 2587)

Friedman, U. *The Ten Biggest American Intelligence Failures.* Available: http://www.foreignpolicy.com/articles/2012/1/3/the_ten_biggest_american_intelligence_failures. Viewed: January 6, 2012. (RW 5382)

Friman, H. "Innovation, Change and Experimentation: New Challenges for Military Intelligence," *American Intelligence Journal,* Vol. 25, No. 1, 2007, pp. 29. (RW 3221)

Frini, A. & Boury-Brisset, A. "An Intelligence Process Model Based on a Collaborative Approach", *16th ICCRTS: Collective C2 in Multinational Civil-Military Operations,* Quebec City, Canada, June 21-23, 2011. (RW 5545)

Fry, J. "In Search of Serendipity: Can Online Papers Recreate a Joy of Print?" *wsj.com,* 2007 (RW 2080)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Fryer, D. "Federated Search," *Online Magazine,* March/April, 2004, pp. 16. (RW 1420)

Fryxell, D.A. *How to Write Fast (while Writing Well),* Writer's Digest Books, Cincinnati, Ohio, 1992. (RW 1864)

Fu, W. & Pirolli, P. "SNIF-ACT: A Cognitive Model of User Navigation on the World Wide Web," *Human-Computer Interaction,* Vol. 22, 2007, pp. 355-412. (RW 5483)

Fuell, D.L. "Understanding the Enemy as a Complex System: A Multidisciplinary Analytic Problem Requiring a Multidisciplinary Team Approach," *Air & Space Power Journal,* Summer, 2009 (RW 3501)

Fugelsang, J.A. & Dunbar, K.N. "A Cognitive Neuroscience Framework for Understanding Causal Reasoning and the Law," *Phil. Trans. R. Soc. Lond. B,* Vol. 359, 2004, pp. 1749. (RW 1802)

Fugelsang, J.A., Stein, C.B., Green, A.E. & Dunbar, K.N. "Theory and Data Interactions of the Scientific Mind: Evidence from the Molecular and the Cognitive Laboratory," *Canadian Journal of Experimental Psychology,* Vol. 58, No. 2, 2004, pp. 86. (RW 1796)

Fugelsang, J.A. & Thompson, V.A. "A Dual-Process Model of Belief and Evidence Interactions in Causal Reasoning," *Memory & Cognition,* Vol. 31, No. 5, 2003, pp. 800. (RW 1789)

Fugelsang, J.A., Thompson, V.A. & Dunbar, K.N. "Examining the Representation of Causal Knowledge," *Thinking & Reasoning,* Vol. 12, No. 1, 2006, pp. 1. (RW 1797)

Fukuyama, F. "The Challenges of Uncertainty: An Introduction," in *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics*, ed. F. Fukuyama, Brookings Institution Press, Washington, DC, 2007, pp. 1-6. (RW 4602)

Fuld, L.M. *The New Competitor Intelligence: The Complete Resource for Finding, Analyzing, and using Information about Your Competitors,* J. Wiley, New York, NY, 1995. (RW 1116)

Fulghum, D.A. "Intelligence Analysis Shifts Closer to Combat," *Aviation Week and Space Technology,* Vol. 154, No. 25, 2001, pp. 179. (RW 1665)

Fuller, G. "Intelligence Immaculately Conceived," *National Interest,* 1991-1992, pp. 95-99. (RW 1248)

Fulwider, J. *Do Moderators Matter? Answering a Jury Deliberation Challenge to Deliberative Democracy,* 2005. (RW 2062)

Funtowicz, S.O. "Managing Uncertainty and Quality in Policy-Related Research," in *Chemistry and Environment: Legislations, Methodologies, and Applications,* eds. S. Fachetti & D. Pitea, Kluwer Academic Publishers, Dordrecht; Boston, 1995, pp. 45. (RW 2406)

Funtowicz, S.O. "Post-Normal Science: A New Scientific Methodology for Global Environmental Issues," in *Chemistry and Environment: Legislations, Methodologies, and Applications*, eds. S. Fachetti & D. Pitea, Kluwer Academic Publishers, Dordrecht; Boston, 1995, pp. 55. (RW 2419)

Funtowicz, S.O. & Ravetz, J.R. *Uncertainty and Quality in Science for Policy,* Kluwer Academic Publishers, Dordrecht, the Netherlands; Norwell, MA, U.S.A., 1990. (RW 2407)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Furnham, A. & Ribchester, T. "Tolerance of Ambiguity: A Review of the Concept, its Measurement and Applications," *Current Psychology*, Vol. 14, No. 3, 1995, pp. 179-199. (RW 5364)

Fyffe, G. "The Future of Intelligence Analysis", *New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities*, Rome, Italy, 31 March - 2 April, 2004, pp.91-96. (RW 2838)

Gabel, D. *Handbook of Research on Science Teaching and Learning*, Macmillan, New York, NY, 1994. (RW 5320)

Gage, J.T. *The Shape of Reason: Argumentative Writing in College*, Macmillan Pub. Co., New York, 1986. (RW 2180)

Galbraith, D. "Self-Monitoring, Discovery through Writing and Individual Differences in Drafting Strategy," in *Theories, Models and Methodology in Writing Research*, eds. G. Rijlaarsdam, H. van den Bergh & M. Couzijn, Amsterdam University Press, Amsterdam, 1996, pp. 121. (RW 2132)

Galbraith, D., Torrance, M. & Hallam, J. "Effects of Writing on Conceptual Coherence", *Proceedings of the 28th Annual Conference of the Cognitive Science Society*, July 26-29, 2006, pp. 1340. (RW 1989)

Galdi, S., Arcuri, L. & Gawronski, B. "Automatic Mental Associations Predict Future Choices of Undecided Decision-Makers," *Science*, Vol. 321, No. 5892, 2008, pp. 1100. (RW 3241)

Galinsky, E. *Mind in the Making: The Seven Essential Life Skills Every Child Needs*, HarperStudio, New York, NY, 2010. (RW 4984)

Gallagher, E.J. "Diagnostic Reasoning in Medicine: A Cognitive Paradigm for Unstructured Problem-Solving," *The Journal of Emergency Medicine*, Vol. 14, No. 6, 1996, pp. 755. (RW 2575)

Galotti, K.M., Blythe, M.C., Ainsworth, K.H., Lavin, B. & Mansfield, A.F. "A New Way of Assessing Ways of Knowing: The Attitudes Toward Thinking and Learning Survey (ATTLS)," *Sex Roles*, Vol. 40, No. 9/10, 1999, pp. 745-766. (RW 4627)

Galster, K.H. *The Face of the Foe: Pitfalls and Perspectives of Military Intelligence*, 2010. (RW 4325)

Galstyan, A. & Cohen, P.R. "Identifying Covert Sub-Networks through Iterative Node Classification," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 848)

Gamerman, E. "When Voters Lie," *Wall Street Journal*, August 2, 2008. (RW 3234)

Gamma, E. *Design Patterns: Elements of Reusable Object-Oriented Software*, Addison-Wesley, Reading, MA, 1995. (RW 2550)

Gammil, D. "Learning the Write Way," *The Reading Teacher*, Vol. 59, No. 8, 2006, pp. 754-762. (RW 5260)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Ganley, G.D. & Ganley, O.H. *Unexpected War in the Information Age: Communications and Information in the Falklands Conflict*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1984. (RW 1003)

Gannon, J.C. *The CIA in the New World Order: Intelligence Challenges through 2015. Remarks by the Chairman of the National Intelligence Council to the Smithsonian Associates 'Campus on the Mall,'* 2000. (RW 167)

Gannon, J.C. *The Impact of Technology on Analysis and Production. Remarks.* 2000. (RW 168)

Gannon, J.C. "The Strategic use of Open-Source Information," in *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, eds. R.Z. George & R.D. Kline, National Defense University Press, Washington, DC, 2004, pp. 279-284. (RW 693)

Gannon, J.C. *Intelligence and Homeland Security After 9/11*, Center for Information Policy Research. Harvard University, Cambridge, MA, 2005. (RW 1147)

Gannon, J.C. "Managing Analysis in the Information Age," in *Analyzing Intelligence: Origins, Obstacles, and Innovations*, eds. R.Z. George & J.B. Bruce, 2008, pp. 213. (RW 3105)

Gardiner, L.K. "Dealing with Intelligence-Policy Disconnects," in *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992*, ed. H.B. Westerfield, Yale University Press, New Haven, CT, 1995, pp. 344-356. (RW 890)

Gardner, D. *Building a Better Forecast*. Available: http://www2.canada.com/ottawacitizen/news/archives/story.html?id=2b7ca8da-e492-4876-920d-c6f6ca695c8d, Viewed: January 6, 2012. (RW 5381)

Gardner, D. *Future Babble: Why Expert Predictions are Next to Worthless and You can do Better*, Dutton, New York, NY, 2011. (RW 4727)

Gardner, H. *Changing Minds: The Art and Science of Changing our Own and Other People's Minds*, 2004. (RW 1724)

Gardner, S.B. "A Decentralized Data Fusion Framework for Horizontal Integration of Intelligence Data," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 600)

Garfield, E. "Meta-Analysis and the Metamorphosis of the Scientific Literature Review," *Current Contents*, 43, 1991, pp. 170. (RW 2250)

Garfield, E. "A Retrospective and Prospective View of Information Retrieval and Artificial Intelligence in the 21st Century," *Journal of the American Society for Information Science*, Vol. 52, No. 1, 2001, pp. 18-21. (RW 904)

Garfield, E. *A Prospective View of Citation Indexing and Information Retrieval in the 21st Century*, 2005. (RW 2098)

Garfinkel, H. *Studies in Ethnomethodology*, Prentice-Hall, Englewood Cliffs, NJ, 1967. (RW 1537)

Garigue, P. "Toward Effective Strategic Analysis - New Applications of Information Technology (Book Review)," *International Journal*, Vol. 37, No. 4, 1982, pp. 648. (RW 1576)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Garin, T.A. *"Focused Free Thinking" in Military Intelligence Analysis: Lessons from Best Practices,* Doctor of Public Administration dissertation, University of Southern California, 2003. (RW 4541)

Garin, T.A. "Appraising Best Practices in Defense Intelligence Analysis," in *Bringing Intelligence about: Practitioners Reflect on Best Practices,* eds. R.G. Swenson, Joint Military Intelligence College (U.S.) & Center for Strategic Intelligence Research, Joint Military Intelligence College, Center for Strategic Intelligence Research, Washington, DC, 2003, pp. 61. (RW 1489)

Garland, D.J., Wise, J.A. & Hopkin, V.D. *Handbook of Aviation Human Factors,* L. Erlbaum Associates, Mahwah, NJ, 1999. (RW 2822)

Garrett-Ingram, C. "Something to Believe in: The Relationship between Epistemological Beliefs and Study Strategies", *Annual Meeting of the American Educational Research Association,* Chicago, IL, (RW 4842)

Garrick, B.J. "Perspectives on the use of Risk Assessment to Address Terrorism," *Risk Analysis,* Vol. 22, No. 3, 2002, pp. 421-423. (RW 4733)

Garrow, D.J. "Crimes of History," *Wilson Quarterly,* Vol. 29, No. 1, 2005, pp. 112-114. (RW 606)

Garst, R.D. *Intelligence Types: The Role of Personality in the Intelligence Profession,* Joint Military Intelligence College, Washington, DC, 1993. (RW 1273)

Garst, R.D. & Gross, M.L. "On Becoming an Intelligence Analyst," *Defense Intelligence Journal,* Vol. 6, No. 2, 1997, pp. 47-59. (RW 1069)

Garstka, J.J. *Information Superiority for the Warfighter,* 2001. (RW 1171)

Garthoff, R. *On Estimating and Imputing Intentions,* 1978. (RW 1280)

Garthoff, R.L. *Intelligence Assessment and Policymaking: A Decision Point in the Kennedy Administration,* Brookings Institution, Washington, DC, 1984. (RW 1105)

Garthoff, R.L. "A Commentary on Merom's Methodology," *Intelligence and National Security,* Vol. 15, No. 3, 2000, pp. 146-153. (RW 178)

Garvin, L. *Small Business and the False Dichotomies of Contract Law,* Ohio State University Moritz College of Law Working Paper Series No. 1, Ohio State University, Columbus, OH, 2004. (RW 1123)

Gates, R. "Analysis. Discussion." in *Intelligence Requirements for the 1990s: Collection, Analysis, Counterintelligence, and Covert Action,* ed. R. Godson, Lexington Books, Lexington, MA, 1989, pp. 111-125. (RW 150)

Gates, R. *Emerging Missile Threats to North America. Statement for the Record. Hearings of the Senate Select Committee on Intelligence* 1996. (RW 443)

Gates, R.M. "The Prediction of Soviet Intentions," *Studies in Intelligence,* Vol. 17, No. 1, 1973, pp. 39-46. (RW 565)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Gates, R.M. "Annex V: The CIA and American Foreign Policy," in *Estimative Intelligence: The Purposes and Problems of National Intelligence Estimating*, ed. H.P. Ford, Defense Intelligence College, Washington, D.C, 1989, pp. 247-261. (RW 1528)

Gates, R.M. *Statement on Change in CIA and the Intelligence Community,* 1992. (RW 1231)

Gates, R.M. *From the Shadows: The Ultimate Insider's Story of Five Presidents and how they Won the Cold War,* Touchstone, New York, NY, 1997. (RW 166)

Gauthier, M. *Validation Workshop of the DRDC Concept Map Knowledge Model: Issues in Intelligence Analysis*, CR-2010-057, CAE Professional Services (Canada) Inc., Ottawa, ONT, 2010. (RW 4858)

Gawande, A. *The Checklist Manifesto: How to Get Things Right,* Metropolitan Press, New York, NY, 2009. (RW 3882)

Gazen, C., Carbonell, J. & Hayes, P. "Novelty Detection in Data Streams: A Small Step Towards Anticipating Strategic Surprise," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 861)

Gazit, S. *Intelligence Estimates Vs. Intelligence Forecasting*, 1979. (RW 1281)

Gazit, S. "Intelligence Estimates and the Decision-Maker," in *Leaders and Intelligence*, ed. M.I. Handel, F. Cass, London, UK, 1989, pp. 261-287. (RW 908)

Gazit, S. "Estimates and Fortune-Telling in Intelligence Work," in *Strategic Intelligence: Theory and Application*, eds. D.H. Dearth, Army War College & Joint Military Intelligence Training Center, 1991, pp. 113. (RW 3807)

Ge, X. & Land, S.M. "A Conceptual Framework for Scaffolding Ill-Structured Problem-Solving Processes using Question Prompts and Peer Interactions," *Educational Technology Research & Development*, Vol. 52, No. 2, 2004, pp. 5. (RW 2620)

Geddes, B.W. & Stevenson, R.J. "Explicit Learning of a Dynamic System with a Non-Salient Pattern," *The Quarterly Journal of Experimental Psychology,* Vol. 50, 1997, pp. 742. (RW 2161)

Geitz, S., Moon, B., D'Amico, A., Hoffman, R.R. & Page, R. "Beyond Requirements: Improving Software Tools for Intelligence Analysts", *Proceedings of the Human Factors and Ergonomics Society 49th Meeting,* pp. 932. (RW 3574)

Gelernter, D. "Artificial Intelligence is Lost in the Woods," *Technology Review,* July/August, 2007 (RW 2493)

Gelwick, R. *The Way of Discovery: An Introduction to the Thought of Michael Polanyi,* Oxford University Press, New York, 1977. (RW 3905)

Gendron, A. "Just War, just Intelligence: An Ethical Framework for Foreign Espionage," *International Journal of Intelligence and Counterintelligence*, Vol. 18, No. 3, 2005, pp. 398-434. (RW 1176)

General Intelligence Training Council. *Shaping the Global Intelligence Professional to Achieve Mission Success. Conference Announcement.* 2010. (RW 4443)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Gentner, D. & Stevens, A.L. *Mental Models,* L. Erlbaum Associates, Hillsdale, NJ, 1983. (RW 1320)

Gentry, J. "Intelligence Learning and Adaptation: Lessons from Counterinsurgency Wars," *Intelligence and National Security,* Vol. 25, No. 1, 2010, pp. 50. (RW 3937)

Gentry, J.A. *Lost Promise: How CIA Analysis Misserves the Nation,* University Press of America, Lanham, MD, 1993. (RW 11)

Gentry, J.A. *A Framework for Reform of the US Intelligence Community,* Available: http://www.fas.org/irp/gentry, Viewed: September 9, 2005. (RW 663)

Gentry, J.A. "Intelligence analyst/manager Relations at the CIA," *Intelligence and National Security,* Vol. 10, No. 4, 1995, pp. 133-146. (RW 130)

Gentry, J.A. "Intelligence Failure Reframed," *Political Science Quarterly,* Vol. 123, No. 2, 2008, pp. 247-270. (RW 4246)

Gentry, J.A. "Assessing Intelligence Performance," in *Oxford Handbook of National Security Intelligence,* ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 87-106. (RW 4704)

George, A.L. *The Scientific Status of Propaganda Analysis,* 1954. (RW 3033)

George, A.L. *Propaganda Analysis: A Study of Inferences made from Nazi Propaganda in World War II,* Row, Peterson, Evanston, Ill., 1959. (RW 2972)

George, A.L. "The Causal Nexus between Cognitive Beliefs and Decision-Making Behavior: The "Operational Code" Belief System," in *Psychological Models in International Politics,* ed. L.S. Falkowski, Westview Press, Boulder, CO, 1979, pp. 95-124. (RW 5821)

George, A.L. "From Groupthink to Contextual Analysis of Policy-Making Groups," in *Beyond Groupthink: Political Group Dynamics and Foreign Policy-Making,* eds. P.'. Hart, E.K. Stern & B. Sundelius, University of Michigan Press, Ann Arbor, 1997, pp. 35-53. (RW 4410)

George, D. "The Estimative Process," in *Intelligence and Arms Control: A Marriage of Convenience,* ed. T.J. Hirschfeld, Lyndon B. Johnson School of Public Affairs, Austin, TX, 1987, pp. 19-29. (RW 1059)

George, R.Z. "Fixing the Problem of Analytical Mind-Sets: Alternative Analysis," *International Journal of Intelligence and Counterintelligence,* Vol. 17, No. 3, 2004, pp. 385-404. (RW 307)

George, R.Z. "Meeting 21st Century Transnational Challenges: Building a Global Intelligence Paradigm," *Studies in Intelligence,* Vol. 51, No. 3, 2007 (RW 2801)

George, R.Z. "The Art of Strategy and Intelligence," in *Analyzing Intelligence: Origins, Obstacles, and Innovations,* eds. R.Z. George & J.B. Bruce, 2008, pp. 107. (RW 3099)

George, R.Z. *National Security Enterprise: Navigating the Labyrinth,* Georgetown University Press, Washington, DC, 2011. (RW 4505)

George, R.Z. "Reflections on CIA Analysis: Is it Finished?" *Intelligence and National Security,* Vol. 26, No. 1, 2011, pp. 72-81. (RW 4729)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

George, R.Z. & Bruce, J.B. "Conclusion: The Age of Analysis," in *Analyzing Intelligence: Origins, Obstacles, and Innovations*, eds. R.Z. George & J.B. Bruce, 2008, pp. 295. (RW 3111)

George, R.Z. & Kline, R.D. *Intelligence and the National Security Strategist: Enduring Issues and Challenges,* National Defense University Press, Washington, DC, 2004. (RW 691)

George, R.Z. "Beyond Analytic Tradecraft," *International Journal of Intelligence and Counterintelligence,* Vol. 23, No. 2, 2010, pp. 296-306. (RW 3897)

Gerber, C. *New Technology is Helping Defense Intelligence Analysts Sort through Huge Volumes of Data,* 2005. (RW 1581)

Gerecht, R.M. "The Sorry State of the CIA," *Weekly Standard,* Vol. 9, No. 42, 2004 (RW 622)

Gerecht, R.M. "The Sorry State of the CIA," *American Enterprise Institute for Public Policy Research. On the Issues.,* 2004 (RW 623)

Gerling, K., Gruener, H.P., Kiel, A. & Schulte, E. *Information Acquisition and Decision Making in Committees: A Survey,* 2003. (RW 2063)

Gerras, C.S.J. *Thinking Critically about Critical Thinking: A Fundamental Guide for Strategic Leaders,* U. S. Army War College, Carlisle, PA, 2006. (RW 4252)

Gersh, J., Lewis, B., Montemayor, J., Piatko, C. & Turner, R. "Supporting Insight-Based Information Exploration in Intelligence Analysis," *Communications of the ACM,* Vol. 49, No. 4, 2006, pp. 63. (RW 1519)

Gershon, N.D. "Analysis in the Future: Community, Analysis by Doing, and Office Design," in *A Handbook of the Psychology of Intelligence Analysis,* ed. R.L. Rees, 2008, pp. 376. (RW 3658)

Gerybadze, A. "Technology Forecasting as a Process of Organizational Intelligence," *R&D Management,* Vol. 24, No. 2, 1994, pp. 131-140. (RW 81)

Gess-Newsome, J. "Pedagogical Content Knowledge: An Introduction and Orientation," in *Examining Pedagogical Content Knowledge: The Construct and its Implications for Science Education,* eds. N.G. Lederman & J. Gess-Newsome, Kluwer Academic, Dordrecht, 1999, pp. 3-17. (RW 5327)

Gess-Newsome, J. "Secondary Teachers' Knowledge and Beliefs about Subject Matter and their Impact on Instruction," in *Examining Pedagogical Content Knowledge: The Construct and its Implications for Science Education,* eds. N.G. Lederman & J. Gess-Newsome, Kluwer Academic, Dordrecht, 1999, pp. 51-94. (RW 5369)

Getzels, J.W. & Csikszentmihalyi, M. *The Creative Vision: A Longitudinal Study of Problem Finding in Art,* Wiley, New York, 1976. (RW 2977)

Geva, N. & Mintz, A. *Decisionmaking on War and Peace: The Cognitive-Rational Debate,* Lynne Rienner Publishers, Boulder, Colo., 1997. (RW 4412)

Ghauri, P.N., Grønhaug, K. & Kristianslund, I. *Research Methods in Business Studies: A Practical Guide,* Prentice Hall, New York, 1995. (RW 2546)

Gholson, B. *Psychology of Science: Contributions to Metascience,* Cambridge University Press, Cambridge; New York, 1989. (RW 4030)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Ghose, T. *Like Math? Thank Your Motivation, Not IQ.* Available: http://www.scientificamerican.com/article.cfm?id=like-math-thank-your-moti&W T.mc_id=SA_CAT_SP_20130102, Viewed: January 7, 2013. (RW 5889)

Giangrande, R. "Electronic journals: a literature review 1995-1999", *Esb Forum,* [Online]. Available from: http://www.burioni.it/forum. 2002. (RW 1542)

Giannoulis, A. *Intelligence Failure and the Importance of Strategic Foresight to the Preservation of National Security,* Research Paper No. 155, Research Institute for European and American Studies, Athens, Greece, 2011. (RW 5540)

Gibson, E.J. & McGarvey, H.R. "Experimental Studies of Thought and Reasoning," *The Psychological Bulletin,* Vol. 34, No. 6, 1937, pp. 327-350. (RW 4483)

Gibson, G. *Managing the Information Tsunami,* 2007. (RW 3192)

Gibson, S.D. "In the Eye of the Perfect Storm: Re-Imagining, Reforming and Refocusing Intelligence for Risk, Globalisation and Changing Societal Expectation," *Risk Management,* Vol. 7, No. 4, 2005, pp. 23-41. (RW 5357)

Gibson, S.D. *Open Source Intelligence (OSINT): A Contemporary Intelligence Lifeline,* Ph.D. dissertation, Cranfield University, 2007. (RW 5550)

Giere, R.N. *Explaining Science: A Cognitive Approach,* University of Chicago Press, Chicago, 1988. (RW 1820)

Gigerenzer, G. *Gut Feelings: The Intelligence of the Unconscious,* Penguin Books, New York, NY, 2008. (RW 5685)

Gigone, D. & Hastie, R. "The Impact of Information on Small Group Choice," *Journal of Personality and Social Psychology,* Vol. 72, No. 1, 1997, pp. 132-140. (RW 1932)

Gilad, B. "What is Intelligence Analysis? Part II," *Competitive Intelligence Magazine,* Vol. 1, No. 3, 1998, pp. 29-31. (RW 1090)

Gilad, B. & Herring, J.P. "CI Certification: Do we Need it?" *Competitive Intelligence Magazine,* Vol. 4, No. 2, 2001, pp. 28-31. (RW 3946)

Gilad, B. *Early Warning: Using Competitive Intelligence to Anticipate Market Shifts, Control Risk, and Create Powerful Strategies,* American Management Association, New York, 2004. (RW 3385)

Gilad, B. & Herring, J.P. *The Art and Science of Business Intelligence Analysis,* JAI Press, Greenwich, CT, 1996. (RW 5468)

Gilbert, S., McCay-Peet, L. & Toms, E.G. "Supporting Task with Information Appliances: Taxonomy of Needs", *HCIR 2010: Proceedings of the Fourth Workshop on Human-Computer Interaction and Information Retrieval,* New Brunswick, NJ, August 22, 2010, pp. 103. (RW 4318)

Gilboa, A. & Lapid, E. *Israel's Silent Defender: An Inside Look at Sixty Years of Israeli Intelligence,* Gefen Publisher, New York, NY, 2012. (RW 5493)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Gilboa, I., Postlewaite, A. & Schmeidler, D. *Rationality of Belief. Or, Why Bayesianism is neither Necessary nor Sufficient for Rationality,* Cowles Foundation Discussion Paper No. 1484, Yale University, New Haven, CT, 2004. (RW 1915)

Gilchrist, S. *Identifying Personality Types of Intelligence Analysts,* MSAI thesis, Mercyhurst College, 2007. (RW 3711)

Gill, P. "Securing the Globe: Intelligence and the Post-9/11 Shift from 'Liddism' to'Drainisn'," *Intelligence and National Security,* Vol. 19, No. 3, 2004, pp. 467. (RW 1666)

Gill, P. ""Knowing the Self, Knowing the Other": The Comparative Analysis of Security Intelligence," in *Handbook of Intelligence Studies,* ed. L.K. Johnson, 2007, pp. 82. (RW 2459)

Gill, P. *Theories of Intelligence: The Next Steps?* 2007. (RW 2979)

Gill, P. "Security Intelligence and Human Rights: Illuminating the 'Heart of Darkness'?" *Intelligence and National Security,* Vol. 24, No. 1, 2009, pp. 78. (RW 3451)

Gill, P. "Theories of Intelligence: Where are we, Where should we Go and how might we Proceed?" in *Intelligence Theory: Key Questions and Debates,* eds. P. Gill, S. Marrin & M. Phythian, 2009, pp. 208. (RW 3413)

Gill, P. "Theories of Intelligence," in *Oxford Handbook of National Security Intelligence,* ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 43-58. (RW 4703)

Gill, P. "Intelligence, Threat, Risk and the Challenge of Oversight," *Intelligence and National Security,* Vol. 27, No. 2, 2012, pp. 206-222. (RW 5613)

Gill, P., Marrin, S. & Phythian, M. "Introduction," in *Intelligence Theory: Key Questions and Debates,* eds. P. Gill, S. Marrin & M. Phythian, 2009, pp. 1. (RW 3366)

Gill, P. & Phythian, M. *Issues in the Theorisation of Intelligence. Paper Presented at the International Studies Association Conference, Montreal.* 2004. (RW 1308)

Gill, P. & Phythian, M. *Intelligence in an Insecure World,* Polity Press, Cambridge, UK, 2006. (RW 2501)

Gillenwater, J.Y. & Gray, M. "Evidence: What is it, Where do we Find it, and How do we use it?" *European Urology Supplements,* Vol. 2, No. 5, 2003, pp. 3. (RW 2227)

Gilluly, J. "The Scientific Philosophy of G. K. Gilbert," in *The Fabric of Geology,* ed. C.C. Albritton, Freeman, Cooper, & Co., Stanford, CA, 1963, pp. 218-224. (RW 5445)

Gilovich, T. *How we Know what Isn't so: The Fallibility of Human Reason in Everyday Life,* Free Press, New York, NY, 1991. (RW 2289)

Gilovich, T. "Unbiased in a Biased World," in *A Handbook of the Psychology of Intelligence Analysis,* ed. R.L. Rees, 2008, pp. 103. (RW 3644)

Giorgi, A. *Phenomenology and Psychological Research,* Duquesne University Press, Pittsburgh, PA, 1985. (RW 2718)

Girden, E.R. *Evaluating Research Articles from Start to Finish,* 2nd ed., Sage Publications, Thousand Oaks, CA, 2001. (RW 2243)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Givens, A. "A Systems-Based Approach to Intellience Reform," *Journal of Strategic Security*, Vol. 5, No. 1, 2012, pp. 64-84. (RW 5539)

Gjelten, T. *A Peek Inside the CIA, as it Tries to Assess Iran*. Available: http://www.npr.org/2012/05/23/153428611/a-peek-inside-the-cia-as-it-tries-to-assess-iran, Viewed: May 25, 2012. (RW 5663)

Gladwell, M. "The New Boy Network: What do Job Interviews really Tell Us?" *The New Yorker*, Vol. 76, No. 13, 2000, pp. 68-86. (RW 902)

Gladwell, M. "The Social Life of Paper," *The New Yorker*, 2002, pp. 92. (RW 1376)

Gladwell, M. "Connecting the Dots," *The New Yorker*, Vol. 79, No. 3, 2003, pp. 83-88. (RW 749)

Gladwell, M. "The Epistemology of Surprise," *The New Yorker*, 2003. (RW 1377)

Gladwell, M. "Open Secrets," *The New Yorker*, January 8, 2007. (RW 1896)

Gladwell, M. "Most Likely to Succeed," *The New Yorker*, Vol. 84, No. 41, 2008, pp. 36. (RW 3476)

Gladwell, M. "How David Beats Goliath," *The New Yorker*, Vol. 85, No. 13, 2009, pp. 40. (RW 3475)

Gladwell, M. "Small Change: Why the Revolution Will Not be Tweeted," *The New Yorker*, 2010 (RW 4433)

Glaser, B.G. *Emergence Vs Forcing: Basics of Grounded Theory Analysis*, Sociology Press, Mill Valley, CA, 1992. (RW 2695)

Glaser, E.M. *An Experiment in the Development of Critical Thinking*, AMS Press Inc., New York, NY, 1941. (RW 3812)

Glees, A. & Davies, P.H.J. "Intelligence, Iraq and the Limits of Legislative Accountability during Political Crisis," *Intelligence and National Security*, Vol. 21, No. 5, 2006, pp. 848. (RW 2087)

Gleick, J. *The Information: A History, a Theory, a Flood*, Pantheon Books, New York, NY, 2011. (RW 4549)

Glenberg, A.M. "Mental Models, Space, and Embodied Cognition," in *Creative Thought: An Investigation of Conceptual Structures and Processes*, eds. T.B. Ward, S.M. Smith & J. Vaid, 1997, pp. 495. (RW 1765)

Glenn, D. "Cloak and Classroom," *Chronicle of Higher Education*, Vol. 51, No. 29, 2005, pp. A14. (RW 2039)

Globerson, T. & Zelniker, T. "What is the Relationship between Cognitive Style and Cognitive Development?" in *Cognitive Style and Cognitive Development*, eds. T. Globerson & T. Zelniker, Ablex Publishing, Norwood, NJ, 1989, pp. 71-85. (RW 5167)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Godfrey, E.D. & Harris, D.R. *Basic Elements of Intelligence: A Manual of Theory, Structure and Procedures for use by Law Enforcement Agencies Against Organized Crime,* US GPO, Washington, DC, 1971. (RW 1109)

Godlewski, R.J. "Cultivating Creativity within Intelligence Analysis," *American Intelligence Journal,* Vol. 25, No. 2, 2007/2008, pp. 85. (RW 3228)

Godlewski, R.J. "Human Intelligence: Perceiving an Enemy's Thoughts," *American Intelligence Journal,* Vol. 27, No. 1, 2009, pp. 29. (RW 3987)

Godson, R. "Intelligence Requirements for the 1980's: An Introduction," in *Intelligence Requirements for the 1980's*, ed. R. Godson, National Strategy Information Center, Washington, DC, 1979, pp. 3-8. (RW 151)

Godson, R. *Intelligence and Policy*, Lexington Books, Lexington, MA, 1986. (RW 1096)

Godson, R. "Intelligence for the 1990s," in *Intelligence Requirements for the 1990s: Collection, Analysis, Counterintelligence, and Covert Action,* ed. R. Godson, Lexington Books, Lexington, MA, 1989, pp. 1-29. (RW 156)

Godson, R. *Intelligence Requirements for the 1990s: Collection, Analysis, Counterintelligence, and Covert Action,* Lexington Books, Lexington, MA, 1989. (RW 1110)

Godson, R. "Intelligence Reorganization," *American Intelligence Journal,* Vol. 13, No. 1/2, 1992, pp. 25-29. (RW 4472)

Godson, R. "Strategic Intelligence in the Coming Years: Foreign Policy and Defense Asset," in *Managing Contemporary Conflict*, eds. M.G. Manwaring & W.J. Olson, Westview Press, Boulder, CO, 1996, pp. 245-262. (RW 1219)

Godson, R. *Government and Gangs,* 2001. (RW 1447)

Godson, R., May, E.R. & Schmitt, G.J. *U.S. Intelligence at the Crossroads: Agendas for Reform,* Brassey's US, Washington, DC, 1995. (RW 247)

Godson, R. & Wirtz, J.J. "Strategic Denial and Deception," *International Journal of Intelligence and Counterintelligence,* Vol. 13, No. 4, 2000, pp. 424-437. (RW 57)

Godson, R., with comments by Kerr, Richard & May, E. "Covert Action: Neither Exceptional Tool nor Magic Bullet," in *U.S. Intelligence at the Crossroads: Agendas for Reform*, eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 154-177. (RW 644)

Goel, A., Morse, E., Raja, A., Scholtz, J. & Stasko, J. *Introspective Self-Explanations for Report Generation in Intelligence Analysis* [undated]. (RW 5568)

Goel, A., Morse, E., Raja, A., Scholtz, J. & Stasko, J. "Introspective Self-Explanations for Report Generation in Intelligence Analysis [Powerpoint Presentation], *Proceedings of IJCAI-2009 Workshop on Explanation-Aware Computing,* Pasadena, CA, July 11-12, 2009. (RW 5569)

Goff, M. & Ackerman, P.L. "Personality-Intelligence Relations: Assessment of Typical Intellectual Engagement," *Journal of Educational Psychology,* Vol. 84, No. 4, 1992, pp. 537-552. (RW 4946)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Goldberg, J. "The Unknown: The CIA and the Pentagon Take on Al Qaeda and Iraq," *The New Yorker,* February 10, 2003. (RW 4197)

Goldberg, R.A. "Who Profited from the Crime? Intelligence Failure, Conspiracy Theories and the Case of September 11," *Intelligence and National Security,* Vol. 19, No. 2, 2004, pp. 249-261. (RW 468)

Goldman, A.I. "Epistemics: The Regulative Theory of Cognition," *Journal of Philosophy,* Vol. 55, 1978, pp. 509-523. (RW 5052)

Goldman, A.I. *Epistemology and Cognition,* Harvard University Press, Cambridge, MA, 1986. (RW 5027)

Goldman, A.I. *Knowledge in a Social World,* Clarendon Press, Oxford, 1999. (RW 4248)

Goldman, J. *Ethics of Spying: A Reader for the Intelligence Professional,* Scarecrow Press, Lanham, MD, 2006. (RW 5795)

Goldman, J. *Words of Intelligence: A Dictionary,* 2006. (RW 3682)

Goldman, J. *Ethics of Spying: A Reader for the Intelligence Professional,* Scarecrow Press, Lanham, MD, 2010. (RW 5796)

Goldmann, N. *Online Information Hunting,* Windcrest/McGraw-Hill, Blue Ridge Summit PA, 1992. (RW 3848)

Goldstein, K.M. & Blackman, S. *Cognitive Style: Five Approaches and Relevant Research,* Wiley, New York, 1978. (RW 4302)

Goldstein, R., Almenberg, J., Dreber, A., Emerson, J.W., Herschkowitsch, A. & Katz, J. *Do More Expensive Wines Taste Better? Evidence from a Large Sample of Blind Tastings,* AAWE Working Paper No. 16, American Association of Wine Economists, Walla Walla, WA, 2008. (RW 3319)

Goldstone, J.A. *Using Quantitative and Qualitative Models to Forecast Instability,* 2008. (RW 3127)

Golovchinsky, G., Qvarfordt, P. & Pickens, J. "Collaborative Information Seeking," *Computer,* Vol. 42, No. 3, 2009, pp. 47. (RW 3440)

Gomez-Gauchia, H. & McFadyen, R. "Conceptual Mapping as a First Step in Data Modeling," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge,* eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 277-292. (RW 4976)

Gonzalez-Ibanez, R. & Shah, C. "A Proposal for Measuring and Implementing Group's Affective Relevance in Collaborative Information Seeking", *HCIR 2010: Proceedings of the Fourth Workshop on Human-Computer Interaction and Information Retrieval,* New Brunswick, NJ, August 22, 2010, pp.107. (RW 4319)

Goodie, A.S. & Young, D.L. *The Skill Element in Risky Decision Making: Control, Competence Or both?* (RW 2065)

Goodman, A.E. *Testimony for the Senate Select Committee on Intelligence,* 1991. (RW 1236)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Goodman, A.E. "Shifting Paradigms and Shifting Gears: A Perspective on Why there is no Post-Cold War Intelligence Agenda," *Intelligence and National Security,* Vol. 10, No. 4, 1995, pp. 3-9. (RW 133)

Goodman, A.E. "The Future of US Intelligence," *Intelligence and National Security,* Vol. 11, No. 4, 1996, pp. 645-656. (RW 136)

Goodman, A.E. "Testimony: Fact Checking at the CIA," *Foreign Policy,* 102, 1996, pp. 180. (RW 400)

Goodman, A.E. *CIA: The Need for Reform,* Special Report #13, Center for International Policy, 2001. (RW 278)

Goodman, A.E. & Berkowitz, B.D. "Intelligence without the Cold War," *Intelligence and National Security,* Vol. 9, No. 2, 1994, pp. 301-319. (RW 89)

Goodman, M.A. *Failure of Intelligence: The Decline and Fall of the CIA,* Rowman & Littlefield Publishers, Lanham, MD, 2008. (RW 2959)

Goodman, M.A. *The Road to Intelligence Reform: Paved with Good Intentions,* Center for International Policy, Washington, DC, 1996. (RW 405)

Goodman, M.A. "Ending the CIA's Cold War Legacy," *Foreign Policy,* 106, 1997, pp. 128-143. (RW 148)

Goodman, M.A. "Pearl Harbor Redux," *Foreign Policy In Focus,* Vol. 5, No. 36, 2001 (RW 371)

Goodman, M.A. "Revamping the CIA," *Issues in Science and Technology,* Vol. 18, No. 2, 2001-2002, pp. 59-65. (RW 378)

Goodman, M.A. "9/11: The Failure of Strategic Intelligence," *Intelligence and National Security,* Vol. 18, No. 4, 2003, pp. 59-71. (RW 258)

Goodman, M.A. "Uses and Misuses of Strategic Intelligence," *International Policy Report,* January, 2004, pp. 1-7. (RW 513)

Goodman, M.S. "Studying and Teaching about Intelligence: The Approach in the United Kingdom," *Studies in Intelligence,* Vol. 50, No. 2, 2006, pp. 57. (RW 1554)

Goodman, M.S. "Learning to Walk: The Origins of the UK's Joint Intelligence Committee," *International Journal of Intelligence and Counterintelligence,* Vol. 21, No. 1, 2008, pp. 40. (RW 2911)

Goodman, M.S. "Jones' Paradigm: The how, Why, and Wherefore of Scientific Intelligence," *Intelligence and National Security,* Vol. 24, No. 2, 2009, pp. 236. (RW 3493)

Goodman, M.S. & Omand, D. "Teaching Intelligence Analysts in the UK: What Analysts Need to Understand: The King's Intelligence Studies Program," *Studies in Intelligence,* Vol. 52, No. 4, 2008, pp. 1-12. (RW 3923)

Goodman, S. & Greenland, S. "Why most Published Research Findings are False: Problems in the Analysis," *PLoS Medicine,* Vol. 4, No. 4, 2007, pp. e168. (RW 3287)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Gookins, A.J. "The Role of Intelligence in Policy Making," *SAIS Review,* Vol. 28, No. 1, 2008, pp. 65. (RW 3326)

Gopen, G.D. *The Sense of Structure: Writing from the Reader's Perspective,* Pearson Longman, New York, 2004. (RW 4477)

Gordon, D. "Evolving Approaches to Analyzing Transnational Threats: Key Challenges and Potential Partnerships", *New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities,* Rome, Italy, 31 March - 2 April, 2004, pp. 87-90. (RW 2837)

Gordon, M. & Kochen, M. "Recall-Precision Trade-Off: A Derivation," *Journal of the American Society for Information Science,* Vol. 40, No. 3, 1989, pp. 145-151. (RW 1210)

Gordon, M. & Pathak, P. "Finding Information on the World Wide Web: The Retrieval Effectiveness of Search Engines," *Information Processing and Management,* Vol. 35, No. 2, 1999, pp. 141-180. (RW 763)

Gorman, M.E. "Scientific and Technological Thinking," *Review of General Psychology,* Vol. 10, No. 2, 2006, pp. 113. (RW 2329)

Gorman, M.E., Tweney, R.D., Gooding, D.C. & Kincannon, A.P. "The Future of Cognitive Studies of Science and Technology," in *Scientific and Technological Thinking,* ed. M.E. Gorman, L. Erlbaum Associates, Mahwah, N.J, 2005, pp. 345. (RW 2141)

Gorman, S. "Worlds Apart," *National Journal,* Vol. 35, No. 1, 2003, pp. 2482-2488. (RW 928)

Gorman, S. "Frustrated Intelligence Reformers See Window of Opportunity," 2004 (RW 469)

Gorman, S. "A Cautionary Tale," *National Journal,* Vol. 37, No. 6, 2005, pp. 350-354. (RW 259)

Gorman, S. "Years of Spotty Data Sharing on Suspects," *Wall Street Journal,* January 8, 2010, (RW 3854)

Gormley, D.M. *New Challenges for Intelligence* (RW 584)

Gormley, D.M. "The Limits of Intelligence: Iraq's Lessons," *Survival,* Vol. 46, No. 3, 2004, pp. 7. (RW 1330)

Goss, P.A. *DCI's Global Intelligence Challenges Briefing. Global Intelligence Challenges 2005: Meeting Long-Term Challenges with a Long-Term Strategy* 2005. (RW 628)

Gottlieb, D.A., Weiss, T. & Chapman, G.B. "The Format in which Uncertainty Information is Presented Affects Decision Biases," *Psychological Science,* Vol. 18, No. 3, 2007, pp. 240. (RW 2482)

Gottschalk, P. "Organizational Structure as Predictor of Intelligence Strategy Implementation in Policing," *International Journal of Law, Crime, and Justice,* Vol. 36, No. 3, 2008, pp. 184-195. (RW 5809)

Gotz, D., Zhou, M.X. & When, Z. "A Study of Information Gathering and Result Processing in Intelligence Analysis", *IUI2006 Workshop on Intelligent User Interfaces for Intelligence Analysis,* January 29, 2006. (RW 3258)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Gough, D. & Elbourne, D. "Systematic Research Synthesis to Inform Policy Practice and Democratic Debate," *Social Policy & Society,* Vol. 1, No. 3, 2002, pp. 225. (RW 2198)

Gough, H.G. & Bradley, P. *CPI 260 Client Feedback Report Example*, CPP, Inc., Mountain View, CA, 2003. (RW 5336)

Gough, N. "From Epistemology to Ecopolitics: Renewing a Paradigm for Curriculum," *Journal of Curriculum Studies,* Vol. 21,1989, pp. 225. (RW 2430)

Gouin, D. & Lavigne, V. "Trends in Human-Computer Interaction to Support Future Intelligence Analysis Capability", *16th International Command and Control Research and Technology Symposium,* Quebec City, Canada, June 21 - 23, 2010, [unpaged]. (RW 5507)

Gourley, R. "Intuitive Intelligence," *Defense Intelligence Journal,* Vol. 6, No. 2, 1997, pp. 61. (RW 1667)

Grabo, C.M. "Strategic Warning: The Problem of Timing," *Studies in Intelligence,* Vol. 16, No. 2, 1972, pp. 79-92. (RW 556)

Grabo, C.M. *Warning Intelligence,* Association of Former Intelligence Officers, McLean, VA, 1987. (RW 682)

Grabo, C.M. *Handbook of Warning Intelligence: Assessing the Threat to National Security,* Scarecrow Press, Lanham, MD, 2010. (RW 5746)

Grabo, C.M. & Goldman, J. *Anticipating Surprise: Analysis for Strategic Warning,* Joint Military Intelligence College, Washington, DC, 2002. (RW 680)

Graening-Clement, D.L. "Handling Criticism - for Newer Analysts," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 410. (RW 3663)

Graff, G. & Birkenstein, C. *They Say I Say: The Moves that Matter in Persuasive Writing,* W.W. Norton, New York, NY, 2007. (RW 4769)

Graham, B. *The Need for Intelligence Reform,* 2004. (RW 1229)

Graham, D.O. "Analysis and Estimates," in *Intelligence Requirements for the 1980's*, ed. R. Godson, National Strategy Information Center, Washington, DC, 1979, pp. 22-33. (RW 153)

Graham, M.M. *Remarks and Q&A by the Deputy Director of National Intelligence for Collection. ODNI Open Source Conference.* 2007. (RW 2728)

Graham, S. & Weiner, B. "Theories and Principles of Motivation," in *Handbook of Educational Psychology*, eds. D.C. Berliner & R.C. Calfee, Simon & Schuster Macmillan, New York, NY, 1996, pp. 63-84. (RW 5307)

Graham, S. & Harris, K.R. "Self-Regulation and Strategy Instruction for Students Who Find Writing and Learning Challenging," in *The Science of Writing: Theories, Methods, Individual Differences, and Applications*, eds. C.M. Levy & S.E. Ransdell, 1996, pp. 347. (RW 1827)

Graham, S. & Harris, K.R. "It can be Taught but it does Not Develop Naturally," *School Psychology Review,* Vol. 26, No. 3, 1997, pp. 414. (RW 2205)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Graham, T. *Intelligence Support to Arms Control Policy. Statement before the House Permanent Select Committee on Intelligence*, 1994. (RW 1050)

Graham, T. & Hansen, K.A. *Preventing Catastrophe: The Use and Misuse of Intelligence in Efforts to Halt the Proliferation of Weapons of Mass Destruction,* Stanford Security Studies/Stanford University Press, Stanford, CA, 2009. (RW 3540)

Grau, L.W. "Something Old, Something New: Guerrillas, Terrorists, and Intelligence Analysis," *Military Review*, Vol. 84, No. 4, 2004, pp. 42-49. (RW 1183)

Graves, D.L. *Bayesian Analysis Methods for Threat Prediction,* 1993. (RW 1291)

Gray, C.S. "Out of the Wilderness: Prime Time for Strategic Culture," *Comparative Strategy*, Vol. 26, No. 1, 2007, pp. 1. (RW 2397)

Gray, W.D., Schoelles, M.J. & Veksler, V.D. "Simborgs and Simulated Task Environments for Engineering Next Generation Workstations for Intelligence Analysts", *HFES 2004: Proceedings of the Human Factors and Ergonomics Society. 48th Annual Meeting.* September 20-24, 2004, pp.362. (RW 2874)

Green, D.W. "Arguments in Mind," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans*, eds. K.I. Manktelow, D.E. Over & S. Elqayam, Psychology Press, Hove, East Sussex, UK, 2011, pp. 53-61. (RW 5704)

Green, G. "In their Own Words: Critical Thinking in Artists' Diaries and Interviews," *Art Education*, Vol. 59, No. 4, 2006, pp. 46-53. (RW 5376)

Greenberg, H.M. "Intelligence of the Past: Intelligence for the Future," in *Strategic Intelligence. Volume 1: Understanding the Hidden Side of Government*, ed. L.K. Johnson, Praeger Security International, Westport, CT, 2007, pp. 169. (RW 2714)

Greenberg, H.M. "Is the Department of Homeland Security an Intelligence Agency?" *Intelligence and National Security*, Vol. 24, No. 2, 2009, pp. 216. (RW 3494)

Greenberg, M.R. & Haass, R.N. *Making Intelligence Smarter: The Future of US Intelligence,* Council on Foreign Relations, New York, NY, 1996. (RW 664)

Greenblatt, S., Marcus, S. & Darr, T. "TMODS - Integrated Fusion Dashboard: Applying Fusion of Fusion Systems to Counter-Terrorism," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 877)

Greene, G.E. *Distributed Collaborative Analysis: A New Approach for Intelligence Analysis,* US Army War College, Carlisle Barracks, PA, 2001. (RW 265)

Greene, J.A., Azevedo, R. & Torney-Purta, J. "Modeling Epistemic and Ontological Cognition: Philosophical Perspectives and Methodological Directions." *Educational Psychologist*, Vol. 43, No. 3, 2008, pp. 142-160. (RW 4938)

Greene, J.A. & Azevedo, R. "A Theoretical Review of Winne and Hadwin's Model of Self-Regulated Learning: New Perspectives and Directions," *Review of Educational Research*, Vol. 77, No. 3, 2007, pp. 334-372. (RW 5443)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Greenhalgh, T. *How to Read a Paper: The Basics of Evidence Based Medicine*, 2nd ed., BMJ, London, 2001. (RW 1386)

Greenhalgh, T. & Hurwitz, B. *Narrative Based Medicine: Dialogue and Discourse in Clinical Practice*, BMJ Books, London, 1998. (RW 1387)

Greenhalgh, T. & Hurwitz, B. "Why Study Narrative?" in *Narrative Based Medicine: Dialogue and Discourse in Clinical Practice*, eds. T. Greenhalgh & B. Hurwitz, BMJ Books, London, 1998, pp. 3. (RW 1526)

Greeno, J.C. "Situativity of Knowing, Learning, and Research," *American Psychologist*, Vol. 53, No. 1, 1998, pp. 5. (RW 2650)

Greeno, J.G. "Situations, Mental Models, and Generative Knowledge," in *Complex Information Processing: The Impact of Herbert A. Simon*, eds. H.A. Simon, D. Klahr & K. Kotovsky, L. Erlbaum Associates, Hillsdale, NJ, 1989, pp. 285. (RW 1843)

Greeno, J.G., Collins, A.M. & Resnick, L.B. "Cognition and Learning," in *Handbook of Educational Psychology*, eds. D.C. Berliner & R.C. Calfee, Macmillan Library Reference USA, Simon & Schuster Macmillan, New York, 1996, pp. 15. (RW 1841)

Greenstein, F.I. & Immerman, R.H. "Effective National Security Advising: Recovering the Eisenhower Legacy," *Political Science Quarterly*, Vol. 115, No. 3, 2000, pp. 335. (RW 2829)

Greenwood, A. *The National Assessment of College Student Learning: Identification of the Skills to be Taught, Learned and Assessed: A Report on the Proceedings of the Second Study Design Workshop*, Arlington VA, November 17-18, 1992. (RW 4046)

Greer, B. & Verschaffel, L. "Nurturing Conceptual Change in Mathematics Education," in *Re-Framing the Conceptual Change Approach in Learning and Instruction*, eds. S. Vosniadou, A. Baltas & X. Vamvakoussi, Elsevier, Amsterdam, 2007, pp. 319-328. (RW 5126)

Grefenstette, G. & Shanahan, J.G. "Document Souls: Joining Personalities to Documents to Produce Pro-Active Documents Engaged in Contextualized, Independent Search", *Context-Based Information Retrieval*, Paris, July 5, 2005 (RW 4870)

Gregg, N. *Written Expression Disorders*, Kluwer Academic Publishers, Dordrecht, 1995. (RW 1866)

Gregory, G.G. & Gregory, H. *A Strategy for Improving Analysis: Using "Analytic Brokers" to Enhance Rigor and Collaboration*, 2006. (RW 2997)

Greitzer, F.L., Cowley, P.J. & Littlefield, R.J. "Monitoring User Activities in the Glass Box Analysis Environment", New Orleans, LA, September 20-24, 2004. (RW 1465)

Greitzer, F.L. *Methodology, Metrics, and Measures for Testing and Evaluation of Intelligence Analysis Tools*, PNWD-3550, (RW 1625)

Greitzer, F.L. *Methodology, Metrics and Measures for Testing and Evaluation of Intelligence Analysis Tools* 2005. (RW 1506)

Greitzer, F.L. "Toward the Development of Cognitive Task Difficulty Metrics to Support Intelligence Analysis Research", (RW 1343)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Greitzer, F.L. & Allwein, K. *Metrics and Measures for Intelligence Analysis Task Difficulty* (RW 1512)

Gressang, D.S. "The Shortest Distance between Two Points Lies in Rethinking the Question: Intelligence and the Information Age Technology Challenge," in *Strategic Intelligence. Volume 2: The Intelligence Cycle: The Flow of Secret Information from Overseas to the Highest Councils of Government,* ed. L.K. Johnson, Praeger Security International, Westport, CT, 2007, pp. 123. (RW 2706)

Gries, D.D. "Intelligence in the 1990s," *Studies in Intelligence,* Vol. 35, No. 1, 1991, pp. 5-11. (RW 70)

Gries, D.D. "Opening Up Secret Intelligence," *Orbis,* Vol. 37, No. 3, 1993, pp. 365-372. (RW 76)

Gries, D.D. "New Links between Intelligence and Policy," in *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992,* ed. H.B. Westerfield, Yale University Press, New Haven, CT, 1995, pp. 357-365. (RW 891)

Griffin, T.D. & Ohlsson, S. "Beliefs Versus Knowledge: A Necessary Distinction for Explaining, Predicting, and Assessing Conceptual Change", *Proceedings of the 23rd Annual Conference of the Cognitive Science Society,* pp.364. (RW 2000)

Grimes, J. *Information Technologies and Multinational Corporations,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1987. (RW 1004)

Grinnell, R.M. *Social Work Research & Evaluation: Quantitative and Qualitative Approaches,* 5th ed., F. E. Peacock Publishers Inc., Itasca, Ill., 1997. (RW 2527)

Groopman, J. "What's the Trouble?" *The New Yorker,* Vol. 82, No. 47, 2007, pp. 36-41. (RW 1975)

Grossman, D.A., Reichart, J., Chowdhury, A., Lundquist, C., Holmes, D. & Frieder, O. *Using Relevance Feedback within the Relational Model for TREC-5* (RW 1556)

Grossman, J.B., Woods, D.D. & Patterson, E.S. "Supporting the Cognitive Work of Information Analysis and Synthesis: A Study of the Military Intelligence Domain", *Proceedings of the Human Factors and Ergonomics Society 51st Meeting,* pp. 348. (RW 3577)

Grundmann, W.R. "Reshaping the Intelligence Production Landscape," *Defense Intelligence Journal,* Vol. 6, No. 2, 1997, pp. 23. (RW 1668)

Guarino, N. "Formal Ontology in Information Systems", *Fois '98,* Trento, Italy, June 6-8, 1998. (RW 662)

Guarino, N., Masolo, C. & Vetere, G. "Ontoseek: Using Large Linguistic Ontologies for Accessing Online Yellow Pages and Product Catalogues," *IEEE Intelligent Systems,* Vol. 14, No. 3, 1999, pp. 70-80. (RW 675)

Guelmezoglu, A.M. *Research Synthesis [Powerpoint Presentation]* 2003. (RW 2200)

Guenther, C.L. & Alicke, M.D. "Self-Enhancement and Belief Perseverance," *Journal of Experimental Social Psychology,* Vol. 44, No. 3, 2008, pp. 706-712. (RW 5352)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Guerin, D.A., Olson, M.J., Zborowsky, T. & Lim, Y. "Exploring Writing-to-Learn in Design," *Journal of Interior Design,* Vol. 25, No. 1, 1999, pp. 26. (RW 3517)

Guillaume, L. "Risk and War in the Twenty-First Century," *Intelligence and National Security,* Vol. 23, No. 3, 2008, pp. 406. (RW 3173)

Guillot, C.W.M. *Critical Thinking for the Military Professional,* Available: http://www.airpower.maxwell.af.mil/airchronicles/cc/guillot.html, Viewed: December 24, 2009. (RW 3804)

Guinn, B. & Aasman, J. "Semantic Real Time Intelligent Decision Automation", *Fifth International Conference on Semantic Technology for Intelligence, Defense, and Security,* Fairfax, VA, 26-29 October 2010. (RW 4860)

Gumahad, A.T. *Cyber Troops and Net War: The Profession of Arms in the Information Age,* 1996. (RW 1437)

Gun, R., Lioma, C. & Larsen, B. "The Tipping Point: F-Score as a Function of the Number of Retrieved Items," *Information Processing and Management,* 2012. (RW 5547)

Gunter, M.M. "The Iraqi Opposition and the Failure of U.S. Intelligence," *International Journal of Intelligence and Counterintelligence,* Vol. 12, No. 2, 1999, pp. 135-167. (RW 402)

Gupta, A. "Problem Framing in Assessment Processes: The Case of Biosafety," in *Global Environmental Assessments: Information and Influence,* ed. R.B. Mitchell, MIT Press, Cambridge, MA, 2006, pp. 344. (RW 2551)

Gustafson, K. "Strategic Horizons: Futures Forecasting and the British Intelligence Community," *Intelligence and National Security,* Vol. 25, No. 5, 2010, pp. 589-610. (RW 4571)

Guthrie, L.F. & Hall, W.S. "Ethnographic Approaches to Reading Research," in *Handbook of Reading Research,* ed. P.D. Pearson, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 91-110. (RW 5181)

Guzick, D.S., Grefenstette, I., Baffone, K., Berga, S.L., Krasnow, J.S., Stovall, D.W. & Naus, G.J. "Infertility Evaluation in Fertile Women - a Model for Assessing the Efficacy of Infertility Testing," *Human Reproduction,* Vol. 9, No. 12, 1994, pp. 2306. (RW 1955)

Guzzetti, B.J. "Learning Counter-Intuitive Science Concepts: What have we Learned from Over a Decade of Research," *Reading & Writing Quarterly,* Vol. 16, No. 2, 2000, pp. 89-98. (RW 4836)

Haas, C. *Writing Technology: Studies on the Materiality of Literacy,* L. Erlbaum Associates, Mahwah, N.J, 1996. (RW 1861)

Haas, M.R. & Hansen, M.T. *Different Knowledge, Different Benefits: Toward a Productivity Perspective on Knowledge Sharing in Organizations,* [undated]. (RW 2993)

Haase, F. "Categories of Critical Thinking in Information Management," *Nómadas,* Vol. 27, No. 3, 2010, pp. 257-275. (RW 5026)

Haave, C.A. *Risk Management in the Department of Defense,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2004. (RW 621)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hacker, D.J. "Comprehension Monitoring as a Writing Process," in *Advances in Cognition and Educational Practice. Volume 2. Children's Writing: Toward a Process Theory of the Development of Skilled Writing*, ed. E.C. Butterfield, Jai, Greenwich, CT; London, 1994, pp. 143. (RW 2126)

Hackman, J.R. "The Team Diagnostic Survey," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 416. (RW 3665)

Hackman, J.R. & O'Connor, M. *What Makes for a Great Analytic Team? Individual Versus Team Approaches to Intelligence Analysis* 2004. (RW 1299)

Hackman, J.R. & Woolley, A.W. *Creating and Leading Analytic Teams,* The Group Brain Project, Technical Report No. 5, 2007. (RW 3015)

Hackman, J.R. & Woolley, A.W. "Social Factors: Creating and Leading Analytic Teams," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 176. (RW 3648)

Haddick, R. "Strategic error: when the big picture misses the point", *Foreign Policy,* [Online], September 10. Available from: http://www.foreignpolicy.com/articles/2012/08/24/strategic_error. 2012 (RW 5806)

Hadjichristidis, C., Handley, S.J., Sloman, S.A., Evans, Jonathan St. B. T., Over, D.E. & Stevenson, R.J. "Iffy Beliefs: Conditional Thinking and Belief Change," *Memory & Cognition,* Vol. 35, No. 8, 2007, pp. 2052-2059. (RW 5695)

Haglund, D.G. "Lies, Damned Lies, and Threat Perceptions: Kriegsgrunde (1941) Revisited, in Light of Iraq," *Comparative Strategy,* Vol. 24, No. 1, 2005, pp. 1-22. (RW 353)

Haglund, L. & Herron, D. "Students with Non-Proficient Information Seeking Skills Greatly Over-Estimate their Abilities," *Evidence Based Library and Information Practice,* Vol. 3, No. 2, 2008, pp. 48-51. (RW 4803)

Hagner, A.F. "Philosophical Aspects of the Geological Sciences," in *The Fabric of Geology*, ed. C.C. Albritton, Freeman, Cooper, & Co., Stanford, CA, 1963, pp. 233-241. (RW 5446)

Hahn, U. & Chater, N. "Concepts and Similarity," in *Knowledge, Concepts and Categories*, eds. K. Lamberts & D.R. Shanks, 1st MIT Press ed., MIT Press, Cambridge, MA, 1997, pp. 43. (RW 2143)

Hahn, U. "Why Rational Norms are Indispensable," *Behavioral and Brain Sciences,* Vol. 34, No. 5, 2011, pp. 257-258. (RW 5489)

Hahn, U. & Oaksford, M. "Rational Argument," in *Oxford Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 277-298. (RW 5500)

Haidar, A.H. & Balfakih, N.M. *United Arab Emirates Science Students' Views about the Epistemology of Science,* 1999. (RW 5520)

Hailes, T. *Develop America's Airmen Today...for Tomorrow. [Powerpoint Presentation],* 2005. (RW 1051)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Haimson, C., Freeman, J., Wilson, C. & Hertel, M. *The Analyst's Analyst: An Assessment and Training System for Intelligence Organizations*, 2004. (RW 1314)

Haimson, C., Freeman, J., Wilson, C. & Richardson, A. "An Assessment and Training System for Imagery Analysis and Reporting," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 814)

Haines, A. & Donald, A. *Getting Research Findings into Practice*, 2nd ed., BMJ Books, London, 2002. (RW 2220)

Hale, C. *Vex, Hex, Smash, Smooch: Let Verbs Power Your Writing*, W. W. Norton & Co., New York, NY, 2012. (RW 5845)

Hale, E. *Critical Thinking Business Seminar Email [Personal Communication]*, Foundation for Critical Thinking, Tomales, CA, 2011. (RW 5361)

Halevy, E. "Understanding the Middle East: A View from Inside the Mossad," *Policy Watch*, 1107, 2006 (RW 1464)

Haley, J.M. "An Evolution in Intelligence Doctrine," *Air & Space Power Journal*, Vol. 26, No. 5, 2012, pp. 33-48. (RW 5797)

Hall, E.T. *Beyond Culture*, Anchor Press, New York, NY, 1989. (RW 1545)

Hall, J.G., Rapanotti, L. & Jackson, M. "Problem Frame Semantics for Software Development," *Software and Systems Modeling*, Vol. 4, No. 2, 2005, pp. 189. (RW 2633)

Hall, J.A., Tickle-Degnen, L., Rosenthal, R. & Mosteller, F. "Hypotheses and Problems in Research Synthesis," in *The Handbook of Research Synthesis*, eds. H.M. Cooper & L.V. Hedges, Russell Sage Foundation, New York, 1994, pp. 17. (RW 2484)

Hall, K.R. *Space Systems as Contributors to Information Superiority*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1999. (RW 1005)

Hall, K.R. "Challenges Faced by US Intelligence," *American Intelligence Journal*, Summer/Fall, 2000, pp. 1-3. (RW 173)

Hall, W.M. *Intelligence Analysis in the 21st Century* 1992. (RW 1290)

Hall, W.M. *Stray Voltage: War in the Information Age*, Naval Institute Press, Annapolis, MD, 2003. (RW 3982)

Hall, W.M. & Citrenbaum, G.M. *Intelligence Analysis: How to Think in Complex Environments*, Praeger Security International, Santa Barbara, CA, 2010. (RW 3878)

Hallden, O., Scheja, M. & Haglund, L. "The Contextuality of Knowledge: An Intentional Approach to Meaning Making and Conceptual Change," in *International Handbook of Research on Conceptual Change*, ed. S. Vosniadou, Routledge, New York, 2008, pp. 509-532. (RW 5123)

Hallett, D., Chandler, M.J. & Krettenauer, T. "Disentangling the Course of Epistemic Development: Parsing Knowledge by Epistemic Content," *New Ideas in Psychology*, Vol. 20, No. 2, 2002, pp. 285. (RW 5301)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hallinan, J.T. *Why We Make Mistakes: How We Look without Seeing, Forget Things in Seconds, and Are all Pretty Sure We are Way Above Average,* Broadway Books, New York, 2009. (RW 3433)

Halperin, M.H. & Kanter, A. *Readings in American Foreign Policy; a Bureaucratic Perspective*, Little, Brown, Boston, 1973. (RW 1289)

Halpern, D.F. *Halpern Critical Thinking Assessment (HCTA)*, Schufried Publishers. Available: http://www.cmc.edu/pages/faculty/dhalpern/index_files/Page1667.html, Viewed: February 7, 2012. (RW 4257)

Halpern, D.F. "Thinking Across the Disciplines: Methods and Strategies to Promote Higher-Order Thinking in Every Classroom," in *Thinking Skills Instruction: Concepts and Techniques*, eds. M. Heiman & J. Slomianko, National Education Association, Washington, DC, 1987, pp. 69-76. (RW 5080)

Halpern, D.F. "Teaching Critical Thinking for Transfer Across Domains," *American Psychologist,* Vol. 53, No. 4, 1998, pp. 449-455. (RW 3972)

Halpern, D.F. "Assessing the Effectiveness of Critical Thinking Instruction," *Journal of General Education,* Vol. 50, No. 4, 2001, pp. 270-287. (RW 3964)

Halpern, D.F. *Thought and Knowledge: An Introduction to Critical Thinking*, L. Erlbaum Associates, Mahwah, NJ, 2003. (RW 3811)

Halvorsen, K.T. "The Reporting Format," in *The Handbook of Research Synthesis*, eds. H.M. Cooper & L.V. Hedges, Russell Sage Foundation, New York, 1994, pp. 425. (RW 2490)

Hambrick, D.Z. & Meinz, E.J. "Limits on the Predictive Power of Domain-Specific Experience and Knowledge in Skilled Performance," *Current Directions in Psychological Science,* Vol. 20, No. 5, 2011, pp. 275-279. (RW 5241)

Hamer, R. & van Rossum, E.J. "Linking Learning Conceptions to Self-Authorship and Beyond," in *Development and Assessment of Self-Authorship: Exploring the Concept Across Cultures*, eds. M.B. Baxter Magolda, E.G. Creamer & P.S. Meszaros, Stylus Pub., Sterling, VA, 2010, pp. 45-68. (RW 4761)

Hamilton, L.H. *Reforming US Intelligence. Extension of Remarks. US House of Representatives,* 1995. (RW 1228)

Hamilton, L.H. *Talking Points on Combating Terrorism,* 2001. (RW 507)

Hamilton, N. *The Mechanics of a Deep Net Metasearch Engine*, [undated]. (RW 1399)

Hammer, D. "Epistemological Beliefs in Introductory Physics," *Cognition and Instruction,* Vol. 12, No. 2, 1994, pp. 151. (RW 4426)

Hammer, D. & Elby, A. "On the Form of a Personal Epistemology," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing*, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 169. (RW 4333)

Hammond, J.D. *So You Want to be an Intelligence Analyst!* Defense Intelligence College, Washington, DC, 1983. (RW 1275)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hammond, T.H. "Why is the Intelligence Community so Difficult to Redesign?" *Governance,* Vol. 20, No. 3, 2007, pp. 401-422. (RW 4611)

Hammond, T.H. "Agenda Control, Organizational Structure, and Bureaucratic Politics," *American Journal of Political Science,* Vol. 30, No. 2, 1986, pp. 379. (RW 1531)

Hammond, T.H. *Intelligence Organizations and the Organization of Intelligence: On the Problem of Drawing Inferences from Data Scattered Around the Bureaucracy,* 2009. (RW 4367)

Hammond, T.H. "Intelligence Organizations and the Organization of Intelligence," *International Journal of Intelligence and Counterintelligence,* Vol. 23, No. 4, 2010, pp. 680-724. (RW 4309)

Hammond, T.H., Jen, K.I. & Maeda, K. "Learning in Hierarchies: An Empirical Test using Library Catalogues," *Journal of Theoretical Politics,* Vol. 19, No. 4, 2007, pp. 425-463. (RW 4685)

Hamre, J.J. *Statement before the Senate Select Committee on Intelligence. Reform and Reorganization of the U.S. Intelligence Community,* 2004. (RW 315)

Hand, B. & Treagust, D. "Linking Pedagogical Requirements to Cognition and Literacy when using Writing to Learn Strategies", *Annual Meeting of the National Association for Research in Science Teaching,* Vancouver, Canada, April 1-3, 2004. (RW 3521)

Handel, M.I. *Perception, Deception, and Surprise: The Case of the Yom Kippur War,* Hebrew University of Jerusalem, Jerusalem, 1976. (RW 714)

Handel, M.I. "The Yom Kippur War and the Inevitability of Surprise," *International Studies Quarterly,* Vol. 21, No. 3, 1977, pp. 461-502. (RW 741)

Handel, M.I. "Avoiding Political and Technological Surprise in the 1980's," in *Intelligence Requirements for the 1980's,* ed. R. Godson, National Strategy Information Center, Washington, DC, 1979, pp. 85-119. (RW 208)

Handel, M.I. "Surprise and Change in International Politics," *International Security,* Vol. 4, No. 4, 1980, pp. 57-85. (RW 740)

Handel, M.I. "The Study of Intelligence," *Orbis,* Vol. 26, No. Winter, 1983, pp. 817-821. (RW 739)

Handel, M.I. *Military Deception in Peace and War,* Magnes Press, Hebrew University, Jerusalem, 1985. (RW 712)

Handel, M.I. "Strategic Surprise: The Politics of Intelligence and the Management of Uncertainty," in *Intelligence--Policy and Process,* eds. A.C. Maurer, M.D. Tunstall & J.M. Keagle, Westview Press, Boulder, CO, 1985, pp. 239-268. (RW 214)

Handel, M.I. "The Politics of Intelligence," *Intelligence and National Security,* Vol. 2, No. 4, 1987, pp. 5-46. (RW 737)

Handel, M.I. *Strategic and Operational Deception in the Second World War,* F. Cass, London, UK, 1987. (RW 717)

Handel, M.I. "Technological Surprise in War," *Intelligence and National Security,* Vol. 2, No. 1, 1987, pp. 1-53. (RW 738)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Handel, M.I. *Leaders and Intelligence,* F. Cass, London, UK, 1989. (RW 743)

Handel, M.I. *War, Strategy, and Intelligence,* F. Cass, London, UK, 1989. (RW 715)

Handel, M.I. *Intelligence and Military Operations,* F. Cass, London, UK, 1990. (RW 716)

Handel, M.I. "Intelligence and the Problem of Strategic Surprise," in *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel,* eds. R.K. Betts & T.G. Mahnken, Frank Cass, London, UK, 2003, pp. 1-58. (RW 209)

Handel, M.I. "Intelligence and Deception," in *Intelligence and the National Security Strategist: Enduring Issues and Challenges,* eds. R.Z. George & R.D. Kline, National Defense University Press, Washington, DC, 2004, pp. 359-387. (RW 696)

Handley, S.J., Newstead, S.E. & Neilens, H. "Thinking before You Decide on the Selection Task: Matching Bias Requires Analytical Reasoning," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans,* eds. K.I. Manktelow, D.E. Over & S. Elqayam, Psychology Press, Hove, East Sussex, UK, 2011, pp. 167-189. (RW 5706)

Haney, P.J. "Soccer Fields and Submarines in Cuba: The Politics of Problem Definition," *Naval War College Review,* Vol. 50, No. 4, 1997, pp. 67. (RW 2770)

Hanig, R.K. & Henshaw, M.E. "Needed: A National Security Simulation Center," *Studies in Intelligence,* Vol. 52, No. 2, 2008, pp. 11. (RW 3161)

Hannaford, P. "Jury News: Surprising, Disturbing, Silly and Mundane: Highlights of Recent Jury Research," *The Court Manager,* Vol. 20, No. 3, 2005, pp. 51. (RW 2036)

Hannay, D. "Three Iraq Intelligence Failures Reconsidered," *Survival,* Vol. 51, No. 6, 2009, pp. 13. (RW 3732)

Hano, K.M. *Jury Decision-Making Study,* 2006. (RW 2096)

Hanrahan, J.P. "Intelligence for the Policy Chiefs," *Studies in Intelligence,* Vol. 11, No. 1, 1967, pp. 1-12. (RW 536)

Hanratty, T., Heilman, E., Dumer, J. & Hammell, R.J. "Knowledge Elicitation to Prototype the Value of Information", *Proceedings of the 23rd Midwest Artificial Intelligence and Cognitive Science Conference,* Cincinnati, OH, April 21-22, 2012, pp.173-179. (RW 5598)

Hansen, B. "Intelligence Reforms," *CQ Researcher,* Vol. 12, No. 3, 2002, pp. 49. (RW 1669)

Hansen, F.S. "An Argument for Reflexivity in Intelligence Work," *Intelligence and National Security,* Vol. 27, No. 3, 2012, pp. 349-370. (RW 5666)

Hansen, J. "US Intelligence Confronts the Future," *International Journal of Intelligence and Counterintelligence,* Vol. 17, No. 4, 2004, pp. 673-709. (RW 413)

Hansen, K.A. *Intelligence and Nuclear Proliferation: Lessons Learned,* Institut Francais des Relations Internationales, Paris, France, 2011. (RW 5552)

Hansen, M.T., Nohria, N. & Tierney, T. "What's Your Strategy for Managing Knowledge?" *Harvard Business Review,* March-April, 1999, pp. 106. (RW 1329)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hantula, D.A., Brockman, D.D. & Smith, C.L. "Online Shopping as Foraging: The Effects of Increasing Delays on Purchasing and Patch Residence," *IEEE Transactions on Professional Communications,* Vol. 51, No. 2, 2008, pp. 147-154. (RW 5484)

Hardcastle, J., McLeod, A., Mellor, B., Richmond, J. & Savva, H. "Growth, Community, and Control in Secondary School Writers," in *Explorations in the Development of Writing: Theory, Research, and Practice,* eds. B.M. Kroll & C.G. Wells, Wiley, Chichester Sussex; New York, 1983, pp. 209. (RW 2285)

Hardman, D. & Ayton, P. "Arguments and Decisions," in *Psychological Investigations of Competence in Decision Making,* eds. K. Smith, J. Shanteau & P.E. Johnson, Cambridge University Press, Cambridge, U.K.; New York, 2004, pp. 163. (RW 2384)

Hardy, J. "Speaking Clearly: A Critical Review of the Self-Talk Literature," *Psychology of Sport and Exercise,* Vol. 7, No. 1, 2006, pp. 81-97. (RW 5790)

Hardy, Q. *Crushing the Cost of Predicting the Future,* Available: http://bits.blogs.nytimes.com/2011/11/17/crushing-the-cost-of-predicting-the-future/, Viewed: January 19, 2012. (RW 5405)

Hardy, T.S. "Intelligence Reform in the Mid-1970s," *Studies in Intelligence,* Vol. 20, No. 2, 1976, pp. 1-15. (RW 538)

Hare, N.P. & Collinson, P. "Organisational Culture and Intelligence Analysis: A Perspective from Senior Managers in the Defence Intelligence Assessments Staff," *Public Policy and Administration,* 2012 (RW 5886)

Hare, W. "Critical Thinking as an Aim of Education," in *Aims of Education,* ed. R. Marples, Routledge, London, UK, 1999, pp. 85-99. (RW 4468)

Harknett, R.J. & Stever, J.A. "The Struggle to Reform Intelligence After 9/11," *Public Administration Review,* Vol. 71, No. 5, 2011, pp. 700-706. (RW 5117)

Harman, D. *Overview of the Second Text Retrieval Conference (TREC-2)* (RW 1584)

Harman, D. *Overview of TREC-1* (RW 1583)

Harman, G. *Change in View: Principles of Reasoning,* MIT Press, Cambridge, MA, 1986. (RW 5895)

Harpaz, Y. *Approaches to Teaching Thinking: Toward a Conceptual Mapping of the Field,* Jerusalem, Israel, [undated]. (RW 5018)

Harper, W. "Rational Belief Change, Popper Functions, and Counterfactuals," *Synthese,* Vol. 30, 1975, pp. 221. (RW 1481)

Harris, D.H. "Critical Thinking Strategies for Intelligence Analysis", *United Nations Regional Criminal Intelligence Conference,* Belgrade, Servia, December 12-13 (RW 5636)

Harris, D.H. "Overcoming the Cognitive Challenges of Intelligence Analysis", *Proceedings of the IALEIA World Intelligence Training Conference,* Mexico City, MX, April 24-28 (RW 5635)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Harris, D.H. "Critical Thinking Training for Intelligence Analysis," *Journal of the International Association of Law Enforcement Intelligence Analysts,* Vol. 20, No. 1, 2011, pp. 76-90. (RW 5637)

Harris, D.R. *Basic Elements of Intelligence,* US GPO, Washington, DC, 1976. (RW 1108)

Harris, D.H. & Spiker, V.A. "Critical Thinking Skills for Intelligence Analysts," in *Ergonomics - a Systems Approach,* ed. I.L. Nunes, InTech, 2012, pp. 209-232. (RW 5623)

Harris, J.W. *Building Leverage in the Long War: Ensuring Intelligence Community Creativity in the Fight Against Terrorism,* Policy Analysis No. 439, Cato Institute, Washington, DC, 2002. (RW 325)

Harris, J.W. "Organizational Factors," in *A Handbook of the Psychology of Intelligence Analysis,* ed. R.L. Rees, 2008, pp. 429. (RW 3670)

Harris, J.W. & Sullivan, J. "Speaking Truth to Power," in *A Handbook of the Psychology of Intelligence Analysis,* ed. R.L. Rees, 2008, pp. 427. (RW 3669)

Harris, J.W. & Sullivan, J. "A Warning System for Politicization," in *A Handbook of the Psychology of Intelligence Analysis,* ed. R.L. Rees, 2008, pp. 425. (RW 3668)

Harris, K.R. & Graham, S. *Making the Writing Process Work: Strategies for Composition and Self-Regulation,* 2nd ed., Brookline Books, Cambridge, MA, 1996. (RW 2203)

Harris, M.J. & Rosenthal, R. "Mediation of Interpersonal Expectancy Effects: 31 Meta-Analyses," *Psychological Bulletin,* Vol. 97, 1985, pp. 363. (RW 2876)

Harris, S. "Beautiful Minds: To Fix the Intelligence Agencies, we must Embrace Maverick Analysts," *Government Executive,* September 19, 2003 (RW 127)

Harris, S. "Intelligence Incorporated," *Government Executive,* Vol. 37, No. 8, 2005, pp. 40. (RW 1673)

Harris, S. "Intelligent Reform," *Government Executive,* February 1, 2005. (RW 418)

Harris, S. *Intelligence Veteran Aims to Motivate Young Analysts,* Available: http://www.govexec.com, Viewed: July 8, 2010. (RW 4172)

Hart, C. *Doing a Literature Review: Releasing the Social Science Research Imagination,* Sage Publications, London; Thousand Oaks, 1998. (RW 2245)

Hart, C. *Doing a Literature Search: A Comprehensive Guide for the Social Sciences,* Sage, London, 2001. (RW 3463)

Hart, D. & Simon, S. "Thinking Straight and Talking Straight: Problems of Intelligence Analysis," *Survival,* Vol. 48, No. 1, 2006, pp. 35-60. (RW 1656)

Harte, D.V. "The Search for 21st Century Mindware," *Community, Technical, and Junior College Journal,* Vol. 58, No. 2, 1987, pp. 50-53. (RW 5788)

Harteis, C., Gruber, H. & Lehner, F. "Epistemological Beliefs and their Impact on Work, Subjectivity, and Learning," in *Work, Subjectivity and Learning: Understanding Learning*

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

through Working Life, eds. S. Billett, T.J. Fenwick & M. Somerville, Springer, Dordrecht, The Netherlands, 2006, pp. 123-140. (RW 2844)

Harter, A.G. & Moon, B.M. "Common Lexicon Initiative: A Concept Mapping Approach to Semiautomated Definition Integration," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge*, eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 131-150. (RW 4969)

Harter, S.P. *Online Information Retrieval: Concepts, Principles, and Techniques,* Academic Press, Orlando, FL, 1986. (RW 1208)

Harter, S.P. "Psychological Relevance and Information Science," *Journal of the American Society for Information Science,* Vol. 43, No. 9, 1992, pp. 602-615. (RW 1212)

Hartley, J. & Tynjälä, P. "New Technology, Writing and Learning," in *Writing as a Learning Tool: Integrating Theory and Practice*, eds. P. Tynjälä, L. Mason & K. Lonka, Kluwer Academic Publishers, Dordrecht Netherlands; Boston, 2001, pp. 161. (RW 4338)

Hartley, K. & Bendixen, L.D. "The use of Comprehension Aids in a Hypermedia Environment: Investigating the Impact of Metacognitive Awareness and Epistemological Beliefs," *Journal of Educational Multimedia and Hypermedia,* Vol. 12, No. 3, 2003, pp. 275-289. (RW 5329)

Hasanbegovic, J., Gruber, H., Rehrl, M. & Bauer, J. "The Two-Fold Role of Epistemological Beliefs in Higher Education: A Review of Research about Innovation in Universities," in *Higher Education and Working Life: Collaborations, Confrontations and Challenges*, eds. P. Tynjälä, J. Välimaa & G. Boulton-Lewis, Elsevier, Oxford, 2006, pp. 163-176. (RW 4264)

Haslam, S.A., Salvatore, J., Kessler, T. & Reicher, S.D. "The Social Psychology of Success," *Scientific American Mind,* Vol. 19, No. 2, 2008, pp. 24. (RW 3176)

Hassebrock, F., Johnson, P.E., Bullemer, P., Fox, P.W. & Moller, J.H. "When Less is More: Representation and Selective Memory in Expert Problem Solving," *The American Journal of Psychology,* Vol. 106, No. 2, 1993, pp. 155-189. (RW 1931)

Hasson, U. & Johnson-Laird, P.N. "Why Believability Cannot Explain Belief Revision", *Proceedings of the 25th Annual Conference of the Cognitive Science Society,* July 31-August 2, 2003, pp. 516. (RW 1982)

Hastedt, G. "The Politics of Intelligence and the Politicization of Intelligence: The American Experience," *Intelligence and National Security,* Vol. 28, No. 1, 2013, pp. 5-31. (RW 5910)

Hastedt, G. "Foreign Policy by Commission: Reforming the Intelligence Community," *Intelligence and National Security,* Vol. 22, No. 4, 2007, pp. 443. (RW 2864)

Hastedt, G.P. "Intelligence Estimates: NIEs vs. the Open Press in the 1958 China Straits Crisis," *International Journal of Intelligence and Counterintelligence,* Vol. 23, No. 1, 2010, pp. 104. (RW 3770)

Hastedt, G. "CIA's Organizational Culture and the Problem of Reform," *International Journal of Intelligence and Counterintelligence,* Vol. 9, No. 3, 1996, pp. 249-269. (RW 37)

Hastedt, G. "CIA's Organizational Culture and the Problem of Reform," *International Journal of Intelligence and Counterintelligence,* Vol. 9, No. 3, 1996, pp. 249-269. (RW 5748)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hastedt, G. "The Politics of Intelligence Accountability," in *Oxford Handbook of National Security Intelligence,* ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 719-734. (RW 4718)

Hastedt, G.P. & Skelley, D. "Intelligence in a Turbulent World: Insights from Organization Theory," in *Intelligence Theory: Key Questions and Debates,* eds. P. Gill, S. Marrin & M. Phythian, 2009, pp. 112. (RW 3408)

Hastie, R. "Thinking," *Annual Review of Psychology,* Vol. 52, 2001, pp. 653. (RW 1958)

Hastie, R. *Inside the Juror: The Psychology of Juror Decision Making,* Cambridge University Press, Cambridge, UK, 1993. (RW 963)

Hastie, R. "Group Processes in Intelligence Analysis," in *Intelligence Analysis: Behavioral and Social Scientific Foundations,* eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, pp. 169-196. (RW 4777)

Hastings, A.L. *The View from the Intelligence Community. Speech,* 2007. (RW 2428)

Hatcher, D.L. *Critical Thinking and the Liberal Arts,* Baker University, Baldwin City, KS, 1990. (RW 4080)

Hatcher, D.L. *Critical Thinking: A New Definition and Defense*, Baker University, Baldwin City, KS, 2000. (RW 4254)

Hatcher, D.L. "Why Percy can't Think: A Response to Bailin," *Informal Logic,* Vol. 21, No. 2, 2001, pp. 171-181. (RW 4111)

Hatcher, D.L. "Stand-Alone Versus Integrated Critical Thinking Courses," *Journal of General Education,* Vol. 55, No. 3-4, 2006, pp. 247-272. (RW 4287)

Hatemi, P.K. & McDermott, R. "The Genetics of Politics: Discovery, Challenges, and Progress," *Trends in Genetics,* Vol. 29, No. 10, 2012, pp. 525-533. (RW 5829)

Hativa, N. & Marincovich, M. *Disciplinary Differences in Teaching and Learning: Implications for Practice,* Jossey-Bass, San Francisco, CA, 1995. (RW 4415)

Hatlebrekke, K.A. & Smith, M.L.R. "Towards a New Theory of Intelligence Failure? The Impact of Cognitive Closure and Discourse Failure," *Intelligence and National Security,* Vol. 25, No. 2, 2010, pp. 147. (RW 4195)

Haus, L. "The Predicament of the Terrorism Analyst," *Studies in Intelligence,* Vol. 29, No. 4, 1985, pp. 13-23. (RW 4203)

Hauser, M.D. *Moral Minds: How Nature Designed our Universal Sense of Right and Wrong,* Ecco, New York, 2006. (RW 1709)

Hautamäki, A. "The Main Paradigms of Cognitive Science," in *Brain, Mind, and Physics,* eds. P. Pylkkänen, P. Pylkkö & A. Hautamäki, IOS Press, Amsterdam, 1997, pp. 26-33. (RW 5672)

Havenstein, H. "Top Secret: CIA Explains its Wikipedia-Like National Security Project," *Computerworld,* 2008 (RW 3157)

Hawkins, J. & Blakeslee, S. *On Intelligence,* Times Books, New York, 2004. (RW 1787)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hawks, M.R., Perram, G.P. & Tuttle, R.F. "Initial Demonstration of Monocular Passive Ranging in the Near Infrared," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 851)

Hawthorne, S. "Knowledge Related to a Purpose: Data-Mining to Detect Terrorism," in *Governance and Public Security* Syracuse University, Syracuse, NY, 2003, pp. 85-98. (RW 578)

Hayden, M.V. *Address to Kennedy Political Union of American University,* 2000. (RW 241)

Hayden, M.V. *Remarks to CIA Employees regarding Strategic Intent 2007-2011,* 2007. (RW 1978)

Hayden, M.V. *DNI Open Source Conference 2008 - Remarks from CIA Director,* 2008. (RW 3256)

Hayes, C.C. & Anderson, R.A. "Benefits of Decision Support Tools for Users with Differing Levels of Domain Expertise", *Proceedings of the Human Factors and Ergonomics Society 50th Meeting,* pp. 358. (RW 3575)

Hayes, C.C. "An Intelligence Application Providing Multiple Coordinated Data Views," *Human Factors and Ergonomics Society Annual Meeting Proceedings*, Vol. 52, No. 7, 2008, pp. 610. (RW 3581)

Hayes, J.R. "Writing Research: The Analysis of a very Complex Task," in *Complex Information Processing: The Impact of Herbert A. Simon*, eds. H.A. Simon, D. Klahr & K. Kotovsky, L. Erlbaum Associates, Hillsdale, NJ, 1989, pp. 209. (RW 1844)

Hayes, J.R. "A New Framework for Understanding Cognition and Affect in Writing," in *The Science of Writing: Theories, Methods, Individual Differences, and Applications*, eds. C.M. Levy & S.E. Ransdell, 1996, pp. 1. (RW 1822)

Haynes, C.M. "The Effects of Context on Cascaded-Inference Evidence Evaluation," *Journal of Economic Psychology,* Vol. 23, No. 4, 2002, pp. 469-485. (RW 5297)

Haynes, J., Sakai, K., Rees, G., Gilbert, S., Frith, C. & Passingham, D. "Reading Hidden Intentions in the Human Brain," *Current Biology,* Vol. 17, No. 4, 2007, pp. 323. (RW 2165)

Hays, R.B., Jolly, B.C., Caldon, L.J.M., McCrorie, P., McAvoy, P.A., McManus, I.C. & Rethans, J.J. "Is Insight Important? Measuring Capacity to Change Performance," *Medical Education,* Vol. 36, No. 10, 2002, pp. 965. (RW 2193)

Hazlitt, H. *Thinking as a Science*, E. P. Dutton & Co., New York, NY, 1916. (RW 4461)

He, B. & Chang, K.C. "A Holistic Paradigm for Large Scale Schema Matching," *SIGMOD Record,* Vol. 33, No. 4, 2004, pp. 20-25. (RW 1396)

He, B., Patel, M., Zhang, Z. & Chang, K.C. "Accessing the Deep Web," *Communications of the ACM*, Vol. 50, No. 5, 2007, pp. 95. (RW 2753)

Healy, A.F. *Experimental Cognitive Psychology and its Applications,* American Psychological Association, Washington, DC, 2005. (RW 2313)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Heard, J., Prokop, J., Grossman, D. & Frieder, O. "Scalability Assessment of Complex Boolean Queries," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 867)

Hearst, M.A. "Clustering Versus Faceted Categories for Information Exploration," *Communications of the ACM*, Vol. 49, No. 4, 2006, pp. 59. (RW 1518)

Heath, T. "Why PLA Watchers Keep Missing Changes to China's Military Strategy," *American Intelligence Journal*, Vol. 27, No. 1, 2009, pp. 67. (RW 3991)

Heazle, M. "Policy Lessons from Iraq on Managing Uncertainty in Intelligence Assessment: Why the Strategic/Tactical Distinction Matters," *Intelligence and National Security*, Vol. 25, No. 3, 2010, pp. 290. (RW 4199)

Hecht, F. *The Aha! Factor*, 1979. (RW 1282)

Hecker, U., Dutke, S. & Sedek, G. *Generative Mental Processes and Cognitive Resources: Integrative Research on Adaptation and Control*, Kluwer Academic, Dordrecht; Boston, 2000. (RW 3275)

Hedges, L.V. & Wassington, T. "From Evidence to Knowledge to Policy: Research Synthesis for Policy Formation," *Review of Educational Research*, Vol. 63, No. 3, 1993, pp. 345. (RW 2196)

Hedley, J.H. "The Intelligence Community: Is it Broken? How to Fix it?" *Studies in Intelligence*, Vol. 39, No. 5, 1996, pp. 9. (RW 2931)

Hedley, J.H. "The Evolution of Intelligence Analysis," in *Analyzing Intelligence: Origins, Obstacles, and Innovations*, eds. R.Z. George & J.B. Bruce, 2008, pp. 19. (RW 3093)

Hedley, J.H. "The CIA's New Openness," *International Journal of Intelligence and Counterintelligence*, Vol. 7, No. 2, 1994, pp. 129-141. (RW 193)

Hedley, J.H. *Checklist for the Future of Intelligence*, Institute for the Study of Diplomacy, Edmund A. Walsh School of Foreign Service, Georgetown University, Washington, DC, 1995. (RW 147)

Hedley, J.H. "Learning from Intelligence Failures," *International Journal of Intelligence and Counterintelligence*, Vol. 18, No. 3, 2005, pp. 435-450. (RW 922)

Hedley, J.H. "Analysis for Strategic Intelligence," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 211. (RW 2469)

Hedley, J.H. "The Challenges of Intelligence Analysis," in *Strategic Intelligence. Volume 1: Understanding the Hidden Side of Government*, ed. L.K. Johnson, Praeger Security International, Westport, CT, 2007, pp. 123. (RW 2712)

Heidenrich, J.G. "The Intelligence Community's Neglect of Strategic Intelligence," *Studies in Intelligence*, Vol. 51, No. 2, 2007, pp. 15. (RW 2498)

Heijden, K.v.d. "Probabilistic Planning and Scenario Planning," in *Subjective Probability*, eds. G. Wright & P. Ayton, Wiley, Chichester; New York, 1994, pp. 549. (RW 3363)

Heine, M.H. "Reassessing and Extending the Precision and Recall Concepts," *MIRA '99*, Glasgow, Scotland, April 14-16, 1999. (RW 1561)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Heit, E. "Knowledge, Concepts, and Categories," in *Knowledge, Concepts and Categories*, eds. K. Lamberts & D.R. Shanks, 1st MIT Press ed., MIT Press, Cambridge, MA, 1997, pp. 7. (RW 2144)

Heldon, C.E. "Exploratory Intelligence Tools," in *Strategic Thinking in Criminal Intelligence*, ed. J. Ratcliffe, 2nd ed., Federation Press, Sydney, 2009, pp. 124-146. (RW 5703)

Heller, K.J. "The Cognitive Psychology of Circumstantial Evidence," *Michigan Law Review*, Vol. 105, 2006, pp. 241. (RW 2040)

Hellner, M. "Evidence and Inference in Foreign Intelligence," in *Information System Science and Technology;Papers Prepared for the Third Congress*, eds. D.E. Walker, United States & Mitre Corporation, Thompson Book Co, Washington, 1967, pp. 295. (RW 1361)

Helms, R. "Intelligence in American Society," *Studies in Intelligence*, Vol. 11, No. 3, 1967, pp. 1-16. (RW 537)

Henderson, A. "Promoting Professional Learning: Individual and Institutional Practices and Imperatives," in *Developing Learning Professionals*, eds. S. Billett & A. Henderson, Springer, Dordrecht, 2011, pp. 201-214. (RW 4907)

Henderson, S.M., Pascual, R.G. & Outteridge, C. *Critiquing in IO, EBA, and Intelligence Analysis*, QinetiQ, Farnborough, UK, 2008. (RW 5647)

Hendler, J. & Mannes, A. "Enlist IT Tools -- Not More People -- to Improve Intel," *Federal Times*, Vol. 46, No. 15, 2010, pp. 23. (RW 4492)

Hendrickson, N. "Critical Thinking in Intelligence Analysis," *International Journal of Intelligence and Counterintelligence*, Vol. 21, No. 4, 2008, pp. 679-693. (RW 3251)

Heng, Y. "Old Wine in New Bottles? Reconfiguring Net Assessment for 21st Century Security Analysis," *Contemporary Security Policy*, Vol. 28, No. 3, 2007, pp. 423. (RW 2909)

Henninger, M. *The Hidden Web: Finding Quality Information on the Net*, 2nd ed., UNSW Press, Sydney, N.S.W., 2008. (RW 3115)

Henriksson, A. "Hindsight into the Future," *Wilson Quarterly*, Vol. 24, No. 1, 2000, pp. 26-30. (RW 103)

Henstroem, J. "Five personality dimensions and their influence on information behaviour", *Information Research*, [Online], vol. 9, no. 1, pp. October 5, 2010. Available from: http://informationr.net/ir/9-1/paper165.html. 2003. (RW 4373)

Herbert, M. "The Intelligence Analyst as Epistemologist," *International Journal of Intelligence and Counterintelligence*, Vol. 19, No. 4, 2006, pp. 666-684. (RW 1637)

Herek, G.M., Janis, I.L. & Huth, P. "Decision Making during International Crises: Is Quality of Process Related to Outcome," *Journal of Conflict Resolution*, Vol. 31, No. 2, 1987, pp. 203-226. (RW 4691)

Herman, L. & Vervaeck, B. *Handbook of Narrative Analysis*, University of Nebraska Press, Lincoln, 2005. (RW 4180)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Herman, M. "Assessment Machinery: British and American Models," *Intelligence and National Security,* Vol. 10, No. 4, 1995, pp. 13-33. (RW 132)

Herman, M. *Intelligence Power in Peace and War,* Cambridge University Press, Cambridge, UK, 1996. (RW 16)

Herman, M. "Ethics and Intelligence After September 2001," *Intelligence and National Security,* Vol. 19, No. 2, 2000, pp. 342-358. (RW 436)

Herman, M. *Intelligence Services in the Information Age: Theory and Practice,* Frank Cass, London; Portland, OR, 2001. (RW 3400)

Herman, M. "11 September: Legitimizing Intelligence," *International Relations,* Vol. 16, No. 2, 2002, pp. 227-241. (RW 5387)

Herman, M. "Intelligence as Threats and Reassurance," *Intelligence and National Security,* Vol. 26, No. 6, 2011, pp. 791-817. (RW 5389)

Herres, R. *A CINC's View of Defense Organization,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1986. (RW 1006)

Herres, R. *The Role of the Joint Chiefs After the 1986 Defense Reorganization Act,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1990. (RW 1007)

Herring, J. "What is Intelligence Analysis? Part I," *Competitive Intelligence Magazine,* Vol. 1, No. 2, 1998, pp. 13-16. (RW 1089)

Herrmann, R.K. & Choi, J.K. "From Prediction to Learning," *International Security,* Vol. 31, No. 4, 2007, pp. 132. (RW 2293)

Hersh, S.M. "Missed Messages," *The New Yorker,* 2002, pp. 40. (RW 1378)

Hertwig, R., Pachur, T. & Kurzenhaeuser, S. "Judgments of Risk Frequencies: Tests of Possible Cognitive Mechanisms," *Journal of Experimental Psychology: Learning, Memory, & Cognition,* Vol. 31, No. 4, 2005, pp. 621-642. (RW 1937)

Herzog, J.O. "Using Economic Intelligence to Achieve Regional Security Objectives," *International Journal of Intelligence and Counterintelligence,* Vol. 21, No. 2, 2008, pp. 302. (RW 2971)

Herzog, S.M. & Hertwig, R. "The Wisdom of Many in One Mind: Improving Individual Judgments with Dialectical Bootstrapping," *Psychological Science,* Vol. 20, No. 2, 2009, pp. 231. (RW 3496)

Hess, J.H. *Improving Intelligence in a Counterinsurgency Or Counterterrorism Environment through the Application of a Critical Thinking-Based Framework,* Ph.D. dissertation, Louisiana State University, 2011. (RW 5600)

Hess, J. & Friedel, C. "Applying Critical Thinking to Intelligence Analysis," *American Intelligence Journal,* Vol. 26, No. 1, 2008, pp. 31-44. (RW 3624)

Hessenbruch, A. ""The Mutt Historian": The Perils and Opportunities of Doing History of Science on-Line," in *The Historiography of Science, Technology, and Medicine: Writing Recent*

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Science, eds. R.E. Doel & T. Söderqvist, Routledge, London; New York, 2006, pp. 279. (RW 3199)

Hetzler, E. "Analytic Tools: The Psychology of Human-Computer Interaction," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 373. (RW 3657)

Heuer, R. "Strategies for Analytical Judgment," *Studies in Intelligence*, Vol. 25, No. 2, 1981, pp. 65-78. (RW 1379)

Heuer, R.J. *ACH Tutorial*, 2007. (RW 2939)

Heuer, R.J. *Small Group Processes for Intelligence Analysis*, 2007. (RW 3175)

Heuer, R.J. "Computer-Aided Analysis of Competing Hypotheses," in *Analyzing Intelligence: Origins, Obstacles, and Innovations*, eds. R.Z. George & J.B. Bruce, 2008, pp. 251. (RW 3108)

Heuer, R.J. "Taxonomy of Structured Analytic Techniques", *International Studies Association 2008 Annual Convention*, San Francisco, CA, March 26 - 29, 2008. (RW 3243)

Heuer, R.J. *The Evolution of Structured Analytic Techniques. Speech Presented to the National Academy of Science, Washington, DC*, 2009. (RW 3835)

Heuer, R.J.J. "Adapting Academic Methods and Models to Governmental Needs," in *Quantitative Approaches to Political Intelligence: The CIA Experience*, ed. R.J.J. Heuer, Westview Press, Boulder, CO, 1978, pp. 1-10. (RW 909)

Heuer, R.J.J. "Cognitive Biases: Problems in Hindsight Analysis," *Studies in Intelligence*, Vol. 22, No. 2, 1978, pp. 21-28. (RW 124)

Heuer, R.J.J. "Content Analysis: Measuring Support for Brezhnev," in *Quantitative Approaches to Political Intelligence: The CIA Experience*, ed. R.J.J. Heuer, Westview Press, Boulder, CO, 1978, pp. 105-126. (RW 910)

Heuer, R.J.J. *Quantitative Approaches to Political Intelligence: The CIA Experience*, Westview Press, Boulder, CO, 1978. (RW 704)

Heuer, R.J.J. "Do You really Need More Information?" *Studies in Intelligence*, Vol. 23, No. 1, 1979, pp. 15-25. (RW 91)

Heuer, R.J.J. "Improving Intelligence Analysis: Some Insight on Data, Concepts, and Management in the Intelligence Community," *Bureaucrat*, Vol. 8, No. 4, 1979-80, pp. 2-11. (RW 88)

Heuer, R.J.J. "Biases in Evaluation of Evidence," *Studies in Intelligence*, Winter, 1981, pp. 31-45. (RW 90)

Heuer, R.J.J. "Cognitive Factors in Deception and Counterdeception," in *Strategic Military Deception*, eds. D.C. Daniel & K.L. Herbig, Pergamon Press, New York, NY, 1981, pp. 31-69. (RW 92)

Heuer, R.J.J. "Strategic Deception and Counterdeception: A Cognitive Process Approach," *International Studies Quarterly*, Vol. 25, No. 2, 1981, pp. 294-327. (RW 142)

Heuer, R.J.J. *Breaking Mind Sets*, 1991. (RW 13)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Heuer, R.J.J. *Analysis of Competing Hypotheses*, 1993. (RW 86)

Heuer, R.J.J. *Psychology of Intelligence Analysis,* Center for the Study of Intelligence, Washington, DC, 1999. (RW 453)

Heuer, R.J.J. "Limits of Intelligence Analysis," *Orbis,* Vol. 49, No. 1, 2005, pp. 75-94. (RW 221)

Heuer, R.J., Good, L., Shrager, J., Stefik, M., Pirolli, P. & Card, S. *ACH 1.1: A Tool for Analyzing Competing Hypotheses. Technical Description for Version 1.1* 2005. (RW 2938)

Heuer, R.J. & Pherson, R.H. *Structured Analytic Techniques for Intelligence Analysis,* CQ Press, Washington, DC, 2011. (RW 3837)

Hewish, M. "A Lenticular Display shows Images in Alternating Perspectives that Allow the Human Brain to Fuse them into a Three-Dimensional Picture. Panning for Gold." *Jane's International Defense Review,* 2001, pp. 24-29. (RW 1063)

Hey, J. *Effective Framing in Design,* 2005. (RW 2624)

Hicks, D.C. "The art and science of intelligence analysis," *Policing and Society,* [Online]. Available from: http://dx.doi.org/10.1080/10439463.2012.671827. 2012, (RW 5534)

Hidi, S. "Interest, Reading, and Learning: Theoretical and Practical Considerations," *Educational Psychology Review,* Vol. 13, No. 3, 2001, pp. 191-209. (RW 4605)

Hidi, S. & Harackiewicz, J.M. "Motivating the Academically Unmotivated: A Critical Issue for the 21st Century," *Review of Research in Education,* Vol. 70, No. 2, 2000, pp. 151-180. (RW 4626)

Hiemstra, R. & Brier, E.M. *Professional Writing: Processes, Strategies, and Tips for Publishing in Educational Journals*, Krieger Pub. Co, Malabar, Fla, 1994. (RW 1873)

Hien, N., Santos, E., Zhao, Q. & Wang, H. "Capturing User Intent for Information Retrieval", *HFES 2004: Proceedings of the Human Factors and Ergonomics Society. 48th Annual Meeting.* September 20-24, 2004, pp.371. (RW 2872)

Higgins, J.P.T. & Green, S. (eds) *Cochrane Handbook for Systematic Reviews of Interventions. 4.2.6 [Updated September 2006]*, John Wiley & Sons, Ltd., Chichester, UK, 2006. (RW 2273)

Highsmith, N. *A Critique of the War Powers Resolution of 1973 in Light of the Intelligence Accountability Act of 1980*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1982. (RW 1008)

Hilborn, R. & Mangel, M. *The Ecological Detective: Confronting Models with Data*, 1997. (RW 1954)

Hiler, W. & Paul, R. *The Miniature Guide to Practical Ways for Promoting Active and Cooperative Learning,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3748)

Hill, L. "What does it Take to Change Minds? Intellectual Development of Preservice Teachers," *Journal of Teacher Education,* Vol. 51, No. 1, 2000, pp. 50-62. (RW 5298)

Hill, S.D. *The Next Threat: A Predictive Analysis of the Continuity of Terrorist Organizations,* Ph.D. dissertation, Sam Houston State University, 2002. (RW 4534)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hill, Z. "Trend Analysis," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 145-157. (RW 3620)

Hillebrand, C. "The Role of News Media in Intelligence Oversight," *Intelligence and National Security,* Vol. 27, No. 5, 2012, pp. 689-706. (RW 5839)

Hillen, J. "Know Nothings: US Intelligence Failures Stem from Too Much Information, Not enough Understanding," *National Review,* Vol. 50, 1998, pp. 28. (RW 1371)

Hillenkoetter, R.H. "Using the World's Information Sources," *Army Information Digest,* Vol. III, No. 11, 1948, pp. 3-6. (RW 2952)

Hilsman, R. "Intelligence and Policy-Making in Foreign Affairs," *World Politics,* Vol. 5, No. 1, 1952, pp. 1-45. (RW 2778)

Hilsman, R. *Strategic Intelligence and National Decisions,* Greenwood Press, Westport, CT, 1981. (RW 1104)

Hilton, R. *Roles of the Joint Chiefs of Staff in Crisis Management,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1986. (RW 1009)

Hindley, M. "Teaching Intelligence Project," *Intelligence and National Security,* Vol. 15, No. 1, 2000, pp. 191-218. (RW 459)

Hinsz, V.B., Tindale, R.S. & Vollrath, D.A. "The Emerging Conceptualization of Groups as Information Processors," *Psychological Bulletin,* Vol. 12, No. 1, 1997, pp. 43-64. (RW 5477)

Hintikka, J. *Socratic Epistemology: Explorations of Knowledge-Seeking by Questioning,* Cambridge University Press, Cambridge, UK, 2007. (RW 5815)

Hippler, R. "Scenario Planning," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 54-62. (RW 3610)

Hippner, C. *A Study into the Size of the World's Intelligence Industry,* M. S. in Applied Intelligence thesis, Mercyhurst College, 2009. (RW 3826)

Hirschfeld, T.J. *Intelligence and Arms Control: A Marriage of Convenience,* Lyndon B. Johnson School of Public Affairs, Austin, TX, 1987. (RW 163)

Hirschfeld, T.J. "Exaggerating Threats Shortchanges the Future," *Proceedings of the United States Naval Institute,* Vol. 128, No. 9, 2002, pp. 66-69. (RW 583)

Hisschemoller, M. & Hoppe, R. "Coping with Intractable Controversies: The Case for Problem Structuring in Policy Design," *Knowledge & Policy,* Vol. 8, No. 4, 1995, pp. 40. (RW 2574)

Hitti, M. *Why we Buy: Weighing Pleasure Vs. Pain,* Available: http://www.webmd.com/content/Article/131/117986.htm, (RW 1980)

Hitz, F.P. "The Future of American Espionage," *International Journal of Intelligence and Counterintelligence,* Vol. 13, No. 1, 2000, pp. 1-20. (RW 58)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hitz, F.P. "Unleashing the Rogue Elephant: September 11 and Letting the CIA be the CIA," *Harvard Journal of Law and Public Policy,* Vol. 25, No. 2, 2002, pp. 765-780. (RW 412)

Hitz, F.P. "Human Source Intelligence," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 118. (RW 2462)

Hitz, F.P. *Why Spy?: Espionage in an Age of Uncertainty,* Thomas Dunne Books/St. Martin's Press, New York, 2008. (RW 3390)

Hobus, P.P.M., Schmidt, H.G., Boshuizen, H.P.A. & Patel, V.L. "Contextual Factors in the Activation of First Diagnostic Hypotheses: Expert-Novice Differences," *Medical Education,* Vol. 21, No. 6, 1987, pp. 471. (RW 2765)

Hock, R. *The Extreme Searcher's Internet Handbook: A Guide for the Serious Searcher,* 3rd ed., CyberAge Books, Medford, NJ, 2009. (RW 4504)

Hodder, I. "The Interpretation of Documents and Material Culture," in *Handbook of Qualitative Research*, eds. N.K. Denzin & Y.S. Lincoln, 2nd ed., Sage Publications, Thousand Oaks, CA, 2000, pp. 703. (RW 2672)

Hoddeson, L. "In the Wake of Thomas Kuhn's Theory of Scientific Revolutions: The Perspective of an Historian of Science," in *Re-Framing the Conceptual Change Approach in Learning and Instruction*, eds. S. Vosniadou, A. Baltas & X. Vamvakoussi, Elsevier, Amsterdam, 2007, pp. 25-33. (RW 5592)

Hodges, E.L.V. *Evaluation of the Quality of Current Missile Threat Analysis,* Ph.D. dissertation, University of Phoenix, 2009. (RW 4528)

Hodgins, H.S. & Zuckerman, M. "Beyond Selecting Information: Biases in Spontaneous Questions and Resultant Conclusions," *Journal of Experimental Social Psychology,* Vol. 29, 1993, pp. 387. (RW 2111)

Hodgkinson, G.P. "The Cognitive Analysis of Competitive Structures: A Review and Critique," *Human Relations,* Vol. 50, 1997, pp. 625. (RW 2523)

Hodgkinson, G.P., Bown, N.J., Maule, A.J., Glaister, K.W. & Pearman, A.D. "Breaking the Frame: An Analysis of Strategic Cognition and Decision Making Under Uncertainty," *Strategic Management Journal,* Vol. 20, 1999, pp. 977. (RW 2516)

Hoechst, T.G. *131: Information, Information, Information, and Information,* 2001. (RW 1170)

Hoekstra, P. *Secrets and Leaks: The Costs and Consequences for National Security*, Heritage Lectures No. 897, Heritage Foundation, Washington, DC, 2005. (RW 788)

Hoenkamp, E. "The Influence of Recall Feedback in Information Retrieval on User Satisfaction and User Behavior", *Proceedings of the 23rd Annual Conference of the Cognitive Science Society,* pp. 423. (RW 1999)

Hoenkamp, E. "Why Information Retrieval Needs Cognitive Science: A Call to Arms", *Proceedings of the 27th Annual Conference of the Cognitive Science Society*, 2005, pp. 965-970. (RW 1969)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hofer, B. "Epistemological Beliefs and First-Year College Students: Motivation and Cognition in Different Instructional Contexts", *Annual Meeting of the American Psychological Association,* Los Angeles, CA, August 1994. (RW 4427)

Hofer, B. "Instructional Context in the College Mathematics Classroom: Epistemological Beliefs and Student Motivation," *Journal of Staff, Program, & Organizational Development,* Vol. 16, No. 2, 1999, pp. 73-82. (RW 4840)

Hofer, B. "Dimensionality and Disciplinary Differences in Personal Epistemology," *Contemporary Educational Psychology,* Vol. 25, No. 4, 2000, pp. 378-405. (RW 4634)

Hofer, B. "Personal Epistemology Research: Implications for Learning and Instruction," *Educational Psychology Review,* Vol. 13, No. 4, 2001, pp. 353-382. (RW 4630)

Hofer, B. "Epistemological World Views of Teachers: From Beliefs to Practice," *Issues in Education,* Vol. 8, No. 2, 2002, pp. 167-173. (RW 4632)

Hofer, B. "Exploring the Dimensions of Personal Epistemology in Differing Classroom Contexts: Student Interpretations during the First Year of College," *Contemporary Educational Psychology,* Vol. 29, No. 2, 2004, pp. 129-163. (RW 4635)

Hofer, B. "Paradigmatic Approaches to Personal Epistemology: Introduction to the Special Issue," *Educational Psychologist,* Vol. 39, No. 1, 2004, pp. 1-3. (RW 4628)

Hofer, B. "The Legacy and the Challenges: Paul Pintrich's Contributions to Personal Epistemology Research," *Educational Psychologist,* Vol. 40, No. 2, 2005, pp. 95-105. (RW 4629)

Hofer, B. "Beliefs about Knowledge and Knowing: Domain Specificity and Generality," *Educational Psychology Review,* Vol. 18, No. 1, 2006, pp. 67-76. (RW 4631)

Hofer, B. "Domain Specificity of Personal Epistemology: Resolved Questions, Persistent Issues, New Models," *International Journal of Educational Research,* Vol. 45, No. 1-2, 2006, pp. 85-95. (RW 4636)

Hofer, B.K. "Epistemological Understanding as a Metacognitive Process: Thinking Aloud during Online Searching," *Educational Psychologist,* Vol. 39, No. 1, 2004, pp. 43-55. (RW 3775)

Hofer, B.K. "Epistemological Development," in *Psychology of Classroom Learning: An Encyclopedia,* eds. E.M. Anderman & L.H. Anderman, Macmillan Reference USA/Gale Cengage Learning, Detroit, MI, 2008, pp. 376-380. (RW 4672)

Hofer, B.K. "Personal Epistemology in Asia: Burgeoning Research and Future Directions," *Asia Pacific Education Researcher,* Vol. 19, No. 1, 2010, pp. 179-184. (RW 4633)

Hofer, B.K. "Personal Epistemology, Learning, and Cultural Context: Japan and the U.S." in *Development and Assessment of Self-Authorship: Exploring the Concept Across Cultures,* eds. M.B. Baxter Magolda, E.G. Creamer & P.S. Meszaros, Stylus Pub., Sterling, VA, 2010, pp. 133-150. (RW 5101)

Hofer, B.K. & Bendixen, L.D. "Personal Epistemology: Theory, Research, and Future Directions," in *APA Educational Psychology Handbook,* eds. K.R. Harris, S. Graham & T. Urdan, American Psychological Association, Washington, DC, 2011. (RW 5107)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hofer, B.K. & Pintrich, P.R. "The Development of Epistemological Theories: Beliefs about Knowledge and Knowing and their Relation to Learning," *Review of Educational Research,* Vol. 67, No. 1, 1997, pp. 88-140. (RW 4282)

Hofer, B.K. & Sinatra, G.M. "Epistemology, Metacognition, and Self-Regulation: Musings on an Emerging Field," *Metacognition and Learning,* Vol. 5, No. 1, 2010, pp. 113-120. (RW 4638)

Hofer, B.K. *The Development of Personal Epistemology: Dimensions, Disiplinary Differences and Instructional Practices,* Ph.D. dissertation, University of Michgan, 1997. (RW 5038)

Hofer, B.K. "Personal Epistemology Research: Implications for Learning and Teaching," *Educational Psychology Review,* Vol. 13, No. 4, 2001, pp. 353-383. (RW 4277)

Hofer, B.K. "Personal Epistemology as a Psychological and Educational Construct: An Introduction," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing*, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 1-14. (RW 4331)

Hofer, B.K. "Introduction: Paradigmatic Approaches to Personal Epistemology," *Educational Psychologist,* Vol. 39, No. 1, 2004, pp. 1-3. (RW 4339)

Hofer, B.K. "Personal Epistemology and Culture," in *Knowing, Knowledge and Beliefs: Epistemological Studies Across Diverse Cultures,* ed. M.S. Khine, Springer, Dordrecht, 2008, pp. 3-22. (RW 4292)

Hofer, B.K., Lam, C.F. & Delisi, A. "Understanding Evolutionary Theory: The Role of Epistemological Development and Beliefs," in *Epistemology and Science Education: Understanding the Evolution Vs. Intelligent Design Controversy,* eds. R.S. Taylor & M. Ferrari, Routledge, New York, NY, 2011, pp. 95-110. (RW 4671)

Hoffman, R. *The Bias Bias [Powerpoint Presentation]* 2004. (RW 1173)

Hoffman, R.R. *The Theory of the Handicapped Mind: Revisiting the Psychology of Intelligence Analysts* [undated]. (RW 3713)

Hoffman, R.R. *The Psychology of Intelligence Analysis Revisited: An Update from Developments in Cognitive Science Post-1980,* 2005. (RW 3364)

Hoffman, R.R., Schraagen, J.M., van de Ven, J. & Moon, B.M. "Influencing the Business Model and Innovations of a Research Organization through Concept Mapping," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge*, eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 169-192. (RW 4971)

Hoffman, R.R. & Woods, D.D. "Toward a Theory of Complex and Cognitive Systems," *IEEE Intelligent Systems,* Vol. 20, No. 1, 2005, pp. 76. (RW 1766)

Hoffman, R., Henderson, S., Moon, B., Moore, D.T. & Litman, J.A. "Reasoning Difficulty in Analytical Activity," *Theoretical Issues in Ergonomics Science,* Vol. 12, No. 3, 2011, pp. 225-240. (RW 5535)

Hoffmann, J. *Utilizing Problem Structure in Planning: A Local Search Approach,* Springer-Verlag, Berlin; New York, 2003. (RW 2664)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hofstadter, D.R. "Epilogue: Analogy as the Core of Cognition," in *The Analogical Mind: Perspectives from Cognitive Science*, eds. D. Gentner, K.J. Holyoak & B.N. Kokinov, 2001, pp. 499. (RW 1879)

Hofstadter, D.R. & Dennett, D.C. *The Mind's I: Fantasies and Reflections on Self and Soul,* Basic Books, New York, 2000. (RW 3261)

Hogan, K. "Relating Students' Personal Frameworks for Science Learning to their Cognition in Collaborative Contexts," *Science Education,* Vol. 83, No. 1, 1999, pp. 1-32. (RW 4644)

Hogan, K. "Exploring a Process View of Students' Knowledge about the Nature of Science," *Science Education,* Vol. 84, No. 1, 2000, pp. 51-70. (RW 4664)

Hogan, K. & Maglienti, M. "Comparing the Epistemological Underpinnings of Students' and Scientists' Reasoning about Conclusions," *Journal of Research in Science Teaching,* Vol. 38, No. 6, 2001, pp. 663-87. (RW 5434)

Hogarth, R.M. *Educating Intuition,* University of Chicago Press, Chicago, 2001. (RW 3556)

Hogarth, R.M. & Einhorn, H.J. "Order Effects in Belief Updating: The Belief-Adjustment Model," *Cognitive Psychology,* Vol. 24, No. 1, 1992, pp. 1-55. (RW 5290)

Hoge, J.F. & Rose, G. *How did this Happen? Terrorism and the New War,* PublicAffairs, New York, NY, 2001. (RW 706)

Holland, M. "One Year After a Major Realignment, the Intelligence Community is in Disarray," *The Washington Spectator,* Vol. 32, No. 8, 2006. (RW 1317)

Holland, M. "The Politics of Intelligence Postmortems: Cuba 1962-1963," *International Journal of Intelligence and Counterintelligence,* Vol. 20, No. 3, 2007, pp. 415. (RW 2383)

Holland, M.M. "The Politics of Intelligence Post-Mortems," in *Strategic Intelligence. Volume 2: The Intelligence Cycle: The Flow of Secret Information from Overseas to the Highest Councils of Government*, ed. L.K. Johnson, Praeger Security International, Westport, CT, 2007, pp. 199. (RW 2708)

Holland, R. "Reflexivity," *Human Relations,* Vol. 52, No. 4, 1999, pp. 463-484. (RW 5687)

Holloway, I. *Basic Concepts for Qualitative Research,* Blackwell Science, Oxford; Malden, MA, 1997. (RW 2116)

Hollywood, J., Snyder, D., McKay, K. & Boon, J. *Out of the Ordinary: Finding Hidden Threats by Analyzing Unusual Behavior,* RAND Corporation, Santa Monica, CA, 2004. (RW 471)

Holmes, N. "The Dea[r]Th of Human Understanding," *Computer,* October, 2008, pp. 108. (RW 3292)

Holton, G.J. *Thematic Origins of Scientific Thought: Kepler to Einstein,* Harvard University Press, Cambridge, MA, 1988. (RW 3557)

Holyoak, K.J. "The Pragmatics of Analogical Transfer," *The Psychology of Learning and Motivation,* Vol. 19, 1985, pp. 59. (RW 2150)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Holyoak, K.J. "Analogy," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 117-142. (RW 4001)

Holyoak, K.J., Gentner, D. & Kokinov, B.N. "Introduction: The Place of Analogy in Cognition," in *The Analogical Mind: Perspectives from Cognitive Science*, eds. D. Gentner, K.J. Holyoak & B.N. Kokinov, 2001, pp. 1. (RW 1878)

Holyoak, K.J. & Morrison, R.G. "Thinking and Reasoning: A Reader's Guide," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 1-9. (RW 3999)

Holyoak, K.J. & Morrison, R.G. "Thinking and Reasoning: A Reader's Guide," in *Oxford Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 1-7. (RW 5495)

Holyoak, K.J. & Spellman, B.A. "Thinking," *Annual Review of Psychology*, Vol. 44, 1993, pp. 265-315. (RW 1906)

Holyoak, K.J. & Thagard, P. *Mental Leaps: Analogy in Creative Thought*, MIT Press, Cambridge, MA, 1995. (RW 1626)

Holyoak, K.J. & Thagard, P. "The Analogical Mind," *American Psychologist*, Vol. 52, No. 1, 1997, pp. 35. (RW 1800)

Homans, C. "How does the CIA Know if its Intelligence is any Good?" *Foreign Policy*, 2010 (RW 4218)

Hong, H.-. & Lin, S.-. "Teacher Education Students' Epistemological Belief Change through Collaborative Knowledge Building," *Asia Pacific Education Researcher*, Vol. 19, 2010, pp. 99-110. (RW 5054)

Honig, O.A. "A New Direction for Theory-Building in Intelligence Studies," *International Journal of Intelligence and Counterintelligence*, Vol. 20, No. 4, 2007, pp. 699. (RW 2760)

Honig, O.A. "The Impact of CIA's Organizational Culture on its Estimates Under William Casey," *International Journal of Intelligence and Counterintelligence*, Vol. 24, No. 1, 2011, pp. 44-64. (RW 4578)

Hood, B.M. *Supersense: Why we Believe in the Unbelievable*, HarperOne, New York, NY, 2009. (RW 5851)

Hood, W. "Stop Blaming Angleton," *International Journal of Intelligence and Counterintelligence*, Vol. 17, No. 4, 2004, pp. 757-759. (RW 392)

Hood, W., with comments by Nolan, James & Halpern, S. "Angleton's World: Lessons for U.S. Counterintelligence," in *U.S. Intelligence at the Crossroads: Agendas for Reform*, eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 128-145. (RW 645)

Hook, E.B. *Prematurity in Scientific Discovery: On Resistance and Neglect*, University of California Press, Berkeley, 2002. (RW 1855)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hoover, S.M. & Feldhusen, J.F. "Scientific Problem Solving and Problem Finding: A Theoretical Model," in *Problem Finding, Problem Solving, and Creativity*, ed. M.A. Runco, Ablex Pub. Corp., Norwood, NJ, 1994, pp. 201. (RW 2744)

Hopf, T. "The Promise of Constructivism in International Relations Theory," *International Security*, Vol. 23, No. 1, 1998, pp. 171. (RW 1655)

Hopf, T. *Social Construction of International Politics: Identities & Foreign Policies, Moscow, 1955 and 1999*, Cornell University Press, Ithaca, 2002. (RW 1652)

Hopkinson, H. "An Idiot System for Intelligence," *Studies in Intelligence*, Vol. 6, No. 4, 1962, pp. 17-23. (RW 522)

Horgan, J. *The Undiscovered Mind: How the Human Brain Defies Replication, Medication, and Explanation*, Free Press, New York, 1999. (RW 3312)

Horn, E. "Knowing the Enemy: The Epistemology of Secret Intelligence," *Grey Room*, 11, 2003, pp. 58-85. (RW 350)

Horn, J.L. & Cattell, R.B. "Age Differences in Fluid and Crystallized Intelligence," *Acta Psychologica*, Vol. 26, 1967, pp. 107-129. (RW 4613)

Horn, R.E. "Connecting the Smudges: How Analytic Info-Murals may be of Help in Dealing with Social Messes," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 832)

Horowitz, M.C. & Tetlock, P.E. "Trending upward: how the intelligence community can better see into the future," *Foreign Policy*, [Online], September 10, 2012. Available from: http://www.foreignpolicy.com/articles/2012/09/06/trending_upward. 2012, (RW 5807)

Horowitz, R. "A Framework for Understanding Intelligence," *International Journal of Intelligence and Counterintelligence*, Vol. 8, No. 4, 1996, pp. 389-409. (RW 47)

Horrman, R.R. "The Problem of Extracting the Knowledge of Experts from the Perspective of Experimental Psychology," *AI Magazine*, Vol. 8, No. 2, 1987, pp. 53. (RW 1466)

Horvitz, E.J. *Question and Answer Architecture for Reasoning and Clarifying Intentions, Goals, and Needs from Contextual Clues and Content*, 2007. (RW 3910)

Hossain, M.S., Andrews, C., Ramakrishnan, N. & North, C. "Helping Intelligence Analysts make Connections", *Proceedings of the AAAI '11 Workshop on Scalable Integration and Visualization*, San Francisco, CA, August 7, 2011, [unpaged]. (RW 5513)

Hossain, M.S., Butler, P., Boedihardjo, A.P. & Ramakrishnan, N. "Storytelling in Entity Networks to Support Intelligence Analysis", *Kdd'12*, Beijing, China, August 12-16, 2012 (RW 5677)

House Committee on National Security. *Intelligence Community Act. House Report 104-620.* 1996. (RW 1053)

House Permanent Select Committee on Intelligence. *Intelligence Community Act. House Report 104-620.* 1996. (RW 1052)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

House Permanent Select Committee on Intelligence. House Select Committee on Energy Independence and Global Warming. *National Intelligence Assessment on the National Security Implications of Global Climate Change to 2030. Statement for the Record of Dr. Thomas Fingar.* 2008. (RW 3164)

Howard, R.A. "Decision Analysis and Law," *Cardozo Law Review,* Vol. 22, 2001, pp. 1595. (RW 2044)

Howcroft, J. "Technology, Intelligence, and Trust," *Joint Force Quarterly,* 46, 2007, pp. 20-26. (RW 5622)

Howells, W.D. "Intelligence in Crises," in *Defense '83,* ed. G.R. Copley, 1983, pp. 349. (RW 1249)

Howley, D.C. "The Crucial Role of the Manager-Leader in Intelligence," *American Intelligence Journal,* Summer/Fall, 1990, pp. 37-40. (RW 172)

Hoy, A.W., Davis, H. & Pape, S.J. "Teacher Knowledge and Beliefs," in *Handbook of Educational Psychology*, eds. P.A. Alexander & P.H. Winne, 2nd ed., L. Erlbaum Associates, Mahwah, NJ, 2006, pp. 715-737. (RW 5049)

Hoyt, S.V. "Cold War Pioneers in Combined Intelligence and Analysis," *Intelligence and National Security,* Vol. 23, No. 4, 2008, pp. 463. (RW 3218)

Hsiung, P., Moore, A., Neill, D. & Schneider, J. "Alias Detection in Link Data Sets," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 812)

Hubbard, R.L. "Another Response to Terrorism: Reconstituting Intelligence Analysis for 21st Century Requirements," *Defense Intelligence Journal,* Vol. 11, No. 1, 2002, pp. 71-80. (RW 4291)

Huberman, B.A. *The Laws of the Web: Patterns in the Ecology of Information,* MIT Press, Cambridge, MA, 2001. (RW 5409)

Hudson, W.E. "The Ethical Spy: Towards Intelligence Community Rules of Professional Conduct," *The Georgetown Law Journal,* Vol. 98, No. 5, 2010, pp. 1415-1439. (RW 5604)

Huff, A.S. "Strategic Intelligence Systems," *Information & Management,* Vol. 2, No. 5, 1979, pp. 187-196. (RW 5646)

Huff, A.S. *Mapping Strategic Thought,* Wiley, Chichester; New York, 1990. (RW 2522)

Hughes, F.J. *The Art and Science of the Process of Intelligence Analysis. Case Study #4 (the Sign of the Crescent). Student Handout.* 2003. (RW 1634)

Hughes, F.J. "Evidence Marshaling and Argument Construction," in *Learning with Professionals: Selected Works from the Joint Military Intelligence College,* eds. J.E. Lightfoot, J.S. Major, S.E. Brownfeld & Joint Military Intelligence College, 2005, pp. 125. (RW 1569)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis,* Joint Military Intelligence College, Washington, DC, 2003. (RW 970)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Instructor's Guide,* Joint Military Intelligence College, Washington, DC, 2003. (RW 1380)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #6 (Atlantic Storm). Analysis.* 2005. (RW 1748)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #6 (Atlantic Storm). Student Assignment.* 2005. (RW 1746)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #6 (Atlantic Storm). the Story.* 2005. (RW 1747)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #1 (the Case of General Alpha: Facing Insurgency?). Analysis.* 2006. (RW 1736)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #1 (the Case of General Alpha: Facing Insurgency?). Student Assignment.* 2006. (RW 1735)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #2 (the Case of Wigmore Vs. Al-Qaeda). Analysis.* 2006. (RW 1738)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #2 (the Case of Wigmore Vs. Al-Qaeda). Student Assignment.* 2006. (RW 1737)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #3 (A Case of Espionage). Analysis.* 2006. (RW 1740)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #3 (A Case of Espionage). Student Assignment.* 2006. (RW 1739)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #4 (the Sign of the Crescent). Additional Intelligence Reports.* 2006. (RW 1742)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #4 (the Sign of the Crescent). Analysis.* 2006. (RW 1743)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #4 (the Sign of the Crescent). Student Assignment.* 2006. (RW 1741)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #5 (the Black Swan: A Halo Or Forked Tail?). Analysis.* 2006. (RW 1745)

Hughes, F.J. & Schum, D.A. *The Art and Science of the Process of Intelligence Analysis. Case Study #5 (the Black Swan: A Halo Or Forked Tail?). Student Assignment.* 2006. (RW 1744)

Hughes, P.M. *Open Sources and Intelligent Solutions [Powerpoint Presentation]* (RW 1454)

Hughes, P.M. *Future Threats and Challenges,* Center for Information Policy Research. Harvard University, Cambridge, MA, 2000. (RW 1010)

Hughes, P.M. *Future Conditions: The Character and Conduct of War, 2010 and 2020,* 2003. (RW 1169)

Hughes, P.M. "Back to the Future with Basic Concepts," *American Intelligence Journal,* Vol. 27, No. 1, 2009, pp. 7. (RW 3985)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hughes, R.G. & Stoddart, K. "Hope and Fear: Intelligence and the Future of Global Security a Decade After 9/11," *Intelligence and National Security*, Vol. 27, No. 5, 2012, pp. 625-652. (RW 5838)

Hughes, T.L. *The Fate of Facts in a World of Men: Foreign Policy and Intelligence-Making*, Foreign Policy Association, New York, NY, 1976. (RW 1288)

Huhns, M.N. & Valtorta, M.G. "Ontological Support for Bayesian Evidence Management", *Proceedings of the Second International Ontology for the Intelligence Community Conference OIC-2007*, Columbia, MD, November 28-29, 2007, pp.4747-52. (RW 4821)

Huitt, W. "Critical thinking: An overview," *Educational Psychology Interactive*, [Online], March 22, 2010. Available from: http://www.edpsycinteractive.org/topics/cogsys/critthnk.html.1998, (RW 4076)

Hull, D., Pettifer, S.R. & Kell, D.B. "Defrosting the Digital Library: Bibliographic Tools for the Next Generation Web," *PLoS Computational Biology*, Vol. 4, No. 10, 2008 (RW 3361)

Hull, J.P. *Hue, the Mirror on the Pole View Around the Corner to Future Urban Combat*, MMS thesis, US Marine Corps Command and Staff College, [undated]. (RW 490)

Hulnick, A.S. *Intelligence Reform 2008: Where do we Go from here?* (RW 2984)

Hulnick, A.S. "Presidents and Intelligence," *White House Studies*, Vol. 4, No. 1, 2004, pp. 85. (RW 2045)

Hulnick, A.S. "Managing Intelligence Analysis: Strategies for Playing the End Game," *International Journal of Intelligence and Counterintelligence*, Vol. 2, No. 3, 1988, pp. 321-343. (RW 1283)

Hulnick, A.S. "The Ames Case: How could it Happen?" *International Journal of Intelligence and Counterintelligence*, Vol. 8, No. 2, 1995, pp. 133-154. (RW 51)

Hulnick, A.S. *Fixing the Spy Machine: Preparing American Intelligence for the Twenty-First Century*, Praeger, Westport, CT, 1999. (RW 934)

Hulnick, A.S. "The Downside to Open Source Intelligence," *International Journal of Intelligence and Counterintelligence*, Vol. 15, No. 4, 2002, pp. 565. (RW 1670)

Hulnick, A.S. "Risky Business: Private Sector Intelligence in the United States," *Harvard International Review*, Vol. 24, No. 3, 2002, pp. 68-72. (RW 381)

Hulnick, A.S. "Does the U.S. Intelligence Community Need a DNI?" *International Journal of Intelligence and Counterintelligence*, Vol. 17, No. 4, 2004, pp. 710-730. (RW 297)

Hulnick, A.S. *Keeping Us Safe: Secret Intelligence and Homeland Security*, Praeger, Westport, Conn, 2004. (RW 1688)

Hulnick, A.S. "U.S. Intelligence Reform: Problems and Prospects," *International Journal of Intelligence and Counterintelligence*, Vol. 19, No. 2, 2006, pp. 302. (RW 1751)

Hulnick, A.S. "What's Wrong with the Intelligence Cycle?" *Intelligence and National Security*, Vol. 21, No. 6, 2006, pp. 959. (RW 2081)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Hulnick, A.S. "Intelligence Reform 2007: Fix Or Fizzle?" *International Journal of Intelligence and Counterintelligence*, Vol. 20, No. 4, 2007, pp. 567. (RW 2757)

Hulnick, A.S. "What's Wrong with the Intelligence Cycle?" in *Strategic Intelligence. Volume 2: The Intelligence Cycle: The Flow of Secret Information from Overseas to the Highest Councils of Government*, ed. L.K. Johnson, Praeger Security International, Westport, CT, 2007, pp. 1. (RW 2704)

Hulnick, A.S. "Intelligence Reform 2008: Where to from here?" *International Journal of Intelligence and Counterintelligence*, Vol. 21, No. 4, 2008, pp. 621. (RW 3248)

Hulnick, A.S. "The Dilemma of Open Sources Intelligence: Is OSINT really Intelligence?" in *Oxford Handbook of National Security Intelligence*, ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 229-241. (RW 4706)

Hulnick, A.S. "Intelligence Producer-Consumer Relations in the Electronic Era," *International Journal of Intelligence and Counterintelligence*, Vol. 24, No. 4, 2011, pp. 747-756. (RW 5400)

Humphrey, N. *Seeing Red: A Study in Consciousness*, The Belknap Press of Harvard University Press, Cambridge, MA, 2006. (RW 1717)

Humphrey, P.B. "Seeking Foreign Policy's Oracle at Delphi," *International Journal of Intelligence and Counterintelligence*, Vol. 23, No. 2, 2010, pp. 324. (RW 3899)

Hunt, C.W. *Transforming Intra- and Interagency Processes through Advanced Models and Simulations: An Information Assurance Model*, National Defense University, Washington, DC, [undated]. (RW 969)

Hunt, C.W. *Transforming Intelligence: Improving Inference through Advanced Simulations Better Prediction through Better Inquiry*, National Defense University, Washington, DC, 2003. (RW 968)

Hunt, E. "To Err is Human, to Forgive Requires Systems Analysis. Book Review of Human Error: Cause, Prediction, and Reduction," *Contemporary Psychology*, Vol. 38, No. 11, 1993, pp. 1207-1208. (RW 895)

Hunt, E. "Where are we? Where are we Going? Reflections on the Current and Future State of Research on Intelligence," in *Cambridge Handbook of Intelligence*, eds. R.J. Sternberg & S.B. Kaufman, Cambridge University Press, New York, NY, 2012, pp. 863-885. (RW 5781)

Hunt, E.B. "Revolutions, Leaders, and Diagnosticians: Reflections on the Themes in Chapters 2-4," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 108-127. (RW 5138)

Hunt, J.G. *Leadership: A New Synthesis*, Sage Publications, Newbury Park, CA, 1991. (RW 3048)

Hunt, M.M. *The Universe within: A New Science Explores the Human Mind*, Simon and Schuster, New York, NY, 1982. (RW 4562)

Hurst, K., Dean, A. & Trickey, S. "The Recognition and Non-Recognition of Problem-Solving Stages in Nursing Practice," *Journal of Advanced Nursing*, Vol. 161991, pp. 1444. (RW 2640)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Husain, K. "Neocons: The Men Behind the Curtain," *Bulletin of the Atomic Scientists*, Vol. 59, No. 6, 2003, pp. 62-71. (RW 360)

Hutchings, R. *Strategic Choices, Intelligence Challenges. Speech.* 2003. (RW 1333)

Hutchings, R.L. *Looking Over the Horizon: Assessing America's Strategic Challenges. Testimony at the INR/World Affairs Council Seminar* 2004. (RW 634)

Hutchings, R.L. "Looking Over the Horizon: Strategic Choices, Intelligence Challenges", *New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities,* Rome, Italy, 31 March - 2 April, 2004, pp. 23-28. (RW 4665)

Hutchings, R.L. *The Morning After: How to Reform the Intelligence Reform,* 2007. (RW 2907)

Hutchins, E. *Distributed Cognition* (RW 2053)

Hutchins, E. *Cognition in the Wild,* MIT Press, Cambridge, MA, 1995. (RW 2576)

Hutchins, S.G., Pirolli, P.L. & Card, S.K. "What Makes Intelligence Analysis Different? A Cognitive Task Analysis. Draft Chapter from Book." (RW 1525)

Hutchins, S.G., Pirolli, P. & Card, S. "Use of Critical Analysis Method to Conduct a Cognitive Task Analysis of Intelligence Analysts", October 13-17, 2003, pp.478. (RW 1491)

Hyatt, M. "A Comprehensive Approach to Reasoning," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 797)

Hynd, C. "Conceptual Change in Response to Persuasive Messages," in *Intentional Conceptual Change*, eds. G.M. Sinatra & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2003, pp. 291-315. (RW 4996)

Ignatius, D. "The CIA's Dissidents," *Washington Post,* April 6, 2004, p. A21. (RW 4186)

Ignatius, D. "Can the Spy Agencies Dig Out," *Washington Post,* April 15, 2005, pp. A25. (RW 1671)

Ikle, F.C. "The Role of Character and Intellect in Strategy," in *On Not Confusing Ourselves: Essays on National Security Strategy in Honor of Albert and Roberta Wohlstetter*, eds. A.W. Marshall, J.J. Martin & H.S. Rowen, Westview Press, Boulder, CO, 1991, pp. 312-316. (RW 636)

Ikomi, P.A. *The Prediction of Judgment in Realistic Tasks: Do Judges have Self-Insight?* 1989. (RW 2192)

Ilachinski, A. *Land Warfare and Complexity, Part II: An Assessment of the Applicability of Nonlinear Dynamics and Complex Systems Theory to the Study of Land Warfare,* CRM 96-98, 1996. (RW 3006)

Immerman, R.H. "Intelligence and Strategy: Historicizing Psychology, Policy, and Politics," *Diplomatic History,* Vol. 32, No. 1, 2008, pp. 1-23. (RW 5751)

Immerman, R.H. "Transforming Intelligence Analysis: "The Tail that Wags the Dog"," in *Rethinking Leadership and "Whole of Government" National Security Reform: Problems,*

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Progress, and Prospects, eds. J.R. Cerami & J.A. Engel, US Army War College, Carlisle, PA, 2010, pp. 73-110. (RW 4192)

Immerman, R.H. "Transforming Analysis: The Intelligence Community's Best Kept Secret," *Intelligence and National Security,* Vol. 26, No. 2-3, 2011, pp. 159-181. (RW 4844)

Inch, E.S. & Warnick, B. *Critical Thinking and Communication,* 6th ed., Allyn & Bacon, Boston, MA, 2010. (RW 3921)

Inderfurth, K. & Johnson, L.K. *Decisions of the Highest Order: Perspectives on the National Security Council,* Brooks/Cole, Pacific Grove, CA, 1988. (RW 1093)

Ingvar, D.H. "Memories of the Future: An Essay on the Temporal Organisation of Conscious Awareness," *Human Neurobiology,* Vol. 4, No. 3, 1985, pp. 127. (RW 1348)

Ingwersen, P. "Cognitive Perspectives of Information Retrieval Interaction: Elements of a Cognitive IR Theory," *Journal of Documentation,* Vol. 52, No. 1, 1996, pp. 3. (RW 4398)

Ingwersen, P. *Information Retrieval Interaction,* Taylor Graham, London, 1992. (RW 4442)

Ingwersen, P. "Cognitive Information Retrieval," *Annual Review of Information Science and Technology,* Vol. 34, 1999-2000, pp. 3. (RW 3978)

Ingwersen, P. & Järvelin, K. *The Turn: Integration of Information Seeking and Retrieval in Context,* Springer, Dordrecht, 2005. (RW 3545)

Inman, B.R. "Intelligence in a Democratic Society," in *Thinking about America: The United States in the 1990s*, eds. A.G. Anderson & D.L. Bark, Hoover Institution Press, Stanford, CA, 1988, pp. 527-533. (RW 120)

Inman, B.R. *Managing Intelligence for Effective use,* Program on Information Resources Policy, Harvard University, Cambridge, MA, 1980. (RW 1241)

Inman, B.R. *Issues in Intelligence*, Center for Information Policy Research, Harvard University, Cambridge, MA, 1981. (RW 1242)

Inman, B.R. *Technological Innovation and the Cost of Change*, Center for Information Policy Research, Harvard University, Cambridge, MA, 1986. (RW 1240)

Inman, B.R. "The Military Perspective," in *Intelligence and Arms Control: A Marriage of Convenience,* ed. T.J. Hirschfeld, Lyndon B. Johnson School of Public Affairs, Austin, TX, 1987, pp. 45-60. (RW 1060)

Innocenti, C.W. *Intelligence Analysis for Urban Combat. - Monograph.* ADA403530, US Army Command and General Staff College, Ft. Leavenworth, KS, 2002. (RW 1202)

Institute for Analysis. *IFA Challenge #13: Mapping the Future. Workbook.* 2007. (RW 3290)

Institute for Analysis. *Mapping the Future* 2007. (RW 3289)

Institute for Analysis. *Asking Better Questions. Training Binder.* 2008?. (RW 3356)

Institute for Analysis. *Tradecraft: How to Ask Better Questions* 2008?. (RW 3357)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

International Communication Association. "Communication Yearbook," Vol. 19, 1996 (RW 4378)

Inuzuka, M. "Learning how to Write through Encouraging Metacognitive Monitoring: The Effect of Evaluating Essays Written by Others", *Proceedings of the 27th Annual Conference of the Cognitive Science Society*, July 21-23, 2005, pp. 1018. (RW 1984)

Ioannidis, J.P.A. "Why most Published Research Findings are False," *PLoS Medicine*, Vol. 2, No. 8, 2005, pp. e124. (RW 3284)

Ioannidis, J.P.A. "Why most Published Research Findings are False: Author's Reply to Goodman and Greenland," *PLoS Medicine*, Vol. 4, No. 6, 2007, pp. e215. (RW 3285)

Isaksen, S.G., Dorval, K.B. & Treffinger, D.J. *Creative Approaches to Problem Solving: A Framework for Change*, 2nd ed., Creative Problem Solving Group-- Buffalo, Williamsville, NY, 2000. (RW 2586)

Isaksen, S.G., Stead-Dorval, K.B. & Treffinger, D.J. *Creative Approaches to Problem Solving: A Framework for Innovation and Change*, 3rd ed., Sage, Los Angeles, 2011. (RW 5819)

Isaksen, S.G. & Treffinger, D.J. "Celebrating 50 Years of Reflective Practice: Versions of Creative Problem Solving," *Journal of Creative Behavior*, Vol. 38, No. 2, 2004, pp. 75. (RW 2618)

Ishikawa, H. *Applied Critical Thinking [Powerpoint Presentation]* [undated]. (RW 3756)

Itoh, M., Kawasaki, T. & Hirata, K. "Thinking Style Requirements for Project Managers", *Proceedings of the 28th Annual Conference of the Cognitive Science Society*, July 26-29, 2006, pp. 2512. (RW 1990)

Jackson, M.A. *Problem Frames: Analysing and Structuring Software Development Problems*, Addison-Wesley/ACM Press, Harlow, England; New York, 2001. (RW 2544)

Jackson, M. *Problem Structure and Dependable Architecture* (RW 2641)

Jackson, M. *Problems, Subproblems, and Concerns* 2004. (RW 2634)

Jackson, M. *Solving the Real Problem* 2004. (RW 2643)

Jackson, M. "Problem Frames and Software Engineering," *Information and Software Technology*, Vol. 47, 2005, pp. 903. (RW 2635)

Jackson, P. "On Uncertainty and the Limits of Intelligence," in *Oxford Handbook of National Security Intelligence*, ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 452-471. (RW 4714)

Jackson, W. "Scientific Estimating," *Studies in Intelligence*, Vol. 9, No. 3, 1965, pp. 7-11. (RW 4177)

Jacobs, R.L. *Implementing on-the-Job Learning*, American Society for Training and Development, Alexandria, VA, 2002. (RW 4884)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Jacobson, M.J. & Spiro, R.J. *Hypertext Learning Environments, Cognitive Flexibility, and the Transfer of Complex Knowledge: An Empirical Investigation,* Technical Report No. 573, Center for the Study of Reading, Champaign, IL, 1993. (RW 4912)

Jacoby, L.E. *Statement to Senate Select Committee on Intelligence. Current and Projected National Security Threats to the US,* 2005. (RW 627)

Jaeggi, S.M., Buschkuel, M., Jonides, J. & Perrig, W.J. "Improving fluid intelligence with training on working memory," *Proceedings of the National Academy of Sciences,* [Online], Available from: http://www.pnas.org/content/early/2008/04/25/0801268105.abstract. 2008, (RW 4599)

Jajko, W. "The Future of Defense Intelligence," in *U.S. Intelligence at the Crossroads: Agendas for Reform*, eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 214-231. (RW 647)

Jajko, W. *Department of Defense Information Operations: A Critical Commentary*, Center for Information Policy Research. Harvard University, Cambridge, MA, 2000. (RW 1011)

Jameson, A., Nelson, T.O., Leonesio, R.J. & Narens, L. "The Feeling of another Person's Knowing," *Journal of Memory and Language,* Vol. 32, No. 3, 1993, pp. 320. (RW 2360)

Janesick, V.J. "The Choreography of Qualitative Research Design: Minuets, Improvisations, and Crystallization," in *Handbook of Qualitative Research,* eds. N.K. Denzin & Y.S. Lincoln, 2nd ed., Sage Publications, Thousand Oaks, CA, 2000, pp. 379. (RW 3124)

Janis, I.L. *Groupthink: Psychological Studies of Policy Decisions and Fiascoes,* 2nd ed., Houghton Mifflin, Boston, MA, 1983. (RW 1243)

Janssen, T., Basik, H., Dean, M. & Smith, B. "A Multi-INT Semantic Reasoning Framework for Intelligence Analysis", *Proceedings of the Second International Ontology for the Intelligence Community Conference OIC-2007,* Columbia, MD, November 28-29, 2007, pp. 27-32. (RW 4818)

Jaques, E. & Cason, K. *Human Capability: A Study of Individual Potential and its Application,* Cason Hall & Co., Arlinton, VA, 1994. (RW 3063)

Jardine, N. *How People are Fooled by Evidence*. Available: http://www.scientificamerican.com/article.cfm?id=how-people-are-fooled-by-evidence&WT.mc_id=SA_WR_20111201, Viewed: December 2, 2011. (RW 5319)

Jardines, E.A. *Remarks and Q&A by the Assistant Deputy Director of National Intelligence for Open Source. ODNI Open Source Conference.* 2007. (RW 2724)

Jastrow, J. *Effective Thinking,* World Publishing, Cleveland, OH, 1931. (RW 4464)

Jeffery, G.C. & Underwood, G. "Writing as Problem Solving: The Role of Concrete and Abstract Knowledge in the Production of Written Text," in *Theories, Models and Methodology in Writing Research*, eds. G. Rijlaarsdam, H. van den Bergh & M. Couzijn, Amsterdam University Press, Amsterdam, 1996, pp. 61. (RW 2131)

Jeffreys-Jones, R. "The Historiography of the FBI," in *Handbook of Intelligence Studies,* ed. L.K. Johnson, 2007, pp. 39. (RW 2456)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Jeffreys-Jones, R. "Rise, Fall, and Regeneration: From CIA to EU," *Intelligence and National Security,* Vol. 24, No. 1, 2009, pp. 103. (RW 3452)

Jeffreys-Jones, R. "The Rise and Fall of the CIA," in *Oxford Handbook of National Security Intelligence,* ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 122-137. (RW 4705)

Jehng, J.J., Johnson, S.D. & Anderson, R.C. "Schooling and Students' Epistemological Beliefs," *Contemporary Educational Psychology,* Vol. 18, No. 1, 1993, pp. 23. (RW 4278)

Jelen, G.F. *Information Security: An Elusive Goal,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1985. (RW 1012)

Jenkins, B.M. "Connect the Cops to Connect the Dots," *San Diego Tribune,* June 1, 2003, p. 2. (RW 4533)

Jenkins, B.M. *Don't Move Too Fast on Intelligence Reform,* RAND Corp 2004. (RW 4557)

Jenkins, G.D., Mitra, A., Gupta, N. & Shaw, J.D. "Are Financial Incentives Related to Performance? A Meta-Analytic Review of Empirical Research," *Journal of Applied Psychology,* Vol. 83, No. 5, 1998, pp. 777-787. (RW 4619)

Jensen, C.J. "The Intelligence Officer Training Corps: An ROTC Style Program for the Intelligence Community," *International Journal of Intelligence and Counterintelligence,* Vol. 24, No. 4, 2011, pp. 733-746. (RW 5399)

Jensen, M.A. "Intelligence: An Economic Good," *Defense Intelligence Journal,* Vol. 10-2, 2001, pp. 67. (RW 1370)

Jensen, M.A. "Intelligence Failures: What are they really and what do we do about them?" *Intelligence and National Security,* Vol. 27, No. 2, 2012, pp. 261-282. (RW 5668)

Jepson, R.W. *How to Think Clearly,* Longmans, Green and Company, New York, NY, 1936. (RW 4469)

Jervis, R. *Perception and Misperception in International Politics,* Princeton University Press, Princeton, NJ, 1976. (RW 4546)

Jervis, R. "Improving the Intelligence Process: Informal Norms and Incentives," in *Intelligence: Policy and Process,* eds. A.C. Maurer, M.D. Tunstall & J.M. Keagle, Westview Press, Boulder, CO, 1985, pp. 113-124. (RW 1217)

Jervis, R. "What's Wrong with the Intelligence Process?" *International Journal of Intelligence and Counterintelligence,* Vol. 1, No. 1, 1986, pp. 28-41. (RW 126)

Jervis, R. "Strategic Intelligence and Effective Policy," in *Security and Intelligence in a Changing World: New Perspectives for the 1990s,* eds. A.S. Farson, D. Stafford & W.K. Wark, F. Cass, London, UK, 1991, pp. 165-181. (RW 256)

Jervis, R. "Review of America's Strategic Blunders by Willard C. Matthias," *Political Science Quarterly,* Vol. 116, No. 4, 2001-2, pp. 637-638. (RW 380)

Jervis, R. "Reports, Politics, and Intelligence Failures: The Case of Iraq," *Journal of Strategic Studies,* Vol. 29, No. 1, 2006, pp. 3. (RW 1758)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Jervis, R. "Think Different, CIA," *Boston Globe*, January 17, 2010, (RW 3851)

Jervis, R. *Why Intelligence Fails: Lessons from the Iranian Revolution and the Iraq War,* Cornell University Press, Ithaca, NY, 2010. (RW 3867)

Jervis, R. "Explaining the War in Iraq," in *Why did the United States Invade Iraq?*, eds. J. Cramer & A.T. Thrall, Routledge, London, UK, 2011, pp. 25-48. (RW 5216)

Jesse, L.A. & Kalita, J.K. "Situation Assessment and Prediction in Intelligence Domains," *Knowledge-Based Systems,* Vol. 10, No. 2, 1997, pp. 87-102. (RW 612)

Jesus, M., Garcia, M., Gomez-Becerra, I., Chavez-Brown, M. & Greer, D. "Perspective Taking and Theory of the Mind: Conceptual and Empirical Issues. A Complementary and Pragmatic Proposal," *Salud Mental,* Vol. 29, No. 6, 2006, pp. 5. (RW 2363)

Jin, W., Srihari, R.K. & Ho, H.H. "A Text Mining Model for Hypothesis Generation", *19th IEEE International Conference on Tools with Artificial Intelligence, 2007. ICTAI 2007*, 29-31 Oct. 2007, pp. 156-162. (RW 5578)

Jobbagy, Z. *Literature Survey on Uncertainty, Non-Linearity, Complexity and Chaos. A Ph.D. Study on Measuring Military Effects and Effectiveness,* FEL-04-B061, 2004. (RW 498)

Johnson, D.M. *Korean Airlines Incident: US Intelligence Disclosures*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1984. (RW 1014)

Johnson, E.M. & Halpin, S.M. *Multistage Inference Models for Intelligence Analysis*, Army Research Institute for the Behavioral and Social Sciences, Arlington, VA, 1974. (RW 5542)

Johnson, J.D. *Information Seeking: An Organizational Dilemma,* Quorum, Westport, CT, 1996. (RW 2153)

Johnson, J.G. "Method of Multiple Working Hypotheses: A Chimera," *Geology,* Vol. 18, No. 1, 1990, pp. 44-45. (RW 5205)

Johnson, L. "National Security Intelligence in the U.S.: A Performance Checklist," *Intelligence and National Security*, Vol. 26, No. 5, 2011, pp. 607-615. (RW 5391)

Johnson, L.K. "Seven Sins of Strategic Intelligence," *World Affairs,* Vol. 146, No. 2, 1983, pp. 176-204. (RW 386)

Johnson, L.K. *A Season of Inquiry: The Senate Intelligence Investigation,* University Press of Kentucky, Lexington, KY, 1985. (RW 1111)

Johnson, L.K. *A Season of Inquiry: Congress and Intelligence,* Dorsey Press, Chicago, IL, 1988. (RW 1112)

Johnson, L.K. *America's Secret Power: The CIA in a Democratic Society,* Oxford University Press, New York, NY, 1989. (RW 17)

Johnson, L.K. "Strategic Intelligence: An American Perspective," in *Security and Intelligence in a Changing World: New Perspectives for the 1990s*, eds. A.S. Farson, D. Stafford & W.K. Wark, F. Cass, London, UK, 1991, pp. 46-68. (RW 111)

Johnson, L.K. "Smart Intelligence," *Foreign Policy*, 89, 1993, pp. 53-69. (RW 255)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Johnson, L.K. "Analysis for a New Age," *Intelligence and National Security,* Vol. 11, No. 4, 1996, pp. 657-671. (RW 137)

Johnson, L.K. "The CIA and the Question of Accountability," in *Eternal Vigilance? 50 Years of the CIA*, eds. R. Jeffreys-Jones & C. Andrew, F. Cass, London, UK, 1997, pp. 178-200. (RW 36)

Johnson, L.K. "Intelligence and the Challenge of Collaborative Government," *Intelligence and National Security,* Vol. 13, No. 2, 1998, pp. 177-182. (RW 176)

Johnson, L.K. *Bombs, Bugs, Drugs, and Thugs: Intelligence and America's Quest for Security,* New York University Press, New York, NY, 2000. (RW 933)

Johnson, L.K. "The DCI Vs the Eight-Hundred-Pound Gorilla," *International Journal of Intelligence and Counterintelligence,* Vol. 13, No. 1, 2000, pp. 35-48. (RW 61)

Johnson, L.K. "The Role of Congress in US Strategic Intelligence," *American Intelligence Journal*, Summer/Fall, 2000, pp. 41-45. (RW 174)

Johnson, L.K. "Spies," *Foreign Policy,* 120, 2000, pp. 18-26. (RW 35)

Johnson, L.K. "Spying is a Cold War Anachronism," *Foreign Policy,* September/October, 2000, pp. 18. (RW 391)

Johnson, L.K. "The CIA's Weakest Link: Forget James Bond. what our Intelligence Agencies Need are More Professors," *Washington Monthly,* Vol. 33, No. 7/8, 2001, pp. 9-14. (RW 1064)

Johnson, L.K. "Bricks and Mortar for a Theory of Intelligence," *Comparative Strategy*, Vol. 22, No. 1, 2003, pp. 1-28. (RW 84)

Johnson, L.K. "Preface to a Theory of Strategic Intelligence," *International Journal of Intelligence and Counterintelligence,* Vol. 16, No. 4, 2003, pp. 638-663. (RW 55)

Johnson, L.K. *Remarks before the OPSEC Professionals Society* 2003. (RW 501)

Johnson, L.K. "The Aspin-Brown Intelligence Inquiry: Behind the Closed Doors of a Blue Ribbon Commission," *Studies in Intelligence,* Vol. 48, No. 3, 2004, pp. 1-20. (RW 460)

Johnson, L.K. "A Conversation with Former DCI William E. Colby: Spymaster during the 'Year of the Intelligence Wars'," *Intelligence and National Security,* Vol. 22, No. 2, 2007, pp. 250. (RW 2400)

Johnson, L.K. "Introduction," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 1-14. (RW 2454)

Johnson, L.K. "An Introduction to the Intelligence Studies Literature," in *Strategic Intelligence. Volume 1: Understanding the Hidden Side of Government*, ed. L.K. Johnson, Praeger Security International, Westport, CT, 2007, pp. 1. (RW 2709)

Johnson, L.K. "A Shock Theory of Congressional Accountability for Intelligence," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 343. (RW 2479)

Johnson, L.K. *Strategic Intelligence. Volume 3: Covert Action: Behind the Veils of Secret Foreign Policy,* Praeger Security International, Westport, CT, 2007. (RW 2702)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Johnson, L.K. *Strategic Intelligence. Volume 5: Intelligence and Accountability: Safeguards Against the Abuse of Secret Power.* Praeger Security International, Westport, CT, 2007. (RW 2497)

Johnson, L.K. "The Church Committee Investigation of 1975 and the Evolution of Modern Intelligence Accountability," *Intelligence and National Security,* Vol. 23, No. 2, 2008, pp. 198. (RW 3072)

Johnson, L.K. "Glimpses into the Gems of American Intelligence: The President's Daily Brief and the National Intelligence Estimate," *Intelligence and National Security,* Vol. 23, No. 3, 2008, pp. 333. (RW 3168)

Johnson, L.K. "Ostriches, Cheerleaders, Skeptics, and Guardians: Role Selection by Congressional Intelligence Overseers," *SAIS Review,* Vol. 28, No. 1, 2008, pp. 93. (RW 3329)

Johnson, L.K. "Sketches for a Theory of Strategic Intelligence," in *Intelligence Theory: Key Questions and Debates,* eds. P. Gill, S. Marrin & M. Phythian, 2009, pp. 33. (RW 3404)

Johnson, L.K. "National Security Intelligence," in *Oxford Handbook of National Security Intelligence,* ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 1-32. (RW 4603)

Johnson, L.K. "National Security Intelligence in the United States: A Performance Checklist " *Intelligence and National Security,* Vol. 26, No. 5, 2011, pp. 607-615. (RW 5609)

Johnson, L.K. *The Threat on the Horizon: An Inside Account of America's Search for Security After the Cold War,* Oxford University Press, New York, NY, 2011. (RW 4661)

Johnson, L.K. & Shelton, A.M. "Thoughts on the State of Intelligence Studies: A Survey Report," *Intelligence and National Security,* Vol. 28, No. 1, 2013, pp. 109-120. (RW 5914)

Johnson, L.K. & Wirtz, J.J. *Strategic Intelligence: Windows into a Secret World: An Anthology,* Roxbury Publishers, Los Angeles, CA, 2004. (RW 1103)

Johnson, L.K. & Wirtz, J.J. "Epilogue: The Future of Intelligence," in *Intelligence: The Secret World of Spies,* eds. L.K. Johnson & J.J. Wirtz, 2010, pp. 540. (RW 4341)

Johnson, L.K. & Wirtz, J.J. "Intelligence in the United States: An Introduction," in *Intelligence: The Secret World of Spies,* eds. L.K. Johnson & J.J. Wirtz, 2010, pp. 1. (RW 4148)

Johnson, M.H. *Developmental Cognitive Neuroscience: An Introduction,* 2nd ed., Blackwell, Malden, MA, 2005. (RW 1912)

Johnson, P., Johnson, H. & Wilson, S. "Rapid Prototyping of User Interfaces Driven by Task Models," in *Scenario-Based Design: Envisioning Work and Technology in Systems Development,* ed. J.M. Carroll, Wiley, New York, 1995, pp. 209. (RW 3397)

Johnson, R.T. & Johnson, D.W. "An Overview of Cooperative Learning," in *Creativity and Collaborative Learning,* eds. J. Thousand, A. Villa & A. Nevin, Brookes Press, Baltimore, MD, 1994, pp. 31-44. (RW 4810)

Johnson, S. *The Ghost Map: The Story of London's most Terrifying Epidemic--and how it Changed Science, Cities, and the Modern World,* Riverhead Books, New York, 2006. (RW 5816)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Johnson, S. *Where Good Ideas Come from: The Natural History of Innovation,* Riverhead Books, New York, NY, 2010. (RW 4681)

Johnson, S.E. *Command and Control Education and Research,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1990. (RW 1013)

Johnson-Laird, P.N. *Mental Models: Towards a Cognitive Science of Language, Inference, and Consciousness,* Harvard University Press, Cambridge, MA, 1983. (RW 1318)

Johnson-Laird, P.N. "Mental Models and Thought," in *The Cambridge Handbook of Thinking and Reasoning,* eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 185-208. (RW 4004)

Johnson-Laird, P.N. "Inference with Mental Models," in *Oxford Handbook of Thinking and Reasoning,* eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 134-154. (RW 5499)

Johnston, L.E. "Language, Culture, and Cooperation in Scientific and Technical Intelligence," *Studies in Intelligence,* Vol. 52, No. 2, 2008, pp. 1. (RW 3163)

Johnston, P., Woodside-Jiron, H., Day, J. "Teaching and Learning Literate Epistemologies. CELA Research Report," *Journal of Educational Psychology,* Vol. 93, No. 1, 2001, pp. 223-233. (RW 5299)

Johnston, R. "Foundations for Meta-Analysis: Developing a Taxonomy of Intelligence Analysis Variables," *Studies in Intelligence,* Vol. 47, No. 3, 2003, pp. 61-71. (RW 396)

Johnston, R. "Integrating Methodologists into Teams of Substantive Experts," *Studies in Intelligence,* Vol. 47, No. 1, 2003, pp. 57-65. (RW 688)

Johnston, R. *Analytic Culture in the US Intelligence Community: An Ethnographic Study,* Center for the Study of Intelligence, Washington, DC, 2005. (RW 629)

Johnston, R. "Integrating Methodologists into Teams of Substantive Experts", *New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities,* Rome, Italy, 31 March - 2 April, 2004, pp. 137-152. (RW 4667)

Johnstone, K.M. & Biggs, S.F. "Problem-Based Learning: Introduction, Analysis, and Accounting Curricula Implications," *Journal of Accounting Education,* Vol. 16, No. 3/4, 1998, pp. 407. (RW 4290)

Joint Military Intelligence. College *Research Design and Methods,* 2000. (RW 2773)

Jonas, E., Schulz-Hardt, S., Frey, D. & Thelen, N. "Confirmation Bias in Sequential Information Search After Preliminary Decisions: An Expansion of Dissonance Theoretical Research on Selective Exposure to Information," *Journal of Personality & Social Psychology,* Vol. 80, No. 4, 2001, pp. 557. (RW 5166)

Jonassen, D.H. *Computers as Mindtools for Schools: Engaging Critical Thinking,* 2nd ed., Merrill, Upper Saddle River, NJ, 2000. (RW 4107)

Jonassen, D.H. "Toward a Design Theory of Problem Solving," *Educational Technology Research and Development,* Vol. 48, No. 4, 2000, pp. 63-85. (RW 5285)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Jones, C. "Intelligence Reform: The Logic of Information Sharing," *Intelligence and National Security,* Vol. 22, No. 3, 2007, pp. 384. (RW 2804)

Jones, E., Bruce, H., Klasnja, P. & Jones, W. "I Give Up! Five Factors that Contribute to the Abandonment of Information Management Strategies," *Proceedings of the American Society for Information Science & Technology,* Vol. 45, No. 1, 2008, pp. 1. (RW 4404)

Jones, E.A., Hoffman, S., Moore, L.M., Ratcliff, G., Tibbetts, S. & Click, B.A.L. *National Assessment of College Student Learning: Identifying College Graduates' Essential Skills in Writing, Speech and Listening, and Critical Thinking. Final Project Report,* National Center on Post Secondary Teaching, Learning, and Assessment, University Park, PA, 1995. (RW 3639)

Jones, G. "Working with the CIA," *Parameters,* Vol. 31, No. 4, 2001-02, pp. 28-39. (RW 105)

Jones, I. *The Human Factor: Inside the CIA's Dysfunctional Intelligence Culture,* 2010. (RW 3980)

Jones, J.C. "A Method of Systematic Design," in *Developments in Design Methodology,* ed. N. Cross, Wiley, Chichester; New York, 1984, pp. 9. (RW 2735)

Jones, K.S. "What's the Value of Trec: Is there a Gap to Jump Or a Chasm to Bridge?" *ACM SIGIR Forum,* Vol. 40, No. 1, 2006, pp. 10-20. (RW 4933)

Jones, L. *Patterns of Error: Perceptual and Cognitive Bias in Intelligence Analysis and Decision-Making.* 2005. (RW 1315)

Jones, M.D. *The Thinker's Toolkit: Fourteen Powerful Techniques for Problem Solving,* Three Rivers Press, New York, NY, 1998. (RW 681)

Jones, P.M., Hayes, C.C., Wilkins, D.C., Bargar, R., Sniezek, J., Asaro, P., Menghoel, O., Kessler, D., Lucenti, M., Choi, I., Tu, N. & Schlabach, J. "CoRAVEN: Modeling and Design of a Multimedia Intelligent Infrastructure for Collaborative Intelligence Analysis", *1998 IEEE International Conference on Systems, Man, and Cybernetics,* San Diego, CA, October 11-14, 1998 (RW 677)

Jones, R.V. "The Scientific Intelligencer," *Studies in Intelligence,* Vol. 6, No. 4, 1962, pp. 37-48. (RW 569)

Jones, R.V. *Most Secret War,* Hamilton, London, UK, 1978. (RW 711)

Jones, R.V. *The Wizard War: British Scientific Intelligence, 1939-1945,* Coward, McCann & Geoghegan, New York, NY, 1978. (RW 710)

Jones, R.V. "An Early Epic of ELINT," *Journal of Electronic Defense,* Vol. 6, No. June, 1983, pp. 75-76. (RW 734)

Jones, R.V. "Intelligence and Command," *Intelligence and National Security,* Vol. 3, No. 3, 1988, pp. 288-298. (RW 735)

Jones, R.V. *Reflections on Intelligence,* Heinemann, London, UK, 1989. (RW 709)

Jones, R.V. *Some Lessons in Intelligence. Remarks made at a CIA Symposium.* 1993. (RW 352)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Jones, R.V. "A Sidelight on Bletchley, 1942," *Intelligence and National Security,* Vol. 9, No. 1, 1994, pp. 1-11. (RW 736)

Jones, R.V. "Scientific Intelligence," *Studies in Intelligence,* Vol. 6, No. 3, 1962, pp. 55-76. (RW 553)

Jones, R.A. *Self-Fulfilling Prophecies: Social, Psychological, and Physiological Effects of Expectancies,* L. Erlbaum Associates, Hillsdale, NJ, 1977. (RW 2138)

Jones, W.P. *Keeping found Things found: The Study and Practice of Personal Information Management,* Morgan Kaufmann Publishers, Amsterdam; Boston, 2008. (RW 4125)

Jonsson, A.C. & Allwood, C.M. "Stability and Variability in Realism of Confidence Judgments Over Time, Content Domain, and Gender," *Personality and Individual Differences,* Vol. 34, 2003, pp. 559. (RW 2424)

Jordan, L.F. "The Case for a Holistic Intelligence," *Studies in Intelligence,* Vol. 19, No. 2, 1975, pp. 9-19. (RW 560)

Josephson, J.R. & Tanner, M.C. "Conceptual Analysis of Abduction," in *Abductive Inference: Computation, Philosophy, Technology*, eds. J.R. Josephson & S.G. Josephson, Cambridge University Press, Cambridge, UK, 1994, pp. 5-30. (RW 5471)

Jou, J., Shanteau, J. & Harris, R. "An Information Processing View of Framing Effects: The Role of Causal Schemas in Decision Making," *Memory & Cognition,* Vol. 24, No. 1, 1996, pp. 1. (RW 2375)

Juslin, P. "Naive Empiricism and Dogmatism in Confidence Research: A Critical Examination of the Hard-Easy Effect," *Psychological Review,* Vol. 107, 2000, pp. 384. (RW 2431)

K, J. "Intelligent Design? The Influence of Organizational Factors on Intelligence Analysis," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 208. (RW 3650)

Kaczmarczyk, L.C. & Mikkulainen, R. "The Acquisition of Intellectual Expertise: A Computational Model", *Proceedings of the 26th Annual Conference of the Cognitive Science Society,* pp. 636. (RW 2003)

Kagolovsky, Y., Freese, D., Miller, M., Walrod, T. & Moehr, J. "Towards Improved Information Retrieval from Medical Sources," *International Journal of Medical Informatics,* Vol. 51, No. 2, 1998, pp. 181-195. (RW 954)

Kagolovsky, Y. & Moehr, J. "Current Status of the Evaluation of Information Retrieval," *Journal of Medical Systems,* Vol. 27, No. 5, 2003, pp. 409-424. (RW 758)

Kagolovsky, Y. & Moehr, J. "Terminological Problems in Information Retrieval," *Journal of Medical Systems,* Vol. 27, No. 5, 2003, pp. 399-408. (RW 761)

Kagolovsky, Y. & Moehr, J. "Introducing a Conceptual Information Retrieval (IR) Framework," *Journal of Medical Systems,* Vol. 28, No. 1, 2004, pp. 89-101. (RW 759)

Kagolovsky, Y. & Moehr, J. "A New Look at Information Retrieval Evaluation: Proposal for Solutions," *Journal of Medical Systems,* Vol. 28, No. 1, 2004, pp. 103-116. (RW 760)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Kahan, D., Braman, D. & Jenkins-Smith, H. *Cultural Cognition of Scientific Consensus,* 2010. (RW 4371)

Kahana, E. "Analyzing Israel's Intelligence Failures," *International Journal of Intelligence and Counterintelligence,* Vol. 18, No. 2, 2005, pp. 262-279. (RW 270)

Kahn, D. "The Intelligence Failure of Pearl Harbor," *Foreign Affairs,* Vol. 70, No. 5, 1991-92, pp. 138-152. (RW 579)

Kahn, D. "Toward a Theory of Intelligence," *Quarterly Journal of Military History,* Vol. 7, No. 2, 1994, pp. 92-97. (RW 4581)

Kahn, D. "A Historical Theory of Intelligence," *Intelligence and National Security,* Vol. 16, No. 3, 2001, pp. 79-92. (RW 175)

Kahn, D. "Surprise and Secrecy: Two Thoughts," *Intelligence and National Security,* Vol. 21, No. 6, 2006, pp. 1060. (RW 2092)

Kahn, D. "Intelligence Studies on the Continent," *Intelligence and National Security,* Vol. 23, No. 2, 2008, pp. 249. (RW 3073)

Kahn, D. "An Historical Theory of Intelligence," in *Intelligence Theory: Key Questions and Debates*, eds. P. Gill, S. Marrin & M. Phythian, 2009, pp. 4. (RW 3402)

Kahneman, D. "A Perspective on Judgment and Choice," *American Psychologist,* Vol. 58, No. 9, 2003, pp. 697. (RW 2439)

Kahneman, D. *Thinking, Fast and Slow,* Farrar, Straus and Giroux, New York, NY, 2011. (RW 5106)

Kahneman, D. & Frederick, S. "A Model of Heuristic Judgment," in *The Cambridge Handbook of Thinking and Reasoning,* eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 267-294. (RW 4006)

Kahneman, D. & Klein, G. "Conditions for Intuitive Expertise: A Failure to Disagree," *American Psychologist,* Vol. 64, No. 6, 2009, pp. 515. (RW 4118)

Kahneman, D. & Renshon, J. "Why Hawks Win," *Foreign Policy,* January/February, 2007 (RW 2046)

Kahneman, D., Slovic, P. & Tversky, A. *Judgment Under Uncertainty: Heuristics and Biases,* Cambridge University Press, Cambridge, UK, 1982. (RW 746)

Kahneman, D. & Tversky, A. *Choices, Values, and Frames,* Russell Sage Foundation, New York, 2000. (RW 3310)

Kaiser, F.M. *Congressional Oversight of Intelligence: Current Structure and Alternatives,* 2007. (RW 2172)

Kakai, H. "Re-Examining the Factor Structure of the California Critical Thinking Disposition Inventory," *Perceptual & Motor Skills,* Vol. 96, No. 2, 2003, pp. 435-438. (RW 5359)

Kam, E. "The Recent American Intelligence Failures," *Strategic Assessment,* Vol. 7, No. 4, 2005 (RW 298)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Kamarck, E.C. *Transforming the Intelligence Community: Improving the Collection and Management of Information*, 2005. (RW 1507)

Kameda, T. "Stereotype-Based Expectancy and Academic Evaluation: The Joint Influence of Prior Expectancy and the Diagnosticity of Current Information," *Japanese Psychological Research*, Vol. 271985, pp. 163. (RW 2877)

Kaminski, P.G. *Statement before the House Permanent Select Committee on Intelligence. Enabling Technologies for the 21st Century*. 1995. (RW 1054)

Kampman, C.M., Mangio, C.A. & Parry, T.L. *State of Knowledge Relative to Intelligence Analysis. Volume 2: Information Review*, AFRL-RH-WP-TR-2011-0051, 2006. (RW 5246)

Kampman, C.M., Mangio, C.A. & Parry, T.L. *State of Knowledge Relative to Intelligence Analysis. Volume 3: Information Assessment*, AFRL-RH-WP-TR-2011-0052, 2006. (RW 5247)

Kampman, C.M., Mangio, C.A., Parry, T.L. & Wilkinson, B.J. *State of Knowledge Relative to Intelligence Analysis. Volume 4: Framework for Analytic Cognition (FAC)*, AFRL-RH-WP-TR-2011-0053, 2011. (RW 5248)

Kampman, C.M., Mangio, C.A., Parry, T.L. & Wilkinson, B.J. *Framework for Analytic Cognition (FAC): A Guide for Doing all-Source Intelligence Analysis*, AFRL-RH-WP-TR-2012-0109, 2012. (RW 5625)

Kanai, R. & Banissy, M. *Are Two Heads Better than One? it Depends*. Available: http://www.scientificamerican.com/article.cfm?id=are-two-heads-better-than&sc=CAT_MB_20100901, Viewed: September 2, 2010. (RW 4303)

Kandel, E.R. "The New Science of Mind," *Scientific American Mind*, Vol. 17, No. 2, 2006, pp. 62. (RW 3149)

Kane, R. "Introduction: The Contours of Contemporary Free-Will Debates (Part 2)," in *The Oxford Handbook of Free Will*, ed. R. Kane, 2nd ed., Oxford University Press, Oxford, UK, 2011, pp. 3-35. (RW 5749)

Kane, T.M. "Strategic Analysis: To Hear the Thunder," *Military Intelligence Professional Bulletin*, Vol. 28, No. 1, 2002, pp. 4-7. (RW 1197)

Kang, Y., Gorg, C. & Stasko, J. "The Evaluation of Visual Analytics Systems for Investigative Analysis: Deriving Design Principles from a Case Study", *Visual Analytics Science and Technology, 2009. VAST 2009*. 12-13 Oct. 2009, pp.139-146. (RW 5579)

Kaplan, C.A. & Simon, H.A. "In Search of Insight," *Cognitive Psychology*, Vol. 22, 1990, pp. 374. (RW 1790)

Kaplan, D.E. "An Agenda for Reform," *US News and World Report*, 2004 (RW 1271)

Kaplan, D.E. "Hey, Let's Play Ball," *US News and World Report*, Vol. 141, No. 17, 2006, pp. 52. (RW 1706)

Kaplan, D.E. "Wikis and Blogs, Oh My!" *US News and World Report*, Vol. 141, No. 17, 2006, pp. 52. (RW 1707)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Kaplan, D.E. & Whitelaw, K. "Intelligence Reform - at Last," *US News and World Report,* Vol. 137, No. 22, 2004, pp. 31-32. (RW 752)

Kaplan, D.E. & Whitelaw, K. "Kicking Over the Hornet's Nest," *US News and World Report,* Vol. 137, No. 19, 2004, pp. 22. (RW 753)

Kaplan, D.E. & Whitelaw, K. "Playing Defense," *US News and World Report,* Vol. 141, No. 18, 2006, pp. 44. (RW 1725)

Kaplan, D.E., Whitelaw, K. & Ekman, M.M. "Mission Impossible," *US News and World Report,* Vol. 137, No. 3, 2004, pp. 32. (RW 751)

Kaplan, E.H. "Operations Research and Intelligence Analysis," in *Intelligence Analysis: Behavioral and Social Scientific Foundations,* eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, pp. 31-56. (RW 4771)

Kaplan, J.T., Freedman, J. & Iacoboni, M. "Us Versus them: Political Attitudes and Party Affiliation Influence Neural Response to Faces of Presidential Candidates. Article in Press." *Neuropsychologica,* 2006? (RW 1714)

Kapler, T., Harper, R. & Wright, W. "Correlating Events with Tracked Movements in Time and Space: A GeoTime Case Study," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 833)

Karabenick, S.A. & Moosa, S. "Culture and Personal Epistemology: U.S. and Middle Eastern Students' Beliefs about Scientific Knowledge and Knowing." *Social Psychology of Education,* Vol. 8, No. 4, 2005, pp. 375-393. (RW 4936)

Kardash, C.M. & Howell, K.L. "Effects of Epistemological Beliefs and Topic-Specific Beliefs on Undergraduates' Cognitive and Strategic Processing of Dual-Positional Text," *Journal of Educational Psychology,* Vol. 92, No. 3, 2000, pp. 524-535. (RW 4654)

Kardash, C.M. & Scholes, R.J. "Effects of Preexisting Beliefs, Epistemological Beliefs, and Need for Cognition on Interpretation of Controversial Issues," *Journal of Educational Psychology,* Vol. 88, No. 2, 1996, pp. 260-271. (RW 2845)

Kardash, C.M. & Sinatra, G.M. "Epistemological Beliefs and Dispositions: Are we Measuring the Same Construct?", *Annual Meeting of the American Educational Research Association,* Chicago, IL, April 21-25, 2003 (RW 5380)

Kasschau, R.A., Lachman, R. & Laughery, K.R. *Information Technology and Psychology: Prospects for the Future,* Praeger, New York, NY, 1982. (RW 1062)

Katona, P. *Terrorism and Biological Weapons: Threat and Response [Powerpoint Presentation]* (RW 479)

Katter, R.V., Montgomery, C.A. & Thompson, J.R. *Cognitive Processes in Intelligence Analysis: A Descriptive Model and Review of the Literature,* Technical Report 445, US Army Research Institute for the Behavioral and Social Sciences, Alexandria, VA, 1979. (RW 686)

Katter, R.V., Montgomery, C.A. & Thompson, J.R. *Human Processes in Intelligence Analysis: Phase I Overview,* Research Report 1237, US Army Research Institute for the Behavioral and Social Sciences, Alexandria, VA, 1979. (RW 261)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Katz, Y. & Vardi, Y. "Strategies for Data Gathering and Evaluation in the Intelligence Community," *International Journal of Intelligence and Counterintelligence*, Vol. 5, No. 3, 1991, pp. 313-328. (RW 1224)

Katzenstein, G. "The Debate on Structured Debate: Toward a Unified Theory," *Organizational Behavior and Human Decision*, Vol. 66, No. 3, 1996, pp. 316. (RW 3144)

Kaufman, J.C. & Baer, J. "Introduction: How People Think, Work, and Act Creatively in Diverse Domains," in *Creativity Across Domains: Faces of the Muse*, eds. J.C. Kaufman & J. Baer, L. Erlbaum Associates, Mahwah, NJ, 2005, pp. xiii-xvii. (RW 4986)

Kawada, C.L., Oettingen, G., Gollwitzer, P.M. & Bargh, J.A. "The Projection of Implicit and Explicit Goals," *Journal of Personality and Social Psychology*, Vol. 86, 2004, pp. 545. (RW 3081)

Kay, D. "Denial and Deception: The Lessons of Iraq," in *U.S. Intelligence at the Crossroads: Agendas for Reform*, eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 109-127. (RW 642)

Kay, D. *Statement before the Senate Select Committee on Intelligence* 2004. (RW 313)

Kay, R. *Deep Web* 2005. (RW 1579)

Keahey, T.A. & Eick, S.G. "A Visualization Architecture for Intelligence Analysis," in *Visualization and Data Analysis 2004. Proc. of SPIE - IS&T Electronic Imaging, SPIE Vol. 5295*, ed. R.F. Erbacher, 2004. (RW 1313)

Kean, T.H., Hamilton, L.H. & Lehman, J.F. *Statement before the National Commission on Terrorist Attacks upon the United States before the Senate Select Committee on Intelligence* 2004. (RW 316)

Keane, M.T., O'Brien, M. & Smyth, B. "Are People Biased in their use of Search Engines?" *Communications of the ACM*, Vol. 51, No. 2, 2009, pp. 49. (RW 3470)

Kearney, C.P., Kean, M.H., Roeber, E.D., Stevens, B.L., Baron, J.B., Fremer, J. & Daniel, M. *Assessing Higher Order Thinking Skills*, ERIC/TME Report 90, ERIC Clearinghouse on Tests, Measurement, and Analysis, Princeton, NJ, 1986. (RW 4072)

Keefe, P.R. "Privatized Spying: The Emerging Intelligence Industry," in *Oxford Handbook of National Security Intelligence*, ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 296-309. (RW 4707)

Keegan, J. *Intelligence in War: Knowledge of the Enemy from Napoleon to Al-Qaeda*, Knopf, New York, NY, 2003. (RW 15)

Keegan, J. "Inquiry is Pointless. Intelligence is always Open to Interpretation," *The Telegraph*, 2004, February 3, 2004, (RW 242)

Keen, A. *The Cult of the Amateur: How Today's Internet is Killing our Culture*, Doubleday/Currency, New York, (RW 3198)

Kees, T.S. "Advanced Information Processing and Analysis," *American Intelligence Journal*, Vol. 13, No. 3, 1992, pp. 53-58. (RW 4345)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Kehm, H.D. "Notes on some Aspects of Intelligence Estimates," *Studies in Intelligence,* Vol. 11, No. 3, 1967, pp. 19-37. (RW 544)

Keil, F.C. "Explanation and Understanding," *Annual Review of Psychology,* Vol. 57, 2006, pp. 227. (RW 2332)

Keil, F.C. "Intuitive Belief Systems and Informal Reasoning in Cognitive Development," in *Informal Reasoning and Education*, eds. J.F. Voss, D.N. Perkins & J.W. Segal, L. Erlbaum Associates, Hillsdale, NJ, 1991, pp. 247-264. (RW 5000)

Keithly, D.M. *Leading Intelligence in the 21st Century: Past as Prologue?* 1998. (RW 1284)

Keller, B.A. *Avoiding Surprise: The Role of Intelligence Collection and Analysis at the Operational Level of War,* ADA258103, US Army Command and General Staff College, Ft. Leavenworth, KS, 1992. (RW 263)

Keller, J. "Air Force Eyes Potential $40 Million Project for Intelligence Analysis," *Military and Aerospace Electronics,* Vol. 14, No. 6, 2003, pp. 1. (RW 782)

Keller, J. "IARPA Babel program seeks to provide translation and intelligence analysis for any known language", *Military and Aerospace Electronics,* [Online], Available from: http://www.militaryaerospace.com/index/display/article-display/3343949508/articles/military-aerospace-electronics/executive-watch-2/2011/4/iarpa-babel_program.html. April 10, 2011, (RW 4760)

Kellogg, R.T. "Professional Writing Expertise," in *The Cambridge Handbook of Expertise and Expert Performance*, ed. K.A. Ericsson, Cambridge University Press, Cambridge, UK, 2006, pp. 389. (RW 1948)

Kellogg, R.T. *The Psychology of Writing*, Oxford University Press, New York, NY, 1994. (RW 1605)

Kelly, D.J. *Providing Global Information Services to the Warfighter*, Center for Information Policy Research. Harvard University, Cambridge, MA, 2000. (RW 1015)

Kelly, D., Dumais, S. & Pedersen, J.O. "Evaluation Challenges and Directions for Information-Seeking Support Systems," *Computer*, Vol. 42, No. 3, 2009, pp. 60. (RW 3442)

Kelly, J. "Intelligence Overseer Impractical, Experts Say," *Pittsburgh Post-Gazette*, July 23, 2004. (RW 601)

Kelly-Riley, D., Brown, G., Condon, B. & Law, R. *Washington State University Critical Thinking Project*, The Center for Teaching, Learning, Technology, General Education & The Writing Programs, Pullman, WA, 2001. (RW 4040)

Kelly-Riley, D., Brown, G., Condon, B. & Law, R. *Guide to Rating Critical Thinking*, Washington State University, Pullman, WA, 2004. (RW 4054)

Kelman, M. *The Heuristics Debate*, Oxford University Press, New York, NY, 2011. (RW 4783)

Kempster, P.A. "Looking for Clues," *Journal of Clinical Neuroscience*, Vol. 13, 2006, pp. 178. (RW 3907)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Kendall, E.F., Jacobs, J., McGuinness, D.L. & Schwab, S. "Policies for Public Domain Ontologies for the Intelligence Community", *Proceedings of the Second International Ontology for the Intelligence Community Conference OIC-2007,* Columbia, MD, November 28-29, 2007, pp. 15-18. (RW 4815)

Kendall, W. "The Function of Intelligence," *World Politics,* Vol. 1, No. 6, 1949, pp. 540-552. (RW 2905)

Kendall, W. *Contra Mundum,* University Press of America, Lanham, MD, 1994. (RW 4563)

Kennedy, H. *Intelligence Sharing: 'Still a Battle'* 2006. (RW 1427)

Kennedy, R. *Of Knowledge and Power: The Complexities of National Intelligence,* (RW 3229)

Kent, G.A. "On Analysis," *Air University Review,* Vol. 18, No. 4, 1967, pp. 50-54. (RW 4741)

Kent, G.A. *Thinking about America's Defense: An Analytical Memoir* 2008. (RW 3596)

Kent, S. *Writing History,* F.S. Crofts & Co, New York, NY, 1941. (RW 251)

Kent, S. *Strategic Intelligence for American World Policy,* Princeton University Press, Princeton, NJ, 1949. (RW 257)

Kent, S. "Words of Estimative Probability," *Studies in Intelligence,* Vol. 8, No. 4, 1964, pp. 49-65. (RW 4179)

Kent, S. "Death of an Hypothesis," *Studies in Intelligence,* Vol. 9, No. 2, 1965, pp. 21-24. (RW 527)

Kent, S. *Strategic Intelligence for American World Policy,* Archon Books, Hamden, CT, 1965. (RW 5313)

Kent, S. *Writing History,* 2d ed., Appleton-Century-Crofts, New York, NY, 1967. (RW 252)

Kent, S. "Estimates and Influence," *Studies in Intelligence,* Vol. 12, No. 3, 1968, pp. 11-21. (RW 4178)

Kent, S. "The Yale Report," *Studies in Intelligence,* Vol. 17, No. 2, 1973, pp. 7-21. (RW 571)

Kent, S. "The Need for an Intelligence Literature," *Studies in Intelligence,* Vol. 45th Anniversary Special Edition, No. Fall, 2000, pp. 1-11. (RW 4168)

Kent, S. & Steury, D.P. *Sherman Kent and the Board of National Estimates: Collected Essays,* Center for the Study of Intelligence, Washington, DC, 1994. (RW 249)

Keohane, J. *How Facts Backfire: Researchers Discover a Surprising Threat to Democracy: Our Brains*. Available: http://www.boston.com/bostonglobe/ideas/articles/2010/07/11/how_facts_backfire/. 2010. (RW 4202)

Kerbel, J. "For the intelligence community, creativity is the new secret", *World Politics Review,* [Online], March 25, 2010. Available from: http://www.worldpoliticsreview.com/articles/5329/for-the-intelligence-community-creativity-is-the-new-secret (RW 4119)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Kerbel, J. "Thinking Straight: Cognitive Bias in the US Debate about China," *Studies in Intelligence,* Vol. 48, No. 3, 2004, pp. 27-35. (RW 4170)

Kerbel, J. "Lost for Words: The Intelligence Community's Struggle to Find its Voice," *Parameters,* Vol. 38, No. 2, 2008, pp. 102-112. (RW 3190)

Kerbel, J. & Olcott, A. "Synthesizing with Clients, Not Analyzing for Customers," *Studies in Intelligence,* Vol. 54, No. 4, 2010, pp. 11-27. (RW 4758)

Keren, G. & Schul, Y. "Two is Not always Better than One: A Critical Evaluation of Two-System Theories," *Perspectives on Psychological Science,* Vol. 4, No. 6, 2009, pp. 533-550. (RW 5724)

Kerr, D. *500 Day Plan Hearing before the Intelligence Community Management Subcommittee of the House Permanent Select Committee on Intelligence* 2007. (RW 2892)

Kerr, D. *Remarks and Q&A by the Principal Deputy Director of National Intelligence. the Intelligence and National Security Alliance Leadership Dinner.* 2008. (RW 3022)

Kerr, N.L. & Tindale, R.S. "Group Performance and Decision Making," *Annual Review of Psychology,* Vol. 55, 2004, pp. 623. (RW 1881)

Kerr, R.J. "The Perfect Enemy: Reflections of an Intelligence Officer on the Cold War and Today's Challenges," in *The Handbook of Intelligent Policing: Consilience, Crime Control, and Community Safety,* ed. C. Harfield, Oxford University Press, Oxford, UK, 2008, pp. 37-46. (RW 5735)

Kerr, R.J. "The Track Record: CIA Analysis from 1950 to 2000," in *Analyzing Intelligence: Origins, Obstacles, and Innovations,* eds. R.Z. George & J.B. Bruce, 2008, pp. 35. (RW 3094)

Kerr, R. & Wolfe, T. "A Holistic Vision for the Analytic Unit," *Studies in Intelligence,* Vol. 50, No. 2, 2006, pp. 47-55. (RW 1553)

Kerr, R., Wolfe, T., Donegan, R. & Pappas, A. *Intelligence and Analysis on Iraq: Issues for the Intelligence Community* 2004. (RW 944)

Kerr, R., Wolfe, T., Donegan, R. & Pappas, A. "Collection and Analysis on Iraq: Issues for the US Intelligence Community," *Studies in Intelligence,* Vol. 49, No. 3, 2005, pp. 47-54. (RW 1530)

Kerr, S. "On the Folly of Rewarding A, while Hoping for B," *The Academy of Management Executive,* Vol. 9, No. 1, 1995, pp. 7-14. (RW 4856)

Kerr, S. "The Debate on US Post-Cold War Intelligence: One More New Botched Beginning?" *Defense Analysis,* Vol. 10, No. 3, 1994, pp. 323-350. (RW 80)

Kesselman, R.F. *Verbal Probability Expressions in National Intelligence Estimates: A Comprehensive Analysis of Trends from the Fifties through Post 9/11,* 2008. (RW 3125)

Kettle, K.L. & Haeubl, G. "Motivation by Anticipation: Expecting Rapid Feedback Enhances Performance," *Psychological Science,* 2010 (RW 3993)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Keysar, B., Ginzel, L.E. & Bazerman, M.H. "States of Affairs and States of Mind: The Effect of Knowledge on Beliefs," *Organizational Behavior and Human Decision Processes*, Vol. 64, No. 3, 1995, pp. 283. (RW 2359)

Khalsa, S. *Forecasting Terrorism: Indicators and Proven Analytic Techniques*, Scarecrow Press, Lanham, Md, 2004. (RW 1689)

Khalsa, S. *Terrorism Forecasting: A Web-Based Methodology*, Joint Military Intelligence College, Washington, DC, 2004. (RW 773)

Khalsa, S. "Forecasting Terrorism: Indicators and Proven Analytic Techniques", McLean, Virginia, May 2-6, 2005 (RW 3062)

Kibbe, J. "Congressional Oversight of Intelligence: Is the Solution Part of the Problem?" *Intelligence and National Security*, Vol. 25, No. 1, 2010, pp. 24. (RW 3936)

Kienhues, D., Bromme, R. & Stahl, E. "Changing Epistemological Beliefs: The Unexpected Impact of a Short-Term Intervention," *British Journal of Educational Psychology*, Vol. 78, No. 4, 2008, pp. 545-565. (RW 5267)

Kim, C. & Keller, J.M. "Motivation, Volition and Belief Change Strategies to Improve Mathematics Learning," *Journal of Computer Assisted Learning*, Vol. 26, No. 5, 2010, pp. 407-420. (RW 5243)

Kim, J. & Allard, W.M. "Intelligence Preparation of the Battlespace: A Methodology for Homeland Security Intelligence Analysis," *SAIS Review*, Vol. 28, No. 1, 2008, pp. 75. (RW 3327)

Kim, P.H. "When Private Beliefs Shape Collective Reality: The Effects of Beliefs about Coworkers on Group Discussion and Performance," *Management Science*, Vol. 49, No. 6, 2003, pp. 801. (RW 2354)

Kim, S.H. *Max Weber*. Available: http://plato.stanford.edu/cgi-bin/encyclopedia/archinfo.cgi?entry=weber, Viewed: October 10, 2011. (RW 5162)

Kim, S., Taber, C.S. & Lodge, M. "A Computational Model of the Citizen as Motivated Reasoner: Modeling the Dynamics of the 2000 Presidential Election," *Political Behavior*, Vol. 32, 2010, pp. 1-28. (RW 5455)

Kimminau, J. "A Culminating Point for Air Force Intelligence, Surveillance, and Reconnaissance," *Air & Space Power Journal*, Vol. 26, No. 6, 2012, pp. 113-129. (RW 5865)

Kimminau, J.A. *The Serious Warrior: On Developing a Professional Military Mind*, Air University, Maxwell AFB, AL, 2004. (RW 3562)

Kincaid, B. "Futures-Based Analytical Approach," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 44-53. (RW 3609)

Kinchin, I.M., Hatzipanagos, S. & Turner, N. "Epistemological Separation of Research and Teaching among Graduate Teaching Assistants," *Journal of Further and Higher Education*, Vol. 33, No. 1, 2009, pp. 45-55. (RW 5234)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Kind, S.S. "Heuristic in Crime Investigation " *Journal of the Forensic Science Society,* Vol. 28, No. 3, 1988, pp. 205-206. (RW 5583)

Kindsvater, L.C. "The Need to Reorganize the Intelligence Community," *Studies in Intelligence,* Vol. 47, No. 1, 2003, pp. 33-37. (RW 116)

King, B.A. & Magun-Jackson, S. "Differences in Engineering Students'a Beliefs about Knowledge Across Educational Levels", *ASQ Advancing the STEM Agenda in Education, the Workplace, and Society,* University of Wisconsin-Stout, July 19-20, 2011 (RW 5073)

King, B. & Magun-Jackson, S. "Epistemological Beliefs of Engineering Students," *Journal of Technology Studies,* Vol. 35, No. 2, 2009, [unpaged]. (RW 5013)

King, G. *A Solution to the Ecological Inference Problem: Reconstructing Individual Behavior from Aggregate Data.* Princeton University Press, Princeton, NJ, 1997. (RW 5374)

King, G., Keohane, R.O. & Verba, S. *Designing Social Inquiry: Scientific Inference in Qualitative Research,* Princeton University Press, Princeton, NJ, 1994. (RW 679)

King, P.M. "Formal Reasoning in Adults: A Review and Critique," in *Adult Cognitive Development: Methods and Models*, eds. R.A. Mines & K.S. Kitchener, Praeger, New York, NY, 1986, pp. 1-21. (RW 4899)

King, P.M. "The Role of the Cognitive Dimension of Self-Authorship," in *Development and Assessment of Self-Authorship: Exploring the Concept Across Cultures*, eds. M.B. Baxter Magolda, E.G. Creamer & P.S. Meszaros, Stylus Pub., Sterling, VA, 2010, pp. 167-186. (RW 4762)

King, P.M. & Kitchener, K.S. *Developing Reflective Judgment: Understanding and Promoting Intellectual Growth and Critical Thinking in Adolescents and Adults,* Jossey-Bass Publishers, San Francisco, CA, 1994. (RW 2555)

King, P.M. & Kitchener, K.S. "The Reflective Judgment Model: Twenty Years of Research on Epistemic Cognition," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing*, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 37-61. (RW 2658)

King, P.M. & Kitchener, K.S. "Reflective Judgment: Theory and Research on the Development of Epistemic Assumptions through Adulthood," *Educational Psychologist,* Vol. 39, No. 1, 2004, pp. 5-18. (RW 4270)

King, P.M., Wood, P.K. & Mines, R.A. "Critical Thinking among College and Graduate Students," *The Review of Higher Education,* Vol. 13, No. 2, 1990, pp. 167-186. (RW 4038)

King-Casas, B., Sharp, C., Lomax-Bream, L., Lohrenz, T., Fonagy, P. & Montague, R. "The Rupture and Repair of Cooperation in Borderline Personality Disorder," *Science,* Vol. 321, 2008, pp. 806. (RW 3316)

Kirby, B.C. "Teaching to Think," *Journal of Education,* Vol. 116, No. 14, 1933, pp. 363-364. (RW 4484)

Kirby, D. & Kuykendall, C. *Mind Matters: Teaching for Thinking,* Boynton/Cook Publishers, Portsmouth, NH, 1991. (RW 3698)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Kirsch, I. *How Expectancies Shape Experience*, American Psychological Association, Washington, DC, 1999. (RW 2149)

Kirschenbaum, S.S., McInnis, S.L. & Correll, K.P. "Contrasting Submarine Specialty Training: Sonar and Fire Control," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 271-285. (RW 5145)

Kirshner, D. & Whitson, J.A. "Editors' Introduction to *Situated Cognition: Social, Semiotic, and Psychological Perspectives*," in *Situated Cognition: Social, Semiotic, and Psychological Perspectives*, eds. D. Kirshner & J.A. Whitson, L. Erlbaum Associates, Mahwah, NJ, 1997, pp. 1-16. (RW 5351)

Kirton, M.J. "A Reanalysis of Two Scales of Tolerance of Ambiguity," *Journal of Personality Assessment*, Vol. 45, No. 4, 1981, pp. 407-414. (RW 5252)

Kitaoka, H. *Intelligence in Deep Trouble*, Institute for International Policy Studies, Tokyo, Japan, 2003. (RW 496)

Kitchener, K.S. "The Reflective Judgment Model: Characteristics, Evidence, and Measurement," in *Adult Cognitive Development: Methods and Models*, eds. R.A. Mines & K.S. Kitchener, Praeger, New York, NY, 1986, pp. 76-91. (RW 4998)

Kitchenham, B. *Procedures for Performing Systematic Reviews*, TR/SE-0401, 2004. (RW 3852)

Kizilgunes, B., Tekkaya, C. & Sungur, S. "Modeling the Relations among Students' Epistemological Beliefs, Motivation, Learning Approach, and Achievement," *Journal of Educational Research*, Vol. 102, No. 4, 2009, pp. 243-256. (RW 5430)

Klabbers, J.H.G. "Problem Framing through Gaming: Learning to Manage Complexity, Uncertainty, and Value Adjustment," *Simulation & Gaming*, Vol. 27, No. 1, 1996, pp. 74. (RW 2683)

Klaczynski, P.A. & Narasimham, G. "Development of Scientific Reasoning Biases: Cognitive Versus Ego-Protective Explanations," *Developmental Psychology*, Vol. 34, No. 1, 1998, pp. 175-187. (RW 2325)

Klaczynski, P.A., Gordon, D.H. & Fauth, J. "Goal-Oriented Critical Reasoning and Individual Differences in Critical Reasoning Biases," *Journal of Educational Psychology*, Vol. 89, No. 3, 1997, pp. 470-485. (RW 4945)

Klaczynski, P.A. & Robinson, B. "Personal Theories, Intellectual Ability, and Epistemological Beliefs: Adult Age Differences in Everyday Reasoning Biases," *Psychology and Aging*, Vol. 15, No. 3, 2000, pp. 400-416. (RW 3850)

Klahr, D. & Carver, S.M. "Scientific Thinking about Scientific Thinking," *Monographs of the Society for Research in Child Development*, Vol. 60, No. 4, 1995, pp. 137. (RW 1892)

Klahr, D. & Simon, H.A. "Studies of Scientific Discovery: Complementary Approaches and Convergent Findings," *Psychological Bulletin*, Vol. 125, No. 5, 1999, pp. 524. (RW 1890)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Klahr, D. & Simon, H.A. "What have Psychologists (and Others) Discovered about the Process of Scientific Discovery?" *Current Directions in Psychological Science,* Vol. 10, No. 3, 2001, pp. 75. (RW 1889)

Klahr, D. "Searching for Cognition in Cognitive Models of Science," *Psycoloquy,* Vol. 5, No. 69, 1994 (RW 1761)

Klahr, D., Dunbar, K., Fay, A.L., Penner, D. & Schunn, C.D. *Exploring Science: The Cognition and Development of Discovery Processes,* MIT Press, Cambridge, MA, 2000. (RW 1834)

Klauer, K.C., Beller, S. & Hutter, M. "Conditional Reasoning in Context: A Dual-Source Model of Probabilistic Inference," *Journal of Experimental Psychology: Learning, Memory and Cognition,* Vol. 36, No. 2, 2010, pp. 298-323. (RW 5723)

Klauser, H.A. *Writing on both Sides of the Brain: Breakthrough Techniques for People Who Write,* Perennial Library, San Francisco, 1987. (RW 1849)

Klayman, J. "Varieties of Confirmation Bias," *The Psychology of Learning and Motivation,* Vol. 32, 1995, pp. 385-418. (RW 4857)

Klayman, J. & Ha, T. "Confirmation, Disconfirmation, and Information in Hypothesis Testing," *Psychological Review,* Vol. 94, 1987, pp. 211. (RW 2122)

Klayman, J., Soll, J.B., Gonzalez-Vallejo, C. & Barlas, S. "Overconfidence: It Depends on How, What, and Whom You Ask," *Organizational Behavior and Human Decision Processes,* Vol. 79, No. 3, 1999, pp. 216. (RW 3299)

Klein, E.L. *Children and Computers,* Jossey-Bass, San Francisco, 1985. (RW 4422)

Klein, G.A. & Weitzenfeld, J. "Improvement of Skills for Solving Ill-Defined Problems," *Educational Psychologist,* Vol. 13, No. 1, 1978, pp. 31. (RW 3772)

Klein, G. "Critical Thoughts about Critical Thinking," *Theoretical Issues in Ergonomics Science,* Vol. 12, No. 33, 2011, pp. 210-224. (RW 5206)

Klein, G.A. *Sources of Power: How People make Decisions,* MIT Press, Cambridge, MA, 1998. (RW 659)

Klein, G.A. *The Power of Intuition: How to use Your Gut Feelings to make Better Decisions at Work,* Currency/Doubleday, New York, 2004. (RW 2964)

Klein, G.L. "Intelligence Analysis Problems with Open-Ended Solution Spaces: Testing and Evaluation of Systems," *ITEA Journal,* September October, 2003, pp. 55. (RW 1336)

Klein, G.L. & Adelman, L. "A Collaboration Evaluation Framework," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 795)

Klein, G.L., Drury, J.L., Pfaff, M. & More, L. "COAction: Enabling Collaborative Option Awareness", *15th International Command and Control Research and Technology Symposium,* Santa Monica, CA, June 22-24, 2010 (RW 5680)

Klein, G. & Hoffman, R.R. "Macrocognition, Mental Models, and Cognitive Task Analysis Methodology," in *Naturalistic Decision Making and Macrocognition,* ed. J.M. Schraagen, Ashgate, Aldershot, England; Burlington, VT, 2008, pp. 57. (RW 3306)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Klein, G., Moon, B. & Hoffman, R.R. "Making Sense of Sensemaking 1: Alternative Perspectives," *IEEE Intelligent Systems,* Vol. 21, No. 4, 2006, pp. 70-73. (RW 2540)

Klein, G., Moon, B. & Hoffman, R.R. "Making Sense of Sensemaking 2: A Macrocognitive Model," *IEEE Intelligent Systems,* Vol. 21, No. 5, 2006, pp. 88. (RW 2541)

Klein, G., Phillips, J.K., Rall, E.L. & Peluso, D.A. "A Data-Frame Theory of Sensemaking," in *Expertise Out of Context,* ed. R.R. Hoffman, 2007, pp. 113-155. (RW 2767)

Klein, K. & Boals, A. "Expressive Writing can Increase Working Memory Capacity," *Journal of Experimental Psychology: General,* Vol. 130, No. 3, 2001, pp. 520. (RW 2073)

Kleinmuntz, B. "Why we Still use our Heads Instead of Formulas: Toward an Integrative Approach," *Psychological Bulletin,* Vol. 107, No. 3, 1990, pp. 296. (RW 2867)

Kleinmuntz, D.N. & Schkade, D.A. "Information Displays and Decision Processes," *Psychological Science,* Vol. 4, No. 4, 1993, pp. 221. (RW 4150)

Kleinmuntz, D.N. "Decomposition and the Control of Error in Decision-Analytic Models," in *Insights in Decision Making: A Tribute to Hillel J. Einhorn,* ed. R.M. Hogarth, University of Chicago Press, Chicago, 1990, pp. 107. (RW 2866)

Kleinsmith, E. "Teaching Analytic Best Practices [Powerpoint Presentation]", *Global Intelligence Forum 2010,* Dungarvan, Ireland, July 11-13, 2010 (RW 4227)

Klemp, G.O. & McClelland, D.C. "What Characterizes Intelligent Functioning among Senior Managers?" in *Practical Intelligence: Nature and Origins of Competence in the Everyday World,* eds. R.J. Sternberg & R.K. Wagner, Cambridge University Press, Cambridge Cambridgeshire; New York, 1986, pp. 31. (RW 3253)

Klimek, P., Lambiotte, R. & Thurner, S. "Opinion Formation in Laggard Societies," *Europhysics Letters,* Vol. 82, 2008 (RW 3070)

Kloda, L.A., Koufogiannakis, D. & Mallan, K. "Transferring evidence into practice: what evidence summaries of library and information studies research tell practitioners", *Information Research,* [Online], vol. 16, no. 1, paper 465. Available from: http://InformationR.net/ir/16-1/paper465.html. 2011, (RW 4791)

Kluever, J. "A Mathematical Theory of Communications: Meaning, Information and Topology," *Complexity,* Vol. 16, No. 3, 2010, pp. 10-26. (RW 4524)

Knapp, C.E. "Jean Louis Rodolphe Agassiz," in *Sourcebook of Experiential Education: Key Thinkers and their Contributions,* eds. T.E. Smith & C. Knapp, Routledge, New York, 2011, pp. 86-92. (RW 4924)

Knapp, F.A. "Style and Stereotypes in Intelligence Studies," *Studies in Intelligence,* Vol. 8, No. 2, 1964, pp. A1-A5. (RW 557)

Knapp, F.A.J. "Styles and Stereotypes in Intelligence Studies," *Studies in Intelligence,* Vol. 8, No. 2, 1964 (RW 4204)

Knorr, K.E. *Foreign Intelligence and the Social Sciences,* Princeton University, Princeton, NJ, 1964. (RW 932)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Knorr, K.E. & Morgan, P.M. *Strategic Military Surprise: Incentives and Opportunities,* Transaction Books, New Brunswick, NJ, 1983. (RW 713)

Knott, J.E. "Secrecy and Intelligence in a Free Society," *Studies in Intelligence,* Vol. 19, No. 2, 1975, pp. 1-8. (RW 554)

Knott, S. "Executive Power and the Control of American Intelligence," *Intelligence and National Security,* Vol. 13, No. 2, 1998, pp. 171-176. (RW 179)

Knutson, B., Rick, S., Wimmer, G.E., Prelec, D. & Loewenstein, G. "Neural Predictors of Purchases," *Neuron,* Vol. 53, 2007, pp. 147. (RW 1981)

Kobayashi, K., Wallis, P. & Thom, J.A. "Relevance Judgments for Assessing Recall," *Information Processing and Management,* Vol. 32, No. 3, 1996, pp. 213-286. (RW 757)

Kobayashi, M. *US Failures in the Pearl Harbor Attack: Lessons for Intelligence,* Master of Arts in Law and Diplomacy thesis, Tufts University, 2005. (RW 511)

Kober, S. *Why Spy? the Uses and Misuses of Intelligence,* Policy Analysis No. 265, Cato Institute, Washington, DC, 1996. (RW 415)

Koch, C. "The New Science of Change," *CIO Magazine,* 2006 (RW 1644)

Koedinger, K.R. & Roll, I. "Learning to Think: Cognitive Mechanisms of Knowledge Transfer," in *Oxford Handbook of Thinking and Reasoning,* eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 789-806. (RW 5506)

Koehler, J.J. "The Influence of Prior Beliefs on Scientific Judgments of Evidence Quality," *Organizational Behavior and Human Decision Processes,* Vol. 56, No. 1, 1993, pp. 28-55. (RW 2079)

Kogan, N. "Cognitive Styles as Moderators of Competence: A Commentary," in *Moderators of Competence,* eds. E.D. Neimark, R. De Lisi & J.L. Newman, L. Erlbaum Associates, Hillsdale, NJ, 1985, pp. 175-190. (RW 5098)

Kohler, R. *The Intelligence Industrial Base: Doomed to Extinction?* Consortium for the Study of Intelligence, Washington, DC, 1994. (RW 138)

Kohlschuetter, C. "Exploring the New York Times Corpus with NewsClub", *HCIR 2010: Proceedings of the Fourth Workshop on Human-Computer Interaction and Information Retrieval,* New Brunswick, NJ, August 22, 2010, pp. 37. (RW 4321)

Kokinov, B., Hristova, P. & Petkov, G. "Does Irrelevant Information Play a Role in Judgment?", *Proceedings of the 26th Annual Conference of the Cognitive Science Society,* pp.720. (RW 2002)

Kolodner, J.L. *Case-Based Reasoning,* Morgan Kaufmann Publishers, San Mateo, CA, 1993. (RW 2543)

Koopman, C., Snyder, J. & Jervis, R. "Theory-Driven Vs. Data-Driven Assessment in a Crisis: A Survey of International Security Readers," *Journal of Conflict Resolution,* Vol. 34, No. 4, 1990, pp. 694. (RW 2333)

Koriat, A. "When are Two Heads Better than One and Why?" *Science Magazine,* Vol. 336, No. 6079, 2012, pp. 360-362. (RW 5608)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Korte, R. "Learning how Things Work here: The Socialization of Newcomers in Organizations," in *Supporting Workplace Learning: Towards Evidence-Based Practice*, eds. R.F. Poell & M. van Woerkom, Springer, Dordrecht, 2011, pp. 129-146. (RW 4910)

Koslowski, B. *Theory and Evidence: The Development of Scientific Reasoning*, MIT Press, Cambridge, MA, 1996. (RW 2183)

Kosso, P. "Introduction: The Epistemology of Archaeology," in *Archaeological Fantasies: How Pseudoarchaeology Misrepresents the Past and Misleads the Public*, ed. G.G. Fagan, Routledge, London; New York, 2006, pp. 3-22. (RW 5118)

Kostoff, R.N., Block, J.A., Solka, J.L., Briggs, M.B., Rushenberg, R.L., Stump, J.A., Johnson, D., Lyons, T.J. & Wyatt, J.R. "Literature-Related Discovery," in *Annual Review of Information Science and Technology*, ed. B. Cronin, Medford, NJ, 2009, pp. 241. (RW 4343)

Koufogiannakis, D. "Evidence Based Practice: Science Or Art?" *Evidence Based Library and Information Practice*, Vol. 6, No. 1, 2011, pp. 1-2. (RW 4805)

Kouri, J. *Counterterrorists Need Better Intelligence Analysis*. Available: http://www.mail-archive.com/osint@yahoogroups.com/msg10633.html, Viewed: February 21, 2011. (RW 1)

Kouri, J. *The Politicization and Irrelevance of Intelligence Analysis*. Available: www.renewamerica.us/columns/kouri/060121, (RW 1253)

Kovacs, A. *The Uses and Nonuses of Intelligence*, CISAC, Stanford, CA, 1996. (RW 1077)

Kovacs, A. "The Nonuse of Intelligence," *International Journal of Intelligence and Counterintelligence*, Vol. 10, No. 4, 1997, pp. 383-417. (RW 60)

Kovacs, A. "Using Intelligence," *Intelligence and National Security*, Vol. 12, No. 4, 1997, pp. 145-164. (RW 33)

Kovalerchuk, B. "Advanced Data Mining, Link Discovery and Visual Correlation for Data and Image Analysis," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 808)

Kovalerchuk, B. "Advanced Data Mining, Link Discovery and Visual Correlation for Data and Image Analysis. Tutorial Notes [Powerpoint Presentation]," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 809)

Kovera, M.B., Borgida, E., Gresham, A.W. & Gray, E. "Does Expert Psychological Testimony Inform Or Influence Juror Decision Making? A Social Cognitive Analysis," *Journal of Applied Psychology*, Vol. 82, No. 1, 1997, pp. 178. (RW 2042)

Kovera, M.B., Russano, M.B. & McAuliff, B.D. "Assessment of the Commonsense Psychology Underlying Daubert: Legal Decision Makers' Abilities to Evaluate Expert Evidence in Hostile Work Environment Cases," *Psychology, Public Policy, and Law*, Vol. 8, No. 2, 2002, pp. 180. (RW 2033)

Kozak, M.N., Marsh, A.A. & Wegner, D.M. "What do I Think You're Doing? Action Identification and Mind Attribution," *Journal of Personality and Social Psychology*, Vol. 90, No. 4, 2006, pp. 543. (RW 2350)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Kozlowski, S.W.J. "The Science of Team Success," *Scientific American Mind,* Vol. 18, No. 3, 2007, pp. 54. (RW 3150)

Kozlowski, S.W.J. "Workforce Effectiveness: Acquiring Human Resources and Developing Human Capital," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, pp. 271-308. (RW 4781)

Krakovsky, M. "The Science of Lasting Happiness," *Scientific American,* March 18, 2007. (RW 2259)

Kramer, D. "The Ontogeny of Wisdom in its Variations," in *Handbook of Adult Development*, eds. J. Demick & C. Andreoletti, Kluwer Academic/Plenum, New York, 2003, pp. 131. (RW 4268)

Krantz, S.G. *Techniques of Problem Solving,* American Mathematical Society, Providence, R.I., 1997. (RW 2663)

Krathwohl, D.R. "A Revision of Bloom's Taxonomy: An Overview," *Theory Into Practice,* Vol. 41, No. 4, 2002, pp. 212. (RW 5442)

Krejci, J.W. "Imagery: Stimulating Critical Thinking by Exploring Mental Models," *Journal of Nursing Education,* Vol. 36, No. 10, 1997, pp. 482-484. (RW 3959)

Krepinevich, A.F. *The Army and Vietnam*, Johns Hopkins University Press, Baltimore, 1986. (RW 299)

Kreps, S.E. "Shifting Currents: Changes in National Intelligence Estimates on the Iran Nuclear Threat," *Intelligence and National Security,* Vol. 23, No. 5, 2008, pp. 608. (RW 3453)

Kretz, D. *Bringing Cognitive Science to the Intelligence Community*. Available: http://thehill.com/blogs/congress-blog/homeland-security/261695-bringing-cognitive-science-to-the-intelligence-community, Viewed: October 16, 2012. (RW 5832)

Kreulen, J., Modha, D., Spangler, S. & Strong, R. *An Interactive Approach to Document Classification* (RW 3281)

Krieger, S.H. "Domain Knowledge and the Teaching of Creative Legal Problem Solving," *Clinical Law Review*, Vol. 11, 2004, pp. 149. (RW 2668)

Krieger, W. "US Patronage of German Postwar Intelligence," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 91. (RW 2460)

Krikelas, J. "Information Seeking Behavior: Patterns and Concepts," *Drexel Library Quarterly*, Vol. 19, 1983, pp. 5. (RW 3416)

Krimsky, S. & Golding, D. *Social Theories of Risk*, Praeger, Westport, CT, 1992. (RW 1097)

Kringen, J.A. "How We've Improved Intelligence," *Washington Post*, April 3, 2006, (RW 1316)

Krippendorff, K. *Content Analysis: An Introduction to its Methodology*, 2nd ed., Sage, Thousand Oaks, CA, 2004. (RW 3528)

Kristof, N.D. "What? Me Biased?" *The New York Times*, October 30, 2008, (RW 3343)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Krizan, L. *Intelligence Essentials for Everyone,* Joint Military Intelligence College, Washington, DC, 1999. (RW 338)

Kroll, B. "Writing for Readers: Three Perspectives on Audience," *College Composition and Communication,* Vol. 35, No. 2, 1984, pp. 172-185. (RW 4479)

Kroll, B. "Arguing Differently," *Pedagogy,* Vol. 5, No. 1, 2005, pp. 37-60. (RW 4478)

Kroll, B.M. "Cognitive Egocentrism and the Problem of Audience Awareness in Written Discourse," *Research in the Teaching of English,* Vol. 12, 1978, pp. 269-281. (RW 4486)

Krosnick, J. & Alwin, D. "Aging and Susceptibility to Attitude Change," *Journal of Personality and Social Psychology,* Vol. 57, 1989, pp. 416. (RW 2755)

Krotow, G.S. *The Impact of Cognitive Feedback on the Performance of Intelligence Analysts,* M.S. Information Systems thesis, Naval Postgraduate School, 1992. (RW 1137)

Kroutter, P. & Witkin, H.A. *Field-Dependence Vs. Field-Independence Theory,* 2008. (RW 5276)

Krueger, J.I., Alicke, M.D. & Dunning, D. "Self as Source and Constraint of Social Knowledge," in *The Self in Social Judgment,* eds. M.D. Alicke, D. Dunning & J.I. Krueger, Psychology Press, New York, 2005, pp. 3. (RW 2885)

Kruger, J. & Dunning, D. "Unskilled and Unaware of it: How Difficulties in Recognizing One's Own Incompetence Lead to Inflated Self-Assessments," *Journal of Personality and Social Psychology,* Vol. 77, No. 6, 1999, pp. 1121-1134. (RW 205)

Kruglanski, A.W. & Gigerenzer, G. "Intuitive and Deliberate Judgments are Based on Common Principles," *Psychological Review,* Vol. 118, No. 1, 2011, pp. 97-109. (RW 5681)

Kruglanski, A.W. & Webster, D.M. "Motivated Closing of the Mind: "Seizing" and "Freezing"," *Psychological Review,* Vol. 103, No. 2, 1996, pp. 263-283. (RW 1933)

Krumenaker, L. "A Dillar, a Dollar...Where's that Online Article, Scholar?" *Searcher,* Vol. 7, No. 8, 1999, pp. 36. (RW 1566)

Krupat, E. *Critical Thinking in Medical Education: Assessing What We Mean and What We Know [Powerpoint Presentation]* 2008. (RW 4088)

Ku, K.Y.L. "Assessing Students' Critical Thinking Performance: Urging for Measurements using Multi-Response Format," *Thinking Skills and Creativity,* Vol. 4, No. 1, 2009, pp. 70-76. (RW 3973)

Kuchar, O.A., Hoeft, T.J., Havre, S. & Perrine, K.A. "Isn't it about Time?" *IEEE Computer Graphics and Applications,* Vol. 26, No. 3, 2006, pp. 80. (RW 1483)

Kuechler, W.L. & Vaishnavi, V. "So Talk to Me: The Effect of Explicit Goals on the Comprehension of Business Process Narratives," *MIS Quarterly,* Vol. 30, No. 4, 2006, pp. 961. (RW 2346)

Kuenzer, A.Z., Lanzarini, W.L. & Taveira, E.B. "Concept Mapping in Corporate Education: Experiences at Petrobras University," in *Applied Concept Mapping: Capturing, Analyzing, and*

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Organizing Knowledge, eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 215-228. (RW 4973)

Kuhlthau, C.C., Heinstrom, J. & Todd, R.J. "The 'information search process' revisited: is the model still useful?" *Information Research,* [Online], vol. 13, no. 4, paper 355. Available from: http://InformationR.net/ir/13-4/paper355.html2008, (RW 4785)

Kuhlthau, C.C. *Seeking Meaning: A Process Approach to Library and Information Services,* Ablex Pub. Corp., Norwood, NJ, 1993. (RW 2145)

Kuhlthau, C.C. *Seeking Meaning: A Process Approach to Library and Information Services,* 2nd ed., Libraries Unlimited, Westport, CT, 2004. (RW 2146)

Kuhn, D. "Thinking as Argument," *Harvard Educational Review,* Vol. 62, 1992, pp. 155. (RW 2690)

Kuhn, D., Cheney, R. & Weinstock, M. "The Development of Epistemological Understanding," *Cognitive Development,* Vol. 15, No. 3, 2000, pp. 309-328. (RW 2433)

Kuhn, D. & Dean, D. "Connecting Scientific Reasoning and Causal Inference," *Journal of Cognition and Development,* Vol. 5, No. 2, 2004, pp. 261. (RW 2190)

Kuhn, D. & Dean, D. "Is Developing Scientific Thinking all about Learning to Control Variables?" *Psychological Science,* Vol. 16, No. 11, 2005, pp. 866. (RW 2191)

Kuhn, D., Katz, J. & Dean, D. "Developing Reason," *Thinking & Reasoning,* Vol. 10, No. 2, 2004, pp. 197-219. (RW 2188)

Kuhn, D. & Phelps, E. "The Development of Problem-Solving Strategies," *Advances in Child Development and Behavior,* Vol. 17, 1982 (RW 2336)

Kuhn, D., Schauble, L. & Garcia-Mila, M. "Cross-Domain Development of Scientific Reasoning," *Cognition and Instruction,* Vol. 9, No. 4, 1992, pp. 285. (RW 2189)

Kuhn, D. "Reasoning about Multiple Variables: Control of Variables is Not the Only Challenge," *Science Education,* in press, (RW 2211)

Kuhn, D. *The Skills of Argument,* Cambridge University Press, Cambridge, UK, 1991. (RW 2408)

Kuhn, D. "Connecting Scientific and Informal Reasoning," *Merrill-Palmer Quarterly,* Vol. 39, No. 1, 1993, pp. 74-103. (RW 1885)

Kuhn, D. "A Developmental Model of Critical Thinking," *Educational Researcher,* Vol. 28, No. 2, 1999, pp. 16-25+. (RW 4015)

Kuhn, D. "How do People Know?" *Psychological Science,* Vol. 12, No. 1, 2001, pp. 1-8. (RW 2322)

Kuhn, D. "What is Scientific Thinking and How Does it Develop?" in *Blackwell Handbook of Childhood Cognitive Development,* ed. U.C. Goswami, Blackwell, Malden, MA, 2004, pp. 371. (RW 2184)

Kuhn, D. *Education for Thinking,* Harvard University Press, Cambridge, MA, 2005. (RW 2207)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Kuhn, D. "Jumping to Conclusions," *Scientific American Mind,* Vol. 18, No. 1, 2007, pp. 44. (RW 3147)

Kuhn, D. & Weinstock, M. "What is Epistemological Thinking and Why does it Matter?" in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing*, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 121-144. (RW 2337)

Kuhn, D., White, S.H., Klahr, D. & Carver, S.M. *Strategies of Knowledge Acquisition,* Society for Research in Child Development, Chicago, IL, 1995. (RW 2185)

Kuhns, W. "The Office of Reports and Estimates: CIA's First Center for Analysis," *Studies in Intelligence,* Vol. 51, No. 2, 2007, pp. 27. (RW 2500)

Kuhns, W.J. "Intelligence Failures: Forecasting and the Lessons of Epistemology," in *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel*, eds. M.I. Handel, R.K. Betts & T.G. Mahnken, Frank Cass, London, UK, 2003, pp. 80-100. (RW 217)

Kulacki, G. & Wright, D. *A Military Intelligence Failure? The Case of the Parasite Satellite,* Union of Concerned Scientists, Cambridge, MA, 2004. (RW 491)

Kules, W., Wilson, M.L., Schraefel, M.C. & Shneiderman, B. *From Keyword Search to Exploration: How Result Visualization Aids Discovery on the Web,* 2008. (RW 4403)

Kulkin, C.R. *The Cognitive Thinking Style Workbook,* Institute for Motivational Living, Inc., Boardman, OH, 2007. (RW 3782)

Kulkin, S.G. *The Cognitive Thinking Style Workbook: Understanding how You Think* [unknown] (RW 2373)

Kumar, A., Soares, H. & Serdarevic, F. "Totality of Evidence: One of the Keys to Better Oncology Management," *Journal of Oncology Management,* Vol. 14, No. 1, 2005, pp. 12. (RW 2230)

Kunda, Z. & Thagard, P. "Forming Impressions from Stereotypes, Traits, and Behaviours: A Parallel-Constraint-Satisfaction Theory," *Psychological Review,* Vol. 103, No. 2, 1996, pp. 284. (RW 1837)

Kunda, Z. "The Case for Motivated Reasoning," *Psychological Bulletin,* Vol. 108, No. 3, 1990, pp. 480-498. (RW 2166)

Kunstler, B. "Rethinking Thinking: Three Methods for Achieving More Creative, Responsive Strategic Intelligence Analysis," in *Proteus Futures Digest: A Compilation of Selected Works Derived from the 2007 Proteus Workshop*, eds. J. Auger & W. Wimbish, 2nd ed., U.S. Army War College, Carlisle Barracks, PA, 2007, pp. 199-217. (RW 4813)

Kupchinsky, R. *Information Revolution Feeds Alternative Intelligence Market. Radio Free Europe Broadcast.* 2005. (RW 417)

Kurfiss, J.G. *Critical Thinking: Theory, Research, Practice, and Possibilities,* ASHE-ERIC Higher Education Report No. 2, Association for the Study of Higher Education, Washington, DC, 1988. (RW 4134)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Kurtz, C.F. & Snowden, D.J. "The New Dynamics of Strategy: Sense-Making in a Complex and Complicated World," *IBM Systems Journal,* Vol. 42, No. 3, 2003, pp. 462. (RW 2561)

Kuszewski, A. "You can increase your intelligence: 5 ways to maximize your cognitive potential", *Scientific American,* [Online], Available from: http://www.scientificamerican.com/blog/post.cfm?id=you-can-increase-your-intelligence-2011-03-07. 2011. (RW 4600)

Kuutti, K. "Work Processes: Scenarios as a Preliminary Vocabulary," in *Scenario-Based Design: Envisioning Work and Technology in Systems Development,* ed. J.M. Carroll, Wiley, New York, 1995, pp. 19. (RW 3394)

Kwok, K.L., Deng, P., Dinstl, N., Sun, H.L., Xu, W., Peng, P. & Doyon, J. "CHINET: A Chinese Name Finder System for Document Triage," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 884)

Kwok, K.L., Grunfeld, L., Chan, M., Dinstl, N. & Cool, C. *TREC-7 Ad-Hoc, High Precision and Filtering Experiments using PIRCS* (RW 1562)

Kwon, Y., Lee, J., Shin, D. & Jeong, J. "Changes in Brain Activation Induced by the Training of Hypothesis Generation Skills: An fMRI Study," *Brain and Cognition,* [in press] (RW 3300)

Kyl, F. *The Rumsfeld Commission Report. Comments.* 1998. (RW 1234)

Kyllonen, P.C. & Christal, R.E. "Reasoning Ability is (Little More than) Working Memory Capacity?" *Intelligence,* Vol. 14, 1990, pp. 389. (RW 2434)

Kyza, E.A. "Investigating Students' Collaborative Scientific Reasoning during a Natural Selection Investigation", *Proceedings of the 6th International Conference on Learning Science,* Santa Monica, CA, June 22-26, 2004, pp. 294. (RW 1886)

Lacey, E.J. "Intel Analysis in Academic Research," *American Intelligence Journal,* Vol. 5, No. 1, 1983, pp. 12-13. (RW 4384)

Lacey, E.J. "Game Theory in Intelligence Analysis," *American Intelligence Journal,* Vol. 6, No. 3, 1984, pp. 20-25. (RW 4383)

Lachman, R., Lachman, J.L. & Butterfield, E. *Cognitive Psychology and Information Processing: An Introduction,* L. Erlbaum Associates, New York, NY, 1979. (RW 1061)

Lackie, R.J. *Those Dark Hiding Places: Revealing Secrets of the Invisible Web* (RW 1405)

Lackie, R.J. *Those Dark Hiding Places: Revealing Secrets of the Invisible Web (Version 2)* (RW 1476)

Lagnado, D. "How Do Scientists Think?" *Science Magazine,* Vol. 313, No. 5792, 2006 (RW 3003)

Lagnado, D. "Thinking about Evidence," in *Evidence, Inference and Enquiry,* eds. P. Dawid, W. Twining & M. Vasilaki, 2011, pp. 183-224. (RW 5631)

Lahneman, W. *Intelligence Policy and Organization. Course Description.* 2005. (RW 472)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Lahneman, W.J. *The Role of Intelligence in the Post 9/11 World,* Center for International and Security Studies at Maryland School of Public Affairs, University of Maryland, College Park, MD, 2002. (RW 1374)

Lahneman, W.J. *Knowledge Management: Essential Ingredient for Effective Intelligence Analysis,* 2003. (RW 1375)

Lahneman, W.J. "Outsourcing the IC's Stovepipes?" *International Journal of Intelligence and Counterintelligence,* Vol. 16, No. 4, 2003, pp. 573-593. (RW 56)

Lahneman, W.J. "Knowledge-Sharing in the Intelligence Community After 9/11," *International Journal of Intelligence and Counterintelligence,* Vol. 17, No. 4, 2004, pp. 614-633. (RW 351)

Lahneman, W.J. *The Future of Intelligence Analysis. Volume 1. Final Report.* Center for International and Security Studies at Maryland, College Park, MD, 2006. (RW 1636)

Lahneman, W.J. *The Future of Intelligence Analysis. Volume II. Annotated Bibliography: Publications on Intelligence Analysis and Reform.* 2006. (RW 1647)

Lahneman, W.J. "Is a Revolution in Intelligence Affairs Occurring?" *International Journal of Intelligence and Counterintelligence,* Vol. 20, No. 1, 2007, pp. 1. (RW 1754)

Lahneman, W.J. "The Need for a New Intelligence Paradigm," *International Journal of Intelligence and Counterintelligence,* Vol. 23, No. 2, 2010, pp. 201. (RW 3896)

Lahneman, W.J. *Keeping US Intelligence Effective: The Need for a Revolution in Intelligence Affairs,* Scarecrow Press, Lanham, MD, 2011. (RW 4723)

Lai, T. *Following Clues: Do's and Don't's* (RW 3919)

Lai, T. *A Radically New Look at Scientific Method* (RW 3917)

Lai, T. *What are Clues?* (RW 3920)

Lai, T. "How we make Discoveries," *Synthese,* Vol. 79, No. 3, 1989, pp. 361-392. (RW 3908)

Lai, T. "Discovery as a Problem for the Inventor," *British Journal of Philosophical Science,* Vol. 42, 1991, pp. 327. (RW 3912)

Lai, T. *Is Sherlock Holmes a Logician Or a Theseologist?* 2003. (RW 3916)

Lai, T. *The Art of Detection.* Available: http://plato.ucs.mun.ca/~tlai/Art/ArtTitle.htm, Viewed: March 23, 2012. (RW 3914)

Lai, T. *Following Clues: Making a Difficult Task a Little Easier* 2005. (RW 3915)

Lai, T. *The Art of Detection Aka Scientific Method Explained through Questions and Answers* 2006. (RW 3918)

Laipson, E. "The Robb-Silberman Report, Intelligence, and Nonproliferation," *Arms Control Today,* June, 2005 (RW 271)

Laird, S.K. & Rickard, J.T. "Voltaire: Insider Threat Modeling," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 882)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Lajoie, S.P. "Transitions and Trajectories for Studies of Expertise," *Educational Researcher,* Vol. 32, No. 8, 2003, pp. 21. (RW 2394)

Lajoie, S.P. "Cognitive Tools for the Mind: The Promises of Technology - Cognitive Amplifiers Or Bionic Prosthetics?" in *Intelligence and Technology: The Impact of Tools on the Nature and Development of Human Abilities,* eds. R.J. Sternberg & D. Preiss, L. Erlbaum Associates, Mahwah, N.J., 2005, pp. 87. (RW 2389)

Lajoie, S.P. "Developing Professional Expertise with a Cognitive Apprenticeship Model: Examples from Avionics and Medicine," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments,* ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 61-83. (RW 5136)

Lakoff, G. & Johnson, M. *Philosophy in the Flesh: The Embodied Mind and its Challenge to Western Thought,* Basic Books, New York, 1999. (RW 5917)

Lamanna, L. & Marrin, S. "Intelligence Studies," in *The International Studies Encyclopedia*, ed. R.A. Denemark, Blackwell Publishing, W. Sussex, UK, 2010, (RW 3929)

Lambert, M.E. "Test Review of the California Critical Thinking Skills Test [Revised]," in *The Eighteenth Mental Measurements Yearbook,* eds. R.A. Spies, J.F. Carlson & K.F. Geisinger, Buros Institute, 2010. (RW 5519)

Lampert, M. "When the Problem is Not the Question and the Solution is Not the Answer: Mathematical Knowing and Teaching," *American Educational Research Journal,* Vol. 27, No. 1, 1990, pp. 29-63. (RW 4656)

Lampert, N. "Critical Thinking Dispositions as an Outcome of Art Education," *Studies in Art Education,* Vol. 47, No. 3, 2006, pp. 215-228. (RW 5044)

Landes, D. "Slow Surprise: The Dynamics of Technology Synergy," in *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics,* ed. F. Fukuyama, Brookings Institution Press, Washington, DC, 2007, pp. 23-28. (RW 4697)

Landon-Murray, M. "Social Science and Intelligence Analysis: The Role of Intelligence Education," *Journal of Applied Security Research,* Vol. 6, No. 4, 2011, pp. 491-528. (RW 5537)

Landree, E., Silberglitt, R., Chow, B.G., Sherry, L. & Tseng, M.S. *A Delicate Balance: Portfolio Analysis and Management for Intelligence Information Dissemination Programs,* RAND Corp, Santa Monica CA, 2009. (RW 4556)

Landry, R.M. *Reforming Intelligence: Selling Change,* National Defense University. National War College, [undated]. (RW 448)

Langer, E.J. *Mindfulness,* Addison-Wesley Pub. Co., Reading, MA, 1989. (RW 4980)

Langley, P. *Scientific Discovery: Computational Explorations of the Creative Processes,* MIT Press, Cambridge, MA, 1987. (RW 1359)

Lanier, J. *You are Not a Gadget,* 2010. (RW 3836)

Lanir, Z. & Kahneman, D. "An Experiment in Decision Analysis in Israel in 1975," *Studies in Intelligence,* Vol. 50, No. 4, 2006 (RW 1970)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Lansing, J.S. & Axtell, R.L. "Afterword," in *Nonlinear Models for Archaeology and Anthropology: Continuing the Revolution*, eds. C.S. Beekman & W.W. Baden, Ashgate, Aldershot, England, 2005, pp. 139-145. (RW 5215)

Lanza, S.R. *Beyond the Internet [Powerpoint Presentation]* 2000. (RW 1440)

Lanza, S.R. *Beyond the Internet. [Speaker's Notes for Powerpoint Presentation]*. 2000. (RW 1441)

Lanzara, G.F. "The Design Process: Frames, Metaphors, and Games," in *Systems Design for, with, and by the Users: Proceedings of the IFIP WG 9.1 Working Conference on Systems Design for, with, and by the Users, Riva Del Sole, Italy, 20-24 September 1982*, eds. U. Briefs, C. Ciborra, L. Schneider & International Federation for Information Processing, North-Holland Pub. Co., Amsterdam, 1983, pp. 457. (RW 2591)

Laqueur, W. *The Question of Judgment: Intelligence and Medicine* 1983. (RW 1285)

Laqueur, W. "The Future of Intelligence," *Society,* Vol. 23, No. 1, 1985, pp. 3-11. (RW 1190)

Laqueur, W. *A World of Secrets: The Uses and Limits of Intelligence*, Basic Books, New York, NY, 1985. (RW 23)

Laqueur, W. *The Uses and Limits of Intelligence,* Transaction Publishers, New Brunswick, NJ, 1993. (RW 1102)

Laqueur, W. "The Future of Intelligence (Assessment of the Social Role of the Intelligence Service)," *Society,* Vol. 35, No. 2, 1998, pp. 301-311. (RW 401)

Laran, J. "Goal Management in Sequential Choices: Consumer Choices for Others are More Indulgent than Personal Choices," *Journal of Consumer Research,* Vol. 37, 2010, pp. 304. (RW 4215)

Larichev, O.I. & Moshkovich, E.M. *Verbal Decision Analysis for Unstructured Problems,* Kluwer Academic Publishers, Boston, 1997. (RW 2528)

Larkin, J.H., McDermott, J., Simon, H.A. & Simon, D.P. "Expert and Novice Performances in Solving Physics Problems," *Science,* Vol. 2, No. 8, 1980, pp. 1335. (RW 4149)

Larrick, R.P. "Debiasing," in *Blackwell Handbook of Judgment and Decision Making*, eds. D.J. Koehler & N. Harvey, Blackwell, Malden, MA, 2004, pp. 316-337. (RW 2823)

Larson, B. "Concept Mapping on the Road: Applied Business Concept Mapping in Software Implementation and Training Consulting," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge*, eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 93-108. (RW 4968)

Larson, E.V., Eaton, D., Nichiporuk, B. & Szayna, T.S. *Assessing Irregular Warfare: A Framework for Intelligence Analysis* 2008. (RW 3434)

Laske, O.E. "Four Uses of Self in Cognitive Science: The No-Man's Land between Mindware and Mind," in *Brain, Mind, and Physics*, eds. P. Pylkkänen, P. Pylkkö & A. Hautamäki, IOS Press, Amsterdam, 1997, pp. 13-25. (RW 5701)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Laskey, K.B., Schum, D.A., Costa, P.C.G. & Janssen, T. "Ontology of Evidence", *Proceedings of the Third International Ontology for the Intelligence Community Conference OIC-2008,* Fairfax, VA, December 3-4, 2008, pp. 20-24. (RW 4827)

Lasswell, H.D. "The Structure and Function of Communication in Society," in *The Communication of Ideas: A Series of Addresses*, ed. L. Bryson, Institute for Religious and Social Studies, New York, NY, 1948, pp. 37-51. (RW 4997)

Latham, D. *A View from Inside OSD,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1986. (RW 1016)

Lauber, T.B. & Knuth, B.A. "Educating Citizens about Controversial Issues: The Case of Suburban Goose Management," *Society and Natural Resources,* Vol. 15, 2002, pp. 581. (RW 2536)

Laughlin, P.R., VanderStoep, S.W. & Hollingshead, A.B. "Collective Versus Individual Induction: Recognition of Truth, Rejection of Error, and Collective Information Processing," *Journal of Personality and Social Psychology,* Vol. 61, No. 1, 1991, pp. 50-67. (RW 1921)

Lauren, P.G. *Diplomacy: New Approaches in History, Theory, and Policy,* Free Press, New York, 1979. (RW 3558)

Laurie, C. "A New President, a Better CIA, and an Old War: Eisenhower and Intelligence Reporting on Korea, 1953," *Studies in Intelligence,* Vol. 54, No. 4, 2010, pp. 1-12. (RW 4759)

Lave, J. "The Culture of Acquisition," in *Situated Cognition: Social, Semiotic, and Psychological Perspectives*, eds. D. Kirshner & J.A. Whitson, L. Erlbaum Associates, Mahwah, NJ, 1997, pp. 17-35. (RW 5368)

Lavelle, E. & Guarino, A.J. "A Multidimensional Approach to Understanding College Writing Processes," *Educational Psychology,* Vol. 23, No. 3, 2003, pp. 295-305. (RW 3518)

Lavoix, H. *Enabling Security for the 21st Century: Intelligence & Strategic Foresight and Warning,* S. Rajaratnam School of International Studies, Singapore, 2010. (RW 5760)

Lawal, I. "Science Resources: Does the Internet Make Them Cheaper, Better?" *The Bottom Line: Managing Library Finances,* Vol. 15, No. 3, 2002, pp. 116. (RW 1540)

Lawless, S., O'Connor, A. & Mulwa, C. "A Proposal for the Evaluation of Adaptive Personalized Information Retrieval", *Proceedings of the 2nd International Workshop on Contextual Information Access, Seeking and Retrieval Evaluation,* Milton Keynes, UK, March 28, 2010 (RW 4867)

Lawlor, M. "Googlizing Intelligence," *Signal Online,* June, 2010 (RW 4142)

Lawrence, R. *Global Reach Laydown,* Center for Information Policy Research, Harvard University, Cambridge, MA, 1995. (RW 1168)

Lawson, A.E. & Worsnop, W.A. "Learning about Evolution and Rejecting a Belief in Special Creation: Effects of Reflective Reasoning Skill, Prior Knowledge, Prior Belief and Religious Commitment," *Journal of Research in Science Teaching,* Vol. 29, No. 2, 1992, pp. 143-66. (RW 5093)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Law-Yone, H. "Problem Framing through Gaming and Problematic Games: A Response to Klabbers," *Simulation & Gaming,* Vol. 27, No. 1, 1996, pp. 93. (RW 2684)

Lazear, D.G. "Teaching For, With, and About Multiple Intelligences," in *Developing Minds: A Resource Book for Teaching Thinking*, ed. A.L. Costa, 3rd ed., Association for Supervision and Curriculum Development, Alexandria, VA, 2001, pp. 202-210. (RW 5254)

Leach, J. & Lewis, J. "The Role of Students' Epistemological Knowledge in The Process of Conceptual Change in Science," in *Reconsidering Conceptual Change: Issues in Theory and Practice*, eds. M. Limón & L. Mason, Kluwer Academic, Dordrecht, 2002, pp. 201-216. (RW 5005)

LeBoeuf, R.A. & Shafir, E.B. "Decision Making," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 243-265. (RW 4005)

Lebow, R.N. & Stein, J.G. *We All Lost the Cold War,* Princeton University Press, Princeton, NJ, 1994. (RW 5573)

Ledeen, M. *Bonded to Dysfunction* 2008. (RW 3257)

Lederer, J.M. "Disposition Toward Critical Thinking Among Occupational Therapy Students," *American Journal of Occupational Therapy*, Vol. 61, No. 5, 2007, pp. 519-526. (RW 5045)

Lederman, G. "Making Intelligence Reform Work," *The American Interest,* Vol. 14, No. 4, 2009, pp. 23. (RW 3427)

Lederman, N.G. "Nature of Science: Past, Present and Future," in *Handbook of Research on Science Education,* eds. S.K. Abell & N.G. Lederman, L. Erlbaum Associates, Mahwah, NJ, pp. 831-880. (RW 5515)

Lee, C.Y., Davis, T.E. & Noji, E.K. "Suicide Bombing of the Mineralnye Vody Train: Case Study in using Open-Source Information for Open-Source Health Intelligence," *Prehospital and Disaster Medicine,* Vol. 22, No. 4, 2007, pp. 276-280. (RW 2925)

Lee, J.H. *Online Searching: The Basics, Settings & Management*, Libraries Unlimited, Littleton, CO, 1984. (RW 3462)

Lee, R. "METS as a Tool to Support Intelligence Analysis," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 858)

Lee, R. "The use of Ontologies to Support Intelligence Analysis", *Proceedings of the Second International Ontology for the Intelligence Community Conference OIC-2007*, Columbia, MD, November 28-29, 2007, pp. 19-22. (RW 4816)

Lee, R. "Using New Standards to Develop IC Ontologies", *Fifth International Conference on Semantic Technology for Intelligence, Defense, and Security*, Fairfax, VA, 26-29 October 2010 (RW 4754)

Leedom, D.K. & Eggleston, R.G. "Anticipatory Understanding of Adversary Intent: A Signature-Based Knowledge System", *14th Iccrts,* Washington, DC, June 15-17, 2009 (RW 3552)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Leedom, D.K., Eggleston, R.G. & Ntuen, C.A. *Engineering Complex Human-Technological Work Systems - a Sensemaking Approach* 2007. (RW 2539)

Leedom, D.K., Noble, D.F., Pineau, B.C. & Eggleston, R.G. *A Work-Centered Tool for Assessing the Operational Progress of an Insurgency Campaign,* AFRL-HE-WP-TR-2007-0100, 2007. (RW 2915)

Leedy, P.D. & Ormrod, J.E. *Practical Research: Planning and Design,* 8th ed., Pearson/Merrill Prentice Hall, Upper Saddle River, NJ, 2005. (RW 3092)

Leetaru, K. "The Scope of FBIS and BBC Open-Source Media Coverage, 1979-2008," *Studies in Intelligence,* Vol. 54, No. 1, 2010, pp. 17. (RW 3995)

Lefebvre, S. "A Look at Intelligence Analysis," *International Journal of Intelligence and Counterintelligence,* Vol. 17, No. 2, 2004, pp. 231-264. (RW 1696)

Lefebvre, S.J. "A Look at Intelligence Analysis", *International Studies Association (ISA) 44th Annual International Convention,* Portland, OR, February 25 - March 1, 2003 (RW 339)

Lefebvre, S.J. "Strategic Warning: If Surprise is Inevitable, what Role for Analysis? POSTER Presentation TC99", *International Studies Association (ISA) 44th Annual International Convention,* Portland, OR, February 25 - March 1, 2003 (RW 94)

Lefebvre, S. "Lithuania, the CIA, and Intelligence Reform," *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 3, 2012, pp. 571-594. (RW 5728)

Legrenzi, P. "Dual-Process Theories of Thinking," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans,* eds. K.I. Manktelow, D.E. Over & S. Elqayam, Psychology Press, Hove, East Sussex, UK, 2011, pp. 219-235. (RW 5708)

Lehman, D., Lempert, R. & Nisbett, R. "The Effects of Graduate Training on Reasoning: Formal Discipline and Thinking about Everyday Events," *American Psychologist,* Vol. 43, No. 6, 1988, pp. 431-442. (RW 4784)

Lehmann, C.M. & Heagy, C.D. "An Introduction to the Clinical Case Representation Paradigm for Information Systems Research," *Journal of Information Systems,* Vol. 20, No. 1, 2006, pp. 87. (RW 2630)

Lehner, P.E., Adelman, L., Cheikes, B.A. & Brown, M.J. "Confirmation Bias in Complex Analyses," *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans,* Vol. 38, No. 3, 2008, pp. 584-592. (RW 4690)

Lehner, P.E. & Zirk, D.A. "Cognitive Factors in User/Expert-System Interaction," *Human Factors,* Vol. 29, No. 1, 1987, pp. 97-109. (RW 925)

Lehner, P.E., Adelman, L., DiStassio, R.J., Erie, M.C., Mittel, J.S. & Olson, S.L. *Confirmation Bias in the Analysis of Remote Sensing Data* (RW 2992)

Lehner, P., Michelson, A. & Adelman, L. *Measuring the Forecast Accuracy of Intelligence Products,* Mitre Corporation, McLean, VA, 2010. (RW 5544)

Lehrer, J. "Driven to Market," *Nature,* Vol. 443, 2006, pp. 502. (RW 2049)

Lehrer, J. "The cognitive benefits of nature", [Online], 2008, (RW 3345)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Lehrer, J. "Don't trust an insomniac", [Online], 2008, (RW 3344)

Lehrer, J. "The Eureka Hunt," *The New Yorker,* Vol. 84, No. 22, 2008, pp. 40-45. (RW 3244)

Lehrer, J. "Grape Expectations," *The Boston Globe,* 2008 (RW 3318)

Lehrer, J. *Poverty and the Brain* 2008. (RW 3346)

Lehrer, J. "What's that Name?" *The Boston Globe,* 2008 (RW 3590)

Lehrer, J. *How We Decide*, Houghton Mifflin Harcourt, Boston, 2009. (RW 3419)

Lehrer, J. "Accept Defeat: The Neuroscience of Screwing Up," *Wired Magazine,* Vol. 18, No. 1, 2010, pp. 84. (RW 3793)

Lehrer, J. *Imagine: How Creativity Works,* Houghton Mifflin Harcourt, Boston, MA, 2012. (RW 5469)

Lehrer, K. "Truth, Evidence, and Inference," *American Philosophy Quarterly,* 1974, pp. 79. (RW 1480)

Leigh, I. "The Accountability of Security and Intelligence Agencies," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 67. (RW 2458)

Leinhardt, G. "Capturing Craft Knowledge in Teaching," *Educational Researcher,* Vol. 19, No. 2, 1990, pp. 18. (RW 4377)

Lemozy, S.C. "The Intelligence Research Process as an Applied Science," in *Intelligence Professionalism in the Americas = Profesionalismo De Inteligencia En Las Americas,* eds. R.G. Swenson & S.C. Lemozy, Joint Military Intelligence College, Washington, DC, 2003, pp. 451-472. (RW 940)

Lempert, R. "Can Scenarios Help Policymakers be both Bold and Careful?" in *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics,* ed. F. Fukuyama, Brookings Institution Press, Washington, DC, 2007, pp. 109-119. (RW 4700)

Lenat, D.B., Clarkson, A. & Kiremidjian, G. "An Expert System for Indications and Warning Analysis", *Proceedings of the Eighth International Joint Conference on Artificial Intelligence,* 8-12 August 1983, pp. 259. (RW 1549)

Lenczowski, R.E. *The National Imagery and Mapping Agency* 2003. (RW 1148)

Lenczowski, R.E. *NIMA and the Intelligence Community,* 2003. (RW 1149)

Leonard, D. & Straus, S. "Putting Your Company's Whole Brain to Work," *Harvard Business Review,* Vol. 75, No. 4, 1997, pp. 110-121. (RW 3948)

Leonhart, D.M. *Analytical Techniques for Intelligence Analysis: A System for Selecting Alternative Methods,* (RW 3709)

Lepore, S.J. & Smyth, J.M. *The Writing Cure: How Expressive Writing Promotes Health and Emotional Well-being,* American Psychological Association, Washington, DC, 2002. (RW 2015)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Leshowitz, B., Jenkens, K., Heaton, S. & Bough, T. "Fostering Critical Thinking Skills in Students with Learning Disabilities: An Instructional Program," *Journal of Learning Disabilities,* Vol. 26, No. 7, 1993, pp. 483-490. (RW 3855)

Leslau, O. *Who Needs Intelligence? The use of Intelligence by Decision Makers,* [undated]. (RW 2988)

Leslau, O. "Intelligence and Economics: Two Disciplines with a Common Dilemma," *International Journal of Intelligence and Counterintelligence,* Vol. 20, No. 1, 2007, pp. 106. (RW 1756)

Leslau, O. "The Effect of Intelligence on the Decisionmaking Process," *International Journal of Intelligence and Counterintelligence,* Vol. 23, No. 3, 2010, pp. 426. (RW 4155)

Lesperance, M.M. *The Effects of Problem Based Learning (PBL) on Students' Critical Thinking Skills,* Ph.D. dissertation, The University of North Carolina at Greensboro, 2008. (RW 5088)

Lester, S. *An Introduction to Phenomenological Research* 1999. (RW 1778)

Letsky, M.P. *Macrocognition in Teams: Theories and Methodologies,* Ashgate, Aldershot, Hants, England, 2008. (RW 5642)

Leu, D.J. "Literacy and Technology: Deictic Consequences for Literacy Education in an Information Age," in *Handbook of Reading Research: Volume III*, eds. M.L. Kamil, P.B. Mosenthal, P.D. Pearson & R. Barr, L. Erlbaum Associates, Mahwah, NJ, 2000, pp. 743-770. (RW 5218)

Leu, D.J., Kinzer, C.K., Coiro, J.L. & Cammack, D.W. "Toward a Theory of New Literacies Emerging from the Internet and Other Information and Communication Technologies," in *Theoretical Models and Processes of Reading*, eds. R.B. Ruddell & N. Unrau, 5th ed., 2004. (RW 2796)

Levas, A., Brown, E., Murdock, J.W. & Ferrucci, D. "The Semantic Analysis Workbench (SAW): Towards a Framework for Knowledge Gathering and Synthesis," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 869)

Lever, S.P. "Intelligence and War," in *Oxford Handbook of War*, ed. J. Lindley-French, Oxford University Press, Oxford, UK, 2012, pp. 228-241. (RW 5487)

Levine, J.M. & Kerr, N.L. "Inclusion and Exclusion: Implications for Group Processes," in *Social Psychology: Handbook of Basic Principles*, eds. E.T. Higgins & A.W. Kruglanski, Second ed., 2007, pp. 759. (RW 2896)

Levinson, R.M. *Utility of Quantitative Methods for Political Intelligence Analysis. A Case Study in Latin America. - Master's Thesis.* M.A. thesis, California University, 1995. (RW 1205)

Levite, A. *Intelligence and Strategic Surprises,* Columbia University Press, New York, 1987. (RW 4191)

Levy, C.M. & Ransdell, S.E. *The Science of Writing: Theories, Methods, Individual Differences, and Applications,* L. Erlbaum Associates, Mahwah, NJ, 1996. (RW 2010)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Levy, D.M. *Scrolling Forward: Making Sense of Documents in the Digital Age,* Arcade, New York, 2001. (RW 1389)

Levy, J.S. "Misperception and the Causes of Wars: Theoretical Linkages and Analytical Problems," *World Politics,* Vol. 36, No. 1, 1983, pp. 76-99. (RW 4591)

Levy, J.S. "Learning and Foreign Policy: Sweeping a Conceptual Minefield," *International Organization,* Vol. 48, No. 2, 1994, pp. 279-312. (RW 5365)

Levy, K.E. "A Second Look at Subsecond Response Time", *Eleventh International Computer Measurement Group Conference,* Dallas, TX, December 9-13, 1985, pp. 630-633. (RW 4515)

Lewandowski, D. "Web Searching, Search Engines and Information Retrieval," *Information Services and Use,* Vol. 25, 2005, [draft]. (RW 1403)

Lewandowski, D. "Web Searching, Search Engines and Information Retrieval," *Information Services & Use,* Vol. 25, 2005, pp. 137-147. (RW 2751)

Lewin, J.H. *Incomplete Intelligence: Is the Information Sharing Environment an Effective Platform?* M.A. thesis, Naval Postgraduate School, 2012. (RW 5869)

Lewin, R. *Ultra Goes to War: The First Account of World War II's Greatest Secret Based on Official Documents,* McGraw-Hill, New York, 1978. (RW 2951)

Lewis, D. *Predictive Analysis: An Unnecessary Risk in the Contemporary Operating Environment,* US Army Commend and General Staff College, Ft. Leavenworth, KS, 2004. (RW 1179)

Lewis, G.E. *Army Intelligence Analysis: Transforming Army Intelligence Analysis Training and Doctrine to Serve the Reasonable Expectations and Needs of Echelons Corps and Below Commanders, Consumers, and Customers,* ADA435988, United States Army Command and General Staff College, Ft. Leavenworth, KS, 2005. (RW 1085)

Lewis, H. *A Question of Values: Six Ways We Make the Personal Choices that Shape Our Lives,* Harper & Row, San Francisco, CA, 1990. (RW 4898)

Lewis, T., Petrina, S. & Hill, A.M. "Problem Posing - Adding a Creative Increment to Technological Problem Solving," *Journal of Industrial Teacher Education,* Vol. 36, No. 1, 1998 (RW 2609)

Lewontin, R.C. & Hubby, J.L. "Citation Classic," *Current Contents/Life Sciences,* 43, 1985, pp. 16. (RW 2030)

Leydesdorff, L. "The University-Industry Knowledge Relationship: Analyzing Patents and the Science Base of Technologies," *Journal of the American Society for Information Science & Technology,* Vol. 55, No. 11, 2004, pp. 991. (RW 1411)

Li, A. & Butler, A.B. "The Effects of Participation in Goal Setting and Goal Rationales on Goal Commitment: An Exploration of Justice Mediators," *Journal of Business and Psychology,* Vol. 19, No. 1, 2004, pp. 37. (RW 2566)

Li, H. & Alonso, R. "Managing Analysis Context", *Widm '12,* Maui, HI, November 2, 2012 (RW 5847)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Li, J. "U.S. and Chinese Cultural Beliefs about Learning," *Journal of Educational Psychology*, Vol. 95, 2003, pp. 258-267. (RW 5063)

Li, J. & He, P. "Extended Automatic Reasoning of Criminal Investigation", *2009 International Conference on Industrial Mechatronics and Automation*, 2009, pp. 282. (RW 3911)

Li, J. & Klahr, D. "The Psychology of Scientific Thinking: Implications for Science Teaching and Learning," in *Teaching Science in the 21st Century*, eds. J. Rhoton & P. Shane, NSTA Press, Arlington, Va, 2006, pp. 307. (RW 1887)

Liang, D.W., Moreland, R. & Argote, L. "Group Vs Individual Training and Group Performance: The Mediating Role of Transactive Memory," *Personality and Social Psychology Bulletin*, Vol. 21, No. 4, 1995, pp. 384. (RW 2879)

Liang, J.-., Lee, M.-. & Tsai, C.-. "The Relations between Scientific Epistemological Beliefs and Approaches to Learning Science among Science-Major Undergraduates in Taiwan," *Asia Pacific Education Researcher*, Vol. 19, 2010, pp. 43-59. (RW 5055)

Liang, T.Y. *Organizing Around Intelligence*, World Scientific, Singapore, 2004. (RW 4580)

Liaropoulos, A.N. *A (R)Evolution in Intelligence Affairs? in Search of a New Paradigm*, Research Paper No. 100, Research Institute for European and American Studies (RIEAS), Athens, Greece, 2006. (RW 4583)

Libicki, M.C. & Pfleeger, S.L. *Collecting the Dots: Problem Formulation and Solution Elements* 2004. (RW 2494)

Lichtenstein, S.C. & Fischhoff, B. "Do Those Who Know More Also Know More About How Much They Know?" *Organizational Behavior and Human Performance*, Vol. 20, 1977, pp. 159. (RW 1258)

Lichtenstein, S. & Fischoff, B. "Training for Calibration," *Organizational Behavior and Human Performance*, Vol. 26, No. 2, 1980, pp. 149. (RW 2339)

Liddy, E.D. *Scenario Approach to Question-Answering [Powerpoint Presentation] Presented at the ARDA-NRRC Workshop, June 23-27, 2003.* 2003. (RW 1511)

Lieberthal, K. *The U. S. Intelligence Community and Foreign Policy: Getting Analysis Right* 2009. (RW 3594)

Liem, G.A.D. & Bernardo, A.B.I. "Epistemological Beliefs and Theory of Planned Behavior: Examining Beliefs about Knowledge and Knowing as Distal Predictors of Idonesian Tertiary Students' Intention to Study," *Asia Pacific Education Researcher*, Vol. 19, 2010, pp. 127-142. (RW 5056)

Light, R.J. & Pillemer, D.B. *Summing Up: The Science of Reviewing Research*, Harvard University Press, Cambridge, MA, 1984. (RW 2182)

Lillard, A. "Ethnopsychologies: Cultural Variations in Theories of Mind," *Psychological Bulletin*, Vol. 123, 1998, pp. 3. (RW 3425)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Limon, M. "Conceptual Change in History," in *Reconsidering Conceptual Change: Issues in Theory and Practice*, eds. M. Limón & L. Mason, Kluwer Academic, Dordrecht, 2002, pp. 259-290. (RW 5006)

Limon, M. "The Domain Generality-Specificity of Epistemological Beliefs: A Theoretical Problem, a Methodological Problem Or Both?" *International Journal of Educational Research*, Vol. 45, No. 1-2, 2006, pp. 7. (RW 3693)

Lin, K. & Chen, H. *Automatic Information Discovery from the "Invisible Web"* (RW 1404)

Lindberg, B.C. *Culture: A Neglected Aspect of War*, USMC Small Wars Center of Excellence, Quantico, VA, 1996. (RW 431)

Linn, M.C. & Songer, N.B. "How Do Students Make Sense of Science?" *Merrill-Palmer Quarterly*, Vol. 39, No. 1, 1993, pp. 47-73. (RW 5588)

Linnenbrink, E.A. & Pintrich, P.R. "The Role of Motivational Beliefs in Conceptual Change," in *Reconsidering Conceptual Change: Issues in Theory and Practice*, eds. M. Limón & L. Mason, Kluwer Academic, Dordrecht, 2002, pp. 115-136. (RW 5003)

Linnenbrink, E. & Pintrich, P.R. "Achievement Goals and Intentional Conceptual Change," in *Intentional Conceptual Change*, eds. G.M. Sinatra & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2003, pp. 347-374. (RW 5042)

Lintern, G. "An Interactive Planning Prototype for Task Force Air Defense", *Proceedings of the 51st Human Factors and Ergonomics Society Annual Meeting*, pp. 499. (RW 3623)

Lintern, G. "Structured Information for Support of Knowledge-Based Reasoning," *Human Factors and Ergonomics Society Annual Meeting Proceedings*, Vol. 52, No. 4, 2008, pp. 282. (RW 3580)

Liotta, P.H. & Somes, T.E. "The Art of Reperceiving Scenarios and the Future," *Naval War College Review*, Vol. 57, No. 4, 2003, pp. 120-132. (RW 407)

Lipman, M. "Some Thoughts on the Foundations of Reflective Education," in *Teaching Thinking Skills: Theory and Practice*, eds. J.B. Baron & R.J. Sternberg, Freeman, New York, NY, 1987, pp. 151-161. (RW 3740)

Lipman, M. *Thinking in Education*, 2nd ed., Cambridge University Press, New York, NY, 2003. (RW 3699)

Lipps, J.H. "This is Science!" in *Evolution: Investigating the Evidence*, eds. J. Scotchmoor & D.A. Springer, Paleontological Society, Pittsburgh, PA, 1999, pp. 3-16. (RW 5160)

Lipshitz, R. & Pras, A.A. "Not Only for Experts: Recognition-Primed Decisions in the Laboratory," in *How Professionals Make Decisions*, eds. H. Montgomery, R. Lipshitz & B. Brehmer, L. Erlbaum Associates, Mahwah, NJ, 2005, pp. 15. (RW 1382)

Liscouski, R.P. *Taking Responsibility for our Security*, Center for Information Policy Research, Harvard University, Cambridge, MA, 2005. (RW 1167)

List, C. *Distributed Cognition: A Perspective from Social Choice Theory*, [undated]. (RW 2068)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Lite, J. "Political Science: What being Neat Or Messy Says about Political Leanings," *Scientific American,* 2008 (RW 3293)

Litman, L. & Reber, A.S. "Implicit Cognition and Thought," in *The Cambridge Handbook of Thinking and Reasoning,* eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 431-456. (RW 4012)

Little, E., Laskey, K.B. & Janssen, T. "Ontologies and Probabilities: Working Together for Effective Multi-INT Fusion", *Proceedings of the Second International Ontology for the Intelligence Community Conference OIC-2007,* Columbia, MD, November 28-29, 2007, pp. 33-36. (RW 4819)

Little, W.W. *Applied Logic,* Houghton Mifflin, Boston, MA, 1955. (RW 1543)

Liu, P. "Are Beliefs Believable? An Investigation of College Students' Epistemological Beliefs and Behavior in Mathematics," *Journal of Mathematical Behavior,* Vol. 29, No. 2, 2010, pp. 86-98. (RW 5587)

LNU, L. *The Swarm is Greater than the Parts: Cultivating the Wisdom of Crowds in the Intelligence Community* 2006. (RW 3001)

Lochhead, J. "Research Synthesis on Problem Solving," *Educational Leadership,* October, 1981, pp. 68. (RW 2251)

Locke, E.A. & Latham, G.P. "Building a Practically Useful Theory of Goal Setting and Task Motivation," *American Psychologist,* Vol. 57, No. 9, 2002, pp. 705. (RW 2567)

Locke, E.A. & Latham, G.P. "New Directions in Goal-Setting Theory," *Current Directions in Psychological Science,* Vol. 15, No. 5, 2006, pp. 265. (RW 2564)

Lockheed Martin Inc. *Intelligence Analysis Training,* Lockheed Martin Inc. Available: http://www.lockheedmartin.com/products/intelligence-analysis-training/index.html, Viewed: November 30, 2009. (RW 4062)

Lockwood, J. "LAMP: A New Analytical Method for Prediction," *Military Intelligence Professional Bulletin,* Vol. 21, No. 2, 1995, pp. 29-32. (RW 4737)

Loeb, V. "CIA Goes Deep into Analysis; Agency Opens School, Elevates Analysts," *Washington Post,* 2000, May 4, 2000, p. 23. (RW 3866)

Lohman, D.F. & Lakin, J.M. "Intelligence and Reasoning," in *Cambridge Handbook of Intelligence,* eds. R.J. Sternberg & S.B. Kaufman, Cambridge University Press, New York, NY, 2012, pp. 419-441. (RW 5780)

Lohr, S. "Slow Down, Brave Multitasker, and Don't Read this in Traffic," *New York Times,* March 25, 2007. (RW 3559)

Lohr, S. "The Crowd is Wise (when it's Focused)," *The New York Times,* July 19, 2009. (RW 3525)

Long, J.F., Holleran, T.A. & Esterly, E. "The Effectiveness of Persuasive Messages: Comparing Traditional and Computerized Texts," *Theory into Practice,* Vol. 40, No. 4, 2001, pp. 265. (RW 2787)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Lonka, K. & Lindblom-Ylanne, S. "Epistemologies, Conceptions of Learning, and Study Practices in Medicine and Psychology," *Higher Education*, Vol. 31, No. 1, 1996, pp. 5-24. (RW 4617)

Looney, R.E. "DARPA's Policy Analysis Market for Intelligence: Outside the Box Or Off the Wall?" *International Journal of Intelligence and Counterintelligence*, Vol. 17, No. 3, 2004, pp. 405. (RW 1674)

Lopresti, D. *Web Document Analysis: The Case of the Missing Dimension(s) [Powerpoint Presentation]* (RW 1412)

Lord, K.M. "National Intelligence in the Age of Transparency," in *Strategic Intelligence. Volume 1: Understanding the Hidden Side of Government*, ed. L.K. Johnson, Praeger Security International, Westport, CT, 2007, pp. 181. (RW 2715)

Losee, R.M. *Information from Processes*, Springer, 2012. (RW 5793)

Losey, S. *Intel Workers' Pay System Unfair, Study Says*. Available: http://www.federaltimes.com/article/20100523/benefits/5230306/1041/benefits, Viewed: March 9, 2012. (RW 5474)

Losey, S. "Top Intel Analyst Focuses on Work Force, Data Sharing," *FederalTimes.com*, 2006 (RW 1296)

Lotrionte, C. "The Fault, Dear Brutus, is Not in Individuals, but in our System: CIA's Inspector General Seeks to Find Individuals Accountable for 9/11 and Misses an Opportunity for Effective Intelligence Reform," *SAIS Review*, Vol. 28, No. 1, 2008, pp. 109. (RW 3330)

Louca, L., Elby, A., Hammer, D. & Kagey, T. "Epistemological Resources: Applying a New Epistemological Framework to Science Instruction," *Educational Psychologist*, Vol. 39, No. 1, 2004, pp. 57-68. (RW 5195)

Louie, G. "Tools, Techniques and Teams for Analysis", *New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities*, Rome, Italy, 31 March - 2 April, 2004, pp. 127-136. (RW 2839)

Louie, T.A., Rajan, M.N. & Sibley, R.E. "Tackling the Monday-Morning Quarterback: Applications of Hindsight Bias in Decision-Making Settings," *Social Cognition*, Vol. 25, No. 1, 2007, pp. 32. (RW 2447)

Lovallo, D. & Sibony, O. "The Case for Behavioral Strategy," *McKinsey Quarterly*, March, 2010, pp. 1. (RW 3977)

Lovegrove, E. *Target-Centric Astronomy*. Available: http://astrobites.com/2011/09/25/target-centric-astronomy/, Viewed: October 9, 2011. (RW 5157)

Lovett, M.C. & Anderson, J.R. "Thinking as a Production System," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 401-430. (RW 4011)

Lowenthal, M.M. *DDN Special Reports: Open Source Intelligence: New Myths, New Realities* [undated]. (RW 196)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Lowenthal, M.M. "The Burdensome Concept of Failure," in *Intelligence: Policy and Process*, eds. A.C. Maurer, M.D. Tunstall & J.M. Keagle, Westview Press, Boulder, CO, 1985, pp. 43-56. (RW 1216)

Lowenthal, M.M. "The Intelligence Library: Quantity Vs. Quality," *Intelligence and National Security,* Vol. 2, No. 2, 1987, pp. 368. (RW 3121)

Lowenthal, M.M. "Tribal Tongues: Intelligence Consumers, Intelligence Producers," *The Washington Quarterly,* Vol. 15, No. 1, 1992, pp. 157-167. (RW 12)

Lowenthal, M.M. "Intelligence Epistemology: Dealing with the Unbelievable," *International Journal of Intelligence and Counterintelligence,* Vol. 6, No. 3, 1993, pp. 319-325. (RW 50)

Lowenthal, M.M. *The U.S. Intelligence Community: An Annotated Bibliography,* Garland Publishing, New York, NY, 1994. (RW 1101)

Lowenthal, M.M. *Intelligence: From Secrets to Policy,* CQ Press, Washington, DC, 2000. (RW 666)

Lowenthal, M.M. *Intelligence: From Secrets to Policy,* 2nd ed., CQ Press, Washington, DC, 2003. (RW 667)

Lowenthal, M.M. *Intelligence Analysis,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2004. (RW 171)

Lowenthal, M.M. "Open-Source Intelligence: New Myths, New Realities," in *Intelligence and the National Security Strategist: Enduring Issues and Challenges,* eds. R.Z. George & R.D. Kline, National Defense University Press, Washington, DC, 2004, pp. 273-278. (RW 692)

Lowenthal, M.M. "Intelligence Analysis: Management and Transformation Issues," in *Transforming U.S. Intelligence,* eds. J.E. Sims & B.L. Gerber, Georgetown University Press, Washington, DC, 2005, pp. 220-238. (RW 919)

Lowenthal, M.M. *Intelligence: From Secrets to Policy,* 3rd ed., CQ Press, Washington, DC, 2006. (RW 5720)

Lowenthal, M.M. "The Analytic Environment," in *A Handbook of the Psychology of Intelligence Analysis,* ed. R.L. Rees, 2008, pp. 250. (RW 3651)

Lowenthal, M.M. "Intelligence in Transition: Analysis After September 11 and Iraq," in *Analyzing Intelligence: Origins, Obstacles, and Innovations,* eds. R.Z. George & J.B. Bruce, 2008, pp. 226. (RW 3106)

Lowenthal, M.M. "Towards a Reasonable Standard for Analysis: How Right, How Often on Which Issues?" *Intelligence and National Security,* Vol. 23, No. 3, 2008, pp. 303. (RW 3170)

Lowenthal, M.M. "The Intelligence Time Event Horizon," *International Journal of Intelligence and Counterintelligence,* Vol. 22, No. 3, 2009, pp. 369. (RW 3583)

Lowenthal, M.M. *Intelligence: From Secrets to Policy,* 4th ed., CQ Press, Washington, DC, 2009. (RW 5719)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Lowenthal, M.M. "The Policymaker-Intelligence Relationship," in *Oxford Handbook of National Security Intelligence*, ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 437-451. (RW 4713)

Lowenthal, M.M. *Intelligence: From Secrets to Policy*, 5th ed., SAGE/CQ Press, Los Angeles, CA, 2012. (RW 5718)

Lowrance, J.D., Harrison, I.W. & Rodriguez, A.C. "Capturing Analytic Thought", K-CAP'01, Victoria, British Columbia, Canada, October 22-23, 2001, pp. 84-91. (RW 1493)

Lucas, S. "Recognising Politicization: The CIA and the Path to the 2003 War in Iraq," *Intelligence and National Security*, Vol. 26, No. 2-3, 2011, pp. 203-227. (RW 4847)

Luce, R.D. "Rationality in Choice Under Certainty and Uncertainty," in *Emerging Perspectives on Judgment and Decision Research*, eds. S.L. Schneider & J. Shanteau, Cambridge University Press, Cambridge, UK, 2003, pp. 64-83. (RW 5825)

Luckie, P.T., Smith, D.E. & Wright, G.H. *Investigation of a Bayesian Approach Applied to a Specific Intelligence Problem*, AD0839284, 1968. (RW 1133)

Luke, N.H. *An Investigation into the Complexity of Organizational Problems and Consensual Deliberation in Collaborative Planning* 2006. (RW 2066)

Lund, N.W. "Document Theory," in *Annual Review of Information Science and Technology*, ed. B. Cronin, Medford, NJ, 2009, pp. 399. (RW 4349)

Lundberg, C.C. & Young, C.A. *Foundations for Inquiry: Choices and Trade-Offs in the Organizational Sciences*, Stanford Business Books, Stanford, CA, 2005. (RW 3245)

Lundberg, K. *CIA and the Fall of the Soviet Empire: The Politics of "Getting it Right" Case C16-94-1251.0*, Kennedy School of Government, Harvard University, Cambridge, MA, 1994. (RW 4035)

Lundberg, K. "CIA and the Fall of the Soviet Empire: Part II," *Studies in Intelligence*, Fall, 1995, pp. 31-49. (RW 119)

Lundberg, K. "CIA and the Fall of the Soviet Empire: The Politics of "Getting it Right"," *Studies in Intelligence*, Fall, 1995, pp. 45-66. (RW 118)

Luong, M.A. "The Challenges of Economic Intelligence," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 163. (RW 2465)

Lutz, M. & Radvansky, G.A. "The Fate of Completed Goal Information in Narrative Comprehension," *Journal of Memory and Language*, Vol. 36, 1997, pp. 293. (RW 2376)

Lybrand, S., Dobson, J. & Solomon, S.H. *"JuryThink": The Social Psychology of Group Deliberation* (RW 2058)

Lyden, M. *The Efficacy of Accelerated Analysis in Strategic-Level Estimative Judgments*, M.S. thesis, Mercyhurst College, 2007. (RW 3126)

Lynch, C.G. *Three Things the CIA Learned about Implementing an Enterprise Wiki*, (RW 3232)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Lynch, P. "Imagery Analysis," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 117-124. (RW 3617)

Ma, C. *Individual Differences in Insight Problem Solving,* Ph.D. dissertation, Ohio University, 2002. (RW 3431)

Ma, Y., Seid, D.Y. & Mehrotra, S. "Automated Filtering on Data Streaming for Intelligence Analysis," in *Intelligence and Security Applications: Techniques and Applications*, eds. H. Chen & C.C. Yang, Springer, 2008, pp. 199-213. (RW 5739)

MacCloskey, M. *The American Intelligence Community,* Rosen Press, New York, NY, 1967. (RW 774)

MacCoun, R.J. "Biases in the Interpretation and Use of Research Results," *Annual Review of Psychology,* Vol. 49, 1998, pp. 259-287. (RW 5292)

MacCoun, R.J. "Epistemological Dilemmas in the Assessment of Legal Decision Making," *Law & Human Behavior,* Vol. 23, No. 6, 1999, pp. 723. (RW 2034)

MacDonald, A.P. "Revised Scale for Ambiguity Tolerance: Reliability and Validity," *Psychological Reports,* Vol. 26, No. 3, 1970, pp. 791-798. (RW 5255)

MacEachin, D. *Predicting the Soviet Invasion of Afghanistan: The Intelligence Community's Record,* 2002. (RW 2208)

MacEachin, D. "Analysis and Estimates: Professional Practices in Intelligence Production," in *Transforming U.S. Intelligence*, eds. J.E. Sims & B.L. Gerber, Georgetown University Press, Washington, DC, 2005, pp. 115-133. (RW 918)

MacEachin, D.J., Wolfowitz, P., Despres, J. & Shulsky, A. *The Tradecraft of Analysis: Challenge and Change in the CIA*, Consortium for the Study of Intelligence, Washington, DC, 1994. (RW 121)

Machamer, P. "Kuhn's Philosophical Successes?," in *Re-Framing the Conceptual Change Approach in Learning and Instruction*, eds. S. Vosniadou, A. Baltas & X. Vamvakoussi, Elsevier, Amsterdam, 2007, pp. 35-45. (RW 5593)

MacIntosh-Murray, A. "Organizational Sense Making and Information use," in *Theories of Information Behavior*, eds. K.E. Fisher, S. Erdelez & L. McKechnie, Published for the American Society for Information Science and Technology by Information Today, Medford, N.J, 2005, pp. 265. (RW 3605)

MacKay, D.G. "Constraints on the Theory of Inner Speech," in *Auditory Imagery*, ed. D. Reisberg, L. Erlbaum Associates, Hillsdale, NJ, 1992, pp. 121-149. (RW 5841)

Mackin, J.H. "Rational and Empirical Methods of Investigation in Geology," in *The Fabric of Geology*, ed. C.C. Albritton, Freeman, Cooper, & Co., Stanford, CA, 1963, pp. 135-163. (RW 5214)

Mackintosh, N.J. "History of Theories and Measurement of Intelligence," in *Cambridge Handbook of Intelligence*, eds. R.J. Sternberg & S.B. Kaufman, Cambridge University Press, New York, NY, 2012, pp. 3-19. (RW 5779)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Macknik, S.L., Martinez-Conde, S. & Blakeslee, S. *Sleights of Mind: What the Neuroscience of Magic Reveals About Our Everyday Deceptions,* Henry Holt, New York, 2010. (RW 4521)

Macpherson, R. & Stanovich, K.E. "Cognitive Ability, Thinking Dispositions, and Instructional Set as Predictors of Critical Thinking," *Learning and Individual Differences,* Vol. 17, No. 2, 2007, pp. 115-127. (RW 3340)

MacVean, A. & Harfield, C. "Science Or Sophistry: Issues in Managing Analysts and their Products," in *The Handbook of Intelligent Policing: Consilience, Crime Control, and Community Safety*, ed. C. Harfield, Oxford University Press, Oxford, UK, 2008, pp. 93-104. (RW 5772)

Maddrell, P. "Failing Intelligence: US Intelligence in the Age of Transnational Threats," *International Journal of Intelligence and Counterintelligence,* Vol. 22, No. 2, 2009, pp. 195. (RW 3446)

Madnick, S.E., Moulton, A. & Siegel, M.D. *Context Mediation Demonstration of Counter-Terrorism Intelligence (CTI) Integration,* Working Paper CISL# 2005-03, MIT Sloan School of Management, Cambridge, MA, 2005. (RW 477)

Maehr, M.L. "Paul Pintrich: A Once and Continuing Influence," *Educational Psychologist,* Vol. 40, No. 2, 2005, pp. 129-133. (RW 4981)

Maffeo, S.E. *The Intelligence Revolution: A Historical Perspective,* US GPO, Washington, DC, 1988. (RW 1100)

Magarey, J.M. "Elements of a Systematic Review," *International Journal of Nursing Practice,* Vol. 7, 2001, pp. 376. (RW 2262)

Magee, J.F. *Some Business Analogies to C3I,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1990. (RW 1017)

Maggioni, L., Alexander, P.A. & VanSledright, B. "At the Crossroads: The Development of Epistemological Beliefs and Historical Thinking," *European Journal of School Psychology,* Vol. 2, No. 1-2, 2004, pp. 169. (RW 3688)

Maggioni, L. & Alexander, P.A. *Knowledge Domains and Domain Learning* (RW 3833)

Maggioni, L. & Parkinson, M.M. "The Role of Teacher Epistemic Cognition, Epistemic Beliefs, and Calibration in Instruction," *Educational Psychology Review,* Vol. 20, No. 4, 2008, pp. 445-461. (RW 5431)

Magnussen, L., Ishida, D. & Itano, J. "The Impact of the Use of Inquiry-Based Learning as a Teaching Methodology on the Development of Critical Thinking," *Journal of Nursing Education,* Vol. 39, No. 8, 2000, pp. 360-364. (RW 3960)

Magnusson, P. "The Smart Way to Fix Intelligence," *BusinessWeek,* 3889, 2004, pp. 81-83. (RW 406)

Magolda, M.B.B. "Evolution of a Constructivist Conceptualization of Epistemological Reflection," *Educational Psychologist,* Vol. 39, No. 1, 2004, pp. 31. (RW 4340)

Maguire, E. *Critical Intelligence Community Management Challenges. Inspector General Report.* 2008. (RW 3445)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Mahesh, K. *Text Retrieval Quality: A Primer* (RW 1563)

Mahnken, T.G. *Piercing the Fog of Peace: U.S. Intelligence and Foreign Military Innovation, 1918-1941,* Ph.D. dissertation, Johns Hopkins University, 1997. (RW 651)

Mahnken, T.G. "Spies and Bureaucrats: Getting Intel Right," *The Public Interest,* 159, 2005 (RW 614)

Maines, L.A. "An Experimental Examination of Subjective Forecast Combination," *International Journal of Forecasting,* Vol. 12, No. 2, 1996, pp. 223-233. (RW 5293)

Maisel, E. *Deep Writing: 7 Principles that Bring Ideas to Life,* J.P. Tarcher/Putnam, New York, 1999. (RW 1854)

Major, J.S. *Communicating with Intelligence: Writing and Briefing in the Intelligence and National Security Communities,* Scarecrow Press, Lanham, MD, 2008. (RW 3681)

Major, J.S. *Writing Classified and Unclassified Papers for National Security,* Scarecrow Press, Lanham, MD, 2008. (RW 3680)

Malone, T.W., Laubacher, R. & Dellarocas, C. *Harnessing Crowds: Mapping the Genome of Collective Intelligence,* MIT Sloan Working Paper 4732-09, MIT Sloan School of Management, 2010. (RW 4366)

Manchey, T. "Drawing: Another Path to Understanding," in *Teacher-Researchers at Work,* eds. M.M. Mohr & M.S. MacLean, 1999, [unpaged]. (RW 3519)

Mandel, D.R. & Vartanian, O. "Weighting of Contingency Information in Causal Judgment: Evidence of Hypothesis Dependence and use of a Positive-Test Strategy," *Quarterly Journal of Experimental Psychology,* Vol. 62, No. 12, 2009, pp. 2388-2408. (RW 5783)

Mandel, D.R. "Judgment Under Uncertainty," *Intelligence Analyst Training Newsletter,* June, 2008, pp. 7-9. (RW 4747)

Mandel, D.R. *Applied Behavourial Science in Support of Intelligence: Experiences in Building a Canadian Capability* 2009. (RW 4744)

Mandel, D.R. *Canadian Perspectives: Applied Behavioral Science in Support of Intelligence Analysis [Powerpoint Presentation],* Defence Research & Development Canada, Toronto, Canada, 2009. (RW 4770)

Mandel, D.R. "Confirmation and Positive-Test Biases in Hypothesis Testing," *Intelligence Analyst Training Newsletter,* March, 2010, pp. 8-9. (RW 4746)

Mandel, R. "On Estimating Post-Cold War Enemy Intentions," *Intelligence and National Security,* Vol. 24, No. 2, 2009, pp. 194. (RW 3491)

Mandelbaum, S.J. "Planning Intelligence," *Planning Theory,* Vol. 7, No. 3, 2008, pp. 318-322. (RW 4494)

Manget, F.F. "Intelligence and the Rise of Judicial Intervention," in *Handbook of Intelligence Studies,* ed. L.K. Johnson, 2007, pp. 329. (RW 2478)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Mangio, C.A. & Wilkinson, B.J. "Intelligence Analysis: Once again," in *The International Studies Encyclopedia*, ed. R.A. Denemark, http://www.isacompendium.com/subscriber/tocnode?id=g9781444336597_chunk_g978144433659711_ss1-12 ed., Blackwell Publishing, 2010, [unpaged]. (RW 3933)

Mangio, C.A. & Wilkinson, B.J. *State of Knowledge Relative to Intelligence Analysis. Volume 1: Cognitive Challenges for Intelligence Analysis - Past, Present, and Future*, AFRL-RH-WP-TR-2011-0049, 2011. (RW 5245)

Mani, I. & Klein, G.L. "Evaluating Intelligence Analysis Arguments in Open-Ended Situations," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 841)

Manjoo, F. *True Enough: Learning to Live in a Post-Fact Society*, Wiley, Hoboken, NJ, 2008. (RW 3076)

Manktelow, K.I., Over, D.E. & Elqayam, S. "Paradigms Shift: Jonathan Evans and the Science of Reason," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans*, eds. K.I. Manktelow, D.E. Over & S. Elqayam, Psychology Press, Hove, East Sussex, UK, 2011, pp. 1-15. (RW 5682)

Mann, B.J. *Systemic Thinking: Enhancing Intelligence Preparation and Estimates*, Naval War College, Newport, RI, 2010. (RW 5676)

Mann, S.R. "Chaos Theory and Strategic Thought," *Parameters*, Vol. 22, No. 3, 1992, pp. 54-68. (RW 1068)

Manning, C.D., Raghavan, P. & Schütze, H. *Introduction to Information Retrieval*, Cambridge University Press, New York, 2008. (RW 3901)

Mansfield, M. "Reflections on Service: A Conversation with Former CIA Director Michael Hayden," *Studies in Intelligence*, Vol. 54, No. 2, 2010 (RW 4201)

Mansharamani, V. *All Hail the Generalist.* Available: http://blogs.hbr.org/cs/2012/06/all_hail_the_generalist.html, Viewed: June 11, 2012. (RW 5683)

Manwaring, M.G. & Olson, W.J. *Managing Contemporary Conflict: Pillars of Success*, Westview Press, Boulder, CO, 1996. (RW 1198)

Manzi, J. *Uncontrolled: The Surprising Payoff of Trial-and-Error for Business, Politics, and Society*, Basic Books, New York, NY, 2012. (RW 5655)

Mao, J.Y. & Benbasat, I. "The Effects of Contextualized Access to Knowledge on Judgment," *International Journal of Human-Computer Studies*, Vol. 55, No. 5, 2001, pp. 787. (RW 2358)

Maoz, Z. "Intelligence Failures: An Analytic Framework", *Annual Meeting of the American Political Science Association*, August 31 - September 3 (RW 2919)

Marchetti, V. & Marks, J.D. *The CIA and the Cult of Intelligence*, Knopf, New York, NY, 1974. (RW 778)

Marchio, J.D. "Support to Military Operations: The Evolution and Relevance of Joint Intelligence Centers," *Studies in Intelligence*, Vol. 49, No. 1, 2005, pp. 41-54. (RW 397)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Marchionini, G. *Information Seeking in Electronic Environments*, Cambridge University Press, Cambridge, UK, 1995. (RW 2160)

Marchionini, G. "Exploratory Search: From Finding to Understanding," *Communications of the ACM*, Vol. 49, No. 4, 2006, pp. 41. (RW 1517)

Marchionini, G. & White, R.W. "Information-Seeking Support Systems," *Computer*, Vol. 42, No. 3, 2009, pp. 30. (RW 3437)

Marcus, G. *The Brain in the Machine*. Available: http://www.newyorker.com/online/blogs/newsdesk/2012/11/ibm-brain-simulation-compass.html, Viewed: December 6, 2012. (RW 5877)

Marcus, G.F. *Kluge: The Haphazard Construction of the Human Mind*, Houghton Mifflin, Boston, 2008. (RW 3423)

Marek, P., Jackson, S., Griggs, R. & Christopher, A. "Supplementary Books on Critical Thinking," *Teaching of Psychology*, Vol. 25, No. 4, 1998, pp. 266-269. (RW 3856)

Margolis, E. & Laurence, S. *Concepts: Core Readings*, MIT Press, Cambridge, MA, 1999. (RW 2511)

Margolis, H. *Patterns, Thinking, and Cognition: A Theory of Judgment*, University of Chicago Press, Chicago, IL, 1987. (RW 3863)

Margolis, J.E. "Estimating State Instability," *Studies in Intelligence*, Vol. 56, No. 1, 2012, pp. 13-24. (RW 5898)

Maria, K. "Conceptual Change Instruction: A Social Constructivist Perspective," *Reading & Writing Quarterly*, Vol. 16, No. 1, 2000, pp. 5-22. (RW 4837)

Mariani, J. *The Ineliminable Bias: Identity as a Foundational Source for Error in Intelligence Analysis*, M. A. thesis, Dartmouth College, 2012. (RW 5755)

Marier, V. *US Communications Policy: A Survey and Database of Executive Orders and Congressional Acts Over 24 Years*, Center for Information Policy Research, Harvard University, Cambridge, MA, (RW 1166)

Mark, H. *The Doctrine of Command, Control, Communications, and Intelligence: A Gentle Critique*, Center for Information Policy Research, Harvard University, Cambridge, MA, 2001. (RW 1165)

Markman, A.B. "Knowledge Representation," in *Oxford Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 36-51. (RW 5497)

Markman, A.B. & Gentner, D. "Thinking," *Annual Review of Psychology*, Vol. 52, 2001, pp. 223-247. (RW 1957)

Markowitz, L.M. *An Investigation of the Behavior of Mathematicians Engaged in Testing a Conjecture*, 1980. (RW 3353)

Markus, G. "Emotions in Politics," *Annual Review of Political Science*, Vol. 3, 2000, pp. 221. (RW 4414)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Marra, R.M., Palmer, B. & Litzinger, T.A. "The Effects of a First-Year Engineering Design Course on Student Intellectual Development as Measured by the Perry Scheme," *Journal of Engineering Education,* Vol. 89, No. 1, 2000, pp. 39-46. (RW 5560)

Marra, R. & Palmer, B. "Encouraging Intellectual Growth: Senior College Student Profiles," *Journal of Adult Development,* Vol. 11, No. 2, 2004, pp. 111-122. (RW 5555)

Marra, R. & Palmer, B. "University Science Students Epistemological Orientations and Nature of Science Indicators: How Do They Relate?" *Science Education International,* Vol. 18, No. 3, 2005, pp. 165-184. (RW 5272)

Marrin, S. "CIA's Kent School: A Step in the Right Direction", *International Studies Association (ISA) 43rd Annual International Convention,* New Orleans, LA, March 24-27, 2002 (RW 108)

Marrin, S. *Foreign Policy and Intelligence* 2002. (RW 308)

Marrin, S. "Improving CIA Analysis by Overcoming Institutional Obstacles," in *Bringing Intelligence about: Practitioners Reflect on Best Practices,* ed. R.G. Swenson, Joint Military Intelligence College, Washington, DC, 2003, pp. 41-59. (RW 1488)

Marrin, S. "CIA's Kent School: Improving Training for New Analysts," *International Journal of Intelligence and Counterintelligence,* Vol. 16, No. 4, 2003-2004, pp. 609-637. (RW 1087)

Marrin, S. "Preventing Intelligence Failures by Learning from the Past," *International Journal of Intelligence and Counterintelligence,* Vol. 17, No. 4, 2004, pp. 655-672. (RW 373)

Marrin, S. "Does Proximity between Intelligence Producers and Consumers Matter? The Case of Iraqi WMD Intelligence", *International Studies Association,* (RW 2922)

Marrin, S. "Intelligence Analysis: Turning a Craft into a Profession," 2005 *International Conference on Intelligence Analysis,* McLean, VA, May 2-6, 2005 (RW 331)

Marrin, S. *Intelligence Analysis Professionalization* 2006. (RW 1631)

Marrin, S. *Intelligence Theory and Foreign Policy: Explaining and Predicting Intelligence Roles and Missions* 2006. (RW 2989)

Marrin, S. *Making Better Communicators* 2006. (RW 1639)

Marrin, S. "Adding Value to the Intelligence Product," in *Handbook of Intelligence Studies,* ed. L.K. Johnson, 2007, pp. 199. (RW 2468)

Marrin, S. "At Arm's Length or at the Elbow? Explaining the Distance between Analysts and Decision Makers," *International Journal of Intelligence and Counterintelligence,* Vol. 20, No. 3, 2007, pp. 401. (RW 2382)

Marrin, S. *Intelligence Analysis Theory: Explaining and Predicting Analytic Responsibilities* 2007. (RW 2722)

Marrin, S. "Intelligence Analysis Theory: Explaining and Predicting Analytic Responsibilities," *Intelligence and National Security,* Vol. 22, No. 6, 2007, pp. 821. (RW 3881)

Marrin, S. *Intelligence Analysis: Epistemological Foundations* 2007. (RW 2721)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Marrin, S. "Intelligence Analysis: Structured Methods or Intuition?" *American Intelligence Journal,* Vol. 25, No. 1, 2007, pp. 7-16. (RW 3219)

Marrin, S. "Intelligence Analysis and Decision-Making: Methodological Challenges," in *Intelligence Theory: Key Questions and Debates,* eds. P. Gill, S. Marrin & M. Phythian, 2009, pp. 131. (RW 3409)

Marrin, S. "Training and Educating U.S. Intelligence Analysts," *International Journal of Intelligence and Counterintelligence,* Vol. 22, No. 1, 2009, pp. 131-146. (RW 3359)

Marrin, S. "The 9/11 Terrorist Attacks: A Failure of Policy Not Strategic Intelligence Analysis," *Intelligence and National Security,* Vol. 26, No. 2-3, 2011, pp. 182-202. (RW 4845)

Marrin, S. *Improving Intelligence Analysis: Bridging the Gap between Scholarship and Practice,* Routledge, London, UK, 2011. (RW 4024)

Marrin, S. "Intelligence Studies Centers: Making Scholarship on Intelligence Analysis Useful," *Intelligence and National Security,* Vol. 27, No. 3, 2012, pp. 398-422. (RW 5667)

Marrin, S. "Is Intelligence Analysis an Art Or a Science?" *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 3, 2012, pp. 529-545. (RW 5717)

Marrin, S. "Rethinking Analytic Politicization," *Intelligence and National Security,* Vol. 28, No. 1, 2013, pp. 32-54. (RW 5911)

Marrin, S. "Revisiting Intelligence and Policy: Problems with Politicization and Receptivity," *Intelligence and National Security,* Vol. 28, No. 1, 2013, pp. 1-4. (RW 5909)

Marrin, S.P. "Homeland Security and the Analysis of Foreign Intelligence," *Intelligencer,* Vol. 13, No. 2, 2003, pp. 25. (RW 1675)

Marrin, S.P. *Intelligence Analysis and Decisionmaking: Proximity Matters,* Ph.D. dissertation, University of Virginia, 2009. (RW 4527)

Marrin, S. & Clemente, J.D. "Improving Intelligence Analysis by Looking to the Medical Profession," *International Journal of Intelligence and Counterintelligence,* Vol. 18, No. 4, 2005, pp. 707-729. (RW 1244)

Marrin, S. & Clemente, J.D. "Modeling an Intelligence Analysis Profession on Medicine," *International Journal of Intelligence and Counterintelligence,* Vol. 19, No. 4, 2006, pp. 642-655. (RW 1635)

Marrin, S. & Clemente, J.D. "Modeling an Intelligence Analysis Profession on Medicine," *International Journal of Intelligence and Counterintelligence,* 2006 forthcoming, pp. 1-18. (RW 1245)

Marsh, K.R. & Pastor, D.A. "Stanovich and West's (2007) Actively Open-Minded Thinking Scale: An Examination of Factor Structure", *Annual Meeting of the Association for Psychological Science,* Washington D.C., May 26-29, 2011 (RW 5335)

Marsh, M. *Advanced Analysis Cognition: Critical Thinking,* March, 2012. [in press] (RW 5626)

Marsh, M. *Advanced Analysis Cognition: Thinking Dispositions,* May, 2012 [in press] (RW 5924)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Marsh, R.T. *Air Force C3I Systems*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1982. (RW 1019)

Marsh, R.T. *Critical Foundations: Protecting America's Infrastructure*, Center for Information Policy Research. Harvard University, Cambridge, MA, 2000. (RW 1018)

Marshall, A.W. "A Program to Improve Analytic Methods Related to Strategic Forces," *Policy Sciences*, Vol. 15, No. 1, 1982, pp. 48-50. (RW 720)

Marshall, C. & Rossman, G.B. *Designing Qualitative Research*, Sage Publications, Newbury Park, CA, 1989. (RW 3210)

Marshall, M.G. "Teaching Intelligence Research", *International Studies Association*, (RW 2923)

Martin, A. & Tanji, M. "Farm Teams and Free Agents: The Sporting Way to Solve the Intelligence Community's Talent Woes," *International Journal of Intelligence and Counterintelligence*, Vol. 21, No. 4, 2008, pp. 748. (RW 3249)

Martin, A. & Wilson, P. "The Value of Non-Governmental Intelligence: Widening the Field," *Intelligence and National Security*, Vol. 23, No. 6, 2008, pp. 767-776. (RW 5354)

Martin, A.P. *Key Determinants of Information Availability: A Multiple Case Study* 2003. (RW 1451)

Martin, J.W. "What Basic Intelligence Seeks to do," *Studies in Intelligence*, Vol. 14, No. 2, 1970, pp. 103-113. (RW 575)

Martin, L.E.M. *The Challenge of Internet Literacy: The Instruction-Web Convergence*, Haworth Press, New York, 1997. (RW 3902)

Martin, R. *Stopping the Unthinkable: C3I Dimensions of Terminating a Limited Nuclear War*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1982. (RW 1020)

Martino, J.P. "Technological Forecasting in Managing Technological Systems," in *Management of R&D and Engineering*, ed. D.F. Kocaoglu, North-Holland, Amsterdam; New York, 1992, pp. 265. (RW 3839)

Martino, J.P. *Technological Forecasting for Decision Making*, 2nd ed., North-Holland, New York, 1983. (RW 3838)

Martinson, J.D. *What Makes Leaders "Think War?": Foreign Military Intervention Decision Making in Post-Cold War Germany* 2005. (RW 2645)

Martyn, J. "Information Needs and Uses," *Annual Review of Information Science and Technology*, Vol. 9, No. 1, 1974, pp. 3. (RW 2362)

Marzano, R.J. *Thinking and Reasoning Skills Rubric*, Utah Education Network. Available: http://www.uen.org/Rubric/rubric.cgi?rubric_id=1219, Viewed: February 20, 2010. (RW 4094)

Marzano, R.J. & Paynter, D.E. *New Approaches to Literacy: Helping Students Develop Reading and Writing Skills*, American Psychological Association, Washington, DC, 1994. (RW 2021)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Masback, K., Wade, A., Baxter, J. & Skelly, J. "Human-Systems Effectiveness: An Integrative Concept for the Intelligence Community," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 3469)

Masnick, A.M. & Morris, B.J. "Reasoning from Data: The Effect of Sample Size and Variability on Children's and Adults' Conclusions", *Proceedings of the 24th Annual Conference of the Cognitive Science Society*, pp. 643. (RW 2001)

Mason, L. & Boscolo, P. "Role of Epistemological Understanding and Interest in Interpreting a Controversy and in Topic-Specific Belief Change," *Contemporary Educational Psychology*, Vol. 29, No. 2, 2004, pp. 103. (RW 4281)

Mason, L. "Developing Epistemological Thinking to Foster Conceptual Change in Different Domains," in *Reconsidering Conceptual Change: Issues in Theory and Practice*, eds. M. Limón & L. Mason, Kluwer Academic, Dordrecht, 2002, pp. 301-336. (RW 5007)

Mason, L. "High School Student's Beliefs about Maths, Mathematical Problem Solving, and their Achievement in Maths: A Cross-Sectional Study," *Educational Psychology*, Vol. 23, No. 1, 2003, pp. 73. (RW 5077)

Mason, L. "Personal Epistemologies and Intentional Conceptual Change," in *Intentional Conceptual Change*, eds. G.M. Sinatra & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2003, pp. 199-236. (RW 4436)

Mason, L. "Beliefs about Knowledge and Revision of Knowledge: On the Importance of Epistemic Beliefs for Intentional Conceptual Change in Elementary and Middle School Students," in *Personal Epistemology in the Classroom: Theory, Research, and Implications for Practice*, eds. L.D. Bendixen & F.C. Feucht, Cambridge University Press, Cambridge, UK, 2010, pp. 258-291. (RW 5129)

Mason, L. & Boldrin, A. "Epistemic Metacognition in the Context of Information Searching on the Web," in *Knowing, Knowledge and Beliefs: Epistemological Studies Across Diverse Cultures*, ed. M.S. Khine, Springer, Dordrecht, 2008, pp. 377-404. (RW 4357)

Mason, L., Boldrin, A. & Ariasi, N. "Epistemic Metacognition in Context: Evaluating and Learning Online Information," *Metacognition and Learning*, Vol. 5, No. 1, 2010, pp. 67-90. (RW 4831)

Mason, L., Boscolo, P., Tornatora, M.C. & Ronconi, L. "Besides knowledge: a cross-sectional study on the relations between epistemic beliefs, achievement goals, self-beliefs, and achievement in science", *Instructional Science*, [Online], pp. April 10, 2012. Available from: http://dx.doi.org/10.1007/s11251-012-9210-0. 2012, (RW 5564)

Mason, L. & Boscolo, P. "Role of Epistemological Understanding and Interest in Interpreting a Controversy and in Topic-Specific Belief Change," *Contemporary Educational Psychology*, Vol. 29, No. 2, 2004, pp. 103-128. (RW 5436)

Mason, L. & Bromme, R. "Situating and Relating Epistemological Beliefs into Metacognition: Studies on Beliefs about Knowledge and Knowing," *Metacognition and Learning*, Vol. 5, No. 1, 2010, pp. 1-6. (RW 4835)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Mason, L. & Gava, M. "Effects of Epistemological Beliefs and Learning Text Structure on Conceptual Change," in *Re-Framing the Conceptual Change Approach in Learning and Instruction*, eds. S. Vosniadou, A. Baltas & X. Vamvakoussi, Elsevier, Amsterdam, 2007, pp. 165-196. (RW 5010)

Mason, L. & Scirica, F. "Prediction of Students' Argumentation Skills about Controversial Topics by Epistemological Understanding," *Learning and Instruction,* Vol. 16, No. 5, 2006, pp. 492-509. (RW 5437)

Mason, L. & Scrivani, L. "Enhancing Students' Mathematical Beliefs: An Intervention Study," *Learning and Instruction,* Vol. 14, No. 2, 2004, pp. 153-176. (RW 5096)

Matey, M. *Intelligence Studies at the Dawn of the 21st Century: New Possibilities and Resources for a Recent Topic in International Relations*, UNISCI, Madrid, Spain, 2005. (RW 5662)

Mathams, R.H. *Sub Rosa: Memoirs of an Australian Intelligence Analyst,* Allen & Unwin, Sydney, 1982. (RW 931)

Mathams, R.H. "The Intelligence Analyst's Notebook," in *Strategic Intelligence: Theory and Application*, ed. D.H. Dearth, US Army War College, Carlisle Barracks, PA, 1991, pp. 90-112. (RW 1095)

Mathes, J.C. & Stevenson, D.W. *Designing Technical Reports: Writing for Audiences in Organizations*, 2nd ed., Macmillan, New York, 1991. (RW 4495)

Matt, G.E. & Cook, T.D. "Threats to the Validity of Research Syntheses," in *The Handbook of Research Synthesis*, eds. H.M. Cooper & L.V. Hedges, Russell Sage Foundation, New York, 1994, pp. 503. (RW 2491)

Matthews, M., Tochinsky, P., Blanco, R., Atserias, J., Mika, P. & Zaragoza, H. "Searching through Time in the New York Times", *HCIR 2010: Proceedings of the Fourth Workshop on Human-Computer Interaction and Information Retrieval,* New Brunswick, NJ, August 22, 2010, pp. 41. (RW 4312)

Matthias, W.C. *America's Strategic Blunders: Intelligence Analysis and National Security Policy, 1936-1991,* Pennsylvania State University Press, University Park, PA, 2001. (RW 924)

Mattis, P. "The Analytic Challenge of Understanding Chinese Intelligence Services," *Studies in Intelligence,* Vol. 56, No. 3, 2012, pp. 47-57. (RW 5897)

Mattis, P.L. "Assessing Western Perspectives on Chinese Intelligence," *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 4, 2012, pp. 678-699. (RW 5801)

Mattis, P.L. "Assessing Western Perspectives on Chinese Intelligence," *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 4, 2012, pp. 678-699. (RW 5834)

Maturana, H.R. "Cognitive Strategies," in *Cybernetics of Cybernetics*, ed. H. von Foerster, 1974. (RW 2562)

Matz, D.C. & Wood, W. "Cognitive Dissonance in Groups: The Consequences of Disagreement," *Journal of Personality and Social Psychology,* Vol. 88, No. 1, 2005, pp. 22-37. (RW 1928)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Maudsley, G. & Strivens, J. "'Science', 'Critical Thinking' and 'Competence' for Tomorrow's Doctors. A Review of Terms and Concepts," *Medical Education,* Vol. 34, No. 1, 2000, pp. 53-60. (RW 4115)

Maurer, A.C., Tunstall, M.D. & Keagle, J.M. *Intelligence--Policy and Process,* Westview Press, Boulder, CO, 1985. (RW 1185)

Mavin, T.J. & Murray, P.S. "The Development of Airline Pilot Skills through Simulated Practice," in *Learning Through Practice: Models, Traditions, Orientations, and Approaches*, ed. S. Billett, Springer, Dordrecht, 2010, pp. 268-286. (RW 4964)

May, D.B. & Etkina, E. "College Physics Students' Epistemological Self-Reflection and its Relationship to Conceptual Learning," *American Journal of Physics,* Vol. 70, No. 12, 2002, pp. 1249-58. (RW 5435)

May, E.R. "Intelligence: Backing into the Future," in *U.S. Intelligence at the Crossroads: Agendas for Reform*, eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 36-45. (RW 640)

May, E.R. "Studying and Teaching Intelligence," *Studies in Intelligence,* Vol. 38, No. 5, 1995, pp. 1-5. (RW 67)

May, K. "Abstract Knowing: The Case for Magic in Method," in *Critical Issues in Qualitative Research Methods*, ed. J.M. Morse, Sage Publications, Thousand Oaks, 1994, pp. 10. (RW 2654)

Maybury, M., Chase, P., Cheikes, B., Brackney, D., Matzner, S., Hetherington, T., Wood, B., Sibley, C., Marin, J., Longstaff, T., Spitzner, L., Haile, J., Copeland, J. & Lewandowski, S. "Analysis and Detection of Malicious Insiders," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 816)

Mayer, R.E. "Knowledge and Thought: Mental Models that Support Scientific Reasoning," in *Philosophy of Science, Cognitive Psychology, and Educational Theory and Practice*, eds. R.A. Duschl & R.J. Hamilton, State University of New York Press, Albany, 1992, pp. 226-243. (RW 5482)

Mayer, R.E. *Thinking, Problem Solving, Cognition,* 2nd ed., W.H. Freeman, New York, 1992. (RW 2371)

Mayer, R.E. "Cognitive, Metacognitive, and Motivational Aspects of Problem Solving," *Instructional Science,* Vol. 26, No. 1-2, 1998, pp. 49-63. (RW 5286)

Mayer, R.E. "Understanding Conceptual Change: A Commentary," in *Reconsidering Conceptual Change: Issues in Theory and Practice*, eds. M. Limón & L. Mason, Kluwer Academic, Dordrecht, 2002, pp. 101-114. (RW 5002)

Mayer, R.E. "Advances in Specifying What is to be Learned: Reflections on the Themes in Chapters 6-8," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 203-211. (RW 5142)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Mayer, R.E. & Wittrock, M.C. "Problem Solving," in *Handbook of Educational Psychology*, eds. P.A. Alexander & P.H. Winne, 2nd ed., L. Erlbaum Associates, Mahwah, NJ, 2006, pp. 287. (RW 3846)

Maynard, C.A. "Relationship of Critical Thinking Ability to Professional Nursing Competence," *Journal of Nursing Education,* Vol. 35, No. 1, 1996, pp. 12-18. (RW 3961)

Mayo, R., Schul, Y. & Burnstein, E. *Journal of Experimental Social Psychology,* Vol. 40, 2004, pp. 433. (RW 2792)

McAfee, A. *Enterprise 2.0: New Collaborative Tools for Your Organization's Toughest Challenges,* 2009. (RW 3684)

McBeth, M.S. *Knowledge Elicitation and Learning to Transfer Expertise between Generations of Naval Intelligence Analysts. - Final Rept.* ADA403918, 2002. (RW 1203)

McBeth, M.S. *Approaches to Enhance Sensemaking for Intelligence Analysis,* Naval War College, Newport, RI, 2002. (RW 267)

McCabe, M.C., Grossman, D.A., Alford, K.L., Chowdhury, A., Holmes, D. & Frieder, O. *IIT at TREC-8: Improving Baseline Precision* (RW 1557)

McCallum, A., Corrada-Emmanuel, A. & Wang, X. "A Probabilistic Model for Topic and Role Discovery in Social Networks and Message Text," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 805)

McCarthy, A.C. "The Intelligence Mess: How it Happened, What to do About It," *Commentary,* April, 2004, pp. 11. (RW 2038)

McCarthy, D.S. *The CIA and the Cult of Secrecy,* Ph.D. dissertation, College of William and Mary, 2008. (RW 4536)

McCarthy, E.E. "Human Capital Overview", *75th Military Operations Research Society Symposium,* Annapolis, MD, 1 June 2007, pp.11-32. (RW 4669)

McCarthy, M. *The Relationship between Student Critical Thinking Disposition at the United States Air Command and Staff College and Academic Performance,* Air University, Maxwell Air Force Base, AL, 2001. (RW 5032)

McClanahan, K. "A Perception Based Model for Comparing Intelligence Communities," *American Intelligence Journal,* Vol. 25, No. 2, 2007/2008, pp. 46. (RW 3227)

McClelland, C.V. *The Nature of Science and the Scientific Method*, Geological Society of America, Boulder, CO, 2006. (RW 5580)

McClelland, G.H. "Use of Signal Detection Theory as a Tool for Enhancing Performance and Evaluating Tradecraft in Intelligence Analysis," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, pp. 83-99. (RW 4773)

McComas, W.F. & Olson, J.K. "The Nature of Science in International Science Education Standards Documents," in *The Nature of Science in Science Education: Rationales and Strategies* Kluwer Academic Publishers, Dordrecht, 1998, pp. 41-52. (RW 5516)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

McConnell, J.M. *Annual Threat Assessment of the Director of National Intelligence for the Senate Select Committee on Intelligence* 2008. (RW 2933)

McConnell, J.M. *The Evolution of Intelligence and the Public Policy Debate on Encryption,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1997. (RW 1021)

McConnell, M. *Remarks and Q&A by the Director of National Intelligence. ODNI Open Source Conference.* 2007. (RW 2726)

McConnell, M. *Remarks and Q&A by the Director of National Intelligence. Project on National Security Reform Conference.* 2007. (RW 2729)

McConnell, M. *Strengthening Analytic Practice: Lessons from the World of Journalism. Remarks and Q&A by the Director of National Intelligence.* 2007. (RW 2875)

McConnell, M. "Bill Wrongly Shields Press," *USA Today,* July 28, 2008, (RW 3191)

McConnell, M. "Collaborate, Cooperate, Integrate," *Pathfinder,* Vol. 6, No. 3, 2008, pp. 3. (RW 3128)

McConnell, M. *Remarks and Q&A by the Director of National Intelligence. Foreign Affairs Symposium.* 2008. (RW 3020)

McConnell, M. *Remarks and Q&A by the Director of National Intelligence. Furman University.* 2008. (RW 3021)

McConnell, M. *Remarks and Q&A by the Director of National Intelligence. St. Mary's College of Maryland.* 2008. (RW 2928)

McCoy, J.W. *Mirror Imaging: The CIA's Espionage Psychology,* 2005. (RW 1297)

McCrank, L.J. *Historical Information Science: An Emerging Unidiscipline,* Information Today, Medford, NJ, 2001. (RW 5183)

McCreary, J. & Posner, R.A. "The Latest Intelligence Crisis," *Intelligence and National Security,* Vol. 23, No. 3, 2008, pp. 371. (RW 3172)

McCue, C. *Data Mining and Predictive Analysis: Intelligence Gathering and Crime Analysis,* Butterworth-Heinemann, Boston, 2006. (RW 1629)

McCurdy, D. "Glasnost for the CIA," *Foreign Affairs,* Vol. 73, No. 1, 1994, pp. 125-140. (RW 582)

McCusker, J.P., Lebo, T., Ding, L., Chang, C., Pinheiro da Silva, P. & McGuinness, D.L. "Where Did You Hear That? Information and the Sources They Come From", *International Workshop on Linked Science,* Bonn, Germany, October 14, 2011 (RW 5549)

McCutcheon, C. "Fixing US Intelligence: A Cultural Revolution," *CQ Weekly,* Vol. 59, No. 38, 2001, pp. 2304-2310. (RW 229)

McDermott, I.E. "Confessions of a Serial Clicker: Ulrich's on the Web," *Searcher,* Vol. 10, No. 9, 2002, pp. 8. (RW 1568)

McDermott, R. "Experimental Intelligence," *Intelligence and National Security,* Vol. 26, No. 1, 2011, pp. 82-98. (RW 4730)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

McDonald, J.K. "CIA and Warning Failures," in *Intelligence in the Cold War: Organisation, Role, International Cooperation*, eds. L.C. Jenssen & O. Riste, Norwegian Institute for Defence Studies, Oslo, Norway, 2001, pp. 41. (RW 3181)

McDonald, M. "Would You Believe...Iranian Moderates? (when Will the CIA Get Smart?)," *Washington Monthly*, Vol. 19, No. 10, 1987 (RW 4592)

McDowell, D. *Strategic Intelligence Analysis: Guidelines on Methodology and Application,* Istana Enterprises Pty. Ltd., Cooma N.S.W., 1997. (RW 1532)

McDowell, D. *Strategic Intelligence: A Handbook for Practitioners, Managers and Users,* Istana Enterprises Pty. Ltd, Cooma N.S.W., 1998. (RW 655)

McDowell, D. *Strategic Intelligence and Analysis: Selected Writings,* Istana Enterprises Pty. Ltd, Cooma N.S.W., 2000. (RW 967)

McDowell, D. *Strategic Intelligence: A Handbook for Practitioners, Managers, and Users,* Revised ed., Scarecrow Press, Lanham, MD, 2009. (RW 3678)

McDowell, D. "Sharing the Findings: The Challenge for Strategic Analysts to Justify and Explain Themselves [Powerpoint Presentation]", *Global Intelligence Forum 2010,* Dungarvan, Ireland, July 11-13, 2010 (RW 4228)

McElroy, T. & Seta, J.J. "Framing Effects: An Analytic-Holistic Perspective," *Journal of Experimental Social Psychology,* Vol. 39, 2003, pp. 610. (RW 2423)

McGarry, K.J. *The Changing Context of Information: An Introductory Analysis,* 2nd ed., Library Association Pub, London, 1993. (RW 1870)

McGill, G.M. "OSCINT and the Private Information Sector," *International Journal of Intelligence and Counterintelligence,* Vol. 7, No. 4, 1995, pp. 435-443. (RW 46)

McGill, W. *Actionable Risk Assessment* 2008. (RW 3367)

McGrath, T.A. "Management for the 80s - Theory Z and Beyond," *Computer Security Journal,* Fall-Winter, 1983, pp. 59. (RW 3950)

McGuire, W.J. "A Contextualist Theory of Knowledge: Its Implications for Innovation and Reform in Psychological Research," *Advances in Experimental Social Psychology,* Vol. 16, 1983, pp. 1. (RW 4031)

McGuire, W.J. "Creative Hypothesis Generating in Psychology: Some Useful Heuristics," *Annual Review of Psychology,* Vol. 48, 1997, pp. 1. (RW 1963)

McIlveen, P., Brooks, S., Lichtenberg, A., Smith, M., Torjul, P. & Tyler, J. "Career Development Learning Frameworks for Work-Integrated Learning," in *Developing Learning Professionals*, eds. S. Billett & A. Henderson, Springer, Dordrecht, 2011, pp. 149-168. (RW 4906)

McInerney, D.M. & van Etten, S. *Big Theories Revisited,* Information Age Publishing, Greenwich, CT, 2000. (RW 5530)

McIntosh, K. *Use the Clues: Problem Solving through Logical Reasoning,* 1991. (RW 3913)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

McIntyre, D.B. "James Hutton and the Philosophy of Geology," in *The Fabric of Geology*, ed. C.C. Albritton, Freeman, Cooper, & Co., Stanford, CA, 1963, pp. 1-11. (RW 5444)

McIvor, A.D. "Network Centric Warfare (Book Review)," *American Intelligence Journal*, Vol. 26, No. 2, 2008/2009, pp. 80. (RW 3630)

McKay, R.T. & Dennett, D.C. "The Evolution of Misbelief," *The Behavioral and brain sciences*, Vol. 32, No. 6, 2009, pp. 493-510. (RW 5742)

McKeachie, W.J. & Hofer, B.K. *McKeachie's Teaching Tips: Strategies, Research, and Theory for College and University Teachers*, 11th ed., Houghton Mifflin Co., Boston, 2002. (RW 4674)

McKeachie, W.J., Svinicki, M.D. & Hofer, B.K. *McKeachie's Teaching Tips: Strategies, Research, and Theory for College and University Teachers*, 12th ed., Houghton Mifflin, Boston, 2006. (RW 4673)

McKenzie, C.R.M. "Taking into Account the Strength of an Alternative Hypothesis," *Journal of Experimental Psychology: Learning, Memory, & Cognition*, Vol. 24, No. 3, 1998, pp. 771. (RW 1836)

McKenzie, C.R.M. "Hypothesis Testing and Evaluation," in *Blackwell Handbook of Judgment and Decision Making*, eds. D.J. Koehler & N. Harvey, Blackwell Pub., Malden, MA; Oxford, 2004, pp. 200. (RW 2803)

McKenzie, R., Evans, Jonathan St. B. T. & Handley, S.J. "Conditional Reasoning in Autism: Activation and Integration of Knowledge and Belief," *Developmental Psychology*, Vol. 46, No. 2, 2010, pp. 391-403. (RW 5694)

McKnight, C.E. *C3I Systems at the Joint Level*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1987. (RW 1022)

McKown, L. *Improving Leadership through Better Decision Making: Fostering Critical Thinking*, Air Command and Staff College, Montgomery, AL, 1997. (RW 4256)

McLaughlin, J. *A Bayesian Updating Model for Intelligence Analysis: A Case Study of Iraq's Nuclear Weapons Program*, Center for International Security and Cooperation, Stanford University, Stanford, CA, 2005. (RW 1174)

McLaughlin, J. & Pate-Cornell, M.E. "A Bayesian Approach to Iraq's Nuclear Program Intelligence Analysis: A Hypothetical Illustration," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 793)

McLaughlin, J. "Serving the National Policymaker," in *Analyzing Intelligence: Origins, Obstacles, and Innovations*, eds. R.Z. George & J.B. Bruce, 2008, pp. 71. (RW 3096)

McLaughlin, J. "Action Memorandum," *The American Interest*, Vol. 14, No. 4, 2009, pp. 32. (RW 3426)

McLaughlin, J.E. *Emerging Missile Threats to North America. Statement for the Record. Hearings of the Senate Select Committee on Intelligence* 1996. (RW 433)

McLaughlin, J.E. "New Challenges and Priorities for Analysis," *Defense Intelligence Journal*, Vol. 6, No. 2, 1997, pp. 11-21. (RW 1575)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

McLean, M.B. & Knapp, B.G. *Modeling Intelligence Production Performance,* ARL-CR-444, Army Research Lab, Aberdeen Proving Ground, MD, 1999. (RW 1178)

McLellan, L. & Mandel, D.R. "Cognitive Styles Predict Accuracy and Coherence in Intelligence Analyst's Judgments [Poster Presentation]", *Sixth Annual Southern Ontario Behavioral Decision Research Conference*, Toronto, ON, May 7, 2010 (RW 5362)

McMackin, M.C. *Discourse Synthesis: The Role of Task Impression, Goal Setting, Organization, and Connectivity when Writing from Sources,* Ph.D. dissertation, University of Massachusetts Lowell, 1994. (RW 2299)

McManis, D.Y. *National Security and the Democratization of Information*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1990. (RW 1023)

McMillan, J.H. "Enhancing College Students' Critical Thinking: A Review of Studies," *Research in Higher Education,* Vol. 26, No. 1, 1987, pp. 3-27. (RW 3965)

McMullen, T.H. *A Tactical Commander's View of C3I*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1982. (RW 1024)

McNamara, L.A. & Orlando-Gay, N. "Reading, Sorting, Marking, Shuffling: Mental Model Formation through Information Foraging", *Beliv 2012,* Seattle, WA, October 14-15, 2012 (RW 5831)

McNamara, T.E. *Statement for the Record before the Subcommittee on Intelligence, Information Sharing, and Terrorism Risk Assessment. House Committee on Homeland Security.* 2006. (RW 1390)

McNeese, M.D. "Humane Intelligence: A Human Factors Perspective for Developing Intelligent Cockpits," *IEEE Aerospace and Electronics Systems Magazine,* Vol. 1, No. 9, 1986, pp. 6-12. (RW 5673)

McNeese, M.D. & Ayoub, P.J. "Concept Mapping in the Analysis and Design of Cognitive Systems: A Historical Review," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge*, eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 47-66. (RW 4966)

McPeck, J.E. *Critical Thinking and Education,* St. Martin's Press, New York, NY, 1981. (RW 3700)

McPeck, J.E. "Critical Thinking and Subject Specificity: A Reply to Ennis," *Educational Researcher,* Vol. 19, No. 4, 1990, pp. 10-12. (RW 3706)

McPherson, G.R. "Teaching and Learning the Scientific Method," *American Biology Teacher,* Vol. 63, No. 4, 2001, pp. 242. (RW 4027)

McTighe, J.J. "Teaching for Thinking, of Thinking, and about Thinking," in *Thinking Skills Instruction: Concepts and Techniques*, eds. M. Heiman & J. Slomianko, National Education Association, Washington, DC, 1987, pp. 24-30. (RW 5079)

Mead, J., Gray, S., Hamer, J., James, R., Sorva, J., St. Clair, C. & Thomas, L. *A Cognitive Approach to Identifying Measurable Milestones for Programming Skill Acquisition* 2006. (RW 2071)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Meadows, L.M. & Dodendorf, D.M. "Data Management and Interpretation using Computers to Assist," in *Doing Qualitative Research*, eds. B.F. Crabtree & W.L. Miller, 2nd ed., Sage Publications, Thousand Oaks, Calif, 1999, pp. 195. (RW 2507)

Mechner, F. "Anatomy of Deception: A Behavioral Contingency Analysis," *Behavioural Processes*, Vol. 84, No. 1, 2010, pp. 516-520. (RW 5595)

Medeiros, N. "Reap what You Sow: Harvesting the Deep Web," *OCLC Systems and Services*, Vol. 18, No. 1, 2002, pp. 18. (RW 1408)

Medin, D.L. & Rips, L.J. "Concepts and Categories: Memory, Meaning, and Metaphysics," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 37-72. (RW 3998)

Medina, C. *21st Century Analysis* 2003. (RW 1452)

Medina, C.A. "What to do when Traditional Models Fail," *Studies in Intelligence*, Vol. 46, No. 3, 2002, pp. 23-28. (RW 938)

Medina, C.A. "The New Analysis," in *Analyzing Intelligence: Origins, Obstacles, and Innovations*, eds. R.Z. George & J.B. Bruce, 2008, pp. 238. (RW 3107)

Meinefeld, W. "Hypotheses and Prior Knowledge in Qualitative Research," in *A Companion to Qualitative Research*, eds. U. Flick, E. von Kardorff & I. Steinke, Sage Publications, London; Thousand Oaks, CA, 2004, pp. 153. (RW 3207)

Meiron, D., et. al. *Data Analysis Challenges* 2008. (RW 3514)

Mele, A.R. *Self-Deception Unmasked*, Princeton University Press, Princeton, NJ, 2001. (RW 4408)

Mena, J. *Investigative Data Mining for Security and Criminal Detection*, Butterworth-Heinemann, Amsterdam, 2003. (RW 1690)

Mengshoel, O.J. & Wilkins, D.C. "Abstraction for Belief Revision: Using a Genetic Algorithm to Compute the most Probable Explanation", *Proc. AAAI Spring Symposium Series on Satisficing Models*, March 1998 (RW 926)

Merali, Y. "Individual and Collective Congruence in the Knowledge Management Process," *Journal of Strategic Information Systems*, Vol. 9, No. 2-3, 2000, pp. 213-234. (RW 4586)

Mercado, S. "Sailing the Sea of OSINT in the Information Age," *Studies in Intelligence*, Vol. 48, No. 3, 2004 (RW 4306)

Mercado, S.C. "Reexamining the Distinction between Open Information and Secrets," *Studies in Intelligence*, Vol. 49, No. 2, 2005 (RW 750)

Mercier, H. & Sperber, D. "Why Do Humans Reason? Arguments for an Argumentative Theory," *Behavioral and Brain Sciences*, Vol. 34, 2011, pp. 57-111. (RW 4872)

Mericsko, R.J. *Intelligence Technology Innovation Center Overview Briefing [Powerpoint Presentation]* (RW 1992)

Merkle, J.H. "Policy Bias," *Studies in Intelligence*, Vol. 7, No. 1, 1963, pp. 55-69. (RW 4205)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Merriam, S.B., Caffarella, R.S. & Baumgartner, L. *Learning in Adulthood: A Comprehensive Guide,* 3rd ed., Jossey-Bass, San Francisco, CA, 2007. (RW 5269)

Merton, R.K. "The Matthew Effect II: Cumulative Advantage and the Symbolism of Intellectual Property," *Isis,* Vol. 79, 1988, pp. 606. (RW 2007)

Mescall, P.N. "A Creature of Compromise: The Establishment of the DIA," *International Journal of Intelligence and Counterintelligence,* Vol. 7, No. 3, 1994, pp. 251-274. (RW 191)

Mesher, C. *Mission Critical,* San Jose State University. Available: http://www.sjsu.edu/depts/itl/index.htm, Viewed: February 15, 2010. (RW 4100)

Mesmer-Magnus, J.R. & DeChurch, L.A. "Information Sharing and Team Performance: A Meta-Analysis," *Journal of Applied Psychology,* Vol. 94, No. 2, 2009, pp. 535-546. (RW 5478)

Messick, S. "The Nature of Cognitive Styles: Problems and Promise in Educational Practice," *Educational Psychologist,* Vol. 19, No. 2, 1984, pp. 59-74. (RW 5053)

Messick, S. "The Matter of Style: Manifestations of Personality in Cognition, Learning, and Teaching," *Educational Psychologist,* Vol. 29, No. 3, 1994, pp. 121-136. (RW 4979)

Meszerics, T. & Littvay, L. "Pseudo-Wisdom and Intelligence Failures," *International Journal of Intelligence and Counterintelligence,* Vol. 23, No. 1, 2010, pp. 133. (RW 3771)

Metscher, R. & Gilbride, B. *Intelligence as an Investigative Function* 2005. (RW 3303)

Meyer, H.E. *What's Wrong with the CIA?* Hillsdale College, Hillsdale, MI, 2003. (RW 467)

Meyer, H.E. "Doing intel right", *National Review Online,* [Online], Available from: http://www.nationalreview.com/comment/meyer200504120757.asp, 2005, (RW 483)

Meyerrose, D.W. *Networks, Information Technology, and Paved Cowpaths,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2001. (RW 1164)

Meyerrose, D.W. *Adapting the Military to the Homeland Defense and Homeland Security Missions,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2003. (RW 1163)

Mezirow, J. *Transformative Dimensions of Adult Learning,* Jossey-Bass, San Francisco, CA, 1991. (RW 2652)

Middleton, G.R. "A Maturity Model for Intelligence Education," *American Intelligence Journal,* Vol. 25, No. 2, 2007/2008, pp. 33-44. (RW 3226)

Mihalcea, R. & Tarau, P. "Multi-Document Summarization with Iterative Graph-Based Algorithms," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 859)

Mihelic, F.M. "Generalist Function in Intelligence Analysis," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 846)

Mikulec, J.A. & Pinter, A. "Making the Grade: Academia and its Updated Role in Intelligence Analysis," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 854)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Milburn, M.A. "Sources of Bias in the Prediction of Future Events," *Organizational Behavior and Human Performance,* Vol. 21, No. 1, 1978, pp. 17-26. (RW 1088)

Militello, L.G. & Hutton, R.J.B. "Applied Cognitive Task Analysis (ACTA): A Practitioner's Toolkit for Understanding Cognitive Task Demands," *Ergonomics,* Vol. 41, No. 11, 1998, pp. 203-219. (RW 672)

Miller, A.H. & Damask, N. "Thinking about Intelligence After the Fall of Communism," *International Journal of Intelligence and Counterintelligence,* Vol. 6, No. 3, 1993, pp. 257-269. (RW 45)

Miller, B.H. "Improving all-Source Intelligence Analysis: Elevate Knowledge in the Equation," *International Journal of Intelligence and Counterintelligence,* Vol. 21, No. 2, 2008, pp. 337. (RW 2970)

Miller, B.H. "Soldiers, Scholars, and Spies: Combining Smarts and Secrets," *Armed Forces & Society,* Vol. 36, No. 4, 2010, pp. 695-715. (RW 5590)

Miller, C.S., Lehman, J.F. & Koedinger, K.R. "Goals and Learning in Microworlds," *Cognitive Science,* Vol. 23, 1999, pp. 305. (RW 2164)

Miller, F.P., Vandome, A.F. & McBrewster, J. *Intelligence Analysis,* [not provided], 2010. (RW 4502)

Miller, G.R. "Human Information Processing: Some Research Guidelines," in *Conceptual Frontiers in Speech-Communication: Report,* eds. R.J. Kibler, L.L. Barker & Speech Association of America, Speech Association of America, New York, 1969, pp. 513. (RW 2157)

Miller, J.E., Patterson, E.S. & Woods, D.D. "Critiquing as a Cognitive Task Analysis (CTA) Methodology", *Proceedings of the Human Factors and Ergonomics Society 45th Annual Meeting,* Santa Monica, CA, pp. 518-522. (RW 356)

Miller, P.D. "Working for the "War Czar": Lessons for Intelligence Support to Policymaking during Crises," *Studies in Intelligence,* Vol. 54, No. 2, 2010, pp. 49-56. (RW 4200)

Miller, P. *The Smart Swarm: How Understanding Flocks, Schools, and Colonies Can Make Us Better at Communicating, Decision Making, and Getting Things Done,* Avery, New York, 2010. (RW 4247)

Miller, S. *Web Searching Strategies: An Introductory Curriculum for Students and Teachers,* 2nd ed., International Society for Technology in Education, Eugene, OR, 2003. (RW 3543)

Miller, T. & Agne, S. "Attention-Based Information Retrieval using Eye Tracker Data", *K-Cap '05,* Banff, Alberta, Canada, October 2-5, 2005, pp. 209. (RW 1536)

Miller, W.L. & Crabtree, B.F. "Qualitative Analysis: How to Begin Making Sense," *Family Practice Research Journal,* Vol. 14, No. 3, 1994, pp. 289. (RW 2674)

Miller, W.L. & Crabtree, B.F. "Clinical Research: A Multimethod Typology and Qualitative Roadmap," in *Doing Qualitative Research,* eds. B.F. Crabtree & W.L. Miller, 2nd ed., Sage Publications, Thousand Oaks, Calif, 1999, pp. 3. (RW 2425)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Miller, W.L. & Crabtree, B.F. "The Dance of Interpretation," in *Doing Qualitative Research*, eds. B.F. Crabtree & W.L. Miller, 2nd ed., Sage Publications, Thousand Oaks, Calif, 1999, pp. 127. (RW 2503)

Millman, A.B. "Critical Thinking Attitudes: A Framework for the Issues," *Informal Logic*, Vol. 10, No. 1, 1988, pp. 45-50. (RW 5025)

Mills, G.H. *The Role of Rhetorical Theory in Intelligence Analysis: A Soldier's Guide to Rhetorical Theory*, Air University Press, Maxwell AFB, AL, 2003. (RW 382)

Milo, P. *Your Flying Car Awaits: Robot Butlers, Lunar Vacations, and Other Dead-Wrong Predictions of the Twentieth Century*, Harper Paperbacks, New York, 2009. (RW 3823)

Minbashian, A., Earl, J. & Bright, J.E.H. "Openness to Experience as a Predictor of Job Performance Trajectories," *Applied Psychology*, Vol. 62, No. 1, 2013, pp. 1-12. (RW 5872)

Minihan, K.A. *Shaping the Intelligence Environment in the Information Age*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1999. (RW 1025)

Minnery, B. *Integrated Cognitive-Neuroscience Architectures for Understanding Sensemaking [Powerpoint Presentation]* 2010. (RW 4518)

Minsky, M.L. *The Emotion Machine: Commonsense Thinking, Artificial Intelligence, and the Future of the Human Mind*, 2006. (RW 1807)

Mitchell, K.J. "The Genetics of Brain Wiring: From Molecule to Mind," *PLoS Biology*, Vol. 5, No. 4, 2007 (RW 2294)

Mitelman, L.T. "Preface to a Theory of Intelligence," *Studies in Intelligence*, Vol. 18, No. 3, 1974, pp. 19-22. (RW 550)

Mitroff, I.I. & Featheringham, T.R. "On Systematic Problem Solving and the Error of the Third Kind," *Behavioural Sciences*, Vol. 29, No. 6, 1974, pp. 383. (RW 2682)

Mitroff, I.I. & Linstone, H.A. *The Unbounded Mind: Breaking the Chains of Traditional Business Thinking*, Oxford University Press, New York, 1993. (RW 2870)

Mizzaro, S. "How Many Relevances in Information Retrieval?" *Interacting with Computers*, Vol. 10, 1998, pp. 305. (RW 3474)

Mlodinow, L. *Subliminal: How Your Unconscious Mind Rules Your Behavior*, Pantheon Books, New York, NY, 2012. (RW 5849)

Mocanu, M. "Open Source Exploitation and the Concepts of Knowledge Development/Understanding", *The International Scientific Conference: Strategies XXI. The Complex and Dynamic Nature of the Security Environment*, Bucharest, Romania, November 22-23, 2012, pp. 136-146. (RW 5874)

Moffitt, T.E., Arseneault, L., Belsky, D., Dickson, N., Hancox, R.J., Harrington, H., Houts, R., Poultron, R., Roberts, B.W., Ross, S., Sears, M.R., Thomson, W.M. & Caspi, A. "A gradient of childhood self-control predicts health, wealth, and public safety", *PNAS Early Edition*, [Online], Available from: www.pnas.org/cgi/doi/10.1073/pnas.1010076108, December 21, 2010, (RW 4838)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Molander, R.C., Riddile, A. & Wilson, P.A. *Strategic Information Warfare: A New Face of War*, RAND Corp., Santa Monica CA, 1996. (RW 4555)

Molden, D.C. & Higgins, E.T. "Motivated Thinking," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 295-320. (RW 4007)

Moldovan, D., Srikanth, M. & Badulescu, A. "Synergist: Topic and User Knowledge Bases from Textual Sources for Collaborative Intelligence Analysis", *CASE PI Conference,* (RW 5108)

Moldoveanu, M. & Langer, E. "False Memories of the Future: A Critique of the Applications of Probabilistic Reasoning to the Study of Cognitive Processes," *Psychological Review*, Vol. 109, No. 2, 2002, pp. 358. (RW 2357)

Mole, C. "Three Philosophical Lessons for the Analysis of Criminal and Military Intelligence," *Intelligence and National Security*, Vol. 27, No. 4, 2012, pp. 441-458. (RW 5812)

Molloy, E. & Keating, J. "Targeted Preparation for Clinical Practice," in *Developing Learning Professionals*, eds. S. Billett & A. Henderson, Springer, Dordrecht, 2011, pp. 59-82. (RW 4903)

Moncrieff, J. "Research Synthesis: Systematic Reviews and Meta-Analysis," *International Review of Psychiatry,* Vol. 10, 1998, pp. 304. (RW 2256)

Monitor 360. *Practical Steps for Improving Intelligence Analysis* 2009. (RW 3532)

Montague, L.L. "The Origins of National Intelligence Estimating," *Studies in Intelligence,* Vol. 16, No. 2, 1972, pp. 63-70. (RW 564)

Montgomery, H., Lipshitz, R. & Brehmer, B. *How Professionals Make Decisions,* L. Erlbaum Associates, Mahwah, NJ, 2005. (RW 1319)

Montgomery, L.G. *Critical Thinking in Medical Education: Systematic Review with an Emphasis on Assessment and Comparison with General Education,* M.S. Ed. dissertation, John Carroll University, 2003. (RW 2234)

Montgomery, M.C. *Cyber Threats: Developing a National Strategy for Defending our Cyberspace*, Center for Information Policy Research, Harvard University, Cambridge, MA, 2001. (RW 1162)

Moon, B.M., Hansberger, J.T. & Tate, A. "Concept Mapping in Virtual Collaboration Environments," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge*, eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 293-316. (RW 4977)

Moon, B.M. & Hoffman, R.R. *How Might "Transformational" Technologies and Concepts be Barriers to Sensemaking in Intelligence Analysis?* 2005. (RW 3379)

Moon, B.M., Hoffman, R.R., Eskridge, T.C. & Coffey, J.W. "Skills in Applied Concept Mapping," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge*, eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 23-46. (RW 4965)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Moonesinghe, R., Khoury, M.J. & Janssens, A. C. J. W. "Most Published Research Findings are False - but a Little Replication Goes a Long Way," *PLoS Medicine*, Vol. 4, No. 2, 2007, pp. e28. (RW 3286)

Moore, B.N. & Parker, R. *Critical Thinking*, 9th ed., McGraw-Hill, Boston, MA, 2009. (RW 3676)

Moore, D.T. *Strengthening Community: Considerations for a Research Agenda* (RW 1346)

Moore, D.T. *Species of Competencies for Intelligence Analysis.* [undated draft]. (RW 244)

Moore, D.T. *Creating Intelligence: Evidence and Inference in the Analysis Process*, MSSI thesis, Joint Military Intelligence College, 2002. (RW 678)

Moore, D.T. *Defining Intelligence Analysis Work Roles* 2005. (RW 3725)

Moore, D.T. *Critical Thinking and Intelligence Analysis*, Joint Military Intelligence College, Washington, DC, 2006. (RW 1624)

Moore, D.T. *Critical Thinking and Intelligence Analysis. Second Edition.* 2007. (RW 2957)

Moore, D.T. *Sensemaking: A Structure for an Intelligence Revolution*, National Defense Intelligence College, Washington, DC, 2011. (RW 5156)

Moore, D.T. & Krizan, L. *Core Competencies for Intelligence Analysts [Powerpoint Presentation]* (RW 1442)

Moore, D.T. & Krizan, L. "Intelligence Analysis: Does NSA have what it Takes?" *Cryptologic Quarterly*, Vol. 20, No. 1-2, 2001, pp. 1-32. (RW 673)

Moore, D.T. & Krizan, L. "Core Competencies for Intelligence Analysis at the National Security Agency," in *Bringing Intelligence about: Practitioners Reflect on Best Practices*, ed. R.G. Swenson, Joint Military Intelligence College, Center for Strategic Intelligence Research, Washington, DC, 2003, pp. 95-131. (RW 1490)

Moore, D.T., Krizan, L. & Moore, E.J. "Evaluating Intelligence: A Competency-Based Model," *International Journal of Intelligence and Counterintelligence*, Vol. 18, No. 2, 2005, pp. 204-220. (RW 301)

Moore, M.H. "Anatomy of the Heroin Problem: An Exercise in Problem Definition," *Policy Review*, Vol. 21976, pp. 639. (RW 2771)

Moorman, T.S. *The Commission to Assess U.S. National Security Space Management and Organizations*, 2001. (RW 1161)

Moray, N. "Mental Models in Theory and Practice," in *Attention and Performance XVII: Cognitive Regulation of Performance: Interaction of Theory and Application*, eds. D. Gopher & A. Koriat, MIT Press, Cambridge, MA, 1999, pp. 223. (RW 2480)

Morgan, G. "Exploring Choice: Reframing the Process of Evaluation," in *Beyond Method: Strategies for Social Research*, ed. G. Morgan, Sage Publications, Beverly Hills, CA, 1983, pp. 392. (RW 3203)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Morgan, G. "In Research, as in Conversation, we Meet Ourselves," in *Beyond Method: Strategies for Social Research*, ed. G. Morgan, Sage Publications, Beverly Hills, CA, 1983, pp. 405. (RW 3204)

Morgan, G. "Knowledge, Uncertainty, and Choice," in *Beyond Method: Strategies for Social Research*, ed. G. Morgan, Sage Publications, Beverly Hills, CA, 1983, pp. 383. (RW 3202)

Morgan, G. "The Significance of Assumptions," in *Beyond Method: Strategies for Social Research*, ed. G. Morgan, Sage Publications, Beverly Hills, CA, 1983, pp. 377. (RW 3201)

Morgan, G. "Toward a More Reflective Social Science," in *Beyond Method: Strategies for Social Research*, ed. G. Morgan, Sage Publications, Beverly Hills, CA, 1983, pp. 368. (RW 3200)

Morin, A. & Everett, J. "Inner Speech as a Mediator of Self-Awareness, Self-Consciousness, and Self-Knowledge: An Hypothesis," *New Ideas in Psychology*, Vol. 8, No. 3, 1990, pp. 337-356. (RW 5789)

Moritz, F. "Cross-Impact Analysis: Forecasting the Future of Rhodesia," in *Quantitative Approaches to Political Intelligence: The CIA Experience*, ed. R.J.J. Heuer, Westview Press, Boulder, CO, 1978, pp. 11-45. (RW 914)

Moritz, F.A. *Predicting Surprise Attack* 2005. (RW 505)

Morley, N.J., Evans, Jonathan St. B. T. & Handley, S.J. "Belief Bias and Figural Bias in Syllogistic Reasoning," *Quarterly Journal of Experimental Psychology: Section A*, Vol. 57, No. 4, 2004, pp. 666-692. (RW 5699)

Morris, E. "The Anosognosic's Dilemma: Something's Wrong but You'll Never Know what it is (Part 1)," *New York Times*, 2010 (RW 4159)

Morris, E. "The Anosognosic's Dilemma: Something's Wrong but You'll Never Know what it is (Part 2)," *New York Times*, 2010 (RW 4160)

Morris, E. "The Anosognosic's Dilemma: Something's Wrong but You'll Never Know what it is (Part 3)," *New York Times*, 2010 (RW 4161)

Morris, E. "The Anosognosic's Dilemma: Something's Wrong but You'll Never Know what it is (Part 4)," *New York Times*, 2010 (RW 4162)

Morris, E. "The Anosognosic's Dilemma: Something's Wrong but You'll Never Know what it is (Part 5)," *New York Times*, 2010 (RW 4163)

Morris, T. & Mietchen, D. "Collaborative Structuring of Knowledge by Experts and the Public", *Proceedings of the 5th Open Knowledge Conference*, London, April 24, 2010, pp. 29-41. (RW 4865)

Morris, T.V. *God and the Philosophers: The Reconciliation of Faith and Reason*, Oxford University Press, New York, NY, 1994. (RW 5814)

Morrison, J.N.L. "British Intelligence Failures in Iraq," *Intelligence and National Security*, Vol. 26, No. 4, 2011, pp. 509-520. (RW 5395)

Morrison, P. *Understanding Patients*, 1994. (RW 2720)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Morse, E., Steves, M.P. & Scholtz, J. "Metrics and Methodologies for Evaluating Technologies for Intelligence Analysts," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 857)

Morse, J.M. "Emerging from the Data: The Cognitive Processes of Analysis in Qualitative Inquiry," in *Critical Issues in Qualitative Research Methods*, ed. J.M. Morse, Sage Publications, Thousand Oaks, 1994, pp. 23. (RW 2115)

Morton, A. & Phillips, L.D. "Fifty Years of Probabilistic Decision Analysis: A View from the UK," *Journal of the Operational Research Society*, Vol. 60, 2009, pp. S33. (RW 4217)

Moser, P.K., Mulder, D. & Trout, J.D. *The Theory of Knowledge: A Thematic Introduction*, Oxford University Press, New York, 1998. (RW 2290)

Moshman, D. "Cognitive Development Beyond Childhood," in *Handbook of Child Psychology, Volume Two*, ed. W. Damon, 5th ed., J. Wiley, New York, NY, 1998, pp. 947-978. (RW 4567)

Moshman, D. & Franks, B.A. "Intellectual Development: Formal Operations and Reflective Judgment," in *Thinking, Reasoning, and Writing*, eds. E.P. Maimon, B.F. Nodine & F.W. O'Connor, Longman, New York, 1989, pp. 9. (RW 4285)

Mostafa, J. *Seeking Better Web Searches* 2005. (RW 1580)

Moustakas, C.E. *Heuristic Research: Design, Methodology, and Applications*, Sage Publications, Newbury Park, CA, 1990. (RW 2669)

Moustakas, C.E. *Phenomenological Research Methods*, Sage, Thousand Oaks, CA, 1994. (RW 2114)

Mozer, M.C., Pashler, H. & Homaei, H. "Optimal Predictions in Everyday Cognition: The Wisdom of Individuals Or Crowds?", *CogSci 2008: 30th Annual Meeting of the Cognitive Science Society*, (RW 3380)

Mueller, P.A. & Stahlberg, D. "The Role of Surprise in Hindsight Bias: A Metacognitive Model of Reduced and Reversed Hindsight Bias," *Social Cognition*, Vol. 25, No. 1, 2007, pp. 165. (RW 2450)

Mueller, R.S. *Testimony before the Select Committee on Intelligence of the United States Senate* 2005. (RW 1341)

Muin, W. & Hussin, Z. "The Development of Epistemological Beliefs of Undergraduates in College of Education in Jordanian Universities," *OIDA International Journal of Sustainable Development*, Vol. 1, No. 9, 2010, pp. 11-19. (RW 5074)

Muis, K.R. "Personal Epistemology and Mathematics: A Critical Review and Synthesis of Research," *Review of Educational Research*, Vol. 74, No. 3, 2004, pp. 317-377. (RW 2789)

Muis, K.R. "The Role of Epistemic Beliefs in Self-Regulated Learning," *Educational Psychologist*, Vol. 42, No. 3, 2007, pp. 173-190. (RW 5300)

Muis, K.R., Bendixen, L.D. & Haerle, F.C. "Domain-Generality and Domain Specificity in Personal Epistemology Research: Philosophical and Empirical Questions in the Development of

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

a Theoretical Model," *Educational Psychology Review*, Vol. 18, No. 1, 2006, pp. 67-76. (RW 5037)

Muis, K.R. & Foy, M.J. "The Effects of Teachers' Beliefs on Elementary Students' Beliefs, Motivation, and Achievement in Mathematics," in *Personal Epistemology in the Classroom: Theory, Research, and Implications for Practice*, eds. L.D. Bendixen & F.C. Feucht, Cambridge University Press, Cambridge, UK, 2010, pp. 435-469. (RW 5131)

Muis, K.R. & Franco, G.M. "Epistemic Profiles and Metacognition: Support for the Consistency Hypothesis," *Metacognition and Learning*, Vol. 5, No. 1, 2010, pp. 27-45. (RW 4833)

Muis, K.R. & Sinatra, G.M. "University Cultures and Epistemic Beliefs: Examining Differences between Two Academic Environments," in *Knowing, Knowledge and Beliefs: Epistemological Studies Across Diverse Cultures*, ed. M.S. Khine, Springer, Dordrecht, 2008, pp. 137-150. (RW 5133)

Muller, D.G. "Intelligence Analysis in Red and Blue," *International Journal of Intelligence and Counterintelligence*, Vol. 21, No. 1, 2008, pp. 1-12. (RW 2910)

Muller, D.G. "Improving Futures Intelligence," *International Journal of Intelligence and Counterintelligence*, Vol. 22, No. 3, 2009, pp. 382. (RW 3584)

Mumford, M.D., Friedrich, T.L., Caughron, J.J. & Antes, A.L. "Leadership Development and Assessment: Describing the Rethinking the State of the Art," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 84-107. (RW 5137)

Mumford, M.D., Reiter-Palmon, R. & Redmond, M.R. "Problem Construction and Cognition: Applying Problem Representations in Ill-Defined Domains," in *Problem Finding, Problem Solving, and Creativity*, ed. M.A. Runco, Ablex Pub. Corp., Norwood, NJ, 1994, pp. 3. (RW 2583)

Mumford, M.D., Strange, J.M., Scott, G.M. & Gaddis, B.P. "Creative Problem-Solving Skills in Leadership: Direction, Actions, and Reactions," in *Creativity Across Domains: Faces of the Muse*, eds. J.C. Kaufman & J. Baer, L. Erlbaum Associates, Mahwah, NJ, 2005, pp. 205. (RW 4330)

Mumm, A.M. & Kersting, R.C. "Teaching Critical Thinking in Social Work Practice Courses," *Journal of Social Work Education*, Vol. 33, No. 1, 1997, pp. 75-84. (RW 4122)

Murphy, J. & Smith, K.W. "Making Intelligence Analysis Responsive to Policy Concerns," *Studies in Intelligence*, Vol. 17, No. 2, 1973, pp. 1-6. (RW 541)

Murphy, P.K. & Alexander, P.A. "What Counts? The Predictive Powers of Subject Matter Knowledge, Strategic Processing, and Interest in Domain-Specific Performance," *Journal of Experimental Education*, Vol. 70, 2002, pp. 197. (RW 3801)

Murphy, P.K. & Alexander, P.A. "Prior Knowledge, Beliefs, and Learning," in *Encyclopedia of Education*, ed. J.W. Guthrie, 2nd ed., Macmillan Reference USA, New York, 2003, pp. 1996. (RW 3721)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Murphy, P.K. & Alexander, P.A. "The Role of Knowledge, Beliefs, and Interest in the Conceptual Change Process: A Synthesis and Meta-Analysis of the Research," in *International Handbook of Research on Conceptual Change*, ed. S. Vosniadou, Routledge, New York, 2008, pp. 583. (RW 3686)

Murphy, P.K., Alexander, P.A., Greene, J.A. & Edwards, M.N. "Epistemological Threads in the Fabric of Conceptual Change Research," in *Re-Framing the Conceptual Change Approach in Learning and Instruction*, eds. S. Vosniadou, A. Baltas & X. Vamvakoussi, Elsevier, Amsterdam, 2007, pp. 105-122. (RW 5009)

Murphy, P.K., Buehl, M.M., Zeruth, J.A., Edwards, M.N., Long, J.F. & Monoi, S. "Examining the Influence of Epistemic Beliefs and Goal Orientations on the Academic Performance of Adolescent Student Enrolled in High-Poverty, High-Minority Schools," in *Personal Epistemology in the Classroom: Theory, Research, and Implications for Practice*, eds. L.D. Bendixen & F.C. Feucht, Cambridge University Press, Cambridge, UK, 2010, pp. 328-367. (RW 5130)

Murphy, P.K. & Mason, L. "Changing Knowledge and Beliefs," in *Handbook of Educational Psychology*, eds. P.A. Alexander & P.H. Winne, 2nd ed., L. Erlbaum Associates, Mahwah, NJ, 2006, pp. 305. (RW 3847)

Murphy, P.W. "Some Reflections on Evidence and Proof," *South Texas Law Review*, Vol. 40, No. 2, 1999, pp. 327. (RW 4184)

Murray, D.M. "Internal Revision: A Process of Discovery," in *Research on Composing: Points of Departure*, eds. C.R. Cooper & L. Odell, National Council of Teachers of English, Urbana, IL, 1978, pp. 85-103. (RW 1585)

Murray, D.M. "Write before Writing," *College Composition and Communication*, Vol. 291978, pp. 375-381. (RW 1604)

Murray, D.M. "The Essential Delay: When Writer's Block Isn't," in *When a Writer can't Write: Studies in Writer's Block and Other Composing-Process Problems*, ed. M. Rose, 1985, pp. 219. (RW 1586)

Murray, D.M. *Write to Learn*, 8th ed., Thomson Wadsworth, Boston, MA, 2005. (RW 1603)

Murray, D.M. *The Craft of Revision*, 5th ed., Thomson/Heinle, Boston, 2004. (RW 3505)

Murray, H.A. *Explorations in Personality*, Oxford University Press, New York, NY, 1938. (RW 5089)

Murrett, R.B. *Intelligence to Support Military Operations*, Center for Information Policy Research, Harvard University, Cambridge, MA, 2004. (RW 620)

Musch, J. "Personality Differences in Hindsight Bias," *Memory*, Vol. 11, No. 4/5, 2003, pp. 473. (RW 2437)

Musch, J. & Wagner, T. "Did Everybody Know it all Along? A Review of Individual Differences in Hindsight Bias," *Social Cognition*, Vol. 25, No. 1, 2007, pp. 64. (RW 2443)

Musso, J., Biller, R. & Myrtle, R. "Tradecraft: Professional Writing as Problem Solving," *Journal of Policy Analysis and Management*, Vol. 19, No. 4, 2000, pp. 635. (RW 3515)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Myers, J.T. *Future Directions for Defense Communications*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1990. (RW 1026)

Myrick, F. *Preceptorship and Critical Thinking in Nursing Education,* Ph.D. dissertation, University of Alberta, 1998. (RW 4123)

Naquin, D. *Remarks and Q&A by the Director of the Open Source Center. ODNI Open Source Conference.* 2007. (RW 2725)

Naquin, D. *Remarks by the Director of the Open Source Center. CIRA Luncheon.* 2007. (RW 2953)

Narvaez, D., van den Broek, P. & Ruiz, A. "The Influence of Reading Purpose on Inference Generation and Comprehension in Reading," *Journal of Educational Psychology*, Vol. 91, No. 3, 1999, pp. 488. (RW 2377)

Nash, J.G. *Writing from Sources: A Structure-Mapping Model,* 1990. (RW 1847)

Nash, J.G., Bravaco, R.J. & Simonson, S. "Assessing Knowledge Change in Computer Science," *Computer Science Education,* Vol. 16, No. 1, 2006, pp. 37. (RW 2091)

Nash, J.G., Schumacher, G.M. & Carlson, B.W. "Writing from Sources: A Structure-Mapping Model," *Journal of Educational Psychology,* Vol. 85, No. 1, 1993, pp. 159. (RW 2070)

National Drug Intelligence Center. *The Multiagency Course: Introduction to Basic Drug Intelligence Analysis*, National Drug Intelligence Center, Johnstown, PA, 2009. (RW 3892)

National Education Goals Panel *Goal 6: Adult Literacy and Lifelong Learning,* National Education Goals Panel. Available: http://govinfo.library.unt.edu/negp/page3-13.htm, Viewed: March 17, 2011. (RW 4660)

National Intelligence Council. 2020 Project. *Mapping the Global Future,* NIC 2004-13, 2004. (RW 362)

National Space Council. *Final Report to the President on the US Space Program,* 1993. (RW 457)

National Visualization and Analytics Center. *Research and Development Agenda for Visual Analytics* 2007. (RW 2173)

Nau, H.R. "Why we Fight Over Foreign Policy," *Policy Review*, 142, 2007 (RW 2261)

Neagoe, V. & Moldova, N. "Methods, Techniques and Tools that can be used for Efficient Cooperation within the National Intelligence Community", *The International Scientific Conference: Strategies XXI. The Complex and Dynamic Nature of the Security Environment,* Bucharest, Romania, November 22-23, 2012, pp. 82-90. (RW 5873)

Neary, P.C. "Intelligence Reform, 2001-2009: Requiescat in Pace?" *Studies in Intelligence,* Vol. 54, No. 1, 2010, pp. 1. (RW 3994)

Nebel, C. *The Dark Side of Creativity: Blocks, Unfinished Works, and the Urge to Destroy,* Whitston Pub. Co, Troy, N.Y, 1988. (RW 1852)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Negroponte, J. *A Vision for Intelligence in a Time of Change: Trying to Figure Out Who is in Charge. Speech Given to the Joint Military Intelligence College Conference, September 29, 2005.* 2005. (RW 1305)

Negroponte, J. *Report on the Progress of the Director of National Intelligence in Implementing the "Intelligence Reform and Terrorism Prevention Act of 2004"* 2006. (RW 1392)

Negroponte, J.D. *Remarks and Q&A by the Director of National Intelligence. Oxford Analytica International Conference.* 2006. (RW 1630)

Negroponte, J.D. *Hearing of the House Permanent Select Committee on Intelligence. Annual Threat Assessment.* 2007. (RW 1972)

Negroponte, J.D. *Hearing of the House Permanent Select Committee on Intelligence. Annual Threat Assessment. Unclassified Statement for the Record.* 2007. (RW 1973)

Negroponte, J.D. *Intelligence Reform Progress Report. Remarks by the Director of National Intelligence.* 2007. (RW 1974)

Negut, S. & Neacsu, M. "From Hard Power to Soft Power: The Intelligent Power", *The International Scientific Conference: Strategies XXI. The Complex and Dynamic Nature of the Security Environment,* Bucharest, Romania, November 22-23, 2012, pp. 216-226. (RW 5875)

Neill, J. *Qualitative Versus Quantitative Research: Key Points in a Classic Debate.* Available: www.wilderdom.com/research/qualitativeversusquantitativeresearch.html, (RW 1779)

Neimark, J. *Night Life,* Available: http://psychologytoday.com/articles/index.php?term=pto-19980701-000025, (RW 2104)

Nelms, H. *Thinking with a Pencil,* 1985. (RW 1544)

Nelson, N. "Writing to Learn: One Theory, Two Rationales," in *Writing as a Learning Tool: Integrating Theory and Practice*, eds. P. Tynjälä, L. Mason & K. Lonka, Kluwer Academic Publishers, Dordrecht Netherlands; Boston, 2001, pp. 23. (RW 4335)

Nemeth, C. "Jury Trials: Psychology and the Law," in *Advances in Experimental Social Psychology*, Vol. 14, 1981, pp. 309. (RW 2026)

Nemeth, C. "Dissent as Driving Cognition, Attitudes and Judgments," *Social Cognition*, Vol. 13, 1995, pp. 273. (RW 2027)

Nemeth, C.J. "Minority Dissent and its "Hidden" Benefits," *New Review of Social Psychology,* Vol. 2, 2002, pp. 21. (RW 2028)

Nemeth, C., Rogers, J. & Brown, K. "Devil's Advocate Vs. Authentic Dissent: Stimulating Quantity and Quality," *European Journal of Social Psychology,* Vol. 31, 2001, pp. 707. (RW 2029)

Nemeth, C.J. & Goncalo, J.A. "Influence and Persuasion in Small Groups," in *Persuasion: Psychological Insights and Perspectives*, eds. T.C. Brock & M.C. Green, 2nd ed., 2005, pp. 171. (RW 2025)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Nemeth, C.J. & Nemeth, L. "Understanding the Creative Process: Management of the Knowledge Worker," in *Managing Industrial Knowledge: Creation, Transfer and Utilization*, eds. I. Nonaka & D.J. Teece, 2001, pp. 91. (RW 2024)

Nemeth, C.J. & Nemeth-Brown, B. "Better than Individuals?: The Potential Benefits of Dissent and Diversity for Group Creativity," in *Group Creativity: Innovation through Collaboration*, eds. P.B. Paulus & B.A. Nijstad, 2003, pp. 63. (RW 2023)

Nemeth, E. "Collecting Cultural Intelligence: The Tactical Value of Cultural Property," *International Journal of Intelligence and Counterintelligence*, Vol. 24, No. 2, 2011, pp. 217-238. (RW 4595)

Nendaz, M.R. & Bordage, G. "Promoting Diagnostic Problem Representation," *Medical Education*, Vol. 36, 2002, pp. 760. (RW 2649)

Nerland, M. & Jensen, K. "Objectual Practice and Learning in Professional Work," in *Learning through Practice: Models, Traditions, Orientations, and Approaches*, ed. S. Billett, Springer, Dordrecht, 2010, pp. 82-103. (RW 4957)

Neuendorf, K.A. *The Content Analysis Guidebook*, Sage Publications, Thousand Oaks, Calif, 2002. (RW 3527)

Neumann, P.R. & Smith, M.L.R. "Missing the Plot? Intelligence and Discourse Failure," *Orbis*, Vol. 49, No. 1, 2005, pp. 95-107. (RW 74)

Neustadt, R.E. & May, E.R. *Thinking in Time: The Uses of History for Decision- Makers*, Free Press, New York, NY, 1986. (RW 4559)

Nevell, D.A., Maskell, S.R., Horridge, P.R. & Barnett, H.L. "Fusion of Data from Sources with Different Levels of Trust", *13th Conference on Information Fusion (FUSION)*, Edinburgh, UK, July 26-29, 2010 (RW 5675)

Nevo, Y. *Information Selection in Intelligence Processing*, MS thesis, Naval Postgraduate School, 2011. (RW 5541)

Newby-Clark, I. *We are Creatures of Habit*, Available: www.psychologytoday.com, (RW 3883)

Newcomb, E.A. & Hammell, R.J. "Examining the Effects of the Value of Information on Intelligence Analyst Performance", *2012 Proceedings of the Conference on Information Systems Applied Research*, New Orleans, LA, November 1 - 4, 2012 (RW 5868)

Newell, A. & Simon, H.A. *Human Problem Solving*, Prentice-Hall, Englewood Cliffs, N. J., 1972. (RW 2699)

Newhouse, J. *Assessing the Threats*, Center for Defense Information, Washington, DC, 2002. (RW 425)

Newman, B., Hartman, T. & Taber, C.S. "Social Dominance and the Cultural Politics of Immigration," *Political Psychology*, (RW 5452)

Newman, B., Hartman, T. & Taber, C.S. "Foreign Language Exposure, Cultural Threat, and Opposition to Immigration," *Political Psychology*, 2012 (RW 5453)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Newstead, S.E., Handley, S.J., Harley, C., Wright, H. & Farrelly, D. "Individual Differences in Deductive Reasoning," *Quarterly Journal of Experimental Psychology: Section A*, Vol. 57, No. 1, 2004, pp. 33-60. (RW 2436)

Newton, J.M. "Reflective Learning Groups for Student Nurses," in *Developing Learning Professionals*, eds. S. Billett & A. Henderson, Springer, Dordrecht, 2011, pp. 119-130. (RW 4905)

Neyfakh, L. *The Future of Prediction*,Available: http://articles.boston.com/2012-01-01/ideas/30575781_1_prediction-tarot-sheep, Viewed: January 6, 2012. (RW 5383)

Nguyen, H. *Capturing User Intent for Information*, Ph.D. dissertation, University of Connecticut, 2005. (RW 5644)

Nguyen, P.H. *Supporting Analytical Reasoning and Presentation with Analytic Provenance*, Middlesex University, London, UK, 2012. (RW 5891)

Nicander, L.D. "Understanding Intelligence Community Innovation in the Post-9/11 World," *International Journal of Intelligence and Counterintelligence*, Vol. 24, No. 3, 2011, pp. 534-568. (RW 5403)

Nicholl, J. "Task Definition," in *Strategic Thinking in Criminal Intelligence*, ed. J. Ratcliffe, 2nd ed., Federation Press, Sydney, 2009, pp. 66-84. (RW 5657)

Nichols, S. "Free Will Versus the Programmed Brain," *Scientific American*, 2008 (RW 3240)

Nicholson, N. "How Hardwired is Human Behavior?" *Harvard Business Review*, Vol. 76, No. 4, 1998, pp. 134-147. (RW 900)

Nickerson, R.S. "Experimental Methods in Cognitive Science," in *Encyclopedia of Cognitive Science* (RW 2317)

Nickerson, R.S. "Context is Important but it does Not Explain Everything - Matching Performance and the Similarity Structure of the Stimulus Set - Comment," *Journal of Experimental Psychology: General*, Vol. 110, No. 3, 1981, pp. 297. (RW 2344)

Nickerson, R.S. "Why Interactive Computer Systems are Sometimes Not used by People Who might Benefit from them," *International Journal of Man-Machine Studies*, Vol. 15, No. 4, 1981, pp. 469. (RW 2343)

Nickerson, R.S. "Understanding Understanding," *American Journal of Education*, Vol. 93, No. 2, 1985, pp. 201. (RW 2342)

Nickerson, R.S. "Why Teach Thinking?" in *Teaching Thinking Skills: Theory and Practice*, eds. J.B. Baron & R.J. Sternberg, Freeman, New York, NY, 1987, pp. 27-38. (RW 3734)

Nickerson, R.S. "On Improving Thinking through Instruction," *Review of Research in Education*, Vol. 15, No. 1, 1988, pp. 3-55. (RW 3875)

Nickerson, R.S. "Confirmation Bias: A Ubiquitous Phenomenon in Many Guises," *Review of General Psychology*, Vol. 2, No. 2, 1998, pp. 175. (RW 2297)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Nickerson, R.S. "How we Know - and Sometimes Misjudge - What Others Know: Imputing One's Own Knowledge to Others," *Psychological Bulletin*, Vol. 125, No. 6, 1999, pp. 737-759. (RW 2318)

Nickerson, R.S. "Theory and Application in the Cognitive Regulation of Performance: Discussion of Attention and Performance XVII," in *Attention and Performance XVII: Cognitive Regulation of Performance: Interaction of Theory and Application*, eds. D. Gopher & A. Koriat, MIT Press, Cambridge, MA, 1999, pp. 747. (RW 2311)

Nickerson, R.S. "Teaching Intelligence," in *Encyclopedia of Psychology*, ed. A.E. Kazdin, 2000, pp. 498. (RW 2316)

Nickerson, R.S. "The Projective Way of Knowing: A Useful Heuristic that Sometimes Misleads," *Current Directions in Psychological Research*, Vol. 10, No. 5, 2001, pp. 168. (RW 2338)

Nickerson, R.S. "Assessing the State and Enlarging the Domain of Judgment and Decision Research: Emerging Perspectives on Judgment and Decision Research," *Journal of Mathematical Psychology*, Vol. 48, No. 3, 2004, pp. 199. (RW 2340)

Nickerson, R.S. *Cognition and Chance: The Psychology of Probabilistic Reasoning*, L. Erlbaum Associates, Mahwah, NJ, 2004. (RW 2309)

Nickerson, R.S. "Technology and Cognition Amplification," in *Intelligence and Technology: The Impact of Tools on the Nature and Development of Human Abilities*, eds. R.J. Sternberg & D. Preiss, L. Erlbaum Associates, Mahwah, NJ, 2005, pp. 3. (RW 2314)

Nickerson, R.S., Baddeley, A. & Freeman, B. "Are People's Estimates of What Other People Know Influenced by What They Themselves Know?" *Acta Psychologica*, Vol. 64, No. 3, 1987, pp. 245. (RW 2341)

Nickerson, R.S. & Falk, R. "The Exchange Paradox: Probabilistic and Cognitive Analysis of a Psychological Conundrum," *Thinking & Reasoning*, Vol. 12, No. 2, 2006, pp. 181-213. (RW 2315)

Nickerson, R.S., Perkins, D. & Smith, E.E. *The Teaching of Thinking*, L. Erlbaum Associates, Hillsdale, NJ, 1985. (RW 4146)

Nickerson, R.S. *Aspects of Rationality: Reflections on What it Means to be Rational and Whether We Are*, Psychology Press, New York, NY, 2008. (RW 5777)

Nickerson, R.S. *Mathematical Reasoning: Patterns, Problems, Conjectures, and Proofs*, Psychology Press, New York, NY, 2010. (RW 5817)

Nickerson, R.S. "Norms, Goals, and the Study of Thinking," *Behavioral and Brain Sciences*, Vol. 34, No. 5, 2011, pp. 261-262. (RW 5490)

Nielsen, J. "Scenarios in Discount Usability Engineering," in *Scenario-Based Design: Envisioning Work and Technology in Systems Development*, ed. J.M. Carroll, Wiley, New York, 1995, pp. 59. (RW 3396)

Nielsen, J. *Usability Engineering*, 1993. (RW 4517)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Niemi, M. "Placebo Effect: A Cure in the Mind," *Scientific American Mind,* 2009 (RW 3473)

Nightingale, P. "Technological Capabilities: Invisible Infrastructure and the Un-Social Construction of Predictability: The Overlooked Fixed Costs of Useful Research," *Research Policy,* Vol. 33, No. 9, 2004, pp. 1259. (RW 3495)

Nijstad, B.A., Stroebe, W. & Lodewijkx, H.F.M. "The Illusion of Group Productivity: A Reduction of Failures Explanation," *European Journal of Social Psychology,* Vol. 36, 2006, pp. 31. (RW 1307)

Nirkhi, S.M., Dharaskar, R.V. & Thakre, V.M. "Data Mining: A Prospective Approach for Digital Forensics," *International Journal of Data Mining & Knowledge Management Process,* Vol. 2, No. 6, 2012, pp. 41-48. (RW 5883)

Nisbett, R.E. & Ross, L. *Human Inference: Strategies and Shortcomings of Social Judgment,* Prentice-Hall, Englewood Cliffs, NJ, 1980. (RW 4411)

Nixon, R.M. *Organization and Management of the US Foreign Intelligence Community. Memorandum.* 1971. (RW 1227)

Noble, D. "Structuring Open Source Information to Support Intelligence Analysis," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 871)

Nocera, J. "Tipping Over a Defense of Enron," *New York Times,* January 6, 2007. (RW 1907)

Nolan, C.M. "Seymour Hersh's Impact on the CIA," *International Journal of Intelligence and Counterintelligence,* Vol. 12, No. 1, 1999, pp. 18-34. (RW 456)

Nolan, C.M. "Intelligence Oversight in the USA," in *The International Studies Encyclopedia*, ed. R.A. Denemark, 2010, (RW 3928)

Nolan, C.M. "The PFIAB Personality: Presidents and their Foreign Intelligence Boards," *International Journal of Intelligence and Counterintelligence,* Vol. 23, No. 1, 2010, pp. 27. (RW 3769)

Nolan, J.E., MacEachin, D. & Tockman, K. *Discourse, Dissent, and Strategic Surprise: Formulating US Security Policy in an Age of Uncertainty* 2007. (RW 1976)

Nolan, P. "A Curator Approach to Intelligence Analysis," *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 4, 2012, pp. 786-794. (RW 5803)

Nolte, W. "Keeping Pace with the Revolution in Military Affairs: Operation Iraqi Freedom and the Challenge to Intelligence," *Studies in Intelligence,* Vol. 48, No. 1, 2004 (RW 1676)

Nolte, W. "Preserving Central Intelligence: Assessment and Evaluation in Support of the DCI," *Studies in Intelligence,* Vol. 48, No. 3, 2004, pp. 21-25. (RW 372)

Nolte, W. "Thinking about Rethinking: Examples of Reform in Other Professions," *Studies in Intelligence,* Vol. 52, No. 2, 2008, pp. 19. (RW 3162)

Nolte, W.M. "American Intelligence After the 2008 Election," *International Journal of Intelligence and Counterintelligence,* Vol. 21, No. 3, 2008, pp. 429. (RW 3136)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Nolte, W.M. "Intelligence Analysis in an Uncertain Environment," in *Oxford Handbook of National Security Intelligence*, ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 404-421. (RW 4711)

Nolte, W.M. "Valuing Intelligence: Opening a Conversation," *Intelligence and National Security,* Vol. 26, No. 5, 2011, pp. 616-619. (RW 5392)

Noonan, R.W. "Intelligence," in *How the Army Runs,* 2003, pp. 395-411. (RW 309)

Norgaard, K.M. *Living in Denial: Climate Change, Emotions, and Everyday Life*, MIT Press, Cambridge, MA, 2011. (RW 4792)

Norman, D.R. *How to Identify Credible Sources on the Web,* M. S. of Strategic Intelligence thesis, Joint Military Intelligence College, 2001. (RW 4523)

Norman, D. "The Research-Practice Gap," *Interactions,* Vol. 17, No. 4, 2010, pp. 9-12. (RW 5880)

Norman, D.A. & Bobrow, D.G. "On Data-Limited and Resource-Limited Processes," *Cognitive Psychology,* Vol. 7, No. 1, 1976, pp. 44. (RW 2949)

Norman, D.O. & Kuras, M.L. *Engineering Complex Systems* 2004. (RW 1785)

Norris, S.P. "Syntheses of Research on Critical Thinking," *Educational Leadership,* Vol. 42, No. 8, 1985, pp. 40-45. (RW 4093)

Norris, S.P. "Can we Test Validly for Critical Thinking?" *Educational Researcher,* Vol. 18, No. 9, 1989, pp. 21-26. (RW 4110)

Norris, S.P. "Practical Reasoning in the Production of Scientific Knowledge," in *Philosophy of Science, Cognitive Psychology, and Educational Theory and Practice,* eds. R.A. Duschl & R.J. Hamilton, State University of New York Press, Albany, 1992, pp. 195-225. (RW 5481)

Norris, S.P. "Testing for the Disposition to Think Critically," *Informal Logic,* Vol. 14, No. 2&3, 1992, pp. 157-164. (RW 4018)

Norris, S.P. "The Meaning of Critical Thinking Test Performance: The Effects of Abilities and Dispositions on Scores," in *Critical Thinking: Current Research, Theory and Practice,* ed. D.J. Fasko, Hampton Press, Cresskill, NJ, 2003, pp. 315-329. (RW 4021)

Norris, S.P. & Ennis, R.H. *Evaluating Critical Thinking,* Midwest Publications, Pacific Grove, CA, 1989. (RW 3696)

Northridge, A.R. "Pearl Harbor: Estimating Then and Now," *Studies in Intelligence,* Vol. 9, No. 4, 1965, pp. 65-74. (RW 549)

Nosich, G.M. *Learning to Think Things Through, A Guide to Critical Thinking Across Curriculums (3rd Ed.),* 3rd ed., Pearson Prentice Hall, Upper Saddle River, NJ, 2009. (RW 5752)

Notess, G.R. "The Wayback Machine: The Web's Archive," *Online Magazine,* March/April, 2002, pp. 59. (RW 1459)

Notre Dame College. *Certificate in Intelligence Analysis. 2004-2005 Course Booklet.* (RW 7)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Novak, J.D. & Canas, A.J. "Applying Educational Tools and Ideas in the Corporate World," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge*, eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 3-22. (RW 4877)

Novella, S. *Trusting Intuition Vs. Analysis,* Available: http://www.skepticblog.org/2012/12/17/trusting-intuition-vs-analysis/, Viewed: January 9, 2013. (RW 5893)

Novick, L.R. "Analogical Transfer, Problem Similarity, and Expertise," *Journal of Experimental Psychology: Learning, Memory, & Cognition,* Vol. 14, No. 3, 1988, pp. 510. (RW 1798)

Novick, L.R. & Bassok, M. "Problem Solving," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 321-350. (RW 4008)

Novick, P. *That Noble Dream: The "Objectivity Question" and the American Historical Profession,* Cambridge University Press, Cambridge, UK, 1988. (RW 5467)

Nowinski, E.H. & Kohler, R.J. "The Lost Art of Program Management in the Intelligence Community," *Studies in Intelligence,* Vol. 50, No. 2, 2006, pp. 33. (RW 1552)

Noyes, H. "People, Process and Technology in Risk Management", *DM Review,* [Online], Available from: http://www.information-management.com/issues/20040501/1002514-1.html, 2004, (RW 451)

Nozawa, E.T. *Scientific Semeiotics: As Defined by Charles Sanders Peirce (also Percean Semeiotic)* 2007. (RW 5120)

Nozick, R. *The Nature of Rationality,* Princeton University Press, Princeton, NJ, 1993. (RW 3861)

Nummedal, S.G. "Designing a Process to Assess Higher Order Thinking Skills in College Graduates: Issues of Concern", *National Center for Education Statistics Workshop on Assessing Higher Order Thinking and Communications Skills in College Graduates*, Washington, DC, November 17-19, 1991 (RW 4067)

Nuseibeh, B. *Crosscutting Requirements [Powerpoint Presentation]* 2004. (RW 2623)

Nussbaum, E.M. & Bendixen, L.D. "Approaching and Avoiding Arguments: The Role of Epistemological Beliefs, Need for Cognition, and Extraverted Personality Traits," *Contemporary Educational Psychology,* Vol. 28, 2003, pp. 573. (RW 4376)

Nussbaum, E.M., Sinatra, G.M. & Poliquin, A. "The Role of Epistemological Beliefs and Scientific Argumentation in Promoting Conceptual Change," *International Journal of Science Education,* Vol. 30, No. 15, 2008, pp. 1977-1999. (RW 5333)

Nye, J.S. "Peering into the Future," *Foreign Affairs,* Vol. 73, No. 4, 1994, pp. 82-93. (RW 1086)

Nye, J.S. *Estimating the Future?* Consortium for the Study of Intelligence, Washington, DC, 1995. (RW 139)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Nystrand, M. *What Writers Know: The Language, Process, and Structure of Written Discourse,* Academic Press, New York, 1982. (RW 2159)

Oakeshott, M. *Rationalism in Politics and Other Essays,* LibertyPress, Indianapolis, IN, 1991. (RW 4242)

Oakley, A. "Social Science and Evidence-Based Everything: The Case of Education," *Educational Review,* Vol. 54, No. 3, 2002 (RW 2248)

Oakley, A. "The Researcher's Agenda for Evidence," *Evaluation and Research in Education,* Vol. 18, No. 1/2, 2004, pp. 12. (RW 2252)

Oaksford, M. & Chater, N. "Dual Systems and Dual Processes but a Single Function," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans,* eds. K.I. Manktelow, D.E. Over & S. Elqayam, Psychology Press, Hove, East Sussex, UK, 2011, pp. 339-351. (RW 5713)

Oaksford, M. & Morris, F. "Mood, Reasoning, and Central Executive Processes," *Journal of Experimental Psychology: Learning, Memory & Cognition,* Vol. 22, No. 2, 1996, pp. 476-492. (RW 5122)

Oates, L.C. "Leveling the Playing Field: Helping Students Succeed by Helping them Learn to Read as Expert Lawyers," *St. John's Law Review,* Vol. 80, 2006, pp. 227. (RW 2786)

Oblinger, D.G. & Oblinger, J.L. "Is it Age Or is it IT: First Steps Toward Understanding the Net Generation," in *Educating the Net Generation,* eds. D. Oblinger & J. Oblinger, 2005 (RW 1521)

O'Brien, K.A. "Managing Information Overload," *Jane's Intelligence Review,* Vol. 12, No. 3, 2000, pp. 50-55. (RW 4447)

Ochoa, S.H. "Test Review of the California Critical Thinking Dispositions Inventory," in *The Twelfth Mental Measurements Yearbook,* eds. J.C. Conoley & J.C. Impara, Buros Institute, 1995. (RW 5640)

O'Conell, K. & Tomes, R.R. "Keeping the Information Edge," *Policy Review,* 122, 2003/2004, pp. 19-37. (RW 613)

O'Connell, A.J. "The Architecture of Smart Intelligence: Structuring and Overseeing Agencies in the Post-9/11 World," *California Law Review,* Vol. 94, 2006, pp. 1655. (RW 2483)

O'Connell, K.M. "Intelligence in the Information Age; Spy Data for Sale," *Newsday,* April 8, 2001, p. 2. (RW 4539)

O'Connell, K.M. "Thinking about Intelligence Comparatively," *Brown Journal of World Affairs,* Vol. 11, No. 1, 2004, pp. 189-199. (RW 408)

O'Connell, K.M. "The Role of Science and Technology in Transforming American Intellience," in *The Future of American Intelligence,* ed. P. Berkowitz, Hoover Institution Press, Stanford, CA, 2005, pp. 139-174. (RW 5645)

O'Connell, T. "Paul Petzoldt: Man of the Mountains," in *Sourcebook of Experiential Education: Key Thinkers and their Contributions,* eds. T.E. Smith & C. Knapp, Routledge, New York, 2011, pp. 231-237. (RW 4929)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

O'Connor, T. *Intelligence Analysis of White Collar Crime,* Available: http://www.apsu.edu/oconnort/4200/4200lect05.htm, (RW 3889)

O'Connor, T. *Intelligence Analysis. Lecture Notes.* 2004. (RW 330)

O'Connor, T. *Ethical and Moral Issues in Intelligence. Course Notes,* Austin Peay University, Clarksville, TN, 2005. (RW 300)

O'Connor, T. *Intelligence Analysis. Lecture Notes.* 2005. (RW 2364)

Odell, R. *Avoiding Intelligence Failure: An Approach to Recurring Self-Diagnosis by IC Senior Managers* 2004. (RW 2998)

Odom, W.E. *Testimony for the Senate Select Committee on Intelligence* 1991. (RW 1235)

Odom, W.E. *Fixing Intelligence: For a More Secure America*, Yale University Press, New Haven, 2003. (RW 1691)

Odom, W.E. *Testimony before the Senate Select Committee on Intelligence* 2004. (RW 317)

Odom, W.E. "Intelligence Analysis," *Intelligence and National Security,* Vol. 23, No. 3, 2008, pp. 316. (RW 3171)

Odom, W.E., Graham, W.R., Rich, R.E., Rindskopf, E.R., Soyster, H.E., Treverton, G.F. & Clapper, J.R. *Modernizing Intelligence: Structure and Change for the 21st Century*, National Institute for Public Policy, 1997. (RW 326)

Odom, W.E., Graham, W.R., Rich, R.E., Rindskopf, E.R., Soyster, H.E., Treverton, G.F. & Clapper, J.R. *Modernizing Intelligence: Structure and Change for the 21st Century*, National Institute for Public Policy, 2002. (RW 369)

Odugbemi, S. & Lee, T. *Accountability through Public Opinion: From Intertia to Public Action*, World Bank Publications, Washington, DC, 2011. (RW 5450)

Oettinger, A.G. *Whence and Whither Intelligence, Command and Control? The Certainty of Uncertainty*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1990. (RW 1027)

Oettinger, A.G. & Macdonald, M.S. "Information Overload. Managing Intelligence Technologies," *Harvard International Review*, Vol. 24, No. 3, 2002, pp. 44-48. (RW 324)

Oettle, K.F. *Making Your Point: A Practical Guide to Persuasive Legal Writing*, ALM Media, Inc., New York, NY, 2007. (RW 4459)

Office of Public Affairs. Central Intelligence Agency. *A Consumer's Guide to Intelligence* (RW 2854)

Office of the Director of National Intelligence. *The National Intelligence Strategy of the United States of America*, Office of the Director of National Intelligence, Washington, DC, 2005. (RW 1132)

Office of the Director of National Intelligence. *The National Intelligence Strategy of the United States of America* 2005. (RW 1424)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Office of the Director of National Intelligence. *United States Intelligence Community Centers of Academic Excellence (IC CAE) in National Security Studies. Guidance and Procedures. Program Plan for Fiscal Years 2005-2015* 2005. (RW 3432)

Office of the Director of National Intelligence. *ODDNI/Analytic Integrity and Standards. Pilot Evaluation Standards.* 2006. (RW 1732)

Office of the Director of National Intelligence. *Director of National Intelligence Moves Forward with Intelligence Reform. News Release.* 2007. (RW 2800)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 180. Intelligence Community History Programs.* 2007. (RW 2832)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 202. National Intelligence Board.* 2007. (RW 2816)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 203. Analytic Standards.* 2007. (RW 2817)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 204. Roles and Responsibilities for the National Intelligence Priorities Framework.* 2007. (RW 2831)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 206. Sourcing Requirements for Disseminated Analytic Products.* 2007. (RW 2830)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 302. Document and Media Exploitation.* 2007. (RW 2818)

Office of the Director of National Intelligence. *Intelligence Community Policy Memorandum 2007-500-1. Unevaluated Domestic Threat Tearline Reports* 2007. (RW 3026)

Office of the Director of National Intelligence. *Intelligence Community Policy Memorandum Number 2007-200-2. Preparing Intelligence to Meet the Intelligence Community's "Responsibility to Provide"* 2007. (RW 3056)

Office of the Director of National Intelligence. *An Overview of the United States Intelligence Community* 2007. (RW 1910)

Office of the Director of National Intelligence. *United States Intelligence Community. 500 Day Plan. Integration and Collaboration* 2007. (RW 2826)

Office of the Director of National Intelligence. *ODDNI/Analytic Integrity and Standards. Rating Scale for Tradecraft Standards.* 2007 (?). (RW 2834)

Office of the Director of National Intelligence. *Analytic Transformations – Unleashing the Potential of a Community of Analysts* 2008. (RW 5750)

Office of the Director of National Intelligence. *IC Annual Employee Climate Survey. 2007 Survey Results [Powerpoint Presentation]* 2008. (RW 3010)

Office of the Director of National Intelligence. *Information Sharing Strategy* 2008. (RW 3035)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 205. Analytic Outreach* 2008. (RW 3197)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Office of the Director of National Intelligence. *Intelligence Community Directive Number 207. National Intelligence Council* 2008. (RW 3167)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 610. Competency Directories for the Intelligence Community Workforce.* 2008. (RW 4470)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 650. National Intelligence Civilian Compensation Program: Guiding Principles and Framework* 2008. (RW 3087)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 651. Performance Management System Requirements for the Intelligence Community Civilian Workforce* 2008. (RW 5386)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 652. Occupational Structure for the Intelligence Community Civilian Workforce* 2008. (RW 3088)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 654. Performance-Based Pay for the Intelligence Community Civilian Workforce* 2008. (RW 3086)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 656. Performance Management System Requirements for Intelligence Community Senior Civilian Officers* 2008. (RW 3089)

Office of the Director of National Intelligence. *Data Mining Report* 2009. (RW 3424)

Office of the Director of National Intelligence. *Intelligence Community Directive Number 501. Discovery and Dissemination Or Retrieval of Information within the Intelligence Community.* 2009. (RW 3389)

Office of the Director of National Intelligence. *The National Intelligence Strategy of the United States of America* 2009. (RW 3595)

Office of the Director of National Intelligence. *2010 Data Mining Report* 2010. (RW 4807)

Office of the Director of National Intelligence. Public Affairs Office. *Fact Sheet: Real Progress in Reforming Intelligence* 2007. (RW 1911)

Office of the Director of National Intelligence & Department of Defense. *IC Analyst Qualification Standards* 2009. (RW 3392)

Office of the Director of National Intelligence & Office of General Counsel. *Intelligence Community Legal Reference Book* 2007. (RW 3159)

Office of Training and Education. *Analytic Thinking and Presentation for Intelligence Producers* (RW 1340)

O'Guin, M.C. & Olgilvie, T. "The Science, Not Art, of Business Intelligence," *Competitive Intelligence Review,* Vol. 12, No. 4, 2001, pp. 15-24. (RW 5479)

O'Hanlon, M.E. *The Limitations of Imagination. Prepared Testimony before the House Permanent Select Committee on Intelligence* 2004. (RW 611)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

O'Hora, D. & Maglieri, K.A. "Goal Statements and Goal-Directed Behavior: A Relational Frame Account of Goal Setting in Organizations," *Journal of Organizational Behavior Management,* Vol. 26, No. 1/2, 2006, pp. 131. (RW 2565)

Ojala, M. "Disappearances and Discoveries," *Online Magazine,* September/October, 2005, pp. 5. (RW 1461)

Ojala, M. "Global Information Flows," *Online Magazine,* May/June, 2006, pp. 46. (RW 1463)

Okada, T. "The Role of Hypothesis Formation in a Community of Psychology," in *Designing for Science: Implications from Everyday, Classroom, and Professional Settings*, eds. K.D. Crowley, C.D. Schunn & T. Okada, 2001, pp. 445. (RW 1876)

Olafson, L. & Bendixen, L.D. "Images and Beliefs: Emerging Themes on Pedagogy from Pre-Service Teachers," *Issues in Teacher Education,* Vol. 11, No. 2, 2002, pp. 3-16. (RW 5348)

Olafson, L. & Schraw, G. "Teachers' Beliefs and Practices within and Across Domains," *International Journal of Educational Research,* Vol. 45, No. 1-2, 2006, pp. 71-84. (RW 4993)

Olcott, A. "Revisiting the Legacy: Sherman Kent, Willmoore Kemdall, and George Pettee -- Strategic Intelligence in the Digital Age," *Studies in Intelligence,* Vol. 53, No. 2, 2009, pp. 21-32. (RW 4171)

Olcott, A.C. "The Challenges of Clashing IC Interests," *International Journal of Intelligence and Counterintelligence,* Vol. 23, No. 4, 2010, pp. 623. (RW 4308)

Oldham, M.S. "A Value for Information," *Studies in Intelligence,* Vol. 12, No. 2, 1968, pp. 29-36. (RW 4206)

Oldroyd, D.R. *The Arch of Knowledge: An Introductory Study of the History of the Philosophy and Methodology of Science,* Methuen, New York, 1986. (RW 4165)

O'Leary, J. *Surprise and Intelligence: Towards a Clearer Understanding,* ADA 329100, Air War College, Maxwell AFB, AL, 1997. (RW 4568)

O'Leary, Z. *The Essential Guide to Doing Research,* Sage, London, 2004. (RW 3112)

Oliver, S., Harden, A., Rees, R., Shepherd, J., Brunton, G., Garcia, J. & Oakley, A. "An Emerging Framework for Including Different Types of Evidence in Systematic Reviews for Public Policy," *Evaluation,* Vol. 11, No. 4, 2005, pp. 428. (RW 2238)

Olmer, L. *Intelligence Techniques for the American Business Community,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1987. (RW 1028)

Olmsted, K.S. "Linus Pauling: A Case Study in Counterintelligence Run Amok," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 269. (RW 2473)

Olsen, K.A., Sochats, K.M. & Williams, J.G. "Full Text Searching and Information Overload," *International Information and Library Review,* Vol. 30, No. 2, 1998, pp. 105-122. (RW 671)

Olson, D.R. *The World on Paper: The Conceptual and Cognitive Implications of Writing and Reading,* Cambridge University Press, Cambridge, UK, 1994. (RW 2392)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Olson, D.R. "Technology and Intelligence in a Literate Society," in *Intelligence and Technology: The Impact of Tools on the Nature and Development of Human Abilities*, eds. R.J. Sternberg & D. Preiss, L. Erlbaum Associates, Mahwah, NJ, 2005, pp. 55. (RW 2388)

Olson, D.R. & Torrance, N. "Writing and Criticizing Texts," in *Explorations in the Development of Writing: Theory, Research, and Practice*, eds. B.M. Kroll & C.G. Wells, Wiley, Chichester Sussex, 1983, pp. 31. (RW 2206)

Olson, J.M. "Intelligence and the War on Terror: How Dirty Are We Willing to Get Our Hands?" *SAIS Review*, Vol. 28, No. 1, 2008, pp. 37-45. (RW 4431)

Olson, J.M., Roese, N.J. & Zanna, M.P. "Expectancies," in *Social Psychology: Handbook of Basic Principles*, eds. E.T. Higgins & A.W. Kruglanski, Guilford Press, New York, NY, 1996, pp. 211-238. (RW 1842)

Omestad, T. "Psychology and the CIA: Leaders on the Couch," *Foreign Policy*, Vol. 95, No. Summer, 1994, pp. 105-122. (RW 145)

O'Neil, J. & Marsick, V.J. *Understanding Action Learning*, American Management Association, New York, 2007. (RW 3354)

O'Neill, E.S. & Dluhy, N.M. "A Longitudinal Framework for Fostering Critical Thinking and Diagnostic Reasoning," *Journal of Advanced Nursing*, Vol. 26, No. 4, 1997, pp. 825-832. (RW 3962)

Onley, D.S. "DIA Gets Ahead of the Game," *Government Computer News*, 2005, pp. 18-18. (RW 784)

Opfer, J.E. & Siegler, R.S. "Development of Quantitative Thinking," in *Oxford Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 585-605. (RW 5504)

Ophir, E., Nass, C. & Wagner, A.D. "Cognitive Control in Media Multitaskers," *Proceedings of the National Academy of Sciences Early Edition*, 2009 (RW 3555)

Orleans, L.A. "The Problem of Chinese Statistics," *Studies in Intelligence*, Vol. 17, No. 1, 1973, pp. 47-62. (RW 566)

Ormerod, T.C., Chronicle, E.P. & MacGregor, J.N. "Dynamics and Constraints in Insight Problem Solving," *Journal of Experimental Psychology: Learning, Memory, & Cognition*, Vol. 28, No. 4, 2002, pp. 791. (RW 2741)

Ormond, V.A. *The Role of Intelligence Analysis in the War on Terrorism*, US Army War College, Carlisle Barracks, PA, 2002. (RW 1180)

Ormrod, J.E. *Cognitive Styles and Dispositions*, Education.com, Inc. Available: http://www.education.com/reference/article/cognitive-styles-dispositions/, Viewed: July 27, 2011. (RW 5024)

Ortiz, C.M.A. *Does Philosophy Improve Critical Thinking Skills?* M.A. thesis, University of Melbourne, 2007. (RW 4531)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Orton, J.D. & Callahan, J.L. "Important "Folk Theories" in Intelligence Reorganization," *International Journal of Intelligence and Counterintelligence*, Vol. 8, No. 4, 1996, pp. 411-429. (RW 48)

Ortony, A. *Metaphor and Thought*, Cambridge University Press, Cambridge, UK, 1979. (RW 2592)

Osborne, D. *Out of Bounds: Innovation and Change in Law Enforcement Intelligence Analysis*, Center for Strategic Intelligence Research, Joint Military Intelligence College, Washington, DC, 2006. (RW 2967)

Osborne, J., Collins, S., Ratcliffe, M., Millar, R. & Duschl, R. "What "Ideas-about-Science" should be Taught in School Science? A Delphi Study of the Expert Community," *Journal of Research in Science Teaching*, Vol. 40, No. 7, 2003, pp. 692-720. (RW 5433)

Osias, D. "Presentation of Analytic Uncertainties," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 864)

Ostensoe, J.G. "The Problem of Scientific Surprise," *Studies in Intelligence*, Vol. 5, No. 4, 1961, pp. 15-20. (RW 4207)

OTI/Medical and Psychological Analysis Center. *The Handbook of the Psychology of Analysis. Workshop.* 2005. (RW 2996)

Otis, P. "The Intelligence Pro and the Professor: Toward an Alchemy of Applied Arts and Sciences," in *Bringing Intelligence about: Practitioners Reflect on Best Practices*, eds. R.G. Swenson, Joint Military Intelligence College (U.S.) & Center for Strategic Intelligence Research, Joint Military Intelligence College, Center for Strategic Intelligence Research, Washington, DC, 2003, pp. 7. (RW 1486)

Ott, M.C. "Shaking Up the CIA," *Foreign Policy*, 90, 1994, pp. 132-151. (RW 10)

Ott, M.C. "Partisanship and the Decline of Intelligence Oversight," *International Journal of Intelligence and Counterintelligence*, Vol. 16, No. 1, 2003, pp. 69-94. (RW 194)

Otting, H., Zwaal, W., Tempelaar, D. & Gijselaers, W. "The Structural Relationship between Students' Epistemological Beliefs and Conceptions of Teaching and Learning," *Studies in Higher Education*, Vol. 35, No. 7, 2010, pp. 741-760. (RW 5015)

Ouimet, M., Bedard, P. & Gelineau, F. "Are the h-Index and some of its Alternatives Discriminatory of Epistemological Beliefs and Methodological Preferences of Faculty Members? The Case of Social Scientists in Quebec " *Scientometrics*, Vol. 88, No. 1, 2011, pp. 91-106. (RW 5226)

Overbye, D. "Free Will: Now You Have It, Now You Don't," *New York Times*, January 2, 2007. (RW 1908)

Overton, W.F. "Scientific Methodologies and the Competence Moderator Performance Issue," in *Moderators of Competence*, eds. E.D. Neimark, R. De Lisi & J.L. Newman, L. Erlbaum Associates, Hillsdale, NJ, 1985, pp. 15-41. (RW 5036)

Overy, R. "Strategic Intelligence and the Outbreak of the Second World War," *War in History*, Vol. 5, No. 4, 1998, pp. 451-480. (RW 393)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Owen, L., Goldwasser, C., Choate, K. & Blitz, A. *The Power of Many: ABCs of Collaborative Innovation Throughout the Extended Enterprise* 2007. (RW 2868)

Owens, W.A. "Intelligence in the 21st Century," *American Intelligence Journal,* Vol. 7, No. 1, 1999, pp. 15-21. (RW 99)

Oyama, S., Griffiths, P.E. & Gray, R.D. *Cycles of Contingency: Developmental Systems and Evolution,* MIT Press, Cambridge, MA, 2001. (RW 3924)

Ozkal, K., Tekkaya, C., Sungur, S., Cakiroglu, J. & Cakiroglu, E. "Elementary Students' Scientific Epistemological Beliefs in Relation to Socio-Economic Status and Gender," *Journal of Science Teacher Education,* Vol. 21, No. 7, 2010, pp. 873-885. (RW 5210)

OZTAS, F. "Self-Esteem, Occupational Self-Esteem, and Epistemological Beliefs of Turkish University Students," *Social Behavior & Personality: An International Journal,* Vol. 38, No. 3, 2010, pp. 321-326. (RW 5209)

Pacini, R. & Epstein, S. "The Relation of Rational and Experiential Information Processing Styles to Personality, Basic Beliefs, and the Ratio-Bias Phenomenon," *Journal of Personality & Social Psychology,* Vol. 76, No. 6, 1999, pp. 972. (RW 5165)

Padgett, T., Maniquis, A., Hoffman, M., Miller, W. & Lautenschlager, J. "A Semantic Visualization Tool for Knowledge Discovery and Exploration in a Collaborative Environment," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 806)

Page, S.E. *The Difference: How the Power of Diversity Creates Better Groups, Firms, Schools, and Societies,* Princeton University Press, Princeton, 2007. (RW 2785)

Pajares, M.F. "Teachers' Beliefs and Educational Research: Cleaning Up a Messy Construct," *Review of Educational Research,* Vol. 62, No. 3, 1992, pp. 307-332. (RW 4625)

Pallaris, C. "Open Source Intelligence: A Strategic Enabler of National Security," *CSS Analyses in Security Policy,* Vol. 3, No. 32, 2008 (RW 3058)

Pallaris, C. "The Trouble with Best Practices [Powerpoint Presentation]", *Global Intelligence Forum 2010,* Dungarvan, Ireland, July 11-13, 2010 (RW 4235)

Palmer, B. & Marra, R.M. "College Student Epistemological Perspectives Across Knowledge Domains: A Proposed Grounded Theory," *Higher Education: The International Journal of Higher Education and Educational Planning,* Vol. 47, No. 3, 2004, pp. 311-335. (RW 5268)

Palmer, B. & Marra, R.M. "Individual Domain Specific Epistemologies: Implications for Educational Practice," in *Knowing, Knowledge and Beliefs: Epistemological Studies Across Diverse Cultures*, ed. M.S. Khine, Springer, Dordrecht, 2008, pp. 325-350. (RW 4355)

Palmer, B. *Strategic Intelligence for Law Enforcement,* Australian Bureau of Criminal Intelligence, Canberra, 1991. (RW 653)

Palmer, C.L., Cragin, M.H. & Hogan, T.P. "Weak Information Work in Scientific Discovery," *Information Processing and Management,* Vol. 43, No. 3, 2007, pp. 808. (RW 2345)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Palmer, R.E. *Hermeneutics: Interpretation Theory in Schleiermacher, Dilthey, Heidegger, and Gadamer,* Northwestern University Press, Evanston IL, 1969. (RW 2694)

Palumbo, D. *Writing from the Inside Out: Transforming Your Psychological Blocks to Release the Writer Within,* Wiley, New York, 2000. (RW 1865)

Pappas, A. *Ryszard Kuklinksi: A Case Officer's View,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2005. (RW 1160)

Pappas, A.A. & Simon, J. "The Intelligence Community: 2001-2015. Daunting Challenges, Hard Decisions," *Studies in Intelligence,* Vol. 46, No. 1, 2002 (RW 1677)

Parasuraman, R. & Rizzo, M. *Neuroergonomics: The Brain at Work,* Oxford University Press, Oxford; New York, 2007. (RW 3420)

Park, H. *Inferential Relevance and its Implications to Inferential Information Retrieval,* Ph.D. dissertation, Rutgers University, 1995. (RW 5112)

Park, H. "Inferential Representation of Science Documents," *Information Processing & Management,* Vol. 32, No. 4, 1996, pp. 419-429. (RW 5111)

Parker, A.M. & Fischhof, B. "Decision-Making Competence: External Validation through an Individual-Differences Approach," *Journal of Behavioral Decision Making,* Vol. 18, No. 1, 2005, pp. 1-27. (RW 5379)

Parker, C.F. & Stern, E.K. "Blindsided? September 11 and the Origins of Strategic Surprise," *Political Psychology,* Vol. 23, No. 3, 2002, pp. 601-630. (RW 4346)

Parker, C.A. *Encouraging Development in College Students,* University of Minnesota Press, Minneapolis, 1978. (RW 4420)

Parkington, R.J., Shaker, S.M. & Garra, N. "Analytic Wargaming," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 818)

Pascarella, E.T. "The Development of Critical Thinking: Does College make a Difference?" *Journal of College Student Development,* Vol. 40, No. 5, 1999, pp. 562-569. (RW 4145)

Pascarella, E.T. & Terenzini, P.T. *How College Affects Students: Findings and Insights from Twenty Years of Research,* Jossey-Bass Publishers, San Francisco, 1991. (RW 4418)

Pascarella, E.T. & Terenzini, P.T. *How College Affects Students: A Third Decade of Research,* Jossey-Bass, San Francisco, CA, 2005. (RW 4419)

Pascarella, E., Bohr, L., Amaury, N. & Terenzini, P. *Is Differential Exposure to College Linked to the Development of Critical Thinking?* National Center on Post Secondary Teaching, Learning, and Assessment, University Park, PA, 1994. (RW 4126)

Passig, D. "Future Time Span as a Cognitive Skill in Future Studies," *Futures Research Quarterly,* Winter, 2003, pp. 27. (RW 1331)

Passmore, J. "On Teaching to be Critical," in *The Concept of Education,* ed. R.S. Peters, Humanities Press, New York, NY, 1967, pp. 192-211. (RW 5172)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Pat, M.E. & Blum, D.M. *Bayesian Analysis of Intelligence Or Improved Advice to Decision-Makers,* University of Southern California, Los Angeles, CA, [undated]. (RW 5607)

Pate, E. "Cost-Benefit Analysis," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 21-28. (RW 3606)

Pate-Cornell, M.E. "Fusion of Intelligence Information: A Bayesian Approach," *Risk Analysis,* Vol. 22, No. 3, 2002, pp. 445-454. (RW 4732)

Patel, V.L., Kushniruk, A.W., Yang, S. & Yale, J.F. "Impact of a Computer-Based Patient Record System on Data Collection, Knowledge, Organization, and Reasoning," *Journal of the American Medical Informatics Association,* Vol. 7, No. 6, 2000, pp. 569. (RW 4151)

Patel, V.L., Arocha, J.F. & Zhang, J. "Thinking and Reasoning in Medicine," in *The Cambridge Handbook of Thinking and Reasoning,* eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 727-750. (RW 4013)

Patel, V.L. & Groen, G.J. "The General and Specific Nature of Medical Expertise: A Critical Look," in *Toward a General Theory of Expertise: Prospects and Limits*, eds. K.A. Ericsson & J. Smith, Cambridge University Press, Cambridge; New York, 1991, pp. 93. (RW 2764)

Patterson, C.H. *Principles of Correct Thinking,* Longmans, Green and Co., New York, NY, 1937. (RW 4466)

Patterson, D.A. "Seven Reasons to Shave Your Head and Three Reasons Not To: The Bald Truth," *Communications of the ACM,* Vol. 49, No. 4, 2006, pp. 31. (RW 1514)

Patterson, E.S., Roth, E.M. & Woods, D.D. *Aiding the Intelligence Analyst in Situations of Data Overload: A Simulation Study of Computer-Supported Inferential Analysis Under Data Overload,* ERGO-CSEL 99-TR-02, US Air Force Research Laboratory, Wright Patterson AFB, OH, 1999. (RW 669)

Patterson, E.S., Roth, E.M. & Woods, D.D. "Predicting Vulnerabilities in Computer-Supported Inferential Analysis Under Data Overload," *Cognition, Technology, and Work,* Vol. 3, No. 4, 2001, pp. 224-237. (RW 1467)

Patterson, E., Roth, E. & Woods, D. "Predicting Vulnerabilities in Computer Supported Inferential Analysis Under Data Overload," *Cognition, Technology, and Work,* Vol. 3, 2001, pp. 224. (RW 1520)

Patterson, E.S., Woods, D.D., Tinapple, D. & Roth, E.M. "Using Cognitive Task Analysis (CTA) to Seed Design Concepts for Intelligence Analysts Under Data Overload," in *Proceedings of the Human Factors and Ergonomics Society 45th Annual Meeting: Minneapolis/St. Paul, Minnesota, October 8-12, 2001*, eds. Human Factors and Ergonomics Society. Meeting (45th: 2001: Minneapolis, Minn. and St. Paul, Minn.) & Human Factors and Ergonomics Society, The Society, Santa Monica, CA, 2001, pp. 439. (RW 1592)

Patterson, E.S., Woods, D.D., Tinapple, D., Roth, E.M., Finley, J.M. & Kuperman, G.G. *Aiding the Intelligence Analyst: From Problem Definition to Design Concept Exploration,* AFRL-HE-

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

WP-TR-2001-0116, US Air Force Research Laboratory, Wright Patterson AFB, OH, 2001. (RW 266)

Paul, R. "Teaching Critical Thinking in the "Strong" Sense." *Informal Logic Newsletter*, Vol. 4, No. 2, 1981, pp. 2-7. (RW 4471)

Paul, R.W. "Critical Thinking and the Critical Person," in *Thinking: The Second International Conference*, eds. D.N. Perkins, J. Lochhead & J. Bishop, L. Erlbaum Associates, Hillsdale, NJ, 1987, pp. 373-403. (RW 3975)

Paul, R.W. "Dialogical Thinking: Critical Thought Essential to the Acquisition of Rational Knowledge and Passions," in *Teaching Thinking Skills: Theory and Practice*, eds. J.B. Baron & R.J. Sternberg, Freeman, New York, NY, 1987, pp. 127-148. (RW 3739)

Paul, R.W. & Nosich, G.M. *A Proposal for the National Assessment of Higher-Order Thinking at the Community College, College, and University Levels*, National Center for Education Statistics, Washington, DC, 1991. (RW 5178)

Paul, R. & Elder, L. *The Analysis and Assessment of Thinking (Helping Students Assess their Thinking),*Available: http://www.criticalthinking.org/articles/helping-students-assess-their-thinking.cfm, Viewed: April 30, 2007. (RW 2366)

Paul, R. & Elder, L. *The Thinker's Guide to the Nature and Functions of Critical and Creative Thinking,* Foundation for Critical Thinking, Dillon Beach, CA, 2005. (RW 3783)

Paul, R. & Elder, L. *A Guide for Educators to Critical Thinking Competency Standards,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3781)

Paul, R. & Elder, L. *The International Critical Thinking Reading and Writing Test,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3780)

Paul, R. & Elder, L. *A Miniature Guide for Students and Faculty to Scientific Thinking,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3745)

Paul, R. & Elder, L. *A Miniature Guide for those Who Teach on how to Improve Student Learning,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3746)

Paul, R. & Elder, L. *The Thinker's Guide for Conscientious Citizens on how to Detect Media Bias and Propaganda,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3754)

Paul, R. & Elder, L. *The Thinker's Guide for Students on how to Study and Learn a Discipline using Critical Thinking Concepts and Tools,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3750)

Paul, R. & Elder, L. *The Thinker's Guide to Fallacies: The Art of Mental Trickery and Manipulation,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3753)

Paul, R. & Elder, L. *The Thinker's Guide to how to Read a Paragraph the Art of Close Reading,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3777)

Paul, R. & Elder, L. *The Thinker's Guide to how to Write a Paragraph: The Art of Substantive Writing,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 4767)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Paul, R. & Elder, L. *The Thinker's Guide to the Art of Socratic Questioning,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3755)

Paul, R. & Elder, L. *The Thinker's Guide to Understanding the Foundations of Ethical Reasoning,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3749)

Paul, R. & Elder, L. *The Miniature Guide to Critical Thinking Concepts and Tools,* Foundation for Critical Thinking, Dillon Beach, CA, 2007. (RW 3776)

Paul, R. & Elder, L. *A Miniature Guide to Taking Charge of the Human Mind Thinking Feeling Wanting,* Foundation for Critical Thinking, Dillon Beach, CA, 2007. (RW 3747)

Paul, R., Niewoehner, R. & Elder, L. *The Thinker's Guide to Engineering Reasoning,* Foundation for Critical Thinking, Dillon Beach, CA, 2006. (RW 3752)

Paulsen, D.J., Bair, S. & Helms, D. *Tactical Crime Analysis,* 2010. (RW 3877)

Paulsen, M.B. & Well, C.T. "Domain Differences in the Epistemological Beliefs of College Students," *Research in Higher Education,* Vol. 39, No. 4, 1998, pp. 365-384. (RW 4609)

Paulsen, M.B. & Feldman, K.A. "Student Motivation and Epistemological Beliefs," *New Directions for Teaching & Learning,* No. 78, 1999, pp. 17-25. (RW 5432)

Paulsen, M.B. & Feldman, K.A. "The Conditional and Interaction Effects of Epistemological Beliefs on the Self-Regulated Learning of College Student: Motivational Strategies," *Research in Higher Education,* Vol. 46, No. 7, 2005, pp. 731. (RW 2860)

Paulson, T.M. *Intelligence Issues and Developments,* 2008. (RW 2958)

Paulus, P.B. & Dzindolet, M.T. "Social Influence Processes in Group Brainstorming," *Journal of Personality and Social Psychology,* Vol. 64, No. 4, 1993, pp. 575-586. (RW 1916)

Pavelich, M.J. & Moore, W.S. "Measuring the Effect of Experiential Education using the Perry Model," *Journal of Engineering Education,* Vol. 85, No. 4, 1996, pp. 287-292. (RW 5561)

Pawson, R. "Digging for Nuggets: How "Bad" Research can Yield "Good" Evidence," *International Journal of Social Research Methodology,* Vol. 9, No. 2, 2006, pp. 127. (RW 2240)

Pawson, R., Greenhalgh, T., Harvey, G. & Walshe, K. "Realist Review: A New Method of Systematic Review Designed for Complex Policy Interventions," *Journal of Health Services Research & Policy,* Vol. 10, July Supplement, 2005, pp. 21. (RW 2241)

Peake, C.H. "History's Role in Intelligence Estimating," *Studies in Intelligence,* Vol. 3, No. 1, 1959, pp. 85-91. (RW 530)

Peake, H.B. *The Reader's Guide to Intelligence Periodicals,* NIBC Press, Washington, DC, 1992. (RW 1099)

Peck, M. "U.S. spies use custom videogames to learn how to think", *Wired,* [Online], pp. March 25, 2011. Available from: http://www.wired.com/politics/security/news/2008/04/spy_games?currentPage=all#, 2008, (RW 4695)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Peirce, W. *Designing Rubrics for Assessing Higher Order Thinking,* Available: http://academic.pgcc.edu/~wpeirce/MCCCTR/Designingrubricsassessingthinking.html, Viewed: February 7, 2012. (RW 4060)

Pejtersen, A.M. "A Library System for Information Retrieval Based on a Cognitive Task Analysis and Supported by an Icon-Based Interface", *Proceedings of the 12th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval,* Cambridge, Massachusetts, June 25-28, 1989, pp. 40. (RW 1776)

Pelham, B.W. & Neter, E. "The Effect of Motivation of Judgment Depends on the Difficulty of the Judgment," *Journal of Personality & Social Psychology,* Vol. 68, No. 4, 1995, pp. 581-594. (RW 5360)

Peng, K. & Akutsu, S. "A Mentality Theory of Knowledge Creation and Transfer: Some Smart People Resist New Ideas and Some Don't," in *Managing Industrial Knowledge: Creation, Transfer and Utilization*, eds. I. Nonaka & D.J. Teece, 2001, pp. 105. (RW 2139)

Penner, D.E. & Klahr, D. "When to Trust the Data: Further Investigations of System Error in a Scientific Reasoning Task," *Memory & Cognition,* Vol. 24, No. 5, 1996, pp. 655. (RW 1891)

Pennington, N. & Hastie, R. "Evidence Evaluation in Complex Decision Making," *Journal of Personality and Social Psychology*, Vol. 51, 1986, pp. 242. (RW 1608)

Pennington, N. & Hastie, R. "Explaining the Evidence: Tests of the Story Model for Juror Decision Making," *Journal of Personality and Social Psychology*, Vol. 62, No. 2, pp. 189. (RW 2037)

Pennington, N. & Hastie, R. "Explanation Based Decision Making," in *Program of the Ninth Annual Conference of the Cognitive Science Society:16-18 July 1987, Seattle, Washington* L. Erlbaum Associates, Hillsdale, N.J, 1987. (RW 1654)

Perciful, E.G. & Nester, P.A. "The Effect of an Innovative Clinical Teaching Method on Nursing Students' Knowledge and Critical Thinking Skills," *Journal of Nursing Education*, Vol. 35, No. 1, 1996, pp. 23-28. (RW 4127)

Perera, D. *Intel could Still Fail to Connect the Dots, Says DIA Official,* Available: http://www.fiercehomelandsecurity.com/story/intel-could-still-fail-connect-dots-says-dia-official/2012-01-29, Viewed: January 30, 2012, 2012. (RW 5418)

Perkins, D.N. "Knowledge as Design: Teaching Thinking through Content," in *Teaching Thinking Skills: Theory and Practice*, eds. J.B. Baron & R.J. Sternberg, Freeman, New York, NY, 1987, pp. 62-85. (RW 3736)

Perkins, D.N. "Thinking Frames: An Integrative Perspective on Teaching Cognitive Skills," in *Teaching Thinking Skills: Theory and Practice,* eds. J.B. Baron & R.J. Sternberg, Freeman, New York, NY, 1987, pp. 41-61. (RW 3735)

Perkins, D.N. "Reasoning as it is and could be: An Empirical Perspective," in *Thinking Across Cultures*, eds. D.M. Topping, D.C. Crowell & V.N. Kobayashi, L. Erlbaum Associates, Hillsdale, NJ, 1989, pp. 175-194. (RW 4947)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Perkins, D.N. *Outsmarting IQ: The Emerging Science of Learnable Intelligence*, Free Press, New York, NY, 1995. (RW 3455)

Perkins, D.N., Allen, R. & Hafner, J. "Difficulties in Everyday Reasoning," in *Thinking: The Expanding Frontier*, ed. W. Maxwell, Franklin Institute Press, Philadelphia, PA, 1983, pp. 177-189. (RW 4108)

Perkins, D.N., Jay, E. & Tishman, S. "Beyond Abilities: A Dispositional Theory of Thinking," *The Merrill-Palmer Quarterly*, Vol. 39, No. 1, 1993, pp. 1-21. (RW 2898)

Perkins, D. *The Eureka Effect: The Art and Logic of Breakthrough Thinking*, 2001. (RW 3906)

Perkins, D., Jay, E. & Tishman, S. "New Conceptions of Thinking: From Ontology to Education," *Educational Psychologist*, Vol. 28, No. 1, 1993, pp. 67-85. (RW 5787)

Perkins, D. & Ritchhart, R. "When is Good Thinking?" in *Motivation, Emotion, and Cognition: Integrative Perspectives on Intellectual Functioning and Development*, eds. D.Y. Dai & R.J. Sternberg, L. Erlbaum Associates, Mahwah, NJ, 2004, pp. 351-384. (RW 3458)

Perl, S. *Landmark Essays on Writing Process*, Hermagoras Press, Davis, CA, 1994. (RW 4768)

Pernin, C.G., Moore, L.R. & Comanor, K. *The Knowledge Matrix Approach to Intelligence Fusion* 2007. (RW 2841)

Perr, J. *Cognitive Dissonance, Terrorism and 9/11*,Available: http://www.perrspectives.com, (RW 476)

Perry, W.L. & Gordon, J. *Analytic Support to Intelligence in Counterinsurgencies* 2008. (RW 3189)

Perry, W.G. "Cognitive and Ethical Growth: The Making of Meaning," in *The Modern American College*, Chickering, Arthur W. ed., Jossey-Bass, San Francisco, CA, 1981, pp. 76-116. (RW 4896)

Perry, W.G. *Forms of Intellectual and Ethical Development in the College Years: A Scheme*, Holt, Rinehart and Winston, New York, 1970. (RW 4897)

Personick, M., Bebee, B., Thompson, B., Wang, Y., Jaworowski, M., Parsia, B., Clark, K. & Soechtig, C. "An RDF Prototype System for Federation and Semantic Alignment of Disparate Counter-Terrorism Information Sources," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 866)

Persson, P.-.I. & Nyce, J.M. "Intuitive Tools? Design Lessons from the Military Intelligence Community," *American Intelligence Journal*, Vol. 25, No. 1, 2007, pp. 38. (RW 3222)

Persson, P.I. & Nyce, J.M. "Contradictions, Evolution, and Professionalization in the Intelligence Function," *American Intelligence Journal*, Vol. 28, No. 1, 2010, pp. 93-107. (RW 4475)

Pesce, J. "Astrophysical Best Practices and Intelligence Analysis [Powerpoint Presentation]", *Global Intelligence Forum 2010*, Dungarvan, Ireland, July 11-13, 2010 (RW 4230)

Pesce, J. & Tauss, R. *Science and Intelligence Analysis: The Requirement for "Critical Thinking" Training in the Intelligence Community* 2004. (RW 2999)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Peters, B.G. & Hoornbeek, J. *The Problem of Policy Problems* (RW 2638)

Peters, J.E., Larson, E.V. & Dewar, J.A. *Futures Intelligence: Assessing Intelligence Support to Three Army Long-Range Planning Communities,* RAND Corporation, Santa Monica, CA, 1998. (RW 650)

Peters, K.M. "Intelligence Lost," *Government Executive,* Vol. 28, No. 11, 1996, pp. 20. (RW 1678)

Peters, M.A. *Kinds of Thinking, Styles of Reasoning* (RW 2404)

Peters, R. "Intelligence Failures and the Limits of Logic," *Parameters,* Vol. 17, No. 1, 1987, pp. 43-50. (RW 1192)

Peters, R. *New Glory: Expanding America's Global Supremacy,* Sentinel, New York, NY, 2005. (RW 768)

Peters, R. "Information is Not Intelligence," in *Never Quit the Fight,* ed. R. Peters, Stackpole Books, Mechanicsburg, PA, 2006, pp. 239. (RW 1621)

Peters, R. "Our Strategic Intelligence Problem," *Military Review,* July-August, 2006, pp. 112. (RW 1623)

Petersen, J.L. "Forecasting: It's Not Possible," *Defense Intelligence Journal,* Vol. 31994, pp. 37-45. (RW 180)

Petersen, M. "Managing/Teaching New Analysts," *Studies in Intelligence,* Fall, 1986 (RW 1082)

Petersen, M. "What We Should Demand from Intelligence," *National Security Studies Quarterly,* Vol. 5, Spring, 1999, pp. 107-113. (RW 112)

Petersen, M. "The Challenge for the Political Analyst: Advice from a DI Careerist," *Studies in Intelligence,* Vol. 47, No. 1, 2003, pp. 51-56. (RW 4169)

Petersen, M. "Making the Analytic Review Process Work," *Studies in Intelligence,* Vol. 49, No. 1, 2005 (RW 4362)

Petersen, M. "Toward a Stronger Intelligence Product: Making the Analytic Review Process Work," *Studies in Intelligence,* Vol. 49, No. 1, 2005, pp. 55-61. (RW 395)

Petersen, M. "What I Learned in 40 Years of Doing Intelligence Analysis for US Foreign Policymakers," *Studies in Intelligence,* Vol. 55, No. 1, 2011 (RW 4724)

Peterson, E. "Reified Literals: A Best Practice Candidate Design Pattern for Increased Expressivity in the Intelligence Community", *Fifth International Conference on Semantic Technology for Intelligence, Defense, and Security,* Fairfax, VA, 26-29 October 2010 (RW 4753)

Peterson, J.J. *Appropriate Factors to Consider when Assessing Analytic Confidence in Intelligence Analysis.* 2007. (RW 2980)

Peterson, J.J. *Appropriate Factors to Consider when Assessing Analytic Confidence in Intelligence Analysis,* M. Sc. thesis, Mercyhurst College, 2008. (RW 3029)

Peterson, M. "Organizational Leadership in the Intelligence Community: A New Paradigm," *American Intelligence Journal,* Vol. 27, No. 1, 2009, pp. 55. (RW 3990)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Peterson, S. *Stories and Past Lessons: Understanding US Decisions of Armed Humanitarian Intervention and Nonintervention in the Post-Cold War Era* 2003. (RW 2644)

Petitto, L. & Dunbar, K. *New Findings from Educational Neuroscience on Bilingual Brains, Scientific Brains, and the Educated Mind* (RW 1811)

Petracca, M.P. "Issue Definitions, Agenda-Building, and Policymaking," *Policy Currents,* Vol. 2, No. 3, 1992, pp. 4. (RW 2680)

Pettee, G.S. *The Future of American Secret Intelligence,* Infantry Journal Press, Washington, DC, 1946. RW 2948)

Petticrew, M. & Roberts, H. *Systematic Reviews in the Social Sciences: A Practical Guide,* Blackwell Pub., Malden, MA, 2006. (RW 2233)

Pettigrew, K.E., Fidel, R. & Bruce, H. "Conceptual Frameworks in Information Behavior," *Annual Review of Information Science and Technology,* Vol. 35, 2001, pp. 43-78. (RW 1128)

Pettus, M.C. *It's all in Your Head: Change Your Mind, Change Your Health,* Capital Books, Sterling, VA, 2006. (RW 1719)

Petty, R.E., Brinol, P., Loersch, C. & McCaslin, M.J. "The Need for Cognition," in *Handbook of Individual Differences in Social Behavior,* eds. M.R. Leary & R.H. Hoyle, Guilford Press, New York, NY, 2009, pp. 318-329. (RW 5334)

Petty, R.E., Cacioppo, J.T., Strathman, A.J. & Priester, J.R. "To Think Or Not to Think: Exploring Two Routes to Persuasion," in *Persuasion: Psychological Insights and Perspectives,* eds. T.C. Brock & M.C. Green, 2nd ed., Sage Publication, Thousand Oaks, CA, 2005, pp. 81-116. (RW 2142)

Peverly, S.T. "The Importance of Handwriting Speed in Adult Writing," *Developmental Neuropsychology,* Vol. 29, No. 1, 2006, pp. 197. (RW 2072)

Pfaltzgraff, R.L., Ra'anan, U. & Milberg, W. *Intelligence Policy and National Security,* Archon Books, Hamden, CT, 1981. (RW 742)

Pfautz, J., Fichtl, T., Guarino, S., Carlson, Powell, G. & Roth, E. "Cognitive Complexities Impacting Army Intelligence Activities," *Proceedings of the Human Factors and Ergonomics Society 50th Annual Meeting,* 2006, pp. 452. (RW 2883)

Pfautz, J., Fouse, A., Fichtl, T., Bisantz, A., Roth, E. & Madden, S. "The Impact of Meta-Information on Decision-Making in Intelligence Operations", *Proceedings of the Human Factors and Ergonomics Society 49th Meeting,* pp. 214. (RW 3573)

Pfautz, S.L. & Pfautz, J. "Understanding Social and Organizational Aspects of the Work Domain using Techniques and Technologies from Intelligence Analysis," *Human Factors and Ergonomics Society Annual Meeting Proceedings,* Vol. 52, No. 4, 2008, pp. 443. (RW 3579)

Pfeffer, J. & Sutton, R.I. "Evidence-Based Management," *Harvard Business Review,* January, 2006 (RW 1788)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Pfeifer, N. & Kleiter, G.D. "Uncertain Deductive Reasoning," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans*, eds. K.I. Manktelow, D.E. Over & S. Elqayam, Psychology Press, Hove, East Sussex, UK, 2011, pp. 145-165. (RW 5705)

Pfister, F.R. & Petrick, J.F. "A Heuristic Model for Creating a Writer's Audience," *College Composition and Communication*, Vol. 31, No. 2, 1980, pp. 213-220. (RW 4487)

Pforzheimer, W. "Public Texts in Intelligence (November 1963 Revision of Spring 1961 Edition)," *Studies in Intelligence*, Vol. 8, No. 1, 1963, pp. A31-A42. (RW 551)

Pforzheimer, W., Peake, H.B. & Halpern, S. *In the Name of Intelligence: Essays in Honor of Walter Pforzheimer*, NIBC Press, Washington, DC, 1994. (RW 708)

Phan, H.P. "Examination of Student Learning Approaches, Reflective Thinking, and Epistemological Beliefs: A Latent Variables Approach," *Electronic Journal of Research in Educational Psychology*, Vol. 4, No. 3, 2006 (RW 2861)

Phan, H.P. "Predicting Change in Epistemological Beliefs, Reflective Thinking and Learning Styles: A Longitudinal Study," *British Journal of Educational Psychology*, Vol. 78, 2008, pp. 75-93. (RW 5072)

Phan, H.P. "Amalgamation of Future Time Orientation, Epistemological Beliefs, Achievement Goals and Study Strategies: Empirical Evidence Established," *British Journal of Educational Psychology*, Vol. 79, No. 1, 2009, pp. 155-173. (RW 5266)

Phelps, R.H., Englert, J.A. & Mutter, S.A. *Application of a Cognitive Model for Army Training: Handbook for Strategic Intelligence Analysis*, U.S. Army Research Institute for the Behavioral and Social Sciences, Alexandria, VA, 1984. (RW 1119)

Phelps, R.H., Pliske, R.M. & Mutter, S.A. "Improving Decision Making: A Cognitive Approach," in *Human Productivity Enhancement*, ed. J. Zeidner, Praeger, New York, 1987, pp. 297. (RW 3044)

Pherson Associates, L. *Analysis of Competing Hypotheses: An Eight Step Process* 2007. (RW 2945)

Pherson Associates, L. *Collaborative Analysis of Competing Hypotheses (C-ACH)* 2007. (RW 2944)

Pherson Associates, L. *Coup Vulnerability Tool* 2007. (RW 2943)

Pherson Associates, L. *The Indicators Validator* 2007. (RW 2941)

Pherson Associates, L. *Multiple Hypotheses Generator* 2007. (RW 2942)

Pherson Associates, L. *The Pre-Mortem* 2007. (RW 2946)

Pherson, K.H. & Pherson, R.H. *Critical Thinking for Strategic Intelligence*, 2012. (RW 5904)

Pherson, R. *Overcoming Analytic Mindsets: Five Simple Techniques* 2005. (RW 2937)

Pherson, R. "Applying Best Practices: Two Universal Techniques [Powerpoint Presentation]", *Global Intelligence Forum 2010*, Dungarvan, Ireland, July 11-13, 2010 (RW 4229)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Pherson, R. "How to Identify, Evaluate, and Teach Best Analytic Practices [Powerpoint Presentation]", *Global Intelligence Forum 2010,* Dungarvan, Ireland, July 11-13, 2010 (RW 4231)

Phillips, D. "Introduction to Part II: Analysis - Providing a Context for Intelligence," in *The Handbook of Intelligent Policing: Consilience, Crime Control, and Community Safety*, ed. C. Harfield, Oxford University Press, Oxford, UK, 2008, pp. 89-92. (RW 5771)

Phillips, F. "Accounting Students' Beliefs about Knowledge: Associating Performance with Underlying Belief Dimensions," *Issues in Accounting Education,* Vol. 13, February, 1998, pp. 113. (RW 3085)

Phillips, F. "A Research Note on Accounting Students' Epistemological Beliefs, Study Strategies, and Unstructured Problem-Solving Performance," *Issues in Accounting Education,* Vol. 16, No. 1, 2001, pp. 21. (RW 2538)

Phillips, J. *The Art of Original Thinking: The Making of a Thought Leader,* 9th Element Press, San Diego, CA, 2006. (RW 1718)

Phillips, J. *Creatures of Habit,* Available: http://workingsmarter.typepad.com/my_weblog/2006/04/creatures_of_ha.html, (RW 3887)

Phillips, R.L. & Hunt, J.G. *Strategic Leadership: A Multiorganizational-Level Perspective,* Quorum Books, Westport, CT, 1992. (RW 3045)

Phythian, M. "Intelligence Analysis Today and Tomorrow," *Security Challenges,* Vol. 5, No. 1, 2009, pp. 67-83. (RW 5620)

Phythian, M. "Intelligence Oversight in the UK: The Case of Iraq," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 301. (RW 2476)

Phythian, M. "Intelligence Theory and Theories of International Relations: Shared World or Separate Worlds?" in *Intelligence Theory: Key Questions and Debates*, eds. P. Gill, S. Marrin & M. Phythian, 2009, pp. 54. (RW 3405)

Piaget, J. *The Psychology of Intelligence,* Routledge, London, 2001. (RW 4987)

Piattelli-Palmarini, M. *Inevitable Illusions: How Mistakes of Reason Rule our Minds,* Wiley, New York, 1994. (RW 2288)

Pick, H.L., van den Broek, Paulus Willem, Knill, D.C. & University of Minnesota *Cognition: Conceptual and Methodological Issues,* American Psychological Association, Washington, DC, 1992. (RW 1952)

Pick, S. & Peterson, P. "Analysts in Intelligence Tradecraft," *American Intelligence Journal,* Vol. 25, No. 1, 2007, pp. 18-20. (RW 3220)

Pickering, A. *The Mangle of Practice: Time, Agency, and Science,* University of Chicago Press, Chicago, 1995. (RW 4421)

Pieschl, S., Stahl, E. & Bromme, R. "Epistemological Beliefs and Self-Regulated Learning with Hypertext," *Metacognition and Learning,* Vol. 3, 2008, pp. 17-37. (RW 5064)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Pigott, T.D. "Methods for Handling Missing Data in Research Synthesis," in *The Handbook of Research Synthesis*, eds. H.M. Cooper & L.V. Hedges, Russell Sage Foundation, New York, 1994, pp. 163. (RW 2489)

Piirto, J. *My Teeming Brain: Understanding Creative Writers,* Hampton Press, Cresskill, N.J, 2002. (RW 1853)

Pillar, P. "Good Literature and Bad History: The 9/11 Commission's Tale of Strategic Intelligence," *Intelligence and National Security,* Vol. 21, No. 6, 2006, pp. 1022. (RW 2084)

Pillar, P.R. "Great Expectations: Intelligence as Savior," *Harvard International Review,* Winter, 2006, pp. 16. (RW 2264)

Pillar, P.R. "Adapting Intelligence to Changing Issues," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 148. (RW 2464)

Pillar, P.R. *Inside Track: Sometimes the CIA is Right,* Available: http://www.nationalinterest.org, Viewed: 07/08, 2010. (RW 4173)

Pillar, P.R. "The Politicization of Analysis," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 278. (RW 3652)

Pillar, P.R. "Predictive Intelligence: Policy Support or Spectator Sport?" *SAIS Review,* Vol. 28, No. 1, 2008, pp. 25-35. (RW 3325)

Pillar, P.R. "The Perils of Politicization," in *Oxford Handbook of National Security Intelligence*, ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 472-484. (RW 4715)

Pillar, P.R. *Intelligence and U.S. Foreign Policy: Iraq, 9/11, and Misguided Reform,* Columbia University Press, New York, NY, 2011. (RW 5207)

Pillar, P.R. *Think again: Intelligence,* Available: http://www.foreignpolicy.com/articles/2012/01/03/intelligence, Viewed: January 6, 2012. (RW 5385)

Pincione, G. & Teson, F.R. *Discourse Failure: A Philosophical Essay on Political Deliberation, Democracy, and Consent* 2004. (RW 4244)

Pincus, W. "Law to Spread the Use of CIA's Analysis Approach," *Washington Post,* Dec. 20, 2004, p. A21. (RW 4187)

Pincus, W. and Baker, P. "Dissent on Intelligence is Critical," *Washington Post,* March 30, 2005, p. A01. (RW 1130)

Pinker, S. *The Blank Slate: The Modern Denial of Human Nature,* Viking, New York, 2002. (RW 3252)

Pintrich, P.R., Marx, R.W. & Boyle, R.A. "Beyond Cold Conceptual Change: The Role of Motivational Beliefs and Classroom Contextual Factors in the Process of Conceptual Change," *Review of Educational Research,* Vol. 63, No. 2, 1993, pp. 167-199. (RW 4657)

Pintrich, P.R. "Future Challenges and Directions for Theory and Research on Personal Epistemology," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and*

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Knowing, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 389-414. (RW 2747)

Pintrich, P.R. & Sinatra, G.M. "Future Directions for Theory and Research on Intentional Conceptual Change," in *Intentional Conceptual Change*, eds. G.M. Sinatra & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2003, pp. 429. (RW 4439)

Pioch, N.J., Barlos, F., Fournelle, C. & Stephenson, T. "A Link and Group Analysis Toolkit (LGAT) for Intelligence Analysis," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 802)

Pioch, N.J. & Everett, J.O. "POLESTAR - Collaborative Knowledge Management and Sensemaking Tools for Intelligence Analysts", *ACM Fifteenth Conference on Information and Knowledge Management*, November 6-11, 2006 (RW 1646)

Pipes, R. "Team B: The Reality Behind the Myth," *Commentary,* Vol. 82, 1986, pp. 25-40. (RW 1188)

Pipes, R. "What is Intelligence? With Discussion. Working Group on Intelligence Reform." *Commentary,* March, 1995, pp. 36-43. (RW 79)

Pipes, R. "What to do about the CIA," *Commentary,* Vol. 99, No. 3, 1995, pp. 36-43. (RW 466)

Pirolli, P.L. "The Cognitive Structure of User Sense Making (Keynote Talk)", May 4-6, 2005 (RW 1504)

Pirolli, P. & Card, S.K. *The Sensemaking Process and Leverage Points for Analyst Technology Identified through Cognitive Task Analysis*, Palo Alto Research Center, Inc., Palo Alto, CA, (RW 1470)

Pirolli, P. & Card, S.K. *Information Foraging Models of Browsers for Very Large Document Spaces* 1998. (RW 1472)

Pirolli, P. & Card, S.K. "Information Foraging," *Psychological Review,* Vol. 106, 1999, pp. 643-675. (RW 1468)

Pirolli, P. "Exploring and Finding Information," in *HCI Models, Theories, and Frameworks: Toward a Multidisciplinary Science*, ed. J.M. Carroll, 2003, pp. 157. (RW 1485)

Pirolli, P. *Information Foraging Theory: Adaptive Interaction with Information*, Oxford University Press, Oxford, UK, 2007. (RW 3444)

Pirolli, P. "Powers of 10: Modeling Complex Information-Seeking Systems at Multiple Scales," *Computer*, Vol. 42, No. 3, 2009, pp. 33. (RW 3438)

Pirolli, P.L. *Assisting People to Become Independent Learners in the Analysis of Intelligence: Final Technical Report*, Palo Alto Research Center, Inc., Palo Alto, CA, 2006. (RW 1391)

Pirtilla-Backman, A. & Kajanne, A. "The Development of Implicit Epistemologies during Early and Middle Adulthood," *Journal of Adult Development*, Vol. 8, No. 2, 2001, pp. 81-97. (RW 5228)

Pitman, G.R. *Arms Races and Stable Deterrence*, University of California, Los Angeles, CA, 1969. (RW 718)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Pizzolato, J.E. "What is Self-Authorship?" in *Development and Assessment of Self-Authorship: Exploring the Concept Across Cultures*, eds. M.B. Baxter Magolda, E.G. Creamer & P.S. Meszaros, Stylus Pub., Sterling, VA, 2010, pp. 187-206. (RW 4763)

Plano Clark, V.L. & Creswell, J.W. *The Mixed Methods Reader,* Sage Publications, Thousand Oaks, CA, 2008. (RW 3090)

Plant, E.A., Ericsson, K.A., Hill, L. & Asberg, K. "Why Study Time does Not Predict Grade Point Average Across College Students: Implications of Deliberate Practice for Academic Performance," *Contemporary Educational Psychology,* Vol. 30, 2005, pp. 96. (RW 4130)

Platt, J.R. "Strong Inference," *Science,* Vol. 146, 1964, pp. 347. (RW 1877)

Platt, W. *Strategic Intelligence Production: Basic Principles,* F.A. Praeger, New York, NY, 1957. (RW 930)

Platt, W. *National Character in Action: Intelligence Factors in Foreign Relations,* Rutgers University Press, New Brunswick, NJ, 1961. (RW 994)

Platt, W. & Baker, R.A. "The Relation of the Scientific "Hunch" to Research," *Journal of Chemical Education,* Vol. 8, No. October, 1931, pp. 1969. (RW 1546)

Plehal, J.B. *The National Infrastructure Protection Center,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2004. (RW 1159)

Pockett, S., Banks, W.P. & Gallagher, S. *Does Consciousness Cause Behavior?* MIT Press, Cambridge, MA, 2006. (RW 2101)

Poell, R.F. & Van der Krogt, Ferd J. "Individual Learning Paths of Employees in the Context of Social Networks," in *Learning through Practice: Models, Traditions, Orientations, and Approaches*, ed. S. Billett, Springer, Dordrecht, 2010, pp. 197-221. (RW 4961)

Poell, R.F. & van Woerkom, M. "Introduction: Supporting Workplace Learning," in *Supporting Workplace Learning: Towards Evidence-Based Practice,* eds. R.F. Poell & M. van Woerkom, Springer, Dordrecht, 2011, pp. 1-10. (RW 4908)

Pohl, R.F. "Ways to Assess Hindsight Bias," *Social Cognition,* Vol. 25, No. 1, 2007, pp. 14. (RW 2446)

Pollack, K.M. "Spies, Lies, and Weapons: What Went Wrong?" *Atlantic Monthly,* January, 2004 (RW 1327)

Pollard, G. "Imagescout," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 849)

Pollock, J.L. & Cruz, J. *Contemporary Theories of Knowledge,* 2nd ed., Rowman & Littlefield Publishers, Lanham, MD, 1999. (RW 5110)

Polmar, N. & Allen, T.B. *Spy Book: The Encyclopedia of Espionage,* Random House, New York, NY, 1997. (RW 1196)

Polya, G. & Conway, J.H. *How to Solve It: A New Aspect of Mathematical Method,* Princeton University Press, Princeton NJ, 2004. (RW 2390)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Pomeroy, D. "Implications of Teachers' Beliefs about the Nature of Science: Comparison of the Beliefs of Scientists, Secondary Science Teachers, and Elementary Teachers." *Science Education,* Vol. 77, No. 3, 1993, pp. 261-278. (RW 4939)

Pool, I.d.S. *Trends in Content Analysis: Papers,* University of Illinois Press, Urbana, IL, 1959. (RW 2973)

Pool, I.d.S. "Content Analysis for Intelligence Purposes," *World Politics,* Vol. 12, No. 3, 1960, pp. 478. (RW 2962)

Pool, R. *Field Evaluation in the Intelligence and Counterintelligence Context Workshop Summary.* The National Academies Press, Washington, DC, 2010. (RW 3996)

Poole, J. "Learning Best Practice from Other Domains [Powerpoint Presentation]", *Global Intelligence Forum 2010,* Dungarvan, Ireland, July 11-13, 2010 (RW 4232)

Poovey, M. *A History of the Modern Fact: Problems of Knowledge in the Sciences of Wealth and Society,* University of Chicago Press, Chicago, IL, 1998. (RW 5792)

Popay, J. *Moving Beyond Effectiveness in Evidence Synthesis: Methodological Issues in the Synthesis of Diverse Sources of Evidence* 2006. (RW 2217)

Pope, S. & Josang, A. "Analysis of Competing Hypotheses using Subjective Logic", *Proceedings of the 10th International Command and Control Research and Technology Symposium,* National Defense University, Washington DC, 29. (RW 5574)

Pople, H.E. "Heuristic Methods for Imposing Structure on Ill-Structured Problems: The Structuring of Medical Diagnostics," in *Artificial Intelligence in Medicine,* ed. P. Szolovits, Published by Westview Press for the American Association for the Advancement of Science, Boulder, CO, 1982, pp. 119. (RW 2768)

Porch, D. & Wirtz, J.J. *Strategic Lnsight: Surprise and Intelligence Failure,* Available: http://www.dtic.mil/cgi-bin/GetTRDoc?Location=U2&doc=GetTRDoc.pdf&AD=ADA485164, Viewed: February 21, 2011. (RW 506)

Porteus, S.D. "Looking Out for Economic Interests: An Increased Role for Intelligence," *The Washington Quarterly,* Vol. 19, No. 4, 1996, pp. 191-204. (RW 897)

Posner, M.I. *Foundations of Cognitive Science,* MIT Press, Cambridge, MA, 1989. (RW 2594)

Posner, R.A. *Preventing Surprise Attacks: Intelligence Reform in the Wake of 9/11,* Rowman & Littlefield, Lanham, MD, 2005. (RW 1495)

Posner, R.A. *Uncertain Shield: The U.S. Intelligence System in the Throes of Reform,* Rowman & Littlefield, Lanham, MD, 2006. (RW 1551)

Poteat, E. "The Use and Abuse of Intelligence: An Intelligence Provider's Perspective," *Diplomacy & Statecraft,* Vol. 11, No. 2, 2000, pp. 1-16. (RW 5621)

Poteat, G. *The Intelligence Gap: Hypotheses on the Process of Surprise* 1976. (RW 1292)

Poteat, S.E. "Intelligence Analysis Paralysis," *Periscope Newsletter,* August, 2005, pp. 3. (RW 1550)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Potter, M.L. *From Search to Research: Developing Critical Thinking through Web Research Skills*, Microsoft Corp., Redmond, WA, 2010. (RW 5175)

Potts, J.T., Cook, D.J., Holder, L.B. & Coble, J. "Learning Concepts from Intelligence Data Embedded in a Supervised Graph," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 853)

Pounder, G. "Review of William E. Odom: Fixing Intelligence: For a More Secure America," *Air & Space Power Journal*, Vol. 18, No. 4, 2004, pp. 121-123. (RW 608)

Poundstone, W. *The Labyrinths of Reason: Paradox, Puzzles, and the Frailty of Knowledge*, Anchor Press/Doubleday, New York, 1988. (RW 2301)

Pourret, O. & Naim, P. *Bayesian Networks: A Practical Guide to Applications*, 2008. (RW 3005)

Powell, C. "Cognitive Hurdles in the use of Decision Support Systems to Enhance Problem Understanding," *Group Decision and Negotiation*, Vol. 3, No. 4, 1994, pp. 413-421. (RW 896)

Powell, G. *Army Intelligence Analysis and Interpretation: Assessing the Utility and Limitations of Computational Diagnostic Reasoning* 2004. (RW 2899)

Powell, G. *User-Centric System Design for Information Fusion* 2004. (RW 2901)

Powell, G., Matheus, C.J., Kokar, M. & Lorenz, G.G. *Understanding the Role of Context in the Interpretation of Complex Battlespace Intelligence* 2006. (RW 2900)

Powell, G.M. & Broome, B. *Fusion-Based Knowledge for the Objective Force* 2002. (RW 3140)

Power, M. *The Risk Management of Everything: Rethinking the Politics of Uncertainty*, Davos, London, UK, 2004. (RW 5670)

Powers, T. "The Truth about the CIA (Review of 16 Books)," *New York Review of Books*, Vol. 40, No. 9, 1993, pp. 49-55. (RW 125)

Prabha, C., Connaway, L.S., Olszewski, L. & Jenkins, L.R. "What is enough? Satisficing Information Needs," *Journal of Documentation*, Vol. 63, No. 1, 2007, pp. 74. (RW 3818)

Pradhan, M. "The Crystal Ball - the Future of Informatics and Decision Making", *Australian Rheumatology Association*, May 30, 2001 (RW 2260)

Prados, J. "No Reform Here," *Bulletin of the Atomic Scientists*, Vol. 52, No. 5, 1996, pp. 55-59. (RW 785)

Prados, J. "American Secret Intelligence: A Review Essay," *Political Science Quarterly*, Vol. 118, No. 1, 2003, pp. 127-131. (RW 95)

Prados, J. "Intelligence: No Easy Fix," *Bulletin of the Atomic Scientists*, Vol. 60, No. 5, 2004, pp. 17-19. (RW 336)

Prados, J. "The mouse that roared: State Department intelligence in the Vietnam War. Contextual introduction", *National Security Archive Electronic Briefing Book*, [Online], no. 121. Available from: http://www.gwu.edu/~nsarchiv/NSAEBB/NSAEBB121/prados.htm, 2004, (RW 592)

Prados, J. "Pentagon Power Play," *Bulletin of the Atomic Scientists*, Vol. 61, No. 2, 2005, pp. 21-23. (RW 786)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Prados, J. "The Future of Covert Action," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 289. (RW 2475)

Prados, J. "Certainties, Doubts, and Imponderables: Levels of Analysis in the Military Balance," *Intelligence and National Security,* Vol. 26, No. 6, 2011, pp. 778-790. (RW 5390)

Prakken, B. "Uncertainty, Information, and (Re)Organization," *The Information Society,* Vol. 20, 2004, pp. 53. (RW 2639)

Prawat, R.S. "The Value of Ideas: The Immersion Approach to the Development of Thinking," *Educational Researcher*, Vol. 20, No. 2, 1991, pp. 3-10. (RW 2426)

Prescott, J.J. & Starr, S. *University of Illinois Law Review,* pp. 301-356, 2006. (RW 2043)

Pressler, M.W. "The Handwriting is on the Wall," *Washington Post,* October 11, 2006, pp. A01. (RW 1711)

Pressley, M. & Afflerbach, P. *Verbal Protocols of Reading: The Nature of Constructively Responsive Reading,* L. Erlbaum Associates, Hillsdale, NJ, 1995. (RW 3796)

Price, A.W. *Contextuality in Practical Reason,* Clarendon Press, Oxford, 2008. (RW 3301)

Price, G. & Sherman, C. "Exploring the Invisible Web: Seven Essential Strategies," *Online Magazine,* July-August, 2001, pp. 32. (RW 1462)

Prillaman, W.C. "Mything the Point: What's Wrong with the Conventional Wisdom about the CIA," *Intelligence and National Security,* Vol. 19, No. 1, 2004, pp. 1-28. (RW 159)

Primi, C. & Chiesi, F. "The Role of Relevant Knowledge and Cognitive Abilities in Gambler Fallacy", *7th Congress of European Society for Research in Mathematics Education,* Rzeszow, Poland, February 9-13, 2011 (RW 5759)

Pringle, R.W. "The Limits of OSINT: Diagnosing the Soviet Media, 1985-1989," *International Journal of Intelligence and Counterintelligence,* Vol. 16, No. 2, 2003, pp. 280-289. (RW 49)

Pritchard, M.C. "Intelligence: The Loss of Innocence," *International Journal of Intelligence and Counterintelligence*, Vol. 22, No. 1, 2009, pp. 147. (RW 3360)

Proctor, T.M. "Family Ties in the Making of Modern Intelligence," *Journal of Social History,* Winter, 2005, pp. 451. (RW 2265)

Project Management Institute. *Project Management Institute Practice Standard for Work Breakdown Structures,* Project Management Institute, Newtown Square, PA, 2001. (RW 3263)

Prunckun, H. "The Intelligence Analyst as Social Scientist: A Comparison of Research Methods," *Police Studies*, Vol. 19, No. 3, 1996, pp. 67-80. (RW 5661)

Prunckun, H. *Handbook of Scientific Methods of Inquiry for Intelligence Analysis,* Scarecrow Press, Lanham, MD, 2010. (RW 4025)

Puerta Melguizo, M.C., Boves, L. & Ramos, O.M. "A Proactive Recommendation System for Writing: Helping without Disrupting," *International Journal of Industrial Ergonomics,* Vol. 39, No. 3, 2009, pp. 516. (RW 4394)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Pughe, G.A. "The Dust that Isn't there," *Studies in Intelligence,* Vol. 2, No. 2, 1958, pp. 71-74. (RW 561)

Pulmones, R. "Linking Students' Epistemological Beliefs with their Metacognition in a Chemistry Classroom," *Asia Pacific Education Researcher,* Vol. 19, 2010, pp. 143-159. (RW 5057)

Puskeiler, A. *Scenario-Based Design: A Methodical Tool and a Practical Guide for using Scenarios in the Design Development Process of Products and Product Systems,* Ohio State University, Columbus, Ohio, 2001. (RW 3386)

Pustejovsky, J. & Mani, I. "Event and Temporal Awareness for Intelligence Analysis. Tutorial [Powerpoint Presentation]," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 842)

Puvathingal, B.J. & Hantula, D.A. "Revisiting the Psychology of Intelligence Analysis: From Rational Actors to Adaptive Thinkers," *American Psychologist,* December 26, 2011, pp. [unpaged]. (RW 5462)

Pyle, D. *Business Modeling and Data Mining,* Morgan Kaufmann Publishers, Amsterdam, 2003. (RW 2525)

Pyrczak, F. & Bruce, R.R. *Writing Empirical Research Reports: A Basic Guide for Students of the Social and Behavioral Sciences,* 5th ed., Pyrczak Pub., Glendale, CA, 2005. (RW 2306)

Pyszczynski, T. & Greenberg, J. "Toward an Integration of Cognitive and Motivational Perspectives on Social Inference: A Biased Hypothesis-Testing Model," *Advances in Experimental Social Psychology,* Vol. 20, 1987, pp. 297-340. (RW 5029)

Qi, W. "What is Intelligence Work", *Conference "Intelligence Economique: Recherches Et Applications",* 14-15 April 2003 (RW 515)

Qian, G. & Alvermann, D. "Role of Epistemological Beliefs and Learned Helplessness in Secondary School Students' Learning Science Concepts from Text," *Journal of Educational Psychology,* Vol. 87, No. 2, 1995, pp. 282-292. (RW 4653)

Qian, G. & Alvermann, D. "Relationship between Epistemological Beliefs and Conceptual Change Learning," *Reading and Writing Quarterly,* Vol. 16, No. 1, 2000, pp. 59-74. (RW 4641)

Quarmby, N. "Futures Work in Strategic Criminal Intelligence," in *Strategic Thinking in Criminal Intelligence*, ed. J. Ratcliffe, 2nd ed., Federation Press, Sydney, 2009, pp. 165-186. (RW 5768)

Quek, F., Rose, R.T. & McNeill, D. "Multimodal Meeting Analysis," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 860)

Quellmalz, E.S. "Needed: Better Methods for Teaching Higher-Order Thinking Skills," *Educational Leadership,* Vol. 43, No. 2, 1985, pp. 29-35. (RW 4082)

Quellmalz, E.S. "Developing Reasoning Skills," in *Teaching Thinking Skills: Theory and Practice*, eds. J.B. Baron & R.J. Sternberg, Freeman, New York, NY, 1987, pp. 86-105. (RW 3737)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Quesada, J., Kintsch, W. & Gomez, E. "Complex Problem-Solving: A Field in Search of a Definition?" *Theoretical Issues in Ergonomics Science,* Vol. 6, No. 1, 2005, pp. 5. (RW 2619)

Quiggin, T. *Seeing the Invisible: National Security Intelligence in an Uncertain Age,* World Scientific, Singapore, 2007. (RW 3840)

Quiggin, T. & Ramakrishna, K. "The Future of Strategic Early Warning," *ISN Security Watch,* 2006 (RW 1713)

Quine, W.V. *Word and Object,* Technology Press of the Massachusetts Institute of Technology, Cambridge, 1960. (RW 2303)

Quine, W.V. *From a Logical Point of View,* 2nd ed., Harper & Row, New York, 1963. (RW 2302)

Quine, W.V. & Ullian, J.S. *The Web of Belief,* 2nd ed., Random House, New York, 1978. (RW 2393)

Quinlan, M. "Just Intelligence: Prolegomena to an Ethical Theory," *Intelligence and National Security,* Vol. 22, No. 1, 2007, pp. 1. (RW 2380)

Quinn, J.L.J. "Staffing the Intelligence Community: The Pros and Cons of an Intelligence Reserve," *International Journal of Intelligence and Counterintelligence,* Vol. 13, No. 2, 2000, pp. 160-170. (RW 34)

Rachlinski, J.J. "Heuristics, Biases, and Governance," in *Blackwell Handbook of Judgment and Decision Making,* eds. D.J. Koehler & N. Harvey, Blackwell Pub., Malden, MA; Oxford, 2004, pp. 567. (RW 2825)

Radabaugh, G. *Idiot's Guide to Intelligence* 2000. (RW 318)

Radabaugh, G.C. *Information Operations,* 2002. (RW 1158)

Radford, B. "Senate Intelligence Committee Highlights Need for Skeptical Inquiry," *Skeptical Inquirer,* Vol. 28, No. 6, 2004, pp. 12-14. (RW 225)

Raduege, H.D., Jr. *DISA and NCS,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2001. (RW 1157)

Rae-Dupree, J. *Innovative Minds Don't Think Alike* 2007. (RW 2990)

Raeth, P.G. "Target Nomination for Infrared Surveillance and Persistent Imaging: Applying Predictive Anomaly Detection to Data Reduction for Operational Sensors," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 885)

Raeth, P.G. "Target Nomination for Infrared Surveillance and Persistent Imaging: Applying Predictive Anomaly Detection to Data Reduction for Operational Sensors [Powerpoint Presentation]," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 886)

Raichlen, D.A. & Polk, J.D. "Linking Brains and Brawn: Exercise and the Evolution of Human Neurobiology," *Proceedings of the Royal Society B: Biological Science,* Vol. 280, 2013 (RW 5885)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Raiola, E.O. "Earl C. Kelley: Education for What is Real," in *Sourcebook of Experiential Education: Key Thinkers and their Contributions*, eds. T.E. Smith & C. Knapp, Routledge, New York, 2011, pp. 180-184. (RW 4928)

RAND Corporation *"Connecting the Dots" in Intelligence. RAND Research Brief.* RB-9079, RAND Corporation, Santa Monica, CA, 2005. (RW 374)

Randel, J.M., Pugh, H.L. & Wyman, B.G. *Methods for Conducting Cognitive Task Analysis for a Decision Making Task,* NPRDC-TN-96-10, Navy Personnel Research and Development Center, San Diego, CA, 1996. (RW 1177)

Random, R.A. "Intelligence as a Science," *Studies in Intelligence,* Vol. 2, No. 2, 1958, pp. 75-79. (RW 533)

Ranganath, K.A., Spellman, B.A. & Joy-Gaba, J.A. "Cognitive "Category-Based Induction" Research and Social "Persuasion" Research are each about what Makes Arguments Believable: A Tale of Two Literatures," *Perspectives on Psychological Science,* Vol. 5, No. 2, 2010, pp. 115-122. (RW 4693)

Rankine, R.R. *Military Applications of Commercial SATCOM Systems,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1999. (RW 1029)

Ransom, H.H. *Central Intelligence and National Security,* Harvard University Press, Cambridge, MA, 1958. (RW 776)

Ransom, H.H. *The Intelligence Establishment,* Harvard University Press, Cambridge, MA, 1970. (RW 21)

Rapanotti, L., Hall, J.G. & Li, Z. "Deriving Specifications from Requirements through Problem Reduction," *IEE Proceedings - Software,* Vol. 153, No. 5, 2006, pp. 183. (RW 2573)

Raphael, D., Moss, S.W. & Rosser, M.E. "Evidence Concerning the Construct Validity of Conceptual Level as a Personality Variable," *Canadian Journal of Behavioural Science,* Vol. 11, No. 4, 1979, pp. 327-339. (RW 4614)

Rapoport, A. *Fights, Games, and Debates,* University of Michigan Press, Ann Arbor, 1960. (RW 2961)

Raschke, D. "Asymmetric Warfare Requires Intelligence Community Reorganization," *Signal,* April, 2008 (RW 3055)

Raschke, D.M. "Discretionary Time: An Approach to Encouraging Creativity in Intelligence Analysis," *Intelligencer,* Vol. 16, No. 1, 2008, pp. 23-24. (RW 4428)

Rasmussen, C. *Increasing "Jointness" and Reducing Duplication in DoD Intelligence* 2010. (RW 4434)

Rasmussen, J. *Information Processing and Human-Machine Interaction: An Approach to Cognitive Engineering,* North-Holland, New York, 1986. (RW 3622)

Ratcliffe, J. *Strategic Thinking in Criminal Intelligence,* Federation Press, Sydney, 2004. (RW 5737)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Ratcliffe, J. "Intelligence Research," in *Strategic Thinking in Criminal Intelligence*, ed. J. Ratcliffe, 2nd ed., Federation Press, Sydney, 2009, pp. 108-123. (RW 5702)

Ratcliffe, J. "The Structure of Strategic Thinking," in *Strategic Thinking in Criminal Intelligence*, ed. J. Ratcliffe, 2nd ed., Federation Press, Sydney, 2009, pp. 1-12. (RW 5756)

Ratcliffe, J. & Sheptycki, J. "Setting the Strategic Agenda," in *Strategic Thinking in Criminal Intelligence*, ed. J. Ratcliffe, 2nd ed., Federation Press, Sydney, 2009, pp. 248-268. (RW 5770)

Ratey, J.J. & Hagerman, E. *Spark: The Revolutionary New Science of Exercise and the Brain*, Little, Brown, New York, NY, 2008. (RW 4995)

Rathmell, A. "Towards Postmodern Intelligence," *Intelligence and National Security*, Vol. 17, No. 3, 2002, pp. 87-104. (RW 411)

Ratliff, E. "The Thinking Machine," *Wired*, Vol. 15, No. 3, 2007 (RW 2177)

Rattray, G.J. *Strategic Information Warfare*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1998. (RW 1031)

Rattray, G.J. *Defensive Strategic Information Warfare: Challenges for the United States*, Center for Information Policy Research. Harvard University, Cambridge, MA, 2000. (RW 1030)

Rattray, G.J. *Securing Cyberspace* 2005. (RW 1344)

Ratzan, L. *Understanding Information Systems What They Do and Why We Need Them*, American Library Association, Chicago, IL, 2004. (RW 1117)

Ray, J.J. "The Development and Validation of a Balanced Dogmatism Scale," *Australian Journal of Psychology*, Vol. 22, No. 3, 1970, pp. 253-260. (RW 5341)

Rayner, S. & Cools, E. *Style Differences in Cognition, Learning, and Management: Theory, Research, and Practice*, Routledge, New York, 2011. (RW 4440)

Reagan, R.T., Mosteller, F. & Youtz, C. "Quantitative Meanings of Verbal Probability Expressions," *Journal of Applied Psychology*, Vol. 74, 1989, pp. 433. (RW 2917)

Redlawsk, D.P., Civettini, A.J.W. & Emmerson, K.M. "The Affective Tipping Point: Do Motivated Reasoners Ever "Get it"?" *Political Psychology*, Vol. 31, No. 4, 2010, pp. 563-593. (RW 4794)

Redwood, B.C. *Intelligence Oriented Information Management* 2006. (RW 3000)

Reece, J.E. & Cumming, G. "Evaluating Speech-Based Composition Methods: Planning, Dictation and the Listening Word Processor," in *The Science of Writing: Theories, Methods, Individual Differences, and Applications*, eds. C.M. Levy & S.E. Ransdell, 1996, pp. 361. (RW 1828)

Reed, C. & Norman, T.J. *Argumentation Machines: New Frontiers in Argument and Computation*, Kluwer Academic Publishers, Boston, 2004. (RW 1484)

Reed, C. & Rowe, G. *Araucaria*, University of Dundee School of Computing. Available: http://araucaria.computing.dundee.ac.uk/doku.php, Viewed: November 2, 2009. (RW 3765)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Reed, J.G. & Baxter, P.M. "Using Reference Databases," in *The Handbook of Research Synthesis*, eds. H.M. Cooper & L.V. Hedges, Russell Sage Foundation, New York, 1994, pp. 57. (RW 2486)

Reed, J.H. *Effect of a Model for Critical Thinking on Student Achievement in Primary Source Document Analysis and Interpretation, Argumentative Reasoning, Critical Thinking Dispositions, and History Content in a Community College History Course*, Ph.D. dissertation, University of South Florida, 1998. (RW 3816)

Reich, R.C. "Re-Examining the Team A-Team B Exercise," *International Journal of Intelligence and Counterintelligence*, Vol. 3, No. 3, 1989, pp. 387-403. (RW 1189)

Reichertz, J. "Abduction, Deduction and Induction in Qualitative Research," in *A Companion to Qualitative Research*, eds. U. Flick, E. von Kardorff & I. Steinke, Sage Publications, London; Thousand Oaks, CA, 2004, pp. 159. (RW 3208)

Reininger, D., Mershon, J., Armstrong, J., Kulberda, R., Cohen, A., Bullard, P.R. & Ihrie, D. "Semantic Wiki for Tactical Intelligence Applications: A Demonstration", *Proceedings of the Third International Ontology for the Intelligence Community Conference OIC-2008*, Fairfax, VA, December 3-4, 2008, pp. 16-19. (RW 4826)

Reither, J.A. "Writing and Knowing: Toward Redefining the Writing Process," in *Landmark Essays on Writing Process*, ed. S. Perl, 1994, pp. 141. (RW 1833)

Renear, A.H. & Palmer, C.L. "Strategic Reading, Ontologies, and the Future of Scientific Publishing," *Science*, Vol. 325, 2009, pp. 828. (RW 3799)

Resch, D.T. "Predictive Analysis: The Gap between Academia and Practitioners," *Military Intelligence Professional Bulletin*, Vol. 21, No. 2, 1995, pp. 26. (RW 4260)

Resnick, L.B. *Education and Learning to Think*, National Academy Press, Washington, DC, 1997. (RW 5035)

Resnyansky, L. "The Role of Technology in Intelligence Practice: Linking the Developer and the User Perspectives," *Prometheus*, Vol. 28, No. 4, 2010, pp. 361-374. (RW 5591)

Restak, R.M. *The Naked Brain: How the Emerging Neurosociety is Changing How We Live, Work, and Love*, Harmony Books, New York, NY, 2006. (RW 1808)

Reynolds, G. *Exercise and the Ever-Smarter Human Brain*, Available: http://well.blogs.nytimes.com/2012/12/26/exercise-and-the-ever-smarter-human-brain/, Viewed: December 28, 2012. (RW 5884)

Reynolds, J.E. *Judgment and Decision Making in the Intelligence Analyst's Environment*, [undated]. (RW 202)

Reynolds, R.H., Sinatra, G.M. & Jetton, T.L. "Views of Knowledge Acquisition and Representation: A Continuum from Experience-Centered to Mind-Centered," *Educational Psychologist*, Vol. 31, No. 2, 1996, pp. 93-104. (RW 5328)

Reynolds, R.T. *What Fighter Pilots' Mothers Told them about Tactical Command and Control — and Certainly should have...*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1991. (RW 1033)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Reynolds, R.T. *The Pitfalls of Peacetime Military Bureaucracy,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1997. (RW 1032)

Rezaei, A.R. & Katz, L. "Evaluation of the Reliability and Validity of Cognitive Styles Analysis," *Personality and Individual Differences,* Vol. 36, No. 6, 2004, pp. 1317-1327. (RW 5337)

Ribaux, O. & Margot, P. "Inference Structures for Crime Analysis and Intelligence: The Example of Burglary using Forensic Science Data," *Forensic Science International,* Vol. 100, No. 3, 1999, pp. 193-210. (RW 5472)

Ribaux, O., Baylong, A., Roux, C., Delemont, O., Lock, E., Zingg, C. & Margot, P. "Intelligence-Led Crime Scene Processing. Part I: Forensic Intelligence," *Forensic Science International,* Vol. 195, No. 1-3, 2010, pp. 10-16. (RW 5585)

Ribaux, O., Walsh, S., J. & Margot, P. "The Contribution of Forensic Science to Crime Analysis and Investigation: Forensic Intelligence," *Forensic Science International,* Vol. 156, No. 2-3, 2006, pp. 171-181. (RW 5586)

Rice, R.E., McCreadie, M. & Chang, S.L. *Accessing and Browsing Information and Communication,* MIT Press, Cambridge, MA, 2001. (RW 1620)

Richards, J. *Art and Science of Intelligence Analysis,* Oxford University Press, Oxford, UK, 2010. (RW 5465)

Richardson, B. "Intelligence for the 21st Century," *SAIS Review,* Vol. 28, No. 1, 2008, pp. 145. (RW 3331)

Richardson, J.T.E. *Working Memory and Human Cognition,* Oxford University Press, New York, NY, 1996. (RW 4682)

Richardson, K.A., Cilliers, P. & Lissack, M. "Complexity Science: A 'Grey' Science for the 'Stuff in between'", *Proceedings of ICSTM2000: International Conference on Systems Thinking in Management,* Geelong, Australia, November 8-10, 2000, pp. 532-537. (RW 3788)

Richardson, K.A. "Robustness in Complex Information Systems: The Role of Information "Barriers" in Boolean Networks," *Complexity,* Vol. 15, No. 3, 2010, pp. 26. (RW 3843)

Richardson, L. "Writing: A Method of Inquiry," in *Handbook of Qualitative Research,* eds. N.K. Denzin & Y.S. Lincoln, 2nd ed., Sage Publications, Thousand Oaks, CA, 2000, pp. 923. (RW 2750)

Richardson, R.C. "NATO Nuclear Strategy: A Look Back," *Strategic Review,* Vol. 9, No. 2, 1981, pp. 35-43. (RW 254)

Richelson, J. *The U.S. Intelligence Community,* 4th ed., Westview Press, Boulder, CO, 1999. (RW 951)

Richelson, J.T. "The Technical Collection of Intelligence," in *Handbook of Intelligence Studies,* ed. L.K. Johnson, 2007, pp. 105. (RW 2461)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Richelson, J.T. "The Office that Never Was: The Failed Creation of the National Applications Office," *International Journal of Intelligence and Counterintelligence,* Vol. 24, No. 1, 2011, pp. 65-118. (RW 4577)

Richelson, J.T. "Intelligence Secrets and Unauthorized Disclosures: Confronting some Fundamental Issues," *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 4, 2012, pp. 639-677. (RW 5833)

Richelson, J.T. "Intelligence Secrets and Unauthorized Disclosures: Congronting some Fundamental Issues," *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 4, 2012, pp. 639-677. (RW 5802)

Richter, T., Schroeder, S. & Woehrmann, B. "You Don't have to Believe Everything You Read: Background Knowledge Permits Fast and Efficient Validation of Information," *Journal of Personality and Social Psychology,* Vol. 96, No. 3, 2009, pp. 538-558. (RW 5330)

Richter, T. & Schmid, S. "Epistemological Beliefs and Epistemic Strageties in Self-Regulated Learning," *Metacognition and Learning,* Vol. 5, No. 1, 2010, pp. 47-65. (RW 4832)

Ricks, T.E. "Does the intel suck? Here's why", *Foreign Policy,* [Online], January 14, 2010. Available from: http://ricks.foreignpolicy.com/posts/2010/01/14/does_the_intel_suck_here_s_why, 2010, (RW 3860)

Riding, R. "The Nature and Effects of Cognitive Style," in *Perspectives on Thinking, Learning, and Cognitive Styles,* eds. R.J. Sternberg & L. Zhang, L. Erlbaum Associates, Mahwah, NJ, 2001, pp. 47-72. (RW 3068)

Rieber, S. "Accuracy in Intelligence Predictions: Can Statistical Models Outperform Human Judgment? (How Statistical Models can Help Intelligence Analysts)", *International Studies Association,* [undated]. (RW 2921)

Rieber, S. "Intelligence Analysis and Judgmental Calibration," *International Journal of Intelligence and Counterintelligence,* Vol. 17, No. 1, 2004, pp. 97-112. (RW 54)

Rieber, S. "Communicating Uncertainty in Intelligence Analysis", *Annual Meeting of the International Studies Association,* San Diego, CA, March 22-26, 2006 (RW 2918)

Rieber, S. *Making Intelligence Smarter* 2010. (RW 4589)

Rieber, S. & Thomason, N. "Creation of a National Institute for Analytic Methods," *Studies in Intelligence,* Vol. 49, No. 4, 2005, pp. 71-77. (RW 1496)

Rieh, S.Y. "Cognitive Authority," in *Theories of Information Behavior,* eds. K.E. Fisher, S. Erdelez & L. McKechnie, Published for the American Society for Information Science and Technology by Information Today, Medford, N.J, 2005, pp. 83. (RW 3603)

Rieke, R.D., Sillars, M.O. & Peterson, T.R. *Argumentation and Critical Decision Making,* 7th ed., Pearson/Allyn and Bacon, Boston, 2009. (RW 3602)

Rijlaarsdam, G., van den Bergh, H. & Couzijn, M. "Current Trends in Research on Writing: Theories, Models and Methodology," in *Theories, Models and Methodology in Writing*

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Research, eds. G. Rijlaarsdam, H. van den Bergh & M. Couzijn, Amsterdam University Press, Amsterdam, 1996, pp. ix. (RW 2128)

Rijlaarsdam, G., van den Bergh, H. & Couzijn, M. *Theories, Models and Methodology in Writing Research,* Amsterdam University Press, Amsterdam, 1996. (RW 2012)

Riley, P.R. "The CIA and its Discontents," *International Journal of Intelligence and Counterintelligence,* Vol. 11, No. 3, 1998, pp. 255-269. (RW 63)

Rimanoczy, I. & Turner, E. *Action Reflection Learning,* Davies-Black Publishing, Mountain View, CA, 2008. (RW 5316)

Rips, L.J. "Reasoning," *Annual Review of Psychology,* Vol. 41, 1990, pp. 321-353. (RW 1959)

Risen, J. *State of War: The Secret History of the CIA and the Bush Administration,* Free Press, New York, 2006. (RW 2452)

Rissland, E.L. "Example-Based Reasoning," in *Informal Reasoning and Education*, eds. J.F. Voss, D.N. Perkins & J.W. Segal, L. Erlbaum Associates, Hillsdale, NJ, 1991, pp. 187. (RW 3457)

Riste, O. "Intelligence and the 'Mindset': The German Invasion of Norway in 1940," *Intelligence and National Security*, Vol. 22, No. 4, 2007, pp. 521. (RW 2865)

Ritchey, T. *Modeling Complex Socio-Technical Systems using Morphological Analysis* 2002. (RW 3550)

Ritchey, T. *Wicked Problems: Structuring Social Messes with Morphological Analysis* 2005. (RW 2615)

Ritchey, T. "Problem Structuring using Computer-Aided Morphological Analysis," *Journal of the Operational Research Society,* Vol. 57, 2006, pp. 792. (RW 3549)

Ritchhart, R. & Perkins, D.N. "Learning to Think: The Challenges of Teaching Thinking," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G. Morrison, Cambridge University Press, New York, NY, 2005, pp. 775-802. (RW 3876)

Ritchhart, R. *Intellectual Character: What It Is, Why It Matters, and How to Get It,* Jossey-Bass, San Francisco, CA, 2002. (RW 5170)

Ritchhart, R., Palmer, P., Church, M. & Tishman, S. "Thinking Routines: Establishing Patterns of Thinking in the Classroom", *American Educational Research Association Annual Meeting,* San Francisco, CA, April 7-11, 2006 (RW 5016)

Rittel, H.W.J., Grant, D.P. & Protzen, J. "Second-Generation Design Methods," in *Developments in Design Methodology*, ed. N. Cross, Wiley, Chichester, UK, 1984, pp. 317-327. (RW 2738)

Rittel, H.W.J. & Webber, M.M. "Dilemmas in a General Theory of Planning," *Policy Sciences,* Vol. 4, 1973, pp. 155. (RW 1338)

Rittel, H.W.J. & Webber, M.M. "Planning Problems are Wicked Problems," in *Developments in Design Methodology*, ed. N. Cross, Wiley, Chichester; New York, 1984, pp. 135. (RW 2737)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Rizk, N., Jaber, L., Halwany, S. & Boujaoude, S. "Epistemological Beliefs in Science: An Exploratory Study of Lebanese University Students' Epistemologies," *International Journal of Science and Mathematics Education,* 2011 (RW 5075)

Roach, K. "The Eroding Distinction between Intelligence and Evidence in Terrorism Investigations," in *Counter-Terrorism and Beyond: The Culture of Law and Justice After 911,* eds. N. McGarrity, A. Lynch & G. Williams, Routledge, Abington, UK, 2010, pp. 48-68. (RW 5526)

Robarge, D.S. "The Consumer is Always Right, but Not Always Helpful," in *A Handbook of the Psychology of Intelligence Analysis,* ed. R.L. Rees, 2008, pp. 204. (RW 3649)

Robbins, J.M. & Krueger, J.I. "Social Projection to Ingroups and Outgroups: A Review and Meta-Analysis," *Personality and Social Psychology Review,* Vol. 9, 2005, pp. 32. (RW 2881)

Roberts, A.R. & Yeager, K. *Evidence-Based Practice Manual: Research and Outcome Measures in Health and Human Services,* Oxford University Press, Oxford, UK, 2004. (RW 2526)

Roberts, M. "Intelligence Reform," *Security Management Online,* February, 2005 (RW 389)

Roberts, P. *Text of Senator Pat Roberts' Remarks at the Nixon Center* 2005. (RW 625)

Robertson, S.I. *Problem Solving,* Psychology Press, Hove England, 2001. (RW 2529)

Robertson, S.P. "Generating Object-Oriented Design Representations via Scenario Queries," in *Scenario-Based Design: Envisioning Work and Technology in Systems Development,* ed. J.M. Carroll, Wiley, New York, 1995, pp. 279. (RW 3398)

Robertson, S. "On the History of Evaluation in IR," *Journal of Information Science,* Vol. 34, No. 4, 2008, pp. 439-456. (RW 4859)

Robinson, A. "Lots on Info, Not always Accurate," *Science,* Vol. 33, No. 6051, 2011, pp. 1826-1827. (RW 5201)

Robson, C. *Real World Research: A Resource for Social Scientists and Practitioner-Researchers,* 2nd ed., Blackwell Publishers, Oxford, UK; Madden, MA, 2002. (RW 3154)

Robson, D.W. "Cognitive Rigidity: Methods to Overcome it," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 598)

Roby, C.J. *Challenges Facing the Defense Department in the Twenty-First Century,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2001. (RW 1156)

Roche, J.G. & Watts, B.D. "Choosing Analytic Measures," *The Journal of Strategic Studies,* Vol. 14, No. 2, 1991, pp. 165-209. (RW 227)

Rochefort, D.A. & Cobb, R.W. "Problem Definition: An Emerging Perspective," in *The Politics of Problem Definition: Shaping the Policy Agenda,* eds. D.A. Rochefort & R.W. Cobb, University Press of Kansas, Lawrence, Kan., 1994, pp. 1. (RW 2578)

Rock, A.D. & Garavan, T.N. "Understanding the Relational Characteristics of Effective Mentoring and Developmental Relationships at Work," in *Supporting Workplace Learning: Towards Evidence-Based Practice,* eds. R.F. Poell & M. van Woerkom, Springer, Dordrecht, 2011, pp. 107-128. (RW 4909)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Rockmore, A.J. *Catalyst Entity Extraction and Disambiguation Study Final Report*, IARPA/RDEC, Washington, DC, 2008. (RW 5566)

Rode, B. "Towards a Model of Pattern Recovery in Relational Data," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 879)

Rodgers, R.S. "Improving Analysis: Dealing with Information Processing Errors," *International Journal of Intelligence and Counterintelligence*, Vol. 19, No. 4, 2006, pp. 622-641. (RW 1638)

Rodriguez, A., Boyce, T., Lowrance, J. & Yeh, E. "Angler: Collaboratively Expanding Your Cognitive Horizon," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 819)

Rodriguez, S. "Political Assessment," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 35-43. (RW 3608)

Roemer, A., Leinert, S. & Sachse, P. "External Support of Problem Analysis in Design Problem Solving," *Research in Engineering Design*, Vol. 12, 2000, pp. 144. (RW 2930)

Roese, N.J. & Sherman, J.W. "Expectancy," in *Social Psychology: Handbook of Basic Principles*, eds. E.T. Higgins & A.W. Kruglanski, Second ed., 2007, pp. 91. (RW 2895)

Roets, A. & Van Hiel, A. *Need for Closure Scale Revised* [undated]. (RW 5310)

Rogers, Y. "Introduction," in *Models in the Mind*, eds. Y. Rogers, A. Rutherford & P.A. Bibby, 1992, pp. 1. (RW 1784)

Rogowski, R. "How Inference in the Social (but Not the Physical) Sciences Neglects Theoretical Anomaly," in *Rethinking Social Inquiry: Diverse Tools, Shared Standards*, eds. H.E. Brady & D. Collier, Rowman & Littlefield, Lanham, Md, 2004, pp. 75. (RW 2215)

Rohlman, D.S. *The Role of Problem Representation and Expertise in Hypothesis Testing: A Software Testing Analogue*, 1992. (RW 2530)

Rohrbaugh, C.C. & Shanteau, J. "Context, Process, and Experience: Research on Applied Judgment and Decision Making," in *Handbook of Applied Cognition*, ed. F. Durso, 1999, pp. 115. (RW 2052)

Rokeach, M. "A Method for Studying Individual Differences in "Narrow-Mindedness"," *Journal of Personality*, Vol. 20, No. 2, 1951, pp. 219-233. (RW 5282)

Rokeach, M. "Appendix B: The California F Scale," in *The Open and Closed Mind*, ed. M. Rokeach, Basic Books, New York, NY, 1960, pp. 415-416. (RW 5223)

Rokeach, M. "Appendix C: The Gough-Sanford Rigidity Scale," in *The Open and Closed Mind*, ed. M. Rokeach, Basic Books, New York, NY, 1960, pp. 418-419. (RW 5224)

Rokeach, M. "The Measurement of Open and Closed Systems," in *The Open and Closed Mind*, ed. M. Rokeach, Basic Books, New York, NY, 1960, pp. 71-97. (RW 5168)

Rokeach, M. *Beliefs, Attitudes, and Values: A Theory of Organization and Change*, Jossey-Bass, San Francisco, CA, 1968. (RW 4994)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Rokeach, M., McGovney, W.C. & Denny, M.R. "A Distinction between Dogmatic and Rigid Thinking," *Journal of Abnormal and Social Psychology,* Vol. 51, No. 1, 1955, pp. 87-93. (RW 5281)

Rokeach, M., McGovney, W.C. & Denny, M.R. "Dogmatic Thinking Versus Rigid Thinking: An Experimental Distinction," in *The Open and Closed Mind,* ed. M. Rokeach, Basic Books, New York, NY, 1960, pp. 182-195. (RW 5222)

Rolington, A. "Objective Intelligence or Plausible Denial: An Open Source Review of Intelligence Method and Process since 9/11," *Intelligence and National Security,* Vol. 21, No. 5, 2006, pp. 738. (RW 2085)

Ronczkowski, M. *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations,* CRC Press, Boca Raton, FL, 2004. (RW 1693)

Ronczkowski, M. *Terrorism and Organized Hate Crime: Intelligence Gathering, Analysis, and Investigations,* 2nd ed., CRC Press, Boca Raton, FL, 2006. (RW 3945)

Ronn, K.V. "Democratizing Strategic Intelligence?" *Policing,* 2012, pp. 1-10. (RW 5866)

Ronn, K.V. & Hoffding, S. "The Epistemic Status of Intelligence: an Epistemological Contribution to the Understanding of Intelligence," *Intelligence and National Security,* [Online]. Available from: http://dx.doi.org/10.1080/02684527.2012.701438, 2012. (RW 5808)

Rood, J. "Analyze this: Inside the One Spy Agency that Got Pre-War Intelligence on Iraq - and Much Else - Right," *Washington Monthly,* January-February, 2005 (RW 2099)

Root-Bernstein, B. *The X-Factor: Individual and Organization Essentials [Powerpoint Presentation]* (RW 2851)

Root-Bernstein, R.S. *Discovering,* Harvard University Press, Cambridge, MA, 1989. (RW 2700)

Rosati, J.A. "A Cognitive Approach to the Study of Foreign Policy," in *Foreign Policy Analysis: Continuity and Change in its Second Generation,* eds. L. Neack, J.A.K. Hey & P.J. Haney, Prentice Hall, Englewood Cliffs, NJ, 1995, pp. 49. (RW 4406)

Rose, C. *Congress and C3I,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1981. (RW 1034)

Rose, D. & Levinson, D. "Understanding User Goals in Web Search", *Proceedings of the 13th International Conference on World Wide Web,* New York, NY, May 17-22, 2004, pp. 13. (RW 4402)

Rose, M. *Writer's Block: The Cognitive Dimension,* Southern Illinois University Press, Carbondale, IL, 1984. (RW 1867)

Rosen, S.P. *War and Human Nature,* Princeton University Press, Princeton, NJ, 2005. (RW 164)

Rosenau, J. *The Importance of being Median,* Available: http://scienceblogs.com/tfk/2011/05/the_importance_of_being_median.php, Viewed: June 2, 2011. (RW 4853)

Rosenau, M.D. *Successful Project Management: A Step-by-Step Approach with Practical Examples,* 3rd ed., Wiley, New York, 1998. (RW 3152)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Rosenberg, J. "The Interpretation of Probability in Intelligence Estimation and Strategic Assessment," *Intelligence and National Security,* Vol. 23, No. 2, 2008, pp. 139. (RW 3071)

Rosenberg, R.A. *Defense Science Board Recommendations on Information Architecture for the Battlefield,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1997. (RW 1035)

Rosenberg, R.A. *Improved Application of Information to the Battlefield—Revisited,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2002. (RW 1155)

Rosengren, K.S., Johnson, C.N. & Harris, P.L. *Imagining the Impossible: Magical, Scientific, and Religious Thinking in Children,* Cambridge University Press, Cambridge, UK, 2000. (RW 3082)

Rosenthal, M.C. "The Fugitive Literature," in *The Handbook of Research Synthesis*, eds. H.M. Cooper & L.V. Hedges, Russell Sage Foundation, New York, 1994, pp. 85. (RW 2487)

Rosenthal, R. & Rubin, D.B. "Interpersonal Expectancy Effects: The First 345 Studies," *Behavioral and Brain Sciences,* Vol. 3, 1978, pp. 377. (RW 2878)

Roser, M.E., Fugelsang, J.A., Dunbar, K.N., Corballis, P.M. & Gazzaniga, M.S. "Dissociating Processes Supporting Causal Perception and Causal Inference in the Brain," *Neuropsychology,* Vol. 19, No. 5, 2005, pp. 591. (RW 2331)

Rossignol, M. "Relationship between Selected Discourse Strategies and Student Critical Thinking... the Clinical Post-Conference," *Journal of Nursing Education,* Vol. 36, No. 10, 1997, pp. 467-475. (RW 3968)

Rossmiller, A.J. *Still Broken,* 2008. (RW 2947)

Roth, E.M., Woods, D.D. & Pople, H.E. "Cognitive Simulation as a Tool for Cognitive Task Analysis," *Ergonomics,* Vol. 35, 1992, pp. 1163. (RW 1593)

Roth, E.M., Pfautz, J.D., Mahoney, S.M., Powell, G.M., Carlson, E.C., Guarino, S.L., Fichtl, T.C. & Potter, S.S. "Framing and Contextualizing Information Requests: Problem Formulation as Part of the Intelligence Analysis Process," *Journal of Cognitive Engineering and Decision Making,* Vol. 4, No. 3, 2010, pp. 210-239. (RW 5599)

Roth, W. "From "Wiggly Structures" to "Unshaky Towers": Problem Framing, Solution Finding, and Negotiation of Courses of Actions during a Civil Engineering Unit for Elementary Students," *Research in Science Education,* Vol. 25, No. 4, 1995, pp. 365. (RW 2646)

Roth, W. "Learning in Praxis, Learning for Praxis," in *Learning through Practice: Models, Traditions, Orientations, and Approaches*, ed. S. Billett, Springer, Dordrecht, 2010, pp. 21-36. (RW 4954)

Roth, W. & Roychoudhury, A. "Physics Students' Epistemologies and Views about Knowing and Learning," *Journal of Research in Science Teaching,* Vol. 31, No. 1, 1994, pp. 5. (RW 4441)

Rothenberg, H.C. "Identifying the Future Threat," *Studies in Intelligence,* Vol. 12, No. 4, 1968, pp. 13-21. (RW 532)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Rothkopf, D. "Technology can Fix U.S. Intelligence: The Intelligence Reform Bill Evaded Real Reform," *Technology Review,* Vol. 108, No. 2, 2005, pp. 34. (RW 789)

Rouet, J., Favart, M., Gaonac'h, D. & Lacroix, N. "Writing from Multiple Documents: Argumentation Strategies in Novice and Expert History Students," in *Theories, Models and Methodology in Writing Research*, eds. G. Rijlaarsdam, H. van den Bergh & M. Couzijn, Amsterdam University Press, Amsterdam, 1996, pp. 44. (RW 2148)

Rovner, J. *Pathologies of Intelligence-Policy Relations* 2005. (RW 502)

Rovner, J. "Fixing the Facts or Missing the Mark? Intelligence, Policy, and the War in Iraq", *2011 APSA Annual Meeting,* Seattle, WA, September 1-4, 2011 (RW 5551)

Rovner, J. *Fixing the Facts: National Security and the Politics of Intelligence,* Cornell University Press, Ithaca, NY, 2011. (RW 5378)

Rovner, J. *Intelligence, Policy, and the War in Iraq - Analysis,* Viewed: October 26, 2011. (RW 5213)

Rovner, J. "Is Politicization Ever a Good Thing?" *Intelligence and National Security,* Vol. 28, No. 1, 2013, pp. 55-67. (RW 5912)

Rovner, J. & Long, A. "Intelligence Failure and Reform: Evaluating the 9/11 Commission Report," *Breakthroughs,* Vol. 14, No. 1, 2005, pp. 10-21. (RW 484)

Rovner, J. & Long, A. "The Perils of Shallow Theory: Intelligence Reform and the 9/11 Commission," *International Journal of Intelligence and Counterintelligence,* Vol. 18, No. 4, 2005, pp. 609. (RW 1695)

Rovner, J. & Long, A. "Correspondence. Response to "How Intelligent is Intelligence Reform" *International Security,* Vol. 30, No. 4, 2006, pp. 196. (RW 1697)

Rowe, N.C. "Automatic Detection of Fake File Systems," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 824)

Rowen, H.S. "Reforming Intelligence: A Market Approach," in *U.S. Intelligence at the Crossroads: Agendas for Reform*, eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 232-242. (RW 210)

Roy, M. & Lerch, J. "Overcoming Ineffectual Mental Representations in Base-Rate Problems," *Information Systems Research,* Vol. 7, No. 2, 1996, pp. 233. (RW 2378)

Royce, J.R. "Three Ways of Knowing and the Scientific World View," *Methodology and Science,* Vol. 11, 1978, pp. 146-164. (RW 5050)

Rubino-Hallman, S. "When Gender Goes to Combat: The Impact of Representations in Collective Decision Making," in *Problem Representation in Foreign Policy Decision Making*, eds. D.A. Sylvan & J.F. Voss, 1998, pp. 261-278. (RW 1614)

Rubinstein, M.F. *Patterns of Problem Solving,* Prentice-Hall, Englewood Cliffs, NJ, 1974. (RW 2775)

Rubinstein, M.F. *Tools for Thinking and Problem Solving,* Prentice-Hall, Englewood Cliffs, NJ, 1986. (RW 2697)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Rudman, W.B. *Perspectives on National Security in the Twenty-First Century,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2002. (RW 170)

Rudner, M. "Intelligence Studies in Higher Education: Capacity-Building to Meet Societal Demand," *International Journal of Intelligence and Counterintelligence,* Vol. 22, No. 1, 2009, pp. 110. (RW 3358)

Rudolph, J.W. & Raemer, D.B. "Diagnostic Problem Solving during Simulated Crises in the OR," *Anesthesia and Analgesia,* Vol. 98, No. 5S, 2004, pp. S34. (RW 5258)

Rudolph, J.W. *Into the Big Muddy and Out Again: Error Persistence and Crisis Management in the Operating Room,* Ph.D. dissertation, Boston College, 2003. (RW 1965)

Ruggiero, V.R. *Beyond Feelings: A Guide to Critical Thinking,* 8th ed., McGraw-Hill Higher Education, Boston, MA, 2008. (RW 3480)

Rukavina, I. & Daneman, M. "Integration and its Effects in Acquiring Knowledge about Competing Scientific Theories from Text," *Journal of Educational Psychology,* Vol. 88, No. 2, 1996, pp. 272-287. (RW 4620)

Rumelhart, D.E. "Schemata and the Cognitive System," in *Handbook of Social Cognition*, eds. R.S. Wyer & T.K. Srull, L. Erlbaum Associates, Hillsdale, NJ, 1984, pp. 161. (RW 2950)

Rumsey, S. *How to Find Information*, Open University Press, Maidenhead, 2004. (RW 3118)

Rumsfeld, D.H. *Town Hall Meeting with Rumsfeld* 2001. (RW 1266)

Rumsfeld, D.H. *Defense Department Town Hall Meeting with Secretary of Defense* 2002. (RW 1262)

Rumsfeld, D.H. *Fiscal Year 2003 Defense Budget Testimony - Senate Armed Services Committee (Transcript)* 2002. (RW 1267)

Rumsfeld, D.H. *Prepared Testimony for the Senate Foreign Relations Committee regarding the Moscow Treaty* 2002. (RW 1268)

Rumsfeld, D.H. *Secretary Rumsfeld Speaks on 21st Century Transformation of US Armed Forces (Transcript of Remarks and Question and Answer Period)* 2002. (RW 1269)

Rumsfeld, D.H. *Testimony of US Secretary of Defense before the Senate Armed Services Committee regarding Iraq* 2002. (RW 1270)

Rumsfeld, D.H. *Council on Foreign Relations (Transcript)* 2003. (RW 1261)

Rumsfeld, D.H. *Hearing of the Senate Armed Services Committee on US Intelligence* 2004. (RW 1263)

Rumsfeld, D.H. *Remarks to the Heritage Foundation* 2004. (RW 1264)

Rumsfeld, D.H. *Testimony before the House Armed Services Committee* 2004. (RW 1265)

Runco, M.A. & Chand, I. "Problem Finding, Evaluative Thinking, and Creativity," in *Problem Finding, Problem Solving, and Creativity*, ed. M.A. Runco, Ablex Pub. Corp., Norwood, NJ, 1994, pp. 40. (RW 2743)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Rush, M. "A Neglected Source of Evidence," *Studies in Intelligence*, Vol. 2, No. 3, 1958, pp. 117-125. (RW 520)

Russell, C.A. & Levy, S.J. "The Temporal and Focal Dynamics of Volitional Re-consumption: a Phenomenological Investigation of Repeated Hedonic Experiences," *Journal of Consumer Research*, [Online], Available from: http://www.jstor.org/stable/10.1086/662996?origin=JSTOR-pdf, 2012, (RW 5440)

Russell, D.M. "Industry-Academic Relationships," *Computer*, Vol. 42, No. 3, 2009, pp. 67. (RW 3443)

Russell, D.M., Slaney, M., Qu, Y. & Houston, M. "A Cost Structure Analysis of Manual and Computer-Supported Sensemaking Behavior," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 798)

Russell, K. "The Subjectivity of Intelligence Analysis and Implications for the US National Security Strategy," *SAIS Review*, Vol. 24, No. 1, 2004, pp. 147-162. (RW 204)

Russell, R.L. "What if ... "China Attacks Taiwan"," *parameters*, Vol. 31, No. 3, 2001, pp. 76-91. (RW 4878)

Russell, R.L. "Intelligence Failures," *Policy Review*, 123, 2004 (RW 335)

Russell, R.L. "Spies Like Them," *The National Interest*, 77, 2004, pp. 59-62. (RW 410)

Russell, R.L. "Tug of War: The CIA's Uneasy Relationship with the Military," in *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, eds. R.Z. George & R.D. Kline, National Defense University Press, Washington, DC, 2004, pp. 479-491. (RW 698)

Russell, R.L. "A Weak Pillar for American National Security: The CIA's Dismal Performance Against WMD Threats," *Intelligence and National Security*, Vol. 20, No. 3, 2005, pp. 466. (RW 1749)

Russell, R.L. "Achieving All-Source Fusion in the Intelligence Community," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 189. (RW 2467)

Russell, R.L. *Sharpening Strategic Intelligence: Why the CIA Gets it Wrong and What Needs to be Done to Get it Right*, Cambridge University Press, Cambridge, UK, 2007. (RW 2287)

Russell, R.L. "Competitive Analysis: Techniques for Better Gauging Enemy Political Intentions and Military Capabilities," in *Oxford Handbook of National Security Intelligence*, ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 375-388. (RW 4709)

Russo, J.E. & Schoemaker, P.J.H. *Decision Traps: Ten Barriers to Brilliant Decision- Making and how to Overcome them*, Doubleday / Currency, New York, 1989. (RW 3002)

Ruthven, I. "Integrating Approaches to Relevance," in *New Directions in Cognitive Information Retrieval*, eds. A. Spink & C. Cole, Springer, Dordrecht, 2005, pp. 61. (RW 3544)

Ruthven, I. "Information Retrieval in Context," in *Advanced Topics in Information Retrieval*, eds. M. Melucci & R. Baeza-Yates, Springer, New York, NY, 2011, pp. 195-216. (RW 4876)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Ruthven, I., Baillie, M., Azzopardi, L., Bierig, R., Nicol, E., Sweeney, S. & Yaciki, M. "Contextual Factors Affecting the Utility of Surrogates within Exploratory Search," *Information Processing and Management,* Vol. 44, 2008, pp. 437-462. (RW 4871)

Rutledge, D.N., DePalma, J.A. & Cunningham, M. "A Process Model for Evidence-Based Literature Syntheses," *Oncology Nursing Forum,* Vol. 31, No. 3, 2004, pp. 543. (RW 2254)

Ryan, A. *What is a Systems Approach* 2008. (RW 3352)

Ryan, G.W. & Bernard, H.R. "Data Management and Analysis Methods," in *Handbook of Qualitative Research*, eds. N.K. Denzin & Y.S. Lincoln, 2nd ed., Sage Publications, Thousand Oaks, CA, 2000, pp. 769. (RW 2748)

Ryan, Julie J. C. H. *Information Warfare: A Conceptual Framework,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1997. (RW 1036)

Ryan, M.P. "Conceptions of Prose Coherence: Individual Differences in Epistemological Standards," *Journal of Educational Psychology,* Vol. 76, No. 6, 1984, pp. 1226-1238. (RW 4651)

Ryan, M.P. "Monitoring Text Comprehension: Individual Differences in Epistemological Standards," *Journal of Educational Psychology,* Vol. 76, No. 2, 1984, pp. 249-258. (RW 4652)

Ryan, M. "Filling in the 'Unknowns': Hypothesis-Based Intelligence and the Rumsfeld Commission," *Intelligence and National Security,* Vol. 21, No. 2, 2006, pp. 286-315. (RW 1750)

Ryle, G. *The Concept of Mind,* Hutchinson, London, 1949. (RW 3701)

Sá, W., Kelley, C., Ho, C., Stanovich, K.E. & West, R.F. *Composite Actively Open-Minded Thinking Scale -- 11/6/03* 2003. (RW 4101)

Sa, W.C., Kelley, C.N., Ho, C. & Stanovich, K.E. "Thinking about Personal Theories: Individual Differences in the Coordination of Theory and Evidence," *Personality and Individual Differences,* Vol. 38, No. 5, 2005, pp. 1149-1161. (RW 3339)

Sa, W., West, R. & Stanovich, K.E. "The Domain Specificity and Generality of Belief Bias: Searching for a Generalizable Critical Thinking Skill," *Journal of Educational Psychology,* Vol. 91, No. 3, 1999, pp. 497-510. (RW 3857)

Saari, D.G. *Simpson's Paradox* 1988. (RW 4722)

Sachse, P., Hacker, W. & Leinert, S. "External Thought - Does Sketching Assist Problem Analysis?" *Applied Cognitive Psychology,* Vol. 18, 2004, pp. 415. (RW 2929)

Sacks, R. *Primary (Telephone) Research: Using the Phone to Increase Your Research Results [Powerpoint Presentation]* (RW 1455)

Sadler, W.A. "Holistic Thinking Skills Instruction: An Interdisciplinary Approach to Improving Intellectual Performance," in *Thinking Skills Instruction: Concepts and Techniques*, eds. M. Heiman & J. Slomianko, National Education Association, Washington, DC, 1987, pp. 183-188. (RW 5086)

Safire, W. "The New Groupthink," *New York Times,* July 14, 2004, p. 23. (RW 941)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Safran, C. *Concept-Based Information Retrieval for User-Oriented Knowledge Transfer: Personalized and Contextual Search in the Context of Digital Libraries,* Germany VDM Verlag Dr. Muller, Saarbrucken, 2008. (RW 3539)

Sage, A.P. & Botta, R.F. "On Human Information-Processing and its Enhancement using Knowledge-Based Systems," *Large Scale Systems in Information and Decision Technologies,* Vol. 5, No. 1, 1983, pp. 35-50. (RW 5279)

Sainsbury, R.M. *Paradoxes,* 2nd ed., Cambridge University Press, Cambridge, UK, 1995. (RW 2304)

Salas, E., Wilson, K.A., Burke, C.S. & Bowers, C.A. "Myths about Crew Resource Management Training," *Ergonomics in Design,* Fall, 2002, pp. 20. (RW 2833)

Salinas, C. "Human Rights and Intelligence Reform," *Foreign Policy in Focus,* Vol. 3, No. 20, 1998, pp. 1-4. (RW 311)

Salmon, W.C. *The Foundations of Scientific Inference,* University of Pittsburgh Press, Pittsburgh, PA, 1967. (RW 4033)

Salomon, G. & Perkins, D. "Do Technologies make Us Smarter? Intellectual Amplification with, of, and through Technology," in *Intelligence and Technology: The Impact of Tools on the Nature and Development of Human Abilities,* eds. R.J. Sternberg & D. Preiss, L. Erlbaum Associates, Mahwah, NJ, 2005, pp. 71. (RW 3078)

Salthouse, T.A., Fristoe, N., McGuthry, K.E. & Hambrick, D.Z. "Relation of Task Switching to Speed, Age, and Fluid Intelligence," *Psychology & Aging,* Vol. 13, No. 3, 1998, pp. 445-461. (RW 4694)

Salvendy, G. *Handbook of Human Factors and Ergonomics,* 3rd ed., John Wiley, Hoboken, NJ, 2006. (RW 3213)

Samarapungavan, A. & Westby, E.L. "Predicting and Explaining how People Form Beliefs about the Natural World: The Development of Epistemic Knowledge in Childhood", *Annual Meeting of the American Educational Research Association,* Montreal, QB, (RW 4843)

Samarapungavan, A., Westby, E.L. & Bodner, G.M. "Contextual Epistemic Development in Science: A Comparison of Chemistry Students and Research Chemists," *Science Education,* Vol. 90, No. 3, 2006, pp. 468-495. (RW 4851)

Samford, J.A. "The Intelligence Necessary to the Formulation of a Sound Strategy," *Studies in Intelligence,* Vol. 1, No. 4, 1957, pp. 1-9. (RW 563)

Sample, I. "The Brain Scan that can Read People's Intentions," *The Guardian,* 2007 (RW 2097)

Sampson, M., Zhang, L., Morrison, A., Barrowman, N.J., Clifford, T.J., Platt, R.W., Klassen, T.P. & Moher, D. "An Alternative to the Hand Searching Gold Standard: Validating Methodological Search Filters using Relative Recall," *BMC Medical Research Methodology,* Vol. 6, 2006, pp. 33. (RW 2281)

Samuelson, D. "Agents of Change," *OR/MS Today,* Vol. 32, No. 1, 2005, pp. 26. (RW 1679)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Sana, L.J. & Schwarz, N. "Metacognitive Experiences and Hindsight Bias: It's Not just the Thought (Content) that Counts!" *Social Cognition,* Vol. 25, No. 1, 2007, pp. 185. (RW 2451)

Sanchez, D. & Moreno, A. "A Methodology for Knowledge Acquisition from the Web," *International Journal of Knowledge-based and Intelligent Engineering Systems,* Vol. 10, 2006, pp. 453. (RW 2754)

Sandelowski, M. & Barroso, J. *Handbook for Synthesizing Qualitative Research,* Springer Pub. Co., New York, 2007. (RW 2194)

Sandelowski, M., Trimble, F., Woodard, E.K. & Barroso, J. "From Synthesis to Script: Transforming Qualitative Research Findings for use in Practice," *Qualitative Health Research,* Vol. 16, No. 10, 2006, pp. 1350. (RW 2236)

Sanders, R. *Results of the Fiscal Year 2007 US Intelligence Community Inventory of Core Contractor Personnel* 2008. (RW 3237)

Sandoval, W.A. "Understanding Students' Practical Epistemologies and their Influence on Learning through Inquiry," *Science Education,* Vol. 89, No. 4, 2005, pp. 634-656. (RW 5303)

Sandow-Quirk, M. "A Failure of Intelligence," *Prometheus,* Vol. 20, No. 2, 2002, pp. 131-142. (RW 260)

Sands, A. "Integrating Open Sources into Transnational Threat Assessments," in *Transforming U.S. Intelligence*, eds. J.E. Sims & B.L. Gerber, Georgetown University Press, Washington, D.C, 2005, pp. 63-78. (RW 917)

Sanfilippo, A., Baddeley, B., Cowell, A.J., Gregory, M.L., Hohimer, R. & Tratz, S. "Building a Human Information Discourse Interface to Uncover Scenario Content," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 827)

Sangillo, G. & Gorman, S. "Smarter Intelligence: A Post-9/11 Priority," *National Journal,* Vol. 36, No. 21, 2004, pp. 1572. (RW 1680)

Santos, E., Nguyen, H., Yu, F., Kim, K., Li, D., Wildinson, J., Olson, A. & Russell, J. "Capturing User Intent for Analytic Process," *Lecture Notes in Computer Science,* Vol. 5535, 2009, pp. 349-354. (RW 5652)

Santos, E., Nguyen, H., Yu, F., Kim, K., Li, D., Wilkinson, J., Olson, A. & Russell, J. "Intent-Driven Insider Threat Detection in Intelligence Analyses", *Proceedings of the 2008 IEEE/WIC/ACM International Conference on Intelligent Agent Technology,* Sydney, Australia, December 9-12, 2008, pp. 345-349. (RW 5651)

Santos, E., Nguyen, H., Yu, F., Ling, D. & Wilkinson, J.T. "Impacts of Analysts' Cognitive Styles on the Analytic Process", *IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology,* pp. 601-610. (RW 5596)

Santos, E. & Santos, E. "An Architecture for Distributed Real-Time Large-Scale Information Processing for Intelligence Analysis," in *Intelligent Computing: Theory and Applications II. Proc. of the SPIE Volume 5421*, ed. K.L. Priddy, 2004. (RW 1312)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Santos, E., Zhao, Q., Johnson, G. & Nguyen, H. "A Cognitive Framework for Information Gathering with Deception Detection for Intelligence Analysis," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 794)

Santos, E., Zhao, Q., Nguyen, H. & Wang, H. *Impacts of User Modeling on Personalization of Information Retrieval: An Evaluation with Human Intelligence Analysts* (RW 2176)

Santos, J.P.E. *Epistemological Beliefs, Learning Styles, and Academic Performance of Biology Students in Five High Schools of Central Luzaon State University* 2010?. (RW 5078)

Sapp, E.G. "Decision Trees," *Studies in Intelligence,* Vol. 18, No. 4, 1974, pp. 45-57. (RW 528)

Saracevic, T. "Relevance: A Review of the Literature and a Framework for Thinking on the Notion in Information Science. Part III: Behavior and Effects of Relevance," *Journal of the American Society for Information Science and Technology,* Vol. 58, No. 13, 2007, pp. 2126-2144. (RW 5653)

Saracevic, T. "Relevance: A Review of and a Framework for the Thinking on the Notion in Information Science," *Journal of the American Society for Information Science,* Vol. 26, No. 6, 1975, pp. 321-343. (RW 1211)

Saracevic, T. "Relevance: A Review of the Literature and a Framework for Thinking on the Notion in Information Science. Part II: Nature and Manifestations of Relevance ," *Journal of the American Society for Information Science and Technology,* Vol. 58, No. 13, 2007, pp. 1915-1933. (RW 4934)

Satish, U. "Behavioral Complexity: A Review," *Journal of Applied Social Psychology,* Vol. 27, No. 23, 1997, pp. 2047. (RW 3064)

Satterthwaite, F.G. "Visit to Mazagon Dockyard, Bombay," in *Bringing Intelligence about: Practitioners Reflect on Best Practices,* eds. R.G. Swenson, Joint Military Intelligence College, Center for Strategic Intelligence Research, Washington, DC, 2003, pp. 29. (RW 1487)

Saunders, D. & Thagard, P. "Creativity in Computer Science," in *Creativity Across Domains: Faces of the Muse,* eds. J.C. Kaufman & J. Baer, L. Erlbaum Associates, Mahwah, NJ, 2005, pp. 153. (RW 4329)

Saunders, K.A. *Open Source Information: A True Collection Discipline,* Royal Military College of Canada, 2000. (RW 4537)

Savolainen, R. "The Sense-Making Theory: Reviewing the Interests of a User-Centered Approach to Information Seeking and use," *Information Processing and Management,* Vol. 29, No. 1, 1993, pp. 13. (RW 2534)

Scandura, J.M. *Problem Solving: A Structural/Process Approach with Instructional Implications,* Academic Press, New York, 1977. (RW 2666)

Scardamalia, M. & Bereiter, C. "Research on Written Composition," in *Handbook of Research on Teaching.* 3rd. ed., ed. M.C. Wittrock, 1986, pp. 778. (RW 2283)

Schachter, J.M. *The Eye of the Believer: Psychological Influences on Counter-Terrorism Policy-Making* 2002. (RW 3305)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Schaeffer, N.C. *Thinking and Learning to Think,* L. B. Lippincott Co., Philadelphia PA, 1901. (RW 4501)

Schaeken, W. *The Mental Models Theory of Reasoning: Refinements and Extensions,* L. Erlbaum Associates, Mahwah, NJ, 2005. (RW 1721)

Schafersman, S.D. *An Introduction to Critical Thinking,* Available: www.cybercomputing.com/freeinquiry/files/critical-thinking.html, Viewed: February 13, 2012. (RW 3760)

Schaie, K.W. "A Test of Behavioral Rigidity," *Journal of Abnormal and Social Psychology,* Vol. 51, No. 3, 1955, pp. 604-610. (RW 5343)

Schaller, M. & O'Brien, M. ""Intuitive Analysis of Covariance" and Group Stereotype Formation," *Personality and Social Psychology Bulletin,* Vol. 18, No. 6, 1992, pp. 776-785. (RW 5315)

Schamber, L. "Relevance and Information Behavior," *Annual Review of Information Science and Technology,* Vol. 29, 1994, pp. 3-48. (RW 1477)

Schank, P. *Convince Me: Software,* Available: http://www.soe.berkeley.edu/~schank/convinceme/software.html, Viewed: November 2, 2009. (RW 3762)

Schank, R.C. & Abelson, R.P. *Scripts, Plans, Goals, and Understanding: An Inquiry into Human Knowledge Structures,* L. Erlbaum Associates, Hillsdale, NJ, 1977. (RW 2372)

Scheerer, M. "Problem-Solving," *Scientific American,* Vol. 208, 1963, pp. 118. (RW 2689)

Schiefele, U. "Topic Interest, Text Representation, and Quality of Experience," *Contemporary Educational Psychology,* Vol. 21, No. 1, 1996, pp. 3-18. (RW 4615)

Schiefele, U. & Krapp, A. "Topic Interest and Free Recall of Expository Text," *Learning and Individual Differences,* Vol. 8, No. 2, 1996, pp. 141-160. (RW 4622)

Schilling, D.T. *Strategic Intelligence to Meet Institutional Planning Needs of the Twenty First Century,* US Army War College, Carlisle Barracks, PA, 2004. (RW 602)

Schlesinger, J. *A Review of the Intelligence Community,* 1971. (RW 764)

Schmidt, F.L. & Hunter, J.E. "The Validity and Utility of Selection Methods in Personnel Psychology: Practical and Theoretical Implications of 85 Years of Research Findings," *Psychological Bulletin,* Vol. 124, No. 4, 1998, pp. 262-274. (RW 722)

Schmitt, F., Cassens, J., Kindsmueller, M.C. & Herczeg, M. "Mental Models of Disappearing Systems: Challenges for a Better Understanding", *Proceedings of the 6th International Workshop on Modeling and Reasoning in Context,* Lisbon, August 17, 2010 (RW 4866)

Schmitt, G.J. "Truth to Power? Rethinking Intelligence Analysis," in *The Future of American Intelligence,* ed. P. Berkowitz, Hoover Institution Press, Stanford, CA, 2005, pp. 41-64. (RW 1215)

Schmitz, T.W., De Rosa, E. & Anderson, A.K. "Opposing Influences of Affective State Valence on Visual Cortical Encoding," *Journal of Neuroscience,* Vol. 29, 2009, pp. 7199. (RW 3500)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Schneider, M. "Intelligence in the Formulation of Defense Policy," in *Intelligence and Policy. Intelligence Requirements for the 1980's Vol. 7*, ed. R. Godson, Lexington Books, Lexington, MA, 1986, pp. 55-85. (RW 1139)

Schneider, S.L. & Shanteau, J. *Emerging Perspectives on Judgment and Decision Research,* Cambridge University Press, Cambridge, UK, 2003. (RW 2347)

Schoen, D.A. "Problems, Frames, and Perspectives on Designing," *Design Studies,* Vol. 5, No. 3, 1984, pp. 132. (RW 2688)

Schoen, D.A. *The Reflective Practitioner: How Professionals Think in Action,* Basic Books, New York, 1983. (RW 2547)

Schoen, D.A. *Educating the Reflective Practitioner,* Jossey-Bass, San Francisco, 1990. (RW 2548)

Schoen, D.A. & Rein, M. *Frame Reflection: Toward the Resolution of Intractable Policy Controversies,* BasicBooks, New York, 1994. (RW 2577)

Schoenfeld, A.H. "Beyond the Purely Cognitive: Belief Systems, Social Cognitions, and Metacognitions as Driving Forces in Intellectual Performance," *Cognitive Science,* Vol. 7, 1983, pp. 329. (RW 3773)

Schoenfeld, A.H. "Beyond the Purely Cognitive: Metacognition and Social Cognition as Driving Forces in Intellectual Performance", *American Educational Research Association Annual Meeting,* New York, NY, March 19-23, 1982 (RW 5020)

Schoenfeld, A.H. *Mathematical Problem Solving,* Academic Press, Orlando, FL, 1985. (RW 4416)

Schoenfeld, A.H. & Herrmann, D.J. "Problem Perception and Knowledge Structure in Expert and Novice Mathematical Problem Solvers," *Journal of Experimental Psychology: Learning, Memory, and Cognition,* Vol. 8, No. 5, 1982, pp. 484-494. (RW 4919)

Scholtz, J., Morse, E. & Hewett, T. "In Depth Observational Studies of Professional Intelligence Analysts", *Human Performance, Situation Awareness and Automation Technology Conference,* March 22-25 (RW 3259)

Scholtz, J., Morse, E. & Steves, M.P. "Evaluation Metrics and Methodologies for User-Center Evaluation of Intelligence Systems," *Interacting with Computers,* Vol. 18, No. 6, 2006, pp. 1186. (RW 3260)

Scholtz, J. "Metrics for Evaluation of Software Technology to Support Intelligence Analysis", *Proceedings of the Human Factors and Ergonomics Society 49th Meeting,* pp. 918. (RW 3570)

Scholtz, J., Morse, E. & Hewett, T. "An Analysis of Qualitative and Quantitative Data from Professional Intelligence Analysts," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 813)

Scholtz, J., Steves, M. & Morse, E. *Position Paper for Cognition and Collaboration Workshop: Analyzing Distributed Community Practices for Design* (RW 3268)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Schommer, M. "Effects of Beliefs about the Nature of Knowledge on Comprehension," *Journal of Educational Psychology,* Vol. 82, 1990, pp. 498. (RW 2675)

Schommer, M. "Epistemological Development and Academic Performance among Secondary Students," *Journal of Educational Psychology,* Vol. 85, 1993, pp. 406. (RW 2676)

Schommer, M. "Synthesizing Epistemological Belief Research: Tentative Understandings and Provocative Confusions," *Educational Psychology Review,* Vol. 6, No. 4, 1994, pp. 293-319. (RW 2677)

Schommer, M. "An Emerging Conceptualization of Epistemological Beliefs and their Role in Learning," in *Beliefs about Texts and Instruction with Text,* eds. R. Garner & P.A. Alexander, L. Erlbaum Associates, Hillsdale, NJ, 1994, pp. 25-40. (RW 2813)

Schommer, M. "The Role of Adults' Beliefs about Knowledge in School, Work, and Everyday Life," in *Adult Learning and Development: Perspectives from Educational Psychology*, eds. M.C. Smith & T. Pourchot, L. Erlbaum Associates, Mahwah, NJ, 1998, pp. 127. (RW 4326)

Schommer, M., Crouse, A. & Rhodes, N. "Epistemological Beliefs and Mathematical Text Comprehension: Believing it is Simple Does Not Make it So," *Journal of Educational Psychology,* Vol. 84, No. 4, 1992, pp. 435-443. (RW 4915)

Schommer, M. & Walker, K. "Are Epistemological Beliefs Similar Across Domains?" *Journal of Educational Psychology,* Vol. 87, No. 3, 1995, pp. 424-432. (RW 2717)

Schommer-Aikins, M. & Easter, M. "Ways of Knowing and Epistemological Beliefs Combined Effect on Academic Performance," *Educational Psychology,* Vol. 26, No. 3, 2006, pp. 411-423. (RW 4295)

Schommer-Aikins, M. & Easter, M. "Epistemological Beliefs' Contributions to Study Strategies of Asian Americans and European Americans," *Journal of Educational Psychology,* Vol. 100, No. 4, 2008, pp. 920. (RW 4294)

Schommer-Aikins, M. & Easter, M. "Ways of Knowing and Willingness to Argue," *The Journal of Psychology: Interdisciplinary and Applied,* Vol. 143, No. 2, 2009, pp. 117-132. (RW 4293)

Schommer-Aikins, M. "An Evolving Theoretical Framework for an Epistemological Belief System," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing,* eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 103. (RW 3084)

Schommer-Aikins, M. "Explaining the Epistemological Belief System: Introducing the Embedded Systemic Model and Coordinated Research Approach," *Educational Psychologist,* Vol. 39, No. 1, 2004, pp. 19-29. (RW 4275)

Schommer-Aikins, M. "Applying the Theory of an Epistemological Belief System to the Investigation of Students' and Professors' Mathematical Beliefs," in *Knowing, Knowledge and Beliefs: Epistemological Studies Across Diverse Cultures,* ed. M.S. Khine, Springer, Dordrecht, 2008, pp. 303-323. (RW 4354)

Schommer-Aikins, M., Bird, M. & Bakken, L. "Manifestations of an Epistemological Belief System in Preschool to Grade Twelve Classrooms," in *Personal Epistemology in the Classroom:*

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Theory, Research, and Implications for Practice, eds. L.D. Bendixen & F.C. Feucht, Cambridge University Press, Cambridge, UK, 2010, pp. 31-54. (RW 5099)

Schommer-Aikins, M., Duell, O.K. & Hutter, R. "Epistemological Beliefs, Mathematical Problem-Solving Beliefs, and Academic Performance of Middle School Students," *Elementary School Journal,* Vol. 105, No. 3, 2005, pp. 289-304. (RW 4916)

Schommer-Aikins, M. & Easter, M. "Epistemological Beliefs' Contributions to Study Strategies of Asian Americans and European Americans," *Journal of Educational Psychology,* Vol. 100, No. 4, 2008, pp. 920-929. (RW 4917)

Schonfeld, E. *Keyword Search about to Hit its Breaking Point?* (RW 3080)

Schooler, J.W., Fallshore, M. & Fiore, S.M. "Epilogue: Putting Insight into Perspective," in *The Nature of Insight*, eds. R.J. Sternberg & J.E. Davidson, MIT Press, Cambridge, Mass, 1995, pp. 559. (RW 1949)

Schraagen, J.M. "How Experts Solve a Novel Problem in Experimental Design," *Cognitive Science,* Vol. 17, No. 2, 1993, pp. 285-309. (RW 1938)

Schraagen, J.M. "Designing Training for Professionals Based on Subject Matter Experts and Cognitive Task Analysis," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 157-179. (RW 5140)

Schraefel, M.C. "Building Knowledge: What's Beyond Keyword Search," *Computer,* Vol. 42, No. 3, 2009, pp. 52. (RW 3441)

Schrag, R.C., Pastor, J., Long, C., Peterson, E., Cornwell, M., Forbes, L.A. & Cannon, S. "Contributions to a Semantically Based Intelligence Analysis Enterprise Workflow System", *Ontology for the Intelligence Community,* Fairfax, VA, 20-22 October 2009 (RW 4751)

Schrage, M. "What Percent is 'Slam Dunk'?: Give Us Odds on those Estimates," *Washington Post*, February 20, 2005, pp. B01. (RW 1681)

Schrage, M. "Process Pantomime," *CIO Magazine,* 2006 (RW 1643)

Schraw, G. "The Effect of Metacognitive Knowledge on Local and Global Monitoring," *Contemporary Educational Psychology,* Vol. 19, 1994, pp. 143. (RW 3768)

Schraw, G., Dunkle, M.E. & Bendixen, L.D. "Cognitive Processes in Well-Defined and Ill-Defined Problem Solving," *Applied Cognitive Psychology*, Vol. 9, 1995, pp. 523-528. (RW 5347)

Schraw, G. & Lehman, S. "Situational Interest: A Review of the Literature and Directions for Future Research," *Educational Psychology Review,* Vol. 13, No. 1, 2001, pp. 23-52. (RW 4606)

Schraw, G. & Olafson, L. "Teachers' Epistemological World View and Educational Practice," *Issues in Education,* Vol. 8, No. 2, 2002, pp. 99-148. (RW 4610)

Schraw, G. "Knowledge: Structures and Processes," in *Handbook of Educational Psychology*, eds. P.A. Alexander & P.H. Winne, 2nd ed., L. Erlbaum Associates, Mahwah, NJ, 2006, pp. 245. (RW 3798)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Schraw, G., Bendixen, L.D. & Dunkle, M.E. "Development and Validation of the Epistemic Belief Inventory (EBI)," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing*, eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 261. (RW 3984)

Schraw, G. & Bruning, R. "How Implicit Models of Reading Affect Motivation to Read and Reading Engagement," *Scientific Studies of Reading*, Vol. 3, No. 3, 1999, pp. 281. (RW 5196)

Schraw, G. & Olafson, L. "Teachers' Epistemological World Views and Educational Practices," Vol. 3, No. 2, 2003, pp. 178-235. (RW 5346)

Schraw, G. & Sinatra, G.M. *Epistemological Development and its Impact on Cognition in Academic Domains* 2004. (RW 5114)

Schreckengost, R.C. "Some Limitations in Systems Analysis in Intelligence Activities," *Studies in Intelligence*, Vol. 14, No. 2, 1970, pp. 79-86. (RW 4209)

Schreiber, B.T., Bennett, W., Colegrove, C.M., Portrey, A.M., Greschke, D.A. & Bell, H.H. "Evaluating Pilot Performance," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 247-270. (RW 5144)

Schroeder, S., Richter, T. & Hoever, I. "Getting a Picture that is both Accurate and Stable: Situation Models and Epistemic Validation," *Journal of Memory and Language*, Vol. 59, No. 3, 2008, pp. 237-259. (RW 5331)

Schrunk, D.L. "Metacognition, Self-Regulation, and Self-Regulated Learning: Research Recommendations," *Educational Psychology Review*, Vol. 20, 2008, pp. 463-467. (RW 5051)

Schulman, A.N. "Why Minds are Not Like Computers," *The New Atlantis*, 23, 2009, pp. 46. (RW 3468)

Schulz, K. *Being Wrong: Adventures in the Margin of Error*, HarperCollins, New York, NY, 2010. (RW 4085)

Schulz-Hardt, S., Frey, D., Luethgens, C. & Moscovici, S. "Biased Information Search in Group Decision Making," *Journal of Personality and Social Psychology*, Vol. 78, No. 4, 2000, pp. 655-668. (RW 1927)

Schum, D.A. "Inference Networks and their Many Subtle Properties," *Information and Decision Technologies*, Vol. 16, No. 1, 1990, pp. 69-98. (RW 5280)

Schum, D.A. "Inference Networks and the Evaluation of Evidence: Alternative Analyses", *15th Conference on Uncertainty in Artificial Intelligence*, Stockholm, Sweden, July 30 - August 1, 1999, pp. 575-584. (RW 5296)

Schum, D.A. & Morris, J.R. "Assessing the Competence and Credibility of Human Sources of Intelligence Evidence: Contributions from Law and Probability," *Law, Probability, & Risk*, Vol. 6, No. 1-4, 2007, pp. 247. (RW 3276)

Schum, D. *A Reply to the "Schum Challenge" at UCL* 2005. (RW 2983)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Schum, D. *Modern Studies of Assessing the Competence and Credibility of Human Sources of Evidence. Abstract of Talk.* 2007. (RW 1995)

Schum, D. *Modern Studies of Assessing the Competence and Credibility of Human Sources of Evidence [Powerpoint Presentation]* 2007. (RW 1994)

Schum, D. "Classifying Forms and Combinations of Evidence: Necessary in a Science of Evidence," in *Evidence, Inference and Enquiry*, eds. P. Dawid, W. Twining & M. Vasilaki, 2011, pp. 11-36. (RW 5628)

Schum, D.A. *Evidence and Inference for the Intelligence Analyst. Volume 1,* University Press of America, Lanham, MD, 1987. (RW 950)

Schum, D.A. *Evidence and Inference for the Intelligence Analyst. Volume 2,* University Press of America, Lanham, MD, 1987. (RW 3868)

Schum, D.A. "Knowledge, Probability, and Credibility," *Journal of Behavioral Decision Making,* Vol. 2, No. 1, 1989, pp. 39-62. (RW 965)

Schum, D.A. "Marshaling Thoughts and Evidence during Fact Investigation," *South Texas Law Review,* Vol. 40, No. 2, 1999, pp. 401-454. (RW 1247)

Schum, D.A. "Probabilistic Reasoining and the Science of Complexity," in *Decision Science and Technology: Reflections on the Contributions of Ward Edwards*, eds. W. Edwards, J. Shanteau, B.A. Mellers & D.A. Schum, Klumer Academic, Boston, MA, 1999, pp. 183-209. (RW 5278)

Schum, D.A. *The Evidential Foundations of Probabilistic Reasoning,* Northwestern University Press, Evanston, IL, 2001. (RW 1363)

Schum, D.A. *Contextual and Related Issues in Discovery, Inference, and Choice: Their Bearing on Intelligence Analysis* 2005. (RW 1642)

Schum, D.A. *Narratives in Intelligence Analysis: Necessary but often Dangerous,* George Mason University, Fairfax, VA, 2005. (RW 1632)

Schum, D.A. *Thoughts about a Science of Evidence* 2005. (RW 1633)

Schum, D.A. *Notes on Discovery and Imaginative Reasoning (Class Notes)* 2006. (RW 1734)

Schum, D.A. *Syllabus for IT 944. the Process of Discovery and its Enhancement in Engineering Applications.* 2006. (RW 1733)

Schum, D.A. *Lessons and Stories about Concepts Encountered in Disciple-LTA,* Research Report 2, George Mason University, Fairfax, VA, 2007. (RW 4757)

Schum, D.A., Anderson, W.D. & Morris, J.R. "Cognitive Factors, Part III: A Catalogue of Way to Assess and Report Uncertainty," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 81. (RW 3643)

Schum, D.A., Goldstein, I.L. & Southard, J.F. *The Influence of Experience and Input Information Fidelity upon Posterior Probability Estimation in a Simulated Threat-Diagnosis System,* AMRL TR 65-25, Aerospace Medical Research Laboratories, Wright-Patterson Air Force Base, OH, 1965. (RW 961)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Schum, D.A. & Morris, J.R. *Assessing the Competence and Credibility of Human Sources of Intelligence Evidence: Contributions from Law and Probability* 2007. (RW 3031)

Schum, D.A., Tecuci, G. & Boicu, M. "Analyzing Evidence and its Chain of Custody: A Mixed-Initiative Computational Approach," *International Journal of Intelligence and Counterintelligence,* Vol. 22, No. 2, 2009, pp. 298. (RW 3586)

Schum, D., Tecuci, G., Boicu, M. & Marcu, D. "Substance-Blind Classification of Evidence for Intelligence Analysis", *Ontology for the Intelligence Community*, Fairfax, VA, 20-22 October 2009 (RW 4750)

Schum, D. & Tillers, P. *A Technical Note on Computer-Assisted Wigmorean Argument Structuring,* TR56, 1990. (RW 1362)

Schumacher, G.M. & Nash, J.G. "Conceptualizing and Measuring Knowledge Change due to Writing," *Research in the Teaching of English,* Vol. 25, No. 1, 1991, pp. 67. (RW 2011)

Schunk, D.H., Pintrich, P.R. & Meece, J.L. *Motivation in Education: Theory, Research and Applications,* 3rd ed., Pearson/Merrill Prentice Hall, Upper Saddle River, NJ, 2008. (RW 5531)

Schunk, D.H. & Zimmerman, B.J. *Self-Regulated Learning: From Teaching to Self- Reflective Practice,* Guilford Press, New York, NY, 1998. (RW 4675)

Schunk, D.H. & Zimmerman, B.J. "Competence and Control Beliefs: Distinguishing the Means and Ends," in *Handbook of Educational Psychology*, eds. P.A. Alexander & P.H. Winne, 2nd ed., L. Erlbaum Associates, Mahwah, NJ, 2006, pp. 249-367. (RW 5048)

Schunn, C.D. & Anderson, J.R. "The generality/specificity of Expertise in Scientific Reasoning," *Cognitive Science,* Vol. 23, No. 3, 1999, pp. 337. (RW 2326)

Schunn, C.D. & Dunbar, K. *Priming, Analogy, and Awareness in Complex Reasoning* (RW 1810)

Schunn, C.D. & Klahr, D. "Self vs. Other-Generated Hypotheses in Scientific Discovery", *Proceedings of the 15th Annual Conference of the Cognitive Science Society,* June 18-21, 1993, pp. 900. (RW 1996)

Schunn, C. & Anderson, J. "Acquiring Expertise in Science: Explorations of what, when, and how," in *Designing for Science: Implications from Everyday, Classroom, and Professional Settings*, eds. K.D. Crowley, C.D. Schunn & T. Okada, 2001, pp. 83. (RW 3940)

Schustack, M. & Sternberg, R.J. "Evaluation of Evidence in Causal Inference," *Journal of Experimental Psychology: General,* Vol. 110, No. 1, 1981, pp. 101. (RW 2187)

Schuwirth, L. "Can Clinical Reasoning be Taught or can it Only be Learned?" *Medical Education,* Vol. 36, 2002, pp. 695. (RW 2617)

Schwalbe, S.R. *Scientific and Technical Intelligence for the Operational Commander*, College of Naval Warfare, Newport, RI, 1998. (RW 1181)

Schwartz, D.D. *Conjecture & Proof: An Introduction to Mathematical Thinking,* Saunders College Pub., Fort Worth, TX, 1997. (RW 3309)

Schwartz, P. *The Art of the Long View*, Doubleday/Currency, New York, NY, 1991. (RW 25)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Schwartz, P. & Randall, D. "Ahead of the Curve: Anticipating Strategic Surprise," in *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics*, ed. F. Fukuyama, Brookings Institution Press, Washington, DC, 2007, pp. 93-108. (RW 4699)

Schwartz, P., Webb, G. & Mennin, S. *Problem-Based Learning: Case Studies, Experience and Practice*, Kogan Page, London, 2001. (RW 4879)

Schwarz, F.A.O. "The Church Committee and a New Era of Intelligence Oversight," *Intelligence and National Security*, Vol. 22, No. 2, 2007, pp. 270. (RW 2399)

Schwarz, N., Sanna, L.J., Skurnik, I. & Yoon, C. *Advances in Experimental Social Psychology*, Vol. 39, 2007, pp. 127. (RW 2793)

Schweitzer, N. "Bayesian Analysis for Intelligence: Some Focus on the Middle East," *Studies in Intelligence,* Vol. 20, No. 2, 1976, pp. 31-44. (RW 4174)

Schweitzer, N. "Bayesian Analysis: Estimating the Probability of Middle East Conflict," in *Quantitative Approaches to Political Intelligence: The CIA Experience,* ed. R.J.J. Heuer, Westview Press, Boulder, CO, 1978, pp. 11-30. (RW 913)

Scott, J.N., Markert, R.J. & Dunn, M.M. "Critical Thinking: Change during Medical School and Relationship to Performance in Clinical Clerkships," *Medical Education,* Vol. 13, No. 1, 1998, pp. 14-18. (RW 4039)

Scott, L.V. & Jackson, P. *Understanding Intelligence in the Twenty-First Century: Journeys in Shadows*, Routledge, London, UK, 2004. (RW 1193)

Scott, L. "Sources and Methods in the Study of Intelligence: A British View," *Intelligence and National Security*, Vol. 22, No. 2, 2007, pp. 185. (RW 2398)

Scott, L. "Reflections on the Age of Intelligence," *Intelligence and National Security,* Vol. 27, No. 5, 2012, pp. 617-624. (RW 5837)

Scott, L. & Hughes, R.G. "Intelligence, Crises and Security: Lessons from History?" *Intelligence and National Security*, Vol. 21, No. 5, 2006, pp. 653. (RW 2088)

Scott, L. & Hughes, R.G. "Intelligence in the Twenty-First Century: Change and Continuity or Crisis and Transformation?" *Intelligence and National Security,* Vol. 24, No. 1, 2009, pp. 6. (RW 3449)

Scott, L. & Jackson, P. "The Study of Intelligence in Theory and Practice," *Intelligence and National Security*, Vol. 19, No. 2, 2004, pp. 139-169. (RW 463)

Scott-Lee, P., Martin, E. & Shipman, A. "Performance Versus Intelligence: The Unintended Consequences," in *The Handbook of Intelligent Policing: Consilience, Crime Control, and Community Safety*, ed. C. Harfield, Oxford University Press, Oxford, UK, 2008, pp. 289-302. (RW 5775)

Scriven, M. & Paul, R. *Defining Critical Thinking*, Foundation for Critical Thinking. Available: http://www.criticalthinking.org/page.cfm?PageID=410&CategoryID=51, Viewed: March 16, 2010. (RW 3949)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Seabury, P. "Analysis. Essay," in *Intelligence Requirements for the 1990s: Collection, Analysis, Counterintelligence, and Covert Action*, ed. R. Godson, Lexington Books, Lexington, MA, 1989, pp. 97-110. (RW 154)

Searle, J.R. "Minding the Brain," *New York Review of Books,* Vol. 53, No. 17, 2006 (RW 1712)

Sears, D.O., Huddy, L. & Jervis, R. *Oxford Handbook of Political Psychology,* Oxford University Press, New York, 2003. (RW 3588)

Sebanz, N. "It Takes Two to..." *Scientific American Mind,* Vol. 17, No. 6, 2006, pp. 52. (RW 3148)

Sebastiani, F. "Classification of Text, Automatic," in *Encyclopedia of Language & Linguistics*, ed. K. Brown, 2nd ed., 2006, pp. 457-462. (RW 5221)

Sechser, T.S. "Summary", *Intelligence and Prediction in an Unpredictable World,* Stanford, CA, June 20-21, 2003 (RW 586)

Secretary of the Air Force. *Air Force Instruction 14-202. Volume 3. Intelligence. General Intelligence Rules.* 2008. (RW 3025)

Sedikides, C. & Strube, M.J. "Self-Evaluation: To Thine Own Self be Good, to Thine Own Self be Sure, to Thine Own Self be True, to Thine Own Self be Better," *Advances in Experimental Social Psychology,* Vol. 29, 1997, pp. 209-269. (RW 5237)

Segall, R. "The Intelligence Community: Resolving Conflicts between Agencies for National Security," *American Intelligence Journal,* Vol. 28, No. 1, 2010, pp. 67-77. (RW 4473)

Segell, G.M. "Intelligence Methodologies Applicable to the Madrid Train Bombings, 2004," *International Journal of Intelligence and Counterintelligence,* Vol. 18, No. 2, 2004, pp. 221. (RW 1682)

Seidel, W.E. "Intelligence for Defense Planning," *Studies in Intelligence,* Vol. 8, No. 2, 1964 (RW 535)

Seifert, J.W. *Data Mining and Homeland Security: An Overview* 2007. (RW 2169)

Seliktar, O. & Dutter, L.E. "Assessing the Rationality of Autocrats: The Case of Saddam Hussein," *International Journal of Intelligence and Counterintelligence,* Vol. 22, No. 2, 2009, pp. 275. (RW 3587)

Sen, B.A. "Reflective Writing: A Management Skill," *Library Management,* Vol. 21, No. 1/2, 2010, pp. 79-93. (RW 4793)

Senate Select Committee on Intelligence. *Report of the Select Committee on Intelligence on Prewar Intelligence Assessments about Postwar Iraq* (RW 2391)

Senator, T. "Evidence Extraction and Link Discovery Program [Powerpoint Presentation]", *DARPATech 2002 Symposium,* Anaheim, CA, July 29 - August 2, 2002 (RW 3381)

Senator, T. "Evidence Extraction and Link Discovery Program. Script for Powerpoint Presentation.", *DARPATech 2002 Symposium,* Anaheim, CA, July 29 - August 2, 2002 (RW 3382)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Senge, P.M. & Society for Organizational Learning *Presence: Exploring Profound Change in People, Organizations, and Society*, Doubleday, New York, 2005. (RW 3273)

Serban, M. "Data Analysis: An Important Step in the Process of Development of Economic Intelligence Products," *International Journal of Sustainable Economies Management*, Vol. 1, No. 2, 2012, pp. 33-42. (RW 5624)

Sfard, A. "Reconceptualizing Conceptual Change," in *Re-Framing the Conceptual Change Approach in Learning and Instruction*, eds. S. Vosniadou, A. Baltas & X. Vamvakoussi, Elsevier, Amsterdam, 2007, pp. 329-334. (RW 5011)

Shadish, W.R., Chacon-Moscoso, S. & Sanchez-Meca, J. "Evidence-Based Decision Making: Enhancing Systematic Reviews of Program Evaluation Results in Europe," *Evaluation*, Vol. 11, No. 1, 2005, pp. 95. (RW 2229)

Shadrick, S.B. & Lussier, J.W. "Training Complex Cognitive Skills: A Theme-Based Approach to the Development of Battlefield Skills," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 286-311. (RW 5146)

Shaffer, J.P. "Multiple Hypothesis Testing," *Annual Review of Psychology*, Vol. 46, 1995, pp. 561. (RW 1960)

Shafir, E., Simonson, I. & Tversky, A. "Reason-Based Choice," *Cognition*, Vol. 49, 1993, pp. 11. (RW 1977)

Shafto, P. & Coley, J.D. "Development of Categorization and Reasoning in the Natural World: Novices to Experts, Naive Similarity to Ecological Knowledge," *Journal of Experimental Psychology: Learning, Memory, & Cognition*, Vol. 29, No. 4, 2003, pp. 641-649. (RW 1939)

Shahaf, D. & Guestrin, C. "Connecting the Dots between News Articles", *KDD '10: Proceedings of the 16th ACM SIGKDD International Conference on Knowledge Discovery and Data Mining*, July 2010, pp. 623-632. (RW 5582)

Shai, O. & Reich, Y. "Infused Design. I. Theory," *Research in Engineering Design*, Vol. 15, 2004, pp. 93. (RW 2628)

Shaker, S.M. & Leary, A.E. "War Room Team-Based Analysis", *2003 Command and Control Research and Technology Symposium*, June 17-19, 2003 (RW 1606)

Shanahan, T. "Research Synthesis: Making Sense of the Accumulation of Knowledge in Reading," in *Handbook of Reading Research: Volume III*, ed. M.L. Kamil, L. Erlbaum Associates, Mahwah, NJ, 2000, pp. 209. (RW 3821)

Shane, S. "How Intelligence Fails More Often than Not," *Baltimore Sun*, February 8, 2004, pp. 1C. (RW 226)

Shanks, M. & Tilley, C.Y. *Re-Constructing Archaeology: Theory and Practice*, Cambridge University Press, Cambridge, UK, 1987. (RW 2782)

Shanks, M. & Tilley, C.Y. *Re-Constructing Archaeology: Theory and Practice*, 2nd ed., Routledge, London, 1992. (RW 2783)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Shanteau, J. "How Much Information Does an Expert Use? Is it Relevant?" *Acta Psychologica,* Vol. 81, 1992, pp. 75. (RW 1334)

Shanteau, J. "What Does it Mean when Experts Disagree?" in *Linking Expertise and Naturalistic Decision Making*, eds. E. Salas & G.A. Klein, L. Erlbaum Associates, Mahwah, NJ, 2001, pp. 229-244. (RW 162)

Shapiro, M.J., Bonham, G.M. & Hevadsveit, D. "A Discursive Practices Approach to Collective Decision-Making," *International Studies Quarterly*, Vol. 32, No. 4, 1988, pp. 397-419. (RW 4511)

Shapiro, R.Y. & Jacobs, L.R. *The Oxford Handbook of American Public Opinion and the Media*, Oxford University Press, Oxford, UK, 2011. (RW 5448)

Sharfman, D. & Kahana, E. "Combating Terrorism with Intelligence: The Normative Debate in Israel," *International Journal of Intelligence and Counterintelligence*, Vol. 25, No. 3, 2012, pp. 546-570. (RW 5729)

Sharfman, P. "Intelligence Analysis in an Age of Electronic Dissemination," *Intelligence and National Security*, Vol. 10, No. 5, 1995, pp. 201-211. (RW 128)

Sharma, A. "SWOT Analysis," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 125-130. (RW 3618)

Sharot, T., Riccardi, A.M., Raio, C.M. & Phelps, E.A. "Neural Mechanisms Mediating Optimism Bias," *Nature*, Vol. 450, 2007, pp. 102. (RW 2863)

Sharples, M. "An Account of Writing as Creative Design," in *The Science of Writing: Theories, Methods, Individual Differences, and Applications*, eds. C.M. Levy & S.E. Ransdell, L. Erlbaum Associates, Mahwah, NJ, 1996, pp. 127-148. (RW 1823)

Shea, C. "Empty-Stomach Intelligence," *New York Times*, December 10, 2006 (RW 1769)

Shea, J.R. "Winnowing Wheat from Chaff," *Studies in Intelligence*, Vol. 13, No. 4, 1969, pp. 19-23. (RW 4210)

Shearman, S.M. & Levine, T.R. "Dogmatism Updated: A Scale Revision and Validation," *Communication Quarterly*, Vol. 54, No. 3, 2006, pp. 275-291. (RW 5384)

Shedlock, D.J. & Cornelius, S.W. "Psychological Approaches to Wisdom and its Development," in *Handbook of Adult Development*, eds. J. Demick & C. Andreoletti, Kluwer Academic/Plenum, New York, 2003, pp. 153. (RW 4327)

Sheehan, J.J. *Planning Information Operations for a Changing World*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1999. (RW 1037)

Shelby, R.C. *September 11 and the Imperative of Reform in the U.S. Intelligence Community. Additional Views of Senator Richard C. Shelby Vice Chairman, Senate Select Committee on Intelligence* 2002. (RW 577)

Shelton, A.M. "Framing the Oxymoron: A New Paradigm for Intelligence Ethics," *Intelligence and National Security*, Vol. 26, No. 1, 2011, pp. 23-45. (RW 4728)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Shelton, C. "The Roots of Analytic Failure in the U.S. Intelligence Community," *International Journal of Intelligence and Counterintelligence,* Vol. 24, No. 4, 2011, pp. 637-655. (RW 5398)

Shema, H. *What's Wrong with Citation Analysis?* Available: http://blogs.scientificamerican.com/information-culture/2013/01/01/whats-wrong-with-citation-analysis/, Viewed: January 7, 2013. (RW 5890)

Sheptycki, J. "Policing, Intelligence Theory and the New Human Security Paradigm: Some Lessons from the Field," in *Intelligence Theory: Key Questions and Debates,* eds. P. Gill, S. Marrin & M. Phythian, 2009, pp. 166. (RW 3411)

Sherman, C. & Price, G. "The Invisible Web: Uncovering Sources Search Engines Can't See," *Library Trends,* Vol. 52, No. 2, 2003, pp. 282. (RW 1418)

Sherman, L.W. *Misleading Evidence and Evidence-Led Policy: Making Social Science More Experimental,* Sage Publications, Thousand Oaks, CA, 2003. (RW 2231)

Shermer, M. *Why People Believe Weird Things,* St. Martin's Griffin, New York, NY, 2002. (RW 5740)

Shermer, M. "I Want to Believe," *Scientific American,* Vol. 301, No. 1, 2009, pp. 33-35. (RW 5119)

Shermer, M. *The Believing Brain: From Ghosts and Gods to Politics and Conspiracies--How We Construct Beliefs and Reinforce them as Truths,* Times Books, New York, NY, 2011. (RW 4931)

Shestakov, D., Bhowmick, S.S. & Lim, E. "DEQUE: Querying the Deep Web," *Data & Knowledge Engineering,* Vol. 52, 2005, pp. 273. (RW 1401)

Shilliday, A., Taylor, J., Bringsjord, S. & Arkoudas, K. "Toward Automated Provability-Based Semantic Interoperability between Ontologies for the Intelligence Community", *Proceedings of the Second International Ontology for the Intelligence Community Conference OIC-2007,* Columbia, MD, November 28-29, 2007, pp. 67-72. (RW 4822)

Shirky, C. *Here Comes Everybody: The Power of Organizing without Organizations,* Penguin Press, New York, NY, 2008. (RW 3992)

Shirky, C. *Cognitive Surplus: Creativity and Generosity in a Connected Age,* Penguin Press, New York, NY, 2010. (RW 4679)

Shirley, E.G. "CIA Needs Reform, Not New Missions," *Wall Street Journal,* November 19, 1998, pp. 22. (RW 1372)

Shlaim, A. *Failures in National Intelligence Estimates: The Case of the Yom Kippur War* 1976. (RW 1286)

Shlykov, V. "Fatal Mistakes of the US and Soviet Intelligence: Part One," *International Affairs,* Vol. 43, No. 3, 1997, pp. 159-177. (RW 144)

Shneiderman, B. "Creativity Support Tools: Accelerating Discovery and Innovation," *Communications of the ACM,* Vol. 50, No. 12, 2007, pp. 20. (RW 4395)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Shneiderman, B. & Plaisant, C. "Strategies for Evaluating Information Visualization Tools: Multi-Dimensional in-Depth Long-Term Case Studies", *Beliv '06,* Venice, Italy, May 23, 2006, pp. 1-7. (RW 5691)

Shoham, D. & Ofek, R. "The 2007 U.S. NIE on Iran's Nuclear Program: A Colossal Failure," *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 2, 2012, pp. 292-329. (RW 5617)

Sholander, J. *Whither Iraqi Democracy: An Analysis of Competing Hypotheses (ACH) Study on the Nature and Direction of Iraqi Politics,* M.A. thesis, American Public University System, 2012. (RW 5762)

Shorrock, T. *Spies for Hire,* 2008. (RW 3119)

Shrager, J., Massar, J.P., Billman, D., Convertino, G. & Pirolli, P. *Multistage Collaboration in CACHE: The Bayes Community Model* 2006. (RW 2936)

Shreeve, T.W. "The Intelligence Community Case Method Program: A National Intelligence Estimate on Yugoslavia," in *Intelligence and the National Security Strategist: Enduring Issues and Challenges,* eds. R.Z. George & R.D. Kline, National Defense University Press, Washington, DC, 2004, pp. 327-340. (RW 695)

Shreeve, T.W. & Dowd, J.J. "Building a Learning Organization: Teaching with Cases at CIA," *International Journal of Intelligence and Counterintelligence,* Vol. 10, No. 1, 1997, pp. 97-107. (RW 32)

Shucha, B. "Searching Smarter: Finding Legal Resources on the Invisible Web," *The Colorado Lawyer,* Vol. 34, 2005, pp. 37-39. (RW 1406)

Shugan, S.M. "Defining Interesting Research Problems," *Marketing Science,* Vol. 22, No. 1, 2003, pp. 1. (RW 2629)

Shulman, L.S. "Those Who Understand: Knowledge Growth in Teaching," *Educational Researcher,* Vol. 15, No. 2, 1986, pp. 4-14. (RW 4570)

Shulman, L.S. "The Wisdom of Practice: Managing Complexity in Medicine and Teaching," in *Talks to Teachers: A Festschrift for N.L. Gage,* eds. N.L. Gage, D.C. Berliner & B. Rosenshine, Random House, New York, 1987, pp. 369. (RW 4423)

Shulsky, A. "What is Intelligence? Secrets and Competition among States," in *U.S. Intelligence at the Crossroads: Agendas for Reform,* eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 18-26. (RW 685)

Shulsky, A. "Elements of Strategic Denial and Deception," *Trends in Organized Crime,* Vol. 6, No. 1, 2000, pp. 17-31. (RW 607)

Shulsky, A.N. *Silent Warfare: Understanding the World of Intelligence,* Brassey's US, Washington, DC, 1991. (RW 110)

Shulsky, A.N. & Schmitt, G.J. *Silent Warfare: Understanding the World of Intelligence,* 2nd ed., Brassey's US, Washington, DC, 1993. (RW 27)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Shulsky, A.N. & Sims, J. *What is Intelligence? with Discussion. Working Group on Intelligence Reform.* Consortium for the Study of Intelligence, Washington, DC, 1992. (RW 78)

Shulsky, A. & Schmitt, G. "Intelligence Reform: Beyond the Ames Case," in *U.S. Intelligence at the Crossroads: Agendas for Reform*, eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 46-59. (RW 641)

Si, L. & Callan, J. *Distributed Information Retrieval: The Tool to Probe the Invisible Web Contents [Powerpoint Presentation]* 2003. (RW 1402)

Sickels, S.J. *Collaboration and Analyst System Effectiveness (CASE) Connect*, AFRL-RI-RS-TR-2009-68, Air Force Research Laboratory, Rome, NY, 2009. (RW 4875)

Sieck, W.R. & Arkes, H.R. "The Recalcitrance of Overconfidence and its Contribution to Decision Aid Neglect," *Journal of Behavioral Decision Making*, Vol. 18, No. 1, 2005, pp. 29. (RW 1964)

Sieck, W.R., Klein, G., Peluso, D.A., Smith, J.L. & Harris-Thompson, D. *FOCUS: A Model of Sensemaking*, US Army Research Institute for the Behavioral and Social Sciences Technical Report 1200, 2007. (RW 2716)

Siegel, E. *Predictive Analytics: The Power to Predict Who Will Click, Buy, Lie, Or Die*, John Wiley & Sons, New York, NY, 2013. (RW 5903)

Siegel, H. *Educating Reason: Rationality, Critical Thinking, and Education*, Routledge, New York, NY, 1988. (RW 3702)

Siegel, H. "Not by Skill Alone: The Centrality of Character to Critical Thinking," *Informal Logic*, Vol. 15, No. 3, 1993, pp. 163-177. (RW 3844)

Siegel, J. "Be the Extremist," *Bulletin of the Atomic Scientists*, Vol. 61, No. 5, 2005, pp. 71. (RW 1303)

Siegel, N., Shepard, B., Cabral, J. & Witbrock, M. "Hypothesis Generation and Evidence Assembly for Intelligence Analysis: Cycorp's Nooscape Application," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 847)

Silberman, M.L. *The Handbook of Experiential Learning*, Pfeiffer, San Francisco, CA, 2007. (RW 4885)

Siljee, B.I.J., Bosloper, I.E. & Nijhuis, J.A.G. "A Classification Framework for Storage and Retrieval of Context", *Proceedings of the KI-04 Workshop on Modeling and Retrieval of Context*, Ulm, September 20-21, 2004 (RW 4868)

Silver, N. *The Signal and the Noise: Why so Many Predictions Fail - But Some Don't*, Penguin Press, New York, NY, 2012. (RW 5811)

Silver, N. "The Weatherman is not a Moron," *New York Times Magazine*, [Online]. Available from: http://www.nytimes.com/2012/09/09/magazine/the-weatherman-is-not-a-moron.html?ref=magazine, 2012. (RW 5810)

Silverman, B.G., Rees, R.L., Toth, J.A., Cornwell, J., O'Brien, K., Johns, M. & Caplan, M. "Athena's Prism—A Diplomatic Strategy Role Playing Simulation for Generating Ideas and

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Exploring Alternatives," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 822)

Silverman, D. *Doing Qualitative Research: A Practical Handbook,* 2nd ed., Sage, London, 2005. (RW 3153)

Silverman, D. *Interpreting Qualitative Data: Methods for Analyzing Talk, Text, and Interaction,* 3rd ed., SAGE Publications, Thousand Oaks, CA, 2006. (RW 2696)

Silverman, J.C. "Epistemological Beliefs and Attitudes Toward Inclusion in Pre-Service Teachers," *Teacher Education and Special Education: the journal of the Teacher Education Division of the Council for Exceptional Children,* Vol. 30, No. 1, 2007, pp. 42-51. (RW 4900)

Simon, D., Snow, C.J. & Read, S.J. "The Redux of Cognitive Consistency Theories: Evidence Judgments by Constraint Satisfaction," *Journal of Personality and Social Psychology,* Vol. 86, No. 6, 2004, pp. 814-837. (RW 5294)

Simon, H.A. "The Structure of Ill-Structured Problems," *Artificial Intelligence,* Vol. 4, 1973, pp. 181. (RW 2772)

Simon, H.A. "Human Nature in Politics: The Dialogue of Psychology with Political Science," *American Political Science Review,* Vol. 79, No. 2, 1985, pp. 293. (RW 2335)

Simon, H.A. ""Seek and Ye Shall Find": How Curiosity Engenders Discovery," in *Designing for Science: Implications from Everyday, Classroom, and Professional Settings,* eds. K.D. Crowley, C.D. Schunn & T. Okada, 2001, pp. 5. (RW 1875)

Simon, J.M. *Analysis, Analysts, and their Role in Government and Intelligence,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2003. (RW 269)

Simon, J.M., Jr. *Crucified on a Cross of Goldwater-Nichols,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2001. (RW 1150)

Simon, J.M., Jr. *Analysis, Analysts, and their Role in Government and Intelligence,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2003. (RW 1151)

Simon, J.L. *Basic Research Methods in Social Science: The Art of Empirical Investigation,* Random House, New York, 1969. (RW 3209)

Simpson, G.G. "Historical Science," in *the Fabric of Geology,* ed. C.C.J. Albritton, Freeman, Cooper and Co., Stanford, CA, 1963, pp. 24-48. (RW 5375)

Simpson, M.L. & Nist, S.L. "An Update on Strategic Learning: It's More than Textbook Reading Strategies," *Journal of Adolescent and Adult Literacy,* Vol. 43, No. 6, 2000, pp. 528-541. (RW 4642)

Sims, J. "What is Intelligence? Information for Decision Makers," in *U.S. Intelligence at the Crossroads: Agendas for Reform,* eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 3-16. (RW 684)

Sims, J. "Intelligence to Counter Terror: The Importance of all-Source Fusion," *Intelligence and National Security,* Vol. 22, No. 1, 2007, pp. 38. (RW 2381)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Sims, J. "Intelligence to Counter Terror: The Importance of all-Source Fusion," in *Strategic Intelligence. Volume 4: Counterintelligence and Counterterrorism: Defending the Nation Against Hostile Forces*, ed. L.K. Johnson, Praeger Security International, Westport, CT, 2007, pp. 139. (RW 2703)

Sims, J. "Defending Adaptive Realism: Intelligence Theory Comes of Age," in *Intelligence Theory: Key Questions and Debates*, eds. P. Gill, S. Marrin & M. Phythian, 2009, pp. 151. (RW 3410)

Sims, J.E. "The Nature of Intelligence Analysis," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, CENTRA Technology, Burlington, MA, [in press], pp. 1-19. (RW 3640)

Sims, J.E. "The Domestic Politics of US Intelligence Policy (Understanding Ourselves)", *International Studies Association,* [undated]. (RW 2924)

Sims, J.E. "Decision Advantage and the Nature of Intelligence Analysis," in *Oxford Handbook of National Security Intelligence*, ed. L.K. Johnson, Oxford University Press, Oxford, UK, 2010, pp. 389-403. (RW 4710)

Sims, J.E. & Gerber, B.L. *Transforming U.S. Intelligence,* Georgetown University Press, Washington, DC, 2005. (RW 771)

Sims, J.E. & Gerber, B.L. *Vaults, Mirrors, and Masks: Rediscovering U.S. Counterintelligence,* Georgetown University Press, Washington, DC, 2009. (RW 4601)

Sinatra, G.M., Brem, S.K. & Evans, E.M. "Changing Minds? Implications of Conceptual Change for Teaching and Learning about Biological Evolution." *Evolution Education and Outreach,* Vol. 1, No. 2, 2008, pp. 189-195. (RW 4940)

Sinatra, G.M., Reynolds, R.E. & Jacobson, T. "Knowledge and Beliefs: Empirical Investigation of Conceptual Differences," [in preparation] (RW 5822)

Sinatra, G.M. & Southerland, S.A. "A Little Knowledge is a Dangerous Thing: Using Beliefs and Dispositions to make Judgments about the Validity of Scientific Theories," *Research in Science Education,* [in press] (RW 5109)

Sinatra, G.M. "Knowledge, Beliefs, and Learning," *Educational Psychology Review,* Vol. 13, No. 4, 2001, pp. 321. (RW 4283)

Sinatra, G.M. "Motivational, Social, and Contextual Aspects of Conceptual Change: A Commentary," in *Reconsidering Conceptual Change: Issues in Theory and Practice*, eds. M. Limón & L. Mason, Kluwer Academic, Dordrecht, 2002, pp. 187-200. (RW 5004)

Sinatra, G.M. "The "Warming Trend" in Conceptual Change Research: The Legacy of Paul R. Pintrich," *Educational Psychologist,* Vol. 40, No. 2, 2005, pp. 107-115. (RW 4983)

Sinatra, G.M. & Mason, L. "Beyond Knowledge: Learner Characteristics Influencing Conceptual Change," in *International Handbook of Research on Conceptual Change*, ed. S. Vosniadou, Routledge, New York, 2008, pp. 560-582. (RW 5124)

Sinatra, G.M. & Nadelson, L. "Science and Religion: Ontologically Different Epistemologies?" in *Epistemology and Science Education: Understanding the Evolution Vs. Intelligent Design*

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Controversy, eds. R.S. Taylor & M. Ferrari, Routledge, New York, NY, 2011, pp. 173-194. (RW 4766)

Sinatra, G.M. & Pintrich, P.R. "The Role of Intentions in Conceptual Change Learning," in *Intentional Conceptual Change*, eds. G.M. Sinatra & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2003, pp. 1-18. (RW 4417)

Sinatra, G.M., Southerland, S.A., McConaughy, F. & Demastes, J.W. "Intentions and Beliefs in Students' Understanding and Acceptance of Biological Evolution," *Journal of Research in Science Teaching*, Vol. 40, No. 5, 2003, pp. 510-28. (RW 5094)

Sinclair, R.S. *Thinking and Writing: Cognitive Science and the Directorate of Intelligence*, Center for the Study of Intelligence, Washington, DC, 1980. (RW 123)

Sinclair, R.S. *Thinking and Writing: Cognitive Science and Intelligence Analysis*, Center for the Study of Intelligence 2010. (RW 4071)

Singer, O. "Under the Cloud of Professionalism," *International Journal of Psychosocial Rehabilitation*, Vol. 7, 2002, pp. 35. (RW 3561)

Singletary, B.A. & Howard, N. *Sensemaking in Symbiotic Joint-Cognitive Systems* (RW 1771)

Sintonen, M. "Conceptual Change as Structure Change: Comment on Kuhn's Legacy," in *Re-Framing the Conceptual Change Approach in Learning and Instruction*, eds. S. Vosniadou, A. Baltas & X. Vamvakoussi, Elsevier, Amsterdam, 2007, pp. 89-96. (RW 3720)

Sissens, J. "An Evaluation of the Role of the Intelligence Analyst within the National Intelligence Model," in *The Handbook of Intelligent Policing: Consilience, Crime Control, and Community Safety*, ed. C. Harfield, Oxford University Press, Oxford, UK, 2008, pp. 121-130. (RW 5774)

Skarstedt, V. "The National Defense Intelligence College," *American Intelligence Journal*, Vol. 26, No. 2, 2008/2009, pp. 13-16. (RW 3625)

Skillicorn, D.B. *Knowledge Discovery for Counterterrorism and Law Enforcement*, CRC Press, Boca Raton, FL, 2009. (RW 5638)

Skinner, K.K. "Qualitative Analysis for the Intelligence Community," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, pp. 101-113. (RW 4774)

Skye, A. *Universal Human Truths: Creature of Habit*, Available: http://askye.wordpress.com/2007/08/26/universal-human-truths-creature-of-habit/, (RW 3884)

Slater, J. "The Psychology of Collaboration," *Technology Review*, 2011 (RW 4743)

Sloman, S.A. & Lagnado, D.A. "The Problem of Induction," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 95-116. (RW 4000)

Slotte, V. & Lonka, K. "Note Taking and Essay Writing," in *Writing as a Learning Tool: Integrating Theory and Practice*, eds. P. Tynjälä, L. Mason & K. Lonka, Kluwer Academic Publishers, Dordrecht Netherlands; Boston, 2001, pp. 131. (RW 4337)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Slowiaczek, L.M., Klayman, J., Sherman, S.J. & Skov, R. "Information Selection and use in Hypothesis Testing: What is a Good Question, and what is a Good Answer?" *Memory & Cognition,* Vol. 20, No. 4, 1992, pp. 392. (RW 2112)

Smalheiser, N.R. "Predicting Emerging Technologies with the Aid of Text-Based Data Mining: A Micro Approach," *Technovation,* Vol. 21, 2001, pp. 689. (RW 2414)

Smalheiser, N.R. "Informatics and Hypothesis-Driven Research," *EMBO Reports,* Vol. 3, 2002, pp. 702. (RW 2417)

Smalheiser, N.R. "The Arrowsmith Project: 2005 Status Report," *Lecture Notes in Artificial Intelligence,* Vol. 3735, 2005, pp. 26. (RW 2374)

Small, G. & Vorgan, G. "Meet Your iBrain," *Scientific American Mind,* Vol. 19, No. 5, 2008, pp. 42. (RW 3279)

Smallheiser, N.R. & Torvik, V.I. "Author Name Disambiguation," in *Annual Review of Information Science and Technology,* ed. B. Cronin, Medford, NJ, Vol. 43, 2009, pp. 287-313. (RW 4347)

Smedslund, J. "On the Circular Relation between Logic and Understanding," *Scandinavian Journal of Psychology,* Vol. 11, 1970, pp. 217-219. (RW 5818)

Smith, A.E. "Notes on Capabilities in National Intelligence," *Studies in Intelligence,* Vol. 1, No. 2, 1957, pp. 1-18. (RW 542)

Smith, A.E. "On the Accuracy of National Intelligence Estimates," *Studies in Intelligence,* Vol. 13, No. 4, 1969, pp. 25-35. (RW 547)

Smith, B., Malyuta, T., Salmen, D., Mandrick, W., Parent, K., Bardhan, S. & Johnson, J. *Ontology for the Intelligence Analyst* 2012. (RW 5861)

Smith, E.E. & Kosslyn, S.M. *Cognitive Psychology: Mind and Brain,* Pearson/Prentice Hall, Upper Saddle River, NJ, 2007. (RW 1793)

Smith, F. *Writing and the Writer,* 2nd ed., L. Erlbaum Associates, Hillsdale, NJ, 1994. (RW 1850)

Smith, G.D. & Fahlman, R. "New Eyes on the World: Training Analysts, their Managers, and Overseers," *Journal of Conflict Studies,* Vol. 16, No. 1, 1996 (RW 585)

Smith, K., Shanteau, J. & Johnson, P.E. "Introduction: What does it Mean to be Competent?" in *Psychological Investigations of Competence in Decision Making,* eds. K. Smith, J. Shanteau & P.E. Johnson, Cambridge University Press, Cambridge, UK; New York, 2004, pp. 1. (RW 2368)

Smith, M.D. "The Perils of Analysis: Revisiting Sherman Kent's Defense of SNIE 85-3-62," *Studies in Intelligence,* Vol. 51, No. 3, 2007 (RW 2802)

Smith, M.D. "Truth in Intelligence: A Cautionary Tale," *International Journal of Intelligence and Counterintelligence,* Vol. 22, No. 2, 2009, pp. 320. (RW 3447)

Smith, M.W., Zelik, D., Patterson, E. & Woods, D.D. *Faction Display: Visualizing the Spectrum of Risk Estimates in a Terrorist Attack* 2007. (RW 2280)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Smith, M., Patterson, E.S., Zelik, D. & Woods, D.D. "Faction Display: Visualizing the Spectrum of Risk Estimates in a Terrorist Attack", *Proceedings of the 8th International Conference on Naturalistic Decision Making,* Monterey, CA, June 4-6, 2007 (RW 3130)

Smith, M.U. "Current Status of Research in Teaching and Learning Evolution: I. Philosophical/Epistemological Issues," *Science & Education,* Vol. 19, No. 6-8, 2010, pp. 523-538. (RW 5249)

Smith, R., Keramatian, K., Smallwood, J., Schooler, J., Luus, B. & Christoff, K. "Mind-Wandering with and without Awareness: An fMRI Study of Spontaneous Thought Processes", *Proceedings of the 28th Annual Conference of the Cognitive Science Society,* July 26-29, 2006, pp. 804. (RW 1985)

Smith, R.J. *The Unknown CIA: My Three Decades with the Agency,* Pergamon-Brassey's, Washington, 1989. (RW 4375)

Smith, S.M. & Levin, I.P. "Need for Cognition and Choice Framing Effects," *Journal of Behavioral Decision Making,* Vol. 9, No. 4, 1996, pp. 281-290. (RW 4948)

Smith, S.M. & Ward, T.B. "Cognition and the Creation of Ideas," in *Oxford Handbook of Thinking and Reasoning,* eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 456-474. (RW 5502)

Smith, T.E., Knapp, C., Seaman, J. & Pace, S. "Experiential Education and Learning by Experience," in *Sourcebook of Experiential Education: Key Thinkers and their Contributions,* eds. T.E. Smith & C. Knapp, Routledge, New York, 2011, pp. 1-11. (RW 4886)

Smith, T.E. & Leeming, C.S. "Kurt Lewin: Another Kurt for Experiential Educators to Know," in *Sourcebook of Experiential Education: Key Thinkers and their Contributions,* eds. T.E. Smith & C. Knapp, Routledge, New York, 2011, pp. 173-179. (RW 4927)

Smith, T.J. *Predictive Network-Centric Intelligence: Toward a Total-Systems Transformation of Analysis and Assessment* 2006. (RW 2820)

Smith, T.J. *Predictive Network-Centric Intelligence: Computational Collaboration [Powerpoint Presentation]* 2007. (RW 3129)

Smith, T.J. "Predictive Network-Centric Intelligence: Toward a Total-Systems Transformation of Analysis and Assessment," in *Proteus Futures Digest: A Compilation of Selected Works Derived from the 2007 Proteus Workshop,* eds. J. Auger & W. Wimbish, 2nd ed., U.S. Army War College, Carlisle Barracks, PA, 2007, pp. 249-262. (RW 4814)

Smith, T.J. "Predictive Warning: Teams, Networks, and Scientific Method," in *Analyzing Intelligence: Origins, Obstacles, and Innovations,* eds. R.Z. George & J.B. Bruce, Georgetown University Press, Washington, DC, 2008, pp. 266-280. (RW 3109)

Smith, W., Dowell, J. & Ortega-Lafuente, M.A. "Designing Paper Disasters: An Authoring Environment for Developing Training Exercises in Integrated Emergency Management," *Cognition, Technology, & Work,* Vol. 1, 1999, pp. 119. (RW 3526)

Smither, J.W. "Performance Management," in *Oxford Handbook of Organizational Psychology,* ed. W.J. Kozlowski, Oxford University Press, New York, NY, 2012, pp. 285-329. (RW 5765)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Smucker, M.D. & Jethani, C.P. "Impact of Retrieval Precision on Perceived Difficulty and Other User Measures", *HCIR 2010: Proceedings of the Fourth Workshop on Human-Computer Interaction and Information Retrieval,* New Brunswick, NJ, August 22, 2010, pp. 20. (RW 4313)

Snider, L.B. *Sharing Secrets with Lawmakers: Congress as a User of Intelligence,* Center for the Study of Intelligence, Washington, DC, 1997. (RW 387)

Snider, L.B., comments by Rindskopf, E. & Coleman, J. "Intelligence and Law Enforcement," in *U.S. Intelligence at the Crossroads: Agendas for Reform,* eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 243-264. (RW 648)

Snodgrass, C.W. *Funding C3I,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1981. (RW 1038)

Snook, S.A. *Leading Complex Organizations: Lessons from a Tragic Organizational Failure,* Center for Information Policy Research, Harvard University, Cambridge, MA, 2001. (RW 1154)

Snow, C.E. *Reading for Understanding: Toward a Research and Development Program in Reading Comprehension,* RAND Corporation, Santa Monica, CA, 2002. (RW 3787)

Snowden, D. "Complex Acts of Knowing: Paradox and Descriptive Self-Awareness," *Journal of Knowledge Management,* Vol. 6, No. 2, 2002, pp. 100-111. (RW 4734)

Snowden, D.J. "Multi-Ontology Sense Making: A New Simplicity in Decision Making," *Informatics in Primary Care,* Vol. 13, 2005, pp. 45. (RW 2560)

Snyder, M. "Motivational Foundations of Behavioral Confirmations," in *Advances in Experimental Social Psychology,* ed. M.P. Zanna, Vol, 25, 1992, pp. 67. (RW 2117)

Snyder, M. "When Belief Creates Reality," *Advances in Experimental Social Psychology,* Vol. 18, 1983, pp. 247-305. (RW 5238)

Snyder, M. & Swann, W.B. "Hypothesis-Testing Processes in Social Interaction," *Journal of Personality and Social Psychology,* Vol. 36, No. 11, 1978, pp. 1202. (RW 2109)

So, H.-., Lee, J.-., Roh, S.-. & Lee, S.-. "Examining Epistemological Beliefs of Pre-Service Teachers in Korea," *Asia Pacific Education Researcher,* Vol. 19, 2010, pp. 79-97. (RW 5058)

Socarides, C.W. & Kramer, S. *Work and its Inhibitions: Psychoanalytic Essays,* International Universities Press, Madison, CT, 1997. (RW 1851)

Sofranac, P. "Data Mining and Intelligence Outsourcing," *Marine Corps Gazette,* Vol. 83, No. 3, 1999, pp. 45. (RW 4445)

Sokolov, A.N. *Inner Speech and Thought,* Plenum Press, New York, NY, 1972. (RW 5846)

Sokolski, H. "Fighting Proliferation with Intelligence," *Orbis,* Vol. 38, No. 2, 1994, pp. 245-260. (RW 77)

Solin, G. "The Art of China-Watching," *Studies in Intelligence,* Vol. 19, No. 1, 1975, pp. 23-33. (RW 559)

Soll, J. & Larrick, R. "You Know More than You Think: How to Tap the Wisdom of the Crowd in Your Head," *Scientific American: Mind Matters,* 2009 (RW 3497)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Solomon, M. "A Confederacy of Databases," *Searcher*, Vol. 12, No. 7, 2004, pp. 24. (RW 1428)

Solomon, P. "Discovering Information in Context," *Annual Review of Information Science and Technology*, Vol. 36, 2002, pp. 229-264. (RW 1127)

Solomon, P. "Looking for Information—A Survey of Research on Information Seeking, Needs, and Behavior. Book Review." *Information Retrieval*, Vol. 6, No. 2, 2003, pp. 284-288. (RW 949)

Soman, D. "Framing, Loss Aversion, and Mental Accounting," in *Blackwell Handbook of Judgment and Decision Making*, eds. D.J. Koehler & N. Harvey, Blackwell Pub., Malden, MA; Oxford, 2004, pp. 379. (RW 2824)

Somerville, M.M. & Howard, Z. "Information in context: co-designing workplace structures and systems for organizational learning", *Information Research*, [Online], vol. 15, no. 4, paper 446. Available from: http://InformationR.net/ir/15-4/paper446.html, 2010, (RW 4790)

Sommer, D. *Impact of Social Media on Intelligence Analysis and Intelligence Training*, Available: http://education.ezinemark.com/impact-of-social-media-on-intelligence-analysis-and-intelligence-training-1d8f846e4a3.html, January 4, 2011. (RW 4506)

Songer, N.B. & Linn, M.C. "How do Students' Views of Science Influence Knowledge Integration," *Journal of Research in Science Teaching*, Vol. 28, No. 9, 1991, pp. 761-784. (RW 4647)

Sonnenwald, D.H. "Developing a Theory to Guide the Process of Designing Information Retrieval Systems", *Proceedings of the 15th Annual International ACM SIGIR Conference on Research and Development in Information Retrieval*, Copenhagen, Denmark, June 21-24, 1992, pp. 310. (RW 1786)

Soon, C.S., Brass, M., Heinze, H. & Haynes, J. "Unconscious Determinants of Free Decisions in the Human Brain," *Nature Neuroscience*, 2008 (RW 3066)

Sormunen, E. "Extensions to the STAIRS Study-Empirical Evidence for the Hypothesised Ineffectiveness of Boolean Queries in Large Full-Text Databases," *Information Retrieval*, Vol. 4, No. 3-4, 2001, pp. 257-273. (RW 953)

Southerland, S.A. & Sinatra, G.M. "Learning about Biological Evolution: A Special Case of Intentional Conceptual Change," in *Intentional Conceptual Change*, eds. G.M. Sinatra & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2003, pp. 317. (RW 4437)

Southerland, S.A., Sinatra, G.M. & Matthews, M.R. "Belief, Knowledge, and Science Education," *Educational Psychology Review*, Vol. 13, No. 4, 2001, pp. 325-351. (RW 5087)

Spalding, R. & Parker, C. *Historiography: An Introduction*, Manchester University Press, Manchester, UK, 2007. (RW 3205)

Sparck Jones, K. *Information Retrieval Experiment*, Butterworths, London, UK, 1981. (RW 1207)

Sparck Jones, K. & Willett, P. *Readings in Information Retrieval*, Morgan Kaufman, San Francisco, Calif, 1997. (RW 3536)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Sparkes, J. & Huf, S. *Mental Models Theory and Military Decision-Making: A Pilot Experimental Model,* DSTO-GD-0368, 2003. (RW 1759)

Spatt, B. *Writing from Sources,* 6th edition ed., Bedford/St. Martin's, Boston, MA, 2003. (RW 2308)

Spaulding, S. "Intelligence Restructuring: Just the First Step," *National Strategy Forum Review,* Vol. 14, No. 1, 2004, pp. 23-25. (RW 337)

Specter, M. "Search and Deploy: The Race to Build a Better Search Engine," *The New Yorker,* Vol. 76, No. 13, 2000, pp. 88-100. (RW 901)

Specter, M. *Denialism: How Irrational Thinking Hinders Scientific Progress, Harms the Planet, and Threatens our Lives,* Penguin Press, New York, NY, 2009. (RW 3794)

Spellman, B.A. *Why "Psychology and the Law" does Not Equal "Law and Psychology" (and some Things we can do about it)* (RW 2064)

Spellman, B.A. "Acting as Intuitive Scientists: Contingency Judgments are made while Controlling for Alternative Potential Causes," *Psychological Science,* Vol. 7, No. 6, 1996, pp. 337. (RW 1894)

Spellman, B.A. "Individual Reasoning," in *Intelligence Analysis: Behavioral and Social Scientific Foundations,* eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, pp. 117-141. (RW 4775)

Spellman, B.A. & Holyoak, K.J. "An Inhibitory Mechanism for Goal-Directed Analogical Mapping", *Proceedings of the 15th Annual Conference of the Cognitive Science Society,* June 18-21, 1993, pp. 947. (RW 1998)

Spellman, B.A. & Holyoak, K.J. "Pragmatics in Analogical Mapping," *Cognitive Psychology,* Vol. 31, 1996, pp. 307. (RW 1795)

Spellman, B.A., Lopez, A. & Smith, E.E. "Hypothesis Testing: Strategy Selection for Generalising Versus Limiting Hypotheses," *Thinking & Reasoning,* Vol. 5, No. 1, 1999, pp. 67. (RW 1893)

Spence, M.T. & Brucks, M. "The Moderating Effects of Problem Characteristics on Experts' and Novices' Judgments," *Journal of Marketing Research,* Vol. 34, 1997, pp. 233. (RW 2517)

Sperber, D. "Intuitive and Reflective Beliefs," *Mind & Language,* Vol. 12, No. 1, 1997, pp. 67-83. (RW 5305)

Sperber, D. "An Evolutionary Perspective on Testimony and Argumentation," *Philosophical Topics,* Vol. 29, No. 1 & 2, 2001, pp. 401-413. (RW 5345)

Sperber, D. & Wilson, D. *Relevance: Communication and Cognition,* 2nd ed., Blackwell, Oxford, UK, 1995. (RW 3182)

Sperber, D. & Wilson, D. "Pragmatics, Modularity and Mind-Reading," *Mind & Language,* Vol. 17, No. 1, 2002, pp. 3-23. (RW 5344)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Spicer, K. & Hanks, W.E. "Multiple Measures of Critical Thinking Skills and Predisposition in Assessment of Critical Thinking", *81st Annual Meeting of the Speech Communications Association,* San Antonio, TX, November 18-21, 1995 (RW 4045)

Spiegelhalter, D., Pearson, M. & Short, I. "Visualizing Uncertainty about` the Future," *Science,* Vol. 333, 2011, pp. 1393-1400. (RW 5155)

Spielman Rice, A. *The Role of Imagination in National Security: An Assessment of the Cross-Impact Method for Intelligence Analysis,* M. A. thesis, University of New Haven, 2005. (RW 2810)

Spielmann, K. "Strengthening Intelligence Threat Analysis," *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 1, 2012, pp. 19-43. (RW 5396)

Spillane, J.P., Reiser, B.J. & Gomez, L.M. "Policy Implementation and Cognition: The Role of Human, Social, and Distributed Cognition in Framing Policy Implementation," in *New Directions in Education Policy Implementation: Confronting Complexity,* ed. M.I. Honig, 2006, pp. 47. (RW 1722)

Spiro, R.J., Feltovich, P.J., Jacobson, M.J. & Coulson, R.L. "Knowledge Representation, Content Specification, and the Development of Skill in Situation Specific Knowledge Assembly: Some Constructivist Issues as they Relate to Cognitive Flexibility and Hypertext," *Education Technology,* Vol. 31, No. 9, 1991, pp. 22. (RW 4286)

Spiro, R.J., Coulson, R.L., Feltovich, P.J. & Anderson, D. "Cognitive Flexibility Theory: Advanced Knowledge Acquisition in Ill-Structured Domains", *10th Annual Conference of the Cogntive Science Society,* Montreal, Quebec, Canada, August 17-19, 1988, pp. 375-383. (RW 5325)

Spiro, R.J., Feltovich, P.J. & Coulson, R.L. "Two Epistemic World-Views: Prefigurative Schemas and Learning in Complex Domains," *Applied Cognitive Psychology,* Vol. 10, No. 7, 1996, pp. 51-61. (RW 5031)

Spiro, R.J., Vispoel, W.L., Schmitz, J.G., Samarapungavan, A. & Boerger, A.E. "Knowledge Acquisition for Application: Cognitive Flexibility and Transfer in Complex Content Domains," in *Executive Control Processes in Reading,* eds. B.K. Britton & S.M. Glynn, L. Erlbaum Associates, Hillsdale, NJ, 1987, pp. 177-199. (RW 5323)

Spivack, N. *Making Sense of the Semantic Web [Powerpoint Presentation]* (RW 3079)

Spivey, N.N. *Discourse Synthesis: Constructing Texts in Reading and Writing,* 1983. (RW 2300)

Spracher, W.C. "Mired in Gray: Juggling Legality, Lawfulness, and Ethics as an Intelligence Professisonal," *American Intelligence Journal,* Vol. 25, No. 1, 2007, pp. 63. (RW 3224)

Spracher, W.C. *National Security Intelligence Professional Education: A Map of U. S. Civilian University Programs and Competencies,* Ph.D. dissertation, George Washington University, 2009. (RW 4368)

Spracher, W.C. "Teaching Intelligence in the United States, the United Kingdom, and Canada," in *The International Studies Encyclopedia,* ed. R.A. Denemark, Blackwell Publishing, 2010, pp. [unpaged]. (RW 3931)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Squire, L.R. & Kandel, E.R. *Memory: From Mind to Molecules*, 2nd ed., Roberts & Co., Greenwood Village, CO, 2009. (RW 5791)

Srihari, R.K., Li, W., Crist, L. & Niu, C. "Intelligence Discovery Portal Based on Corpus Level Information Extraction," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2-6 May 2005 (RW 594)

St. B. T. Evans, Jonathan "Deductive Reasoning," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 169-184. (RW 4003)

St. John, J. *Science and Pseudoscience,* Available: http://www1.newark.ohio-state.edu/Professional/OSU/Faculty/jstjohn/Science-and-Pseudoscience.htm, Viewed: October 10, 2011. (RW 5161)

Staar, R.F. "The US Intelligence Community," *Review of Policy Research,* Vol. 20, No. 4, 2003, pp. 713-725. (RW 791)

Stack, K.P. "A Negative View of Competitive Analysis," *International Journal of Intelligence and Counterintelligence*, Vol. 10, No. 4, 1997, pp. 456-464. (RW 62)

Stack, K.P. "Competitive Intelligence," *Intelligence and National Security*, Vol. 13, No. 4, 1998, pp. 194-202. (RW 9)

Stack, K.P. "Appreciating President Ford's Legacy to Intelligence," *International Journal of Intelligence and Counterintelligence*, Vol. 12, No. 1, 1999, pp. 73-79. (RW 192)

Staib, S. "Teaching and Measuring Critical Thinking," *Journal of Nursing Education,* Vol. 42, No. 11, 2003, pp. 498-508. (RW 3969)

Stajner, T., Mladenic, D. & Grobelnik, M. "Exploring Contexts and Actions in Knowledge Processes", *Second International Workshop on Context Information and Ontologies*, Lisbon, October 11, 2010 (RW 4862)

Stankov, L. & Crawford, J.D. "Self-Confidence and Performance on Tests of Cognitive Abilities," *Intelligence*, Vol. 25, No. 2, 1997, pp. 93. (RW 2421)

Stanovich, K.E., West, R.F. & Toplak, M.E. "Intelligence and Rationality," in *Cambridge Handbook of Intelligence*, eds. R.J. Sternberg & S.B. Kaufman, Cambridge University Press, New York, NY, 2012, pp. 784-826. (RW 5417)

Stanovich, K.E. *Distinguishing the Reflective, Algorithmic, and Autonomous Minds: Is it Time for a Tri-Process Theory?* [undated]. (RW 3334)

Stanovich, K.E. *Who is Rational? Studies of Individual Differences in Reasoning*, L. Erlbaum Associates, Mahwah, NJ, 1999. (RW 2420)

Stanovich, K.E. "The Rationality of Educating for Wisdom," *Educational Psychologist,* Vol. 36, No. 4, 2001, pp. 247-251. (RW 3460)

Stanovich, K.E. "Rationality, Intelligence, and Levels of Analysis in Cognitive Science: Is Dysrationalia Possible," in *Why Smart People can be so Stupid*, ed. R.J. Sternberg, Yale University Press, New Haven, 2002, pp. 124. (RW 3484)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Stanovich, K.E. *The Robot's Rebellion: Finding Meaning in the Age of Darwin*, University of Chicago Press, Chicago, IL, 2004. (RW 3322)

Stanovich, K.E. "Distinguishing the Reflective, Algorithmic, and Autonomous Minds: Is it Time for a Tri-Process Theory?" in *In Two Minds: Dual Processes and Beyond*, eds. Evans, Jonathan St. B. T. & K. Frankish, Oxford University Press, Oxford, 2009, pp. 55. (RW 3481)

Stanovich, K.E. *What Intelligence Tests Miss: The Psychology of Rational Thought,* Yale University Press, New Haven, CT, 2009. (RW 3323)

Stanovich, K.E. *Decision Making and Rationality in the Modern World,* Oxford University Press, New York, NY, 2010. (RW 3522)

Stanovich, K.E. "Normative Models in Psychology are here to Stay," *Behavioral and Brain Sciences,* Vol. 34, No. 5, 2011, pp. 268-269. (RW 5412)

Stanovich, K.E. *Rationality and the Reflective Mind,* Oxford University Press, New York, NY, 2011. (RW 4520)

Stanovich, K.E. "Cumulative Progress in Understanding our Multiple Minds," *American Journal of Psychology,* Vol. 125, No. 1, 2012, pp. 116-120. (RW 5419)

Stanovich, K.E. "On the Distinction between Rationality and Intelligence: Implications for Understanding Individual Differences in Reasoning," in *Oxford Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 433-455. (RW 5421)

Stanovich, K.E. "Why Humans are (Sometimes) Less Rational than Other Animals: Cognitive Complexity and the Axioms of Rational Choice," *Thinking & Reasoning,* 2012 (RW 5823)

Stanovich, K.E., Sa, W.C. & West, R.F. "Individual Differences in Thinking, Reasoning, and Decision Making," in *The Nature of Reasoning*, eds. R.J. Sternberg & J.P. Leighton, Cambridge University Press, Cambridge, UK, 2004, pp. 375-409. (RW 2386)

Stanovich, K.E. & Stanovich, P.J. "A Framework for Critical Thinking, Rational Thinking, and Intelligence," in *Innovations in Educational Psychology: Perspectives on Learning, Teaching, and Human Development*, eds. D. Priess & R.J. Sternberg, Springer, New York, NY, 2010, pp. 195-237. (RW 5425)

Stanovich, K.E. & Toplak, M.E. "Defining features versus incidental correlates of Type 1 and Type 2 processing", *Mind & Society*, [Online], 2012, (RW 5420)

Stanovich, K.E., Toplak, M.E. & West, R.F. "The Development of Rational Thought: A Taxonomy of Heuristics and Biases," *Advances in Child Development and Behavior*, Vol. 362008, pp. 251-285. (RW 3335)

Stanovich, K.E. & West, R.F. "Individual Differences in Reasoning: Implications for the Rationality Debate? (Includes Advancing the Rationality Debate)," *Behavioral and Brain Sciences,* Vol. 23, No. 5, 2000, pp. 645-726. (RW 2422)

Stanovich, K.E. & West, R.F. "Reasoning Independently of Prior Belief and Individual Differences in Actively Open-Minded Thinking," *Journal of Educational Psychology,* Vol. 89, No. 2, 1997, pp. 342-357. (RW 2441)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Stanovich, K.E. & West, R.F. "Individual Differences in Rational Thought," *Journal of Experimental Psychology: General,* Vol. 127, No. 2, 1998, pp. 161-188. (RW 2440)

Stanovich, K.E. & West, R.F. "Evolutionary Versus Instrumental Goals: How Evolutionary Psychology Misconceives Human Rationality," in *Evolution and the Psychology of Thinking: The Debate*, ed. D.E. Over, Psychological Press, 2003, pp. 171-230. (RW 5426)

Stanovich, K.E. & West, R.F. "Natural Myside Bias is Independent of Cognitive Ability," *Thinking & Reasoning,* Vol. 13, No. 3, 2007, pp. 225-247. (RW 3338)

Stanovich, K.E. & West, R.F. "On the Failure of Cognitive Ability to Predict Myside and One-Sided Thinking Biases," *Thinking & Reasoning,* Vol. 14, No. 2, 2008, pp. 129-167. (RW 3337)

Stanovich, K.E. & West, R.F. "On the Relative Independence of Thinking Biases and Cognitive Ability," *Journal of Personality and Social Psychology,* Vol. 94, No. 4, 2008, pp. 672-695. (RW 3336)

Stanovich, K.E., West, R.F. & Toplak, M.E. "The Complexity of Developmental Predictions from Dual Process Models," *Developmental Review,* Vol. 31, No. 2-3, 2011, pp. 103-118. (RW 5422)

Stanovich, K.E., West, R.F. & Toplak, M.E. "Individual Differences as Essential Components of Heuristics and Biases Research," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans*, eds. K. Manktelow, D. Over & S. Elqayam, Psychology Press, 2011, pp. 355-396. (RW 5424)

Stapleton-Gray, R. "Watchin' the Analysts," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 792)

Starbuck, W.H. "Keeping a Butterfly and an Elephant in a House of Cards: The Elements of Exceptional Success," *Journal of Management Studies,* Vol. 30, No. 6, 1993 (RW 1339)

Starbuck, W.H. "Unlearning Ineffective or Obsolete Technologies," *International Journal of Technology Management,* Vol. 11, No. 7/8, 1996, pp. 725-737. (RW 1071)

Stark, S.D. *Writing to Win: The Legal Writer: The Complete Guide to Writing Strategies that Will make Your Case-- and Win it,* Broadway Books, New York, NY, 2000. (RW 4261)

Starks, T. *Intel: Lost in the Shuffle* 2008. (RW 3193)

Starks, T. "Issues: Intelligence: Reorganization Fatigue," *CQ Politics,* 2008 (RW 3296)

Starmer, C. "Developments in Non-Expected Utility: The Hunt for a Descriptive Theory of Choice Under Risk," *Journal of Economic Literature,* Vol. 38, No. 2, 2000, pp. 332. (RW 3155)

Starz, J., Losco, J., Kettler, B., Hingst, R. & Rouff, C. "Leveraging Emergent Ontologies in the Intelligence Community", *Proceedings of the Third International Ontology for the Intelligence Community Conference OIC-2008,* Fairfax, VA, December 3-4, 2008, pp. 5-7. (RW 4823)

Stasko, J., Gorg, C. & Liu, Z. "Jigsaw: Supporting Investigative Analysis through Interactive Visualization," *Information Visualization,* Vol. 7, No. 2, 2008, pp. 118-132. (RW 5658)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Stasser, G. "The Uncertain Role of Unshared Information in Collective Choice," in *Shared Cognition in Organizations: The Management of Knowledge*, eds. L.L. Thompson, J.M. Levine & D.M. Messick, L. Erlbaum Associates, Mahwah, NJ, 1999, pp. 49. (RW 2224)

Stasser, G. & Birchmeier, Z. "Group Creativity and Collective Choice," in *Group Creativity: Innovation through Collaboration*, eds. P.B. Paulus & B.A. Nijstad, 2003, pp. 85. (RW 2156)

Stasser, G. & Dietz-Uhler, B. "Collective Choice, Judgment, and Problem Solving," in *Blackwell Handbook of Social Psychology: Group Processes*, eds. M.A. Hogg & R.S. Tindale, Blackwell Publishers, Malden, Mass, 2003, pp. 31. (RW 2222)

Stathopoulou, C. & Vosniadou, S. "Conceptual Change in Physics and Physics-Related Epistemological Beliefs: A Relationship Under Scrutiny," in *Re-Framing the Conceptual Change Approach in Learning and Instruction*, eds. S. Vosniadou, A. Baltas & X. Vamvakoussi, Elsevier, Amsterdam, 2007, pp. 145-163. (RW 5594)

Stathopoulou, C. & Vosniadou, S. "Exploring the Relationship between Physics-Related Epistemological Beliefs and Physics Understanding," *Contemporary Educational Psychology*, Vol. 32, No. 3, 2007, pp. 255-281. (RW 5288)

Staver, J.R. "When public understanding of science thwarts standards-based science education", *Electronic Journal of Science Education*, [Online], vol. 3, no. 4, pp. October 10, 2011. Available from: http://ejse.southwestern.edu/article/view/7613/53801999, (RW 5159)

Staw, J.A. *Unstuck: A Supportive and Practical Guide to Working through Writer's Block*, St. Martin's Press, New York, 2003. (RW 1862)

Stebbing, L.S. *Thinking to some Purpose*, Penguin Books Ltd., Harmondsworth, Middlesex, UK, 1939. (RW 4450)

Stebbins, L.F. *Student Guide to Research in the Digital Age: How to Locate and Evaluate Information Sources*, Libraries Unlimited, Westport, CT, 2006. (RW 3537)

Stech, F.J. *Political and Military Intention Estimation: A Taxonometric Analysis*, Mathtech, Inc., Bethesda, MD, 1979. (RW 689)

Stech, F.J. *Political and Military Intention Estimation: A Taxonometric Analysis*, Office of Naval Research, Dept. of the Nave 1979. (RW 4219)

Stech, F.J. *Estimates of Peacetime Soviet Naval Intentions: An Assessment of Methods*, Office of Naval Research, Dept. of the Navy 1981. (RW 4220)

Stech, F.J. "Midway Revisited: Detecting Deception by Analysis of Competing Hypothesis", *72nd MORS Symposium*, Naval Postgraduate School, Monterey, CA, June 22-24, 2004 (RW 781)

Stech, F.J. & Elsaesser, C. "Deception Detection by Analysis of Competing Hypotheses," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 836)

Stech, F.J. & Elsaesser, C. "Deception Detection by Analysis of Competing Hypotheses [Powerpoint Presentation]," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 835)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Stech, F.J. & Hoffman, K.C. *Methods of Estimating Strategic Intentions*, Office of Naval Research, Dept. of the Navy 1982. (RW 4221)

Steele, R.D. *The New Craft of Intelligence, Personal, Public, & Political: Citizen's Action Handbook for Fighting Terrorism, Genocide, Disease, Toxic Bombs, & Corruption*, OSS International Press, Oakton, VA, 2002. (RW 1640)

Steele, R.D. "Intelligence Reform: More Needs to be done. Letter in Response to Saxby Chambliss Article. Saxby Chambliss Responds to this Letter on p. 137," *Parameters*, Vol. 35, No. 2, 2005, pp. 135-140. (RW 616)

Steele, R.D. *Human Intelligence: All Humans, all Minds, all the Time*, 2010. (RW 4152)

Steele, R.D. "A Critical Evaluation of US National Intelligence Capabilities," *International Journal of Intelligence and Counterintelligence*, Vol. 6, No. 2, 1993, pp. 173-193. (RW 44)

Steele, R.D. "Private Enterprise Intelligence: Its Potential Contribution to National Security," *Intelligence and National Security*, Vol. 10, No. 4, 1995, pp. 212-228. (RW 129)

Steele, R.D. *Intelligence and Counterintelligence: Proposed Program for the 21st Century* 1997. (RW 883)

Steele, R.D. "The New Craft of Intelligence: An Alternative Approach Oriented to the Public", *The Future of Intelligence in the 21st Century*, Priverno, Italy, 14-16 February 2001 (RW 3715)

Steele, R.D. "Crafting Intelligence in the Aftermath of Disaster," *International Journal of Intelligence and Counterintelligence*, Vol. 15, No. 2, 2002, pp. 161-178. (RW 190)

Steele, R.D. "Foreign Liaison and Intelligence Reform: Still in Denial," *International Journal of Intelligence and Counterintelligence*, Vol. 20, No. 1, 2007, pp. 167. (RW 1757)

Steele, R.D. "Open Source Intelligence," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 129. (RW 2463)

Steele, R.D. "Open Source Intelligence," in *Strategic Intelligence. Volume 2: The Intelligence Cycle: The Flow of Secret Information from Overseas to the Highest Councils of Government*, ed. L.K. Johnson, Praeger Security International, Westport, CT, 2007, pp. 95. (RW 2705)

Steele, R.D. "The Open Source Program: Missing in Action," *International Journal of Intelligence and Counterintelligence*, Vol. 21, No. 3, 2008, pp. 609. (RW 3135)

Steele, R.D. "Fixing the White House and National Intelligence," *International Journal of Intelligence and Counterintelligence*, Vol. 23, No. 2, 2010, pp. 353. (RW 3900)

Steele, R.D., Army War College (U.S.) & Strategic Studies Institute *The New Craft of Intelligence Achieving Asymmetric Advantage in the Face of Nontraditional Threats*, Strategic Studies Institute, U.S. Army War College. Available: http://purl.access.gpo.gov/GPO/LPS19526;, (RW 1641)

Stein, D. *Co-Operating with Written Texts: The Pragmatics and Comprehension of Written Texts*, Mouton de Gruyter, Berlin ; New York, 1992. (RW 1869)

Stein, H.F. *Listening Deeply: An Approach to Understanding and Consulting in Organizational Culture*, Westview Press, Boulder, CO, 1994. (RW 2673)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Steinberg, J.B. *Testimony before the National Commission on Terrorist Attacks upon the United States* 2003. (RW 1368)

Steinberg, J.B. "The Policymaker's Perspective: Transparency and Partnership," in *Analyzing Intelligence: Origins, Obstacles, and Innovations*, eds. R.Z. George & J.B. Bruce, 2008, pp. 82. (RW 3097)

Steinberg, J.B., Graham, M. & Eggers, A. "Building Intelligence to Fight Terrorism," *Brookings Institution Policy Brief*, 125, 2003 (RW 1326)

Steinbruner, J.D. *The Mind and Milieu of Policy-Makers: A Case Study of the MLF*, Ph.D. dissertation, Massachusetts Institute of Technology, 1968. (RW 699)

Steinerova, J. "Seeking relevance in academic information use", *Information Research*, [Online], vol. 13, no. 4, paper 380. Available from: http://InformationR.net/ir/13-4/paper380.html, 2008, (RW 4789)

Steingold, S., Fournelle, C. & White, J.V. "Clustering and Threat Detection," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 828)

Stempel, J.D. "Error, Folly, and Policy Intelligence," *International Journal of Intelligence and Counterintelligence*, Vol. 12, No. 3, 1999, pp. 267-281. (RW 189)

Stempel, J.D. "The Impact of Religion on Intelligence," *International Journal of Intelligence and Counterintelligence*, Vol. 18, No. 2, 2005, pp. 280-295. (RW 321)

Stenbit, J.P. *A Conversation with the Assistant Secretary of Defense for C3I*, Center for Information Policy Research, Harvard University, Cambridge, MA, 2003. (RW 1153)

Stengel, L. *Using the "So What?" Factor in Analysis*, Available at: http://www.groupintel.com/2011/02/16/using-the-%E2%80%9Cso-what%E2%80%9D-factor-in-analysis/, 2011. (RW 4552)

Stephenson, B.W. & Hunt, C. "Intellectual and Ethical Development: A Dualistic Curriculum Intervention for College Students," *Counseling Psychologist*, Vol. 6, No. 4, 1977, pp. 39-42. (RW 5270)

Sternberg, R.J. "Component Processes in Analogical Reasoning," *Psychological Review*, Vol. 84, 1977, pp. 353. (RW 2396)

Sternberg, R.J. *Critical Thinking: Its Nature, Measurement, and Improvement*, Yale University, New Haven, CT, 1986. (RW 3632)

Sternberg, R.J. "Introduction," in *Teaching Thinking Skills: Theory and Practice*, eds. J.B. Baron & R.J. Sternberg, Freeman, New York, NY, 1987, pp. 1-5. (RW 3634)

Sternberg, R.J. "Questions and Answers about the Nature and Teaching of Thinking Skills," in *Teaching Thinking Skills: Theory and Practice*, eds. J.B. Baron & R.J. Sternberg, Freeman, New York, NY, 1987, pp. 252-259. (RW 3744)

Sternberg, R.J. "Teaching Intelligence: The Application of Cognitive Psychology to the Improvement of Intellectual Skills," in *Teaching Thinking Skills: Theory and Practice*, eds. J.B. Baron & R.J. Sternberg, Freeman, New York, NY, 1987, pp. 182-218. (RW 3742)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Sternberg, R.J. "Mental Self-Government: A Theory of Intellectual Styles and their Development," *Human Development,* Vol. 31, No. 4, 1988, pp. 197-224. (RW 5030)

Sternberg, R.J. *In Search of the Human Mind,* Harcourt Brace College Publishers, Fort Worth, 1995. (RW 3018)

Sternberg, R.J. *Thinking Styles*, Cambridge University Press, Cambridge, UK, 1997. (RW 2017)

Sternberg, R.J. "Epilogue: What do we Know about Tacit Knowledge? Making the Tacit Become Explicit," in *Tacit Knowledge in Professional Practice: Researcher and Practitioner Perspectives*, eds. R.J. Sternberg & J.A. Horvath, L. Erlbaum Associates, Mahwah, NJ, 1999, pp. 231-236. (RW 2762)

Sternberg, R.J. *Handbook of Creativity,* Cambridge University Press, Cambridge, U.K.; New York, 1999. (RW 2310)

Sternberg, R.J. "Epilogue: Another Mysterious Affair at Styles," in *Perspectives on Thinking, Learning, and Cognitive Styles*, eds. R.J. Sternberg & L. Zhang, L. Erlbaum Associates, Mahwah, NJ, 2001, pp. 249. (RW 3069)

Sternberg, R.J. *Wisdom, Intelligence, and Creativity Synthesized,* Cambridge University Press, Cambridge, UK, 2003. (RW 5413)

Sternberg, R.J. "What do we Know about the Nature of Reasoning?" in *The Nature of Reasoning*, eds. R.J. Sternberg & J.P. Leighton, Cambridge University Press, Cambridge, U.K.; New York, 2004, pp. 443. (RW 2387)

Sternberg, R.J. "The Domain Generality Versus Specificity Debate: How should it be Posed?" in *Creativity Across Domains: Faces of the Muse*, eds. J.C. Kaufman & J. Baer, L. Erlbaum Associates, Mahwah, NJ, 2005, pp. 299-306. (RW 5047)

Sternberg, R.J. "Intelligence," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 751-774. (RW 4014)

Sternberg, R.J. "Understanding Reasoning: Let's Describe What We Really Think About," *Behavioral and Brain Sciences,* Vol. 34, No. 5, 2011, pp. 269-270. (RW 5491)

Sternberg, R.J., Grigorenko, E.L. & Zhang, L. "Styles of Learning and Thinking Matter in Instruction and Assessment," *Perspectives on Psychological Science,* Vol. 3, No. 6, 2008, pp. 486-506. (RW 3052)

Sternberg, R.J. & Grigorenko, E.L. "A Capsule History of Theory and Research on Styles," in *Perspectives on Thinking, Learning, and Cognitive Styles*, eds. R.J. Sternberg & L. Zhang, L. Erlbaum Associates, Mahwah, NJ, 2001, pp. 1-21. (RW 3019)

Sternberg, R.J. & Jordan, J. *A Handbook of Wisdom: Psychological Perspectives,* University of Cambridge Press, Cambridge, UK, 2005. (RW 5414)

Sternberg, R.J., Lubart, T.I., Kaufman, J.C. & Pretz, J.E. "Creativity," in *The Cambridge Handbook of Thinking and Reasoning*, eds. K.J. Holyoak & R.G.J. Morrison, Cambridge University Press, New York, NY, 2005, pp. 351-370. (RW 4009)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Sternberg, R.J. & Wagner, R.K. *MSG Thinkg Styles Inventory* (RW 5275)

Steury, D.P. "Dissecting Soviet Analysis, 1946-50: How the CIA Missed Stalin's Bomb," *Studies in Intelligence*, Vol. 49, No. 1, 2005, pp. 19-26. (RW 310)

Stevens, A. *The Advanced Handbook of Methods in Evidence Based Healthcare*, SAGE Publications, Thousand Oaks, CA, 2001. (RW 2232)

Stevens, K.B. & Price, J.R. "Adult Reading Assessment: Are We Doing the Best With What We Have?" *Applied Neuropsychology*, Vol. 6, No. 2, 1999, pp. 68. (RW 3785)

Stevens-Rayburn, S. & Bouton, E.N. ""If It's Not on the Web, It Doesn't Exist at All": Electronic Information Resources - Myth and Reality," in *Library and Information Services in Astronomy III. ASP Conference Series*, eds. U. Grothkopf, H. Andernach, S. Stevens-Rayburn & M. Gomez, 1998, pp. 195-203. (RW 1541)

Stewart, G.M. "What is a Generalist?" *Studies in Intelligence*, Vol. 2, No. 3, 1958, pp. 1-6. (RW 576)

Stewart, T.A. *The Wealth of Knowledge: Intellectual Capital and the Twenty-First Century Organization*, Currency, New York, 2001. (RW 3819)

Stich, S.P. "Could Man be an Irrational Animal? Some Notes on the Epistemology of Rationality," *Synthese*, Vol. 64, No. 1, 1985, pp. 115-135. (RW 5828)

Stich, S.P. *The Fragmentation of Reason: Preface to a Pragmatic Theory of Cognitive Evaluation*, MIT Press, Cambridge, MA, 1990. (RW 5827)

Sticha, P.J. & Buede, D.M. "Cognitive Factors, Part II: What Analysts Need to Possess and how they Deal with Uncertainty," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 53. (RW 3642)

Sticha, P.J., Buede, D.M. & Rees, R.L. *It's the People Stupid: The Role of Personality and Situational Variables in Predicting Decisionmaker Behavior* 2006. (RW 2840)

Sticha, P., Buede, D. & Rees, R.L. "APOLLO: An Analytical Tool for Predicting a Subject's Decision Making," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 820)

Stickgold, R. & Walker, M.P. "Memory Consolidation and Reconsolidation: What is the Role of Sleep?" *Trends in Neuroscience*, Vol. 28, 2005, pp. 408. (RW 2121)

Stigall, S.M. "A Strategy Framework for the Intelligence Analyst," *Studies in Intelligence*, Vol. 56, No. 3, 2012, pp. 59-64. (RW 5900)

Stilwell, R. *Structure and Mechanisms for Command and Control*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1986. (RW 1039)

Stilwell, R.G. *Policy and National Command*, Center for Information Policy Research. Harvard University, Cambridge, MA, 1982. (RW 1040)

Stitts, B. "Intelligence Analysis and the Semantic Web: An Alternative Semantic Paradigm", *Proceedings of the Third International Ontology for the Intelligence Community Conference OIC-2008*, Fairfax, VA, December 3-4, 2008, pp. 54-56. (RW 4829)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Stix, G. *Homo (Sans) Sapiens: Is Dumb and Dumber our Evolutionary Destiny?* Available: http://blogs.scientificamerican.com/talking-back/2012/11/26/homo-sans-sapiens-is-dumb-and-dumber-our-evolutionary-destiny/, Viewed: December 6, 2012. (RW 5867)

Stojanovic, N. "On the Role of a User's Knowledge Gap in an Information Retrieval Process", *K-Cap '05*, Banff, Alberta, Canada, October 2-5, 2005, pp. 83. (RW 1534)

Stolovitch, H.D. *Training Ain't Performance,* ASTD Press, Alexandria, VA, 2004. (RW 4887)

Stolovitch, H.D. & Keeps, E.J. *Beyond Telling Ain't Training Fieldbook: Methods, Activities, and Tools for Effective Workplace Learning,* ASTD Press, Alexandria, VA, 2005. (RW 4888)

Stolovitch, H.D. & Keeps, E.J. *Beyond Telling Ain't Performance Fieldbook: Strategies, Tools, and Guidance for Effective Workplace Performance,* ASTD Press, Alexandria, VA, 2006. (RW 4889)

Stolovitch, H.D. & Keeps, E.J. *Telling Ain't Training,* ASTD Press, Alexandria, VA, 2011. (RW 4890)

Stone, A.B. *From the "Little Red Book" to the "Purple Book": Transforming Intelligence into a Profession One Page at a Time*, School of Advanced Military Studies, Ft. Leavenworth, KS, 2010. (RW 5679)

Stone, D.N. "Assumptions and Values in the Practice of Information Systems Evaluation," *Journal of Information Systems,* Vol. 4, No. 3, 1990, pp. 1. (RW 2537)

Stone, P.H. "Intelligence Failures Dent US Credibility," *National Journal,* Vol. 36, No. 10, 2004, pp. 732-733. (RW 219)

Stouder, M.D. *SMA Interagency Limited Objectives Experiment: Interagency Collaboration Case Study* 2009. (RW 3598)

Stout, M. "Emigre Intelligence Reporting: Sifting Fact from Fiction," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 253. (RW 2472)

Stoutenburg, S., Obrst, L., McCandless, D., Nichols, D., Franklin, P., Prausa, M. & Sward, R. "Ontologies for Rapid Integration of Heterogeneous Data for Command, Control, and Intelligence", *Proceedings of the Second International Ontology for the Intelligence Community Conference OIC-2007,* Columbia, MD, November 28-29, 2007, pp. 37-42. (RW 4820)

Strachan-Morris, D. "The Future of Civil-Military Intelligence Cooperation Based on Lessons Learned in Iraq," *Intelligence and National Security,* Vol. 24, No. 2, 2009, pp. 257. (RW 3492)

Strachan-Morris, D. "Threat and Risk: What is the Difference and Why does it Matter?" *Intelligence and National Security,* Vol. 27, No. 2, 2012, pp. 172-186. (RW 5612)

Straus, S.G., Parker, A.M. & Bruce, J.B. "The Group Matters: A Review of Processes and Outcomes in Intelligence Analysis," *Group Dynamics: Theory, Research, and Practice,* Vol. 15, No. 2, 2011, pp. 128-146. (RW 5463)

Strauss, A.L. & Corbin, J.M. *Basics of Qualitative Research: Grounded Theory Procedures and Techniques,* Sage Publications, Newbury Park, CA, 1990. (RW 2693)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Strayer, J.R. "The Role of the Consultant in Intelligence Estimates," *Studies in Intelligence*, Vol. 2, No. 4, 1958, pp. 1-5. (RW 568)

Streufert, S. "Complexity: An Integration of Theories," *Journal of Applied Social Psychology,* Vol. 27, No. 23, 1997, pp. 2068. (RW 3065)

Streufert, S. & Swezey, R.W. *Complexity, Managers, and Organizations,* Academic Press, Orlando, 1986. (RW 3046)

Strickland, A.A., Taber, C.S. & Lodge, M. "Motivated Reasoning and Public Opinion," *Journal of Health Politics, Policy and Law,* Vol. 36, No. 6, 2011, pp. 935-944. (RW 5454)

Strickland, F. & Whitlock, C. "The Next Four Years: Intelligence Community Reform - Refining Not Rebooting," *Business of Government,* Fall/Winter, 2012, pp. 58-61. (RW 5881)

Strickland, L.S. "Analytic Myopia, Data Disintegration and Homeland Insecurity," *Bulletin of the American Society for Information Science and Technology,* Vol. 30, No. 6, 2004, pp. 7-12. (RW 224)

Strike, K.A. & Posner, G.J. "A Revisionist Theory of Conceptual Change," in *Philosophy of Science, Cognitive Psychology, and Educational Theory and Practice,* eds. R.A. Duschl & R.J. Hamilton, State University of New York Press, Albany, 1992, pp. 147-176. (RW 5321)

Stroebel, J.T. *America in Vietnam - Part IV, 1968* (RW 473)

Strohman, T., Metzler, D., Turtle, H. & Croft, W.B. "Indri: A Language-Model Based Search Engine for Complex Queries," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 850)

Strømsø, H.I. & Braten, I. "The Role of Personal Epistemology in the Self-Regulation of Internet-Based Learning," *Metacognition and Learning,* Vol. 5, No. 1, 2010, pp. 91-111. (RW 4830)

Stromso, H.I., Braten, I. & Britt, M.A. "Do Students' Beliefs about Knowledge and Knowing Predict their Judgement of Texts' Trustworthiness?" *Educational Psychology,* Vol. 31, No. 2, 2011, pp. 177-206. (RW 5533)

Strong, K. *Men of Intelligence: A Study of the Roles and Decisions of Chiefs of Intelligence from World War I to the Present Day,* Cassell, London, UK, 1970. (RW 4566)

Studeman, W.O. *The Philosophy of Intelligence,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1991. (RW 1041)

Stuhlmacher, A.F. & Gillespie, T.L. "Managing Conflict in the Literature: Meta-Analysis as a Research Method," *International Negotiation,* Vol. 10, 2005, pp. 67. (RW 2249)

Stumpf, S.C. & McDonell, J.T. "Talking about Team Framing: Using Argumentation to Analyse and Support Experiential Learning in Early Design Episodes," *Design Studies,* Vol. 23, No. 1, 2002, pp. 5. (RW 2687)

Sturtevant, M. "Congressional Oversight of Intelligence: One Perspective," *American Intelligence Journal,* Summer, 1992 (RW 430)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Suarez, K.M. *The Structure of Problem Representation and Perceived Control: An Application and Extension of Causal Mapping,* 1991. (RW 2542)

Suchman, L.A. *Plans and Situated Actions: The Problem of Human-Machine Communication,* Cambridge University Press, Cambridge Cambridgeshire, 1987. (RW 2914)

Sugasawa, Y. "The Current State of Competitive Intelligence Activities and Competitive Awareness in Japanese Businesses," *Journal of Competitive Intelligence and Management,* Vol. 2, No. 4, 2004, pp. 7-31. (RW 590)

Sulimma, M. "Relations between Epistemological Beliefs and Culture Classifications," *Multicultural Education & Technology Journal,* Vol. 3, No. 1, 2009, pp. 74-89. (RW 5265)

Sullivan, D. *"Invisible Web" Revealed* 1999. (RW 1414)

Sullivan, D. *Invisible Web Gets Deeper* 2000. (RW 1416)

Sullivan, M. "Internal Recruiting for an Intelligence Analyst," *SCIP.online,* Vol. 1, No. 13, 2002 (RW 361)

Sundy, A. *Accountability: Process and Outcome Systems for Intelligence Analysts,* (RW 3710)

Sunstein, C.R. "Hazardous Heuristics," *University of Chicago Law Review,* Vol. 70, No. 2, 2003, pp. 751-782. (RW 223)

Sunstein, C.R. *Why Societies Need Dissent,* Harvard University Press, Cambridge, MA, 2003. (RW 2008)

Surowiecki, J. *The Wisdom of Crowds: Why the Many are Smarter than the Few and how Collective Wisdom Shapes Business, Economies, Societies and Nations,* Doubleday, New York, 2004. (RW 2009)

Sutherland, B. *Modern Warfare, Intelligence, and Deterrence: The Technologies that are Transforming them,* John Wiley & Sons, Hoboken, NJ, 2012. (RW 5525)

Sutherland, D. "Exploring Culture, Language and the Perception of the Nature of Science," *International Journal of Science Education,* Vol. 24, No. 1, 2002, pp. 1-25. (RW 5441)

Sutton, M. "Problem Representation, Understanding, and Learning Transfer: Implications for Technology Education," *Journal of Industrial Teacher Education,* Vol. 40, No. 4, 2003 (RW 2610)

Sutton, S.A. "The Role of Attorney Mental Models of Law in Case Relevance Determinations: An Exploratory Analysis," *Journal of the American Society for Information Science,* Vol. 45, No. 3, 1994, pp. 186. (RW 1323)

Sutton, S.W. *Unholy Matrimony: Marriage of Operations and Intelligence in C3I,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1990. (RW 1076)

Sveiby, K.E. *The New Organizational Wealth: Managing & Measuring Knowledge-Based Assets,* Berrett-Koehler Publishers, San Francisco, 1997. (RW 1309)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Svendsen, A.D.M. "The Globalization of Intelligence since 9/11: The Optimization of Intelligence Liaison Arrangements," *International Journal of Intelligence and Counterintelligence,* Vol. 21, No. 4, 2008, pp. 661. (RW 3250)

Svendsen, A.D.M. *Understanding the Globalization of Intelligence,* Palgrave Macmillan 2012. (RW 5856)

Swaka, K. "Strategic Intelligence: An Oxymoron," *Competitive Intelligence Magazine,* Vol. 7, No. 1, 2004, pp. 14. (RW 1685)

Swanson, D.R. "Information Retrieval as a Trial-and-Error Process," in *Key Papers in Information Science,* eds. B.C. Griffith & American Society for Information Science, Published for the American Society for Information Science by Knowledge Industry Publications, White Plains, NY, 1979, pp. 328. (RW 1356)

Swanson, D.R. "Undiscovered Public Knowledge," *Library Quarterly,* Vol. 56, No. 2, 1986, pp. 103. (RW 1388)

Swanson, D.R. "Historical Note: Information Retrieval and the Future of an Illusion," *Journal of the American Society for Information Science,* Vol. 39, 1988, pp. 92. (RW 1353)

Swanson, D.R., Smalheiser, N.R. & Bookstein, A. "Information Discovery from Complementary Literature: Categorizing Viruses as Potential Weapons," *Journal of the American Society for Information Science & Technology,* Vol. 52, 2001, pp. 797. (RW 2415)

Swanson, S. "Indications and Warning Post 9/11: Analysing Enemy Intent," *Military Intelligence Professional Bulletin,* Vol. 31, No. 3, 2005, pp. 38. (RW 4259)

Swartz, A.M. "Critical Thinking Attitudes and the Transfer Question," in *Thinking Skills Instruction: Concepts and Techniques,* eds. M. Heiman & J. Slomianko, National Education Association, Washington, DC, 1987, pp. 58-68. (RW 5028)

Swartz, R.J. "Restructuring what we Teach to Teach for Critical Thinking," in *Thinking Skills Instruction: Concepts and Techniques,* eds. M. Heiman & J. Slomianko, National Education Association, Washington, DC, 1987, pp. 111-118. (RW 5082)

Swartz, R.J. "Teaching for Thinking: A Developmental Model for the Infusion of Thinking Skills into Mainstream Instruction," in *Teaching Thinking Skills: Theory and Practice,* eds. J.B. Baron & R.J. Sternberg, Freeman, New York, NY, 1987, pp. 106-126. (RW 3738)

Swartz, R.J. "Making Good Thinking Stick: The Role of Metacognition, Extended Practice, and Teacher Modeling in the Teaching of Thinking," in *Thinking Across Cultures,* eds. D.M. Topping, D.C. Crowell & V.N. Kobayashi, L. Erlbaum Associates, Hillsdale, NJ, 1989, pp. 417-436. (RW 4985)

Swartz, R.J. & Perkins, D.N. *Teaching Thinking: Issues and Approaches,* Midwest Publications, Pacific Grove, CA, 1990. (RW 3872)

Sweet, L. & Glover, P. "Optimising the Follow-through Experience for Midwifery Learning," in *Developing Learning Professionals,* eds. S. Billett & A. Henderson, Springer, Dordrecht, 2011, pp. 83-100. (RW 4904)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Sweetnam, M.S. *Testimony before the House Permanent Select Committee on Intelligence* 2005. (RW 1342)

Sweller, J. "Cognitive Load during Problem Solving: Effects of Learning," *Cognitive Science,* Vol. 12, 1988, pp. 257. (RW 2162)

Swenson, R.G. "Meeting the Intelligence Community's Continuing Need for an Intelligence Literature," in *Learning with Professionals: Selected Works from the Joint Military Intelligence College*, eds. J.E. Lightfoot, J.S. Major, S.E. Brownfeld & Center for Strategic Intelligence Research, Center for Strategic Intelligence Research, Joint Military Intelligence College, Washington, DC, 2005, pp. 1. (RW 2966)

Swenson, R.G. *Bringing Intelligence about: Practitioners Reflect on Best Practices,* Joint Military Intelligence College, Center for Strategic Intelligence Research, Washington, DC, 2003. (RW 660)

Swenson, R.G. "Intelligence Education in the Americas," *International Journal of Intelligence and Counterintelligence*, Vol. 16, No. 1, 2003, pp. 108-130. (RW 444)

Swenson, R.G. & Lemozy, S.C. *Intelligence Professionalism in the Americas = Profesionalismo De Inteligencia En Las Americas,* Joint Military Intelligence College, Washington, DC, 2003. (RW 916)

Swenson, R.G. & Lemozy, S.C. *Intelligence Professionalism in the Americas,* Joint Military Intelligence College, Washington, DC, 2004. (RW 915)

Swetnam, M. *Revolution in Intelligence Affairs: Transforming Intelligence for Emerging Challenges [Powerpoint Presentation]* 2004. (RW 1311)

Sylvan, D.A. *Psychology and Communication in Intelligence Analysis. Instructional Block Outline* [undated]. (RW 4049)

Sylvan, D.A., Grove, A. & Martinson, J. "Problem Representation and Conflict Dynamics in Northern Ireland and the Middle East: Domestic Political Processes with International Impact," *Foreign Policy Analysis*, Vol. 1, No. 3, 2005, pp. 249. (RW 1610)

Sylvan, D.A. & Haddad, D.M. "Reasoning and Problem Representation in Foreign Policy: Groups, Individuals, and Stories," in *Problem Representation in Foreign Policy Decision Making*, eds. D.A. Sylvan & J.F. Voss, 1998, (RW 1649)

Sylvan, D.A. & Haddad, D.M. "Reasoning and Problem Representation in Foreign Policy: Groups, Individuals, and Stories," in *Problem Representation in Foreign Policy Decision Making*, eds. D.A. Sylvan & J.F. Voss, 1998, pp. 187-212. (RW 1651)

Sylvan, D.A., Ostrom, T.M. & Gannon, K. "Case-Based, Model-Based, and Explanation-Based Styles of Reasoning in Foreign Policy," *International Studies Quarterly,* Vol. 38, No. 1, 1994, pp. 61-90. (RW 1337)

Sylvan, D.A. & Thorson, S.J. "Ontologies, Problem Representations, and the Cuban Missile Crisis," *Journal of Conflict Resolution,* Vol. 36, 1992, pp. 709. (RW 1609)

Sylvan, D.A. & Voss, J.F. *Problem Representation in Foreign Policy Decision Making,* Cambridge University Press, Cambridge, UK, 1998. (RW 1618)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Szanton, P. & Allison, G. "Intelligence: Seizing the Opportunity," *Foreign Policy*, 22, 1976, pp. 183. (RW 1259)

Szpunar, K.K., Watson, J.M. & McDermott, K.B. "Neural Substrates of Envisioning the Future," *Proceedings of the National Academy of Sciences*, Vol. 104, No. 2, 2007, pp. 642. (RW 1905)

Tabak, I. & Weinstock, M. "A Sociocultural Exploration of Epistemological Beliefs," in *Knowing, Knowledge and Beliefs: Epistemological Studies Across Diverse Cultures*, ed. M.S. Khine, Springer, Dordrecht, 2008, pp. 177-195. (RW 5071)

Taber, C.S. & Lodge, M. "Motivated Skepticism in the Evaluation of Political Beliefs," *American Journal of Political Science*, Vol. 50, 2006, pp. 755. (RW 3459)

Taber, C.S. *Computational Modeling in Foreign Policy Analysis*, Stony Brook University, Stony Brook, NY, [undated]. (RW 5725)

Taber, C.S. "Political Dogmatism," *Critical Review*, Vol. 20, No. 4, 2008, pp. 481-498. (RW 5457)

Taber, C.S., Cann, D. & Kucsova, S. "The Motivated Processing of Political Arguments," *Political Behavior*, Vol. 31, No. 2, 2009, pp. 137-155. (RW 5456)

Takir, S. *Open Source Intelligence Analysis: A Methodological Approach*, 2009. (RW 4503)

Taleb, N.N. *The Black Swan: Why Don't we Learn that we Don't Learn?* [draft] 2004. (RW 276)

Talmi, D. & Frith, C. "Feeling Right about Doing Right," *Nature*, Vol. 446, No. 19, 2007, pp. 865. (RW 2296)

Tam, C.K. *Behavioral and Psychosocial Considerations in Intelligence Analysis: A Preliminary Review of Literature on Critical Thinking Skills*, AFRL-RH-AZ-TR-1009-0009, Air Force Research Laboratory, Mesa, AZ, 2009. (RW 3834)

Tammen, R.L. *MIRV and the Arms Race: An Interpretation of Defense Strategy*, Praeger, New York, 1973. (RW 635)

Tang, R. & Solomon, P. "Towards an Understanding of the Dynamics of Relevance Judgment: An Analysis of One Person's Search Behavior," *Information Processing and Management*, Vol. 34, 1998, pp. 237. (RW 1548)

Tang, R. *Use of Relevance Criteria Across Stages of Document Evaluation: A Micro Level and Macro Level Analysis*, Ph.D. dissertation, University of North Carolina at Chapel Hill, 1999. (RW 1547)

Tanji, M. *Why Intelligence Reform Matters* 2007. (RW 2882)

Tapscott, D. & Williams, A.D. *Wikinomics: How Mass Collaboration Changes Everything*, Portfolio, New York, 2008. (RW 3120)

Task Force on the Future of U. S. Intelligence *Making Intelligence Smarter: The Future of U. S. Intelligence: A Report of an Independent Task Force*, Council on Foreign Relations. Available: http://www.fas.org/irp/cfr.html, Viewed: December 30, 2009. (RW 3809)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Taube, K.T. "Critical Thinking Ability and Disposition as Factors of Performance on a Written Critical Thinking Test", *Annual Meeting of the American Educational Research Association,* San Francisco, CA, April 18-22, 1995 (RW 4079)

Tauer, J.M. & Harackiewicz, J.M. "The Effects of Cooperation and Competition on Intrinsic Motivation and Performance," *Journal of Personality and Social Psychology,* Vol. 86, No. 6, 2004, pp. 849-861. (RW 1922)

Tavris, C. & Aronson, E. *Mistakes Were Made (but Not by Me): Why we Justify Foolish Beliefs, Bad Decisions, and Hurtful Acts,* Harcourt, Orlando, FL, 2007. (RW 2502)

Taylor, A. "User Relevance Criteria Choices and the Information Search Process," *Information Processing and Management,* Vol. 48, No. 1, 2012, pp. 136-153. (RW 5220)

Taylor, C. *The Ethics of Authenticity,* Harvard University Press, Cambridge, MA, 1991. (RW 2305)

Taylor, R.N. "Nature of Problem Ill-Structuredness: Implications for Problem Formulation and Solution," *Decision Sciences,* Vol. 5, 1974, pp. 632. (RW 2769)

Taylor, S.M. *Full Paper Follow Up to the several Worlds of the Intelligence Analyst* (RW 3726)

Taylor, S.M. "The several Worlds of the Intelligence Analyst," 2005 *International Conference on Intelligence Analysis,* McLean, VA, May 2-6, 2005 (RW 599)

Taylor, S.A. "Counterintelligence Failures in the United States," in *Handbook of Intelligence Studies,* ed. L.K. Johnson, 2007, pp. 237. (RW 2471)

Taylor, S.A. & Goldman, D. "Intelligence Reform: Will More Agencies, Money, and Personnel Help?" *Intelligence and National Security,* Vol. 19, No. 3, 2004, pp. 416-435. (RW 328)

Taylor, S.A. & Ralston, T.J. "The Role of Intelligence in Crisis Management," in *Avoiding War: Problems of Crisis Management,* ed. A.L. George, Westview Press, Boulder, CO, 1991, pp. 395-412. (RW 14)

Tecuci, G. & Boicu, M. *Agent Learning for Mixed-Initiative Knowledge Acquisition,* Air Force Office of Scientific Research, Arlington, VA, 2010. (RW 4749)

Tecuci, G., Boicu, M., Ayers, C. & Cammons, D. *Personal Cognitive Assistants for Military Intelligence Analysis: Mixed-Initiative Learning, Tutoring, and Problem Solving* (RW 2174)

Tecuci, G., Boicu, M. & Ayers, C. *Cognitive Assistants for the Analysts [Powerpoint Presentation]* 2006. (RW 2168)

Tecuci, G., Boicu, M., Marcu, D., Boicu, C. & Barbulescu, M. "Cognitive Assistants for Analysts," in *Proteus Futures Digest: A Compilation of Selected Works Derived from the 2006 Proteus Workshop,* eds. J. Auger & W. Wimbish, US Army War College, Carlisle Barracks, PA, 2006, pp. 303-330. (RW 4756)

Tecuci, G., Boicu, M., Marcu, D., Schum, D. & Hamilton, B. "TIACRITIS System and Textbook: Learning Intelligence Analysis through Practice", *Fifth International Conference on Semantic Technology for Intelligence, Defense, and Security,* Fairfax, VA, October 26-29, 2010 (RW 4752)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Tecuci, G., Boicu, M., Schum, D. & Marcu, D. *Coping with the Complexity of Intelligence Analysis: Cognitive Assistants for Evidence-Based Reasoning,* Research Report No. 7, George Mason University, Fairfax, VA, 2010. (RW 5602)

Tecuci, G., Schum, D., Boicu, M., Marcu, D. & Hamilton, B. "Intelligence Analysis as Agent-Assisted Discovery of Evidence, Hypotheses and Arguments," in *Advances in Intelligent Decision Technologies,* eds. G. Phillips-Wren, L.C. Jain, K. Nakamatsu & R.J. Howlett, 2010, pp. 1-10. (RW 4748)

Tecuci, G., Schum, D., Boicu, M., Marcu, D., Hamilton, B. & Wible, B. "Teaching Intelligence Analysis with TIACRITIS," *American Intelligence Journal,* Vol. 28, No. 2, 2010, pp. 50-65. (RW 4616)

Tecuci, G., Schum, D., Boicu, M., Marcu, D. & Russell, K. "Computational Theory and Cognitive Assistant for Intelligence Analysis", *The Sixth International Conference on Semantic Technologies for Intelligence, Defense, and Security - STIDS,* Fairfax, VA, November 17, 2011, [unpaged]. (RW 5508)

Teevan, J. "How People Recall, Recognize, and Reuse Search Results," *ACM Transactions on Information Systems,* Vol. 26, No. 4 article 19, 2008 (RW 4400)

Teevan, J., Cuttrell, E., Fisher, D., Drucker, S.M., Ramos, G., Andre, P. & Hu, C. "Visual Snippets: Summarizing Web Pages for Search and Revisitation", *Proceedings of the 27th International Conference on Human Factors in Computing Systems,* Boston, MA, April 4-9, 2009, pp. 2023. (RW 4401)

Teitelbaum, L. *The Impact of the Information Revolution on Policymakers' Use of Intelligence Analysis,* Doctor of Public Policy Analysis dissertation, RAND Graduate School, 2004. (RW 4529)

Teitelbaum, L. *The Impact of the Information Revolution on Policymakers' use of Intelligence Analysis,* Pardee RAND Graduate School, 2005. (RW 375)

Tellis, A.J., Szayna, T.S. & Winnefeld, J.A. *Anticipating Ethnic Conflict,* RAND Corp, Santa Monica CA, 1997. (RW 4530)

Tenet, G.J. "The CIA and the Security Challenges of the New Century," *International Journal of Intelligence and Counterintelligence,* Vol. 13, No. 2, 2000, pp. 133-143. (RW 426)

Tenopir, C. "Online Scholarly Journals: How Many?" *Library Journal,* February 1, 2004 (RW 1565)

Tenopir, C. & Barry, J. "Are Online Companies Dinosaurs?" *Library Journal,* May 15, 2000 (RW 1564)

Tenopir, C. & King, D.W. *Communication Patterns of Engineers,* IEEE Press, Piscataway, NJ, 2004. (RW 248)

Tetlock, P.E. & Mellers, B.A. "Intelligent Management of Intelligence Agencies: Beyond Accountability Ping-Pong," *American Psychologist,* Vol. 66, No. 6, 2011, pp. 542-554. (RW 5476)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Tetlock, P.E. & Mitchell, G. "Adversarial Collaboration Aborted, but our Offer Still Stands," *Research in Organizational Behavior*, Vol. 29, 2009, pp. 77-79. (RW 5575)

Tetlock, P. *Expert Political Judgment: How Good is it? How Can We Know?* Princeton University Press, Princeton, NJ, 2005. (RW 769)

Tetlock, P.E. "Social Psychology and World Politics. Draft of Chapter." in *Handbook of Social Psychology*, eds. D. Gilbert, S.T. Fiske & G. Lindsay, Fourth ed., [undated], (RW 390)

Tetlock, P.E. "The Impact of Accountability on Judgment and Social Choice: Toward a Social Contingency Model," in *Advances in Experimental Social Psychology*, ed. M.P. Zanna, 1992, pp. 331. (RW 2155)

Tetlock, P.E. "Close-Call Counterfactuals and Belief-System Defenses: I was Not almost Wrong but I was almost Right," *Journal of Personality and Social Psychology*, Vol. 75, No. 3, 1998, pp. 639-652. (RW 1940)

Tetlock, P.E. "Theory-Driven Reasoning about Plausible Pasts and Probable Futures in World Politics: Are we Prisoners of our Preconceptions?" *American Journal of Political Science*, Vol. 43, No. 2, 1999, pp. 335-366. (RW 906)

Tetlock, P.E. "The Learning Organization," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 319. (RW 3654)

Tetlock, P.E. & Lebow, R.N. "Poking Counterfactual Holes in Covering Laws: Cognitive Styles and Historical Reasoning," *The American Political Science Review*, Vol. 95, No. 4, 2001, pp. 829-843. (RW 1941)

Tetlock, P.E. & Mellers, B.A. "The Great Rationality Debate," *Psychological Science*, Vol. 13, No. 1, 2002, pp. 94-99. (RW 1936)

Tetlock, P.E. & Mellers, B.A. "Structuring Accountability Systems in Organizations: Key Trade-Offs and Critical Unknowns," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, pp. 249-270. (RW 4780)

Tetlock, P.E., Peterson, R.S., McGuire, C., Chang, S. & Feld, P. "Assessing Political Group Dynamics: A Test of the Groupthink Model," *Journal of Personality and Social Psychology*, Vol. 63, No. 3, 1992, pp. 403-425. (RW 1930)

Tett, R.P., Hopper, J.E., Landis, B.D. & Swaim, B.C. "Personality, Motivations, and Attitudes," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, CENTRA Technology, Burlington, MA, [in press], pp. 106-144. (RW 3645)

Thagard, P. "Internet Epistemology: Contributions of New Information Technologies to Scientific Research," in *Designing for Science: Implications from Everyday, Classroom, and Professional Settings*, eds. K.D. Crowley, C.D. Schunn & T. Okada, 2001, pp. 465. (RW 3943)

Thaler, R. *Thaler's Question: An Edge Special Event*, Available: http://edge.org/3rd_culture/thaler10/thaler10_index.html#shubin, Viewed: May 18, 2011. (RW 4839)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Thibault, G. "Perspectives on Intelligence," *Air University Review,* Vol. 33, No. 6, 1982, pp. 108-111. (RW 1048)

Thiele, L.P. *The Heart of Judgment: Practical Wisdom, Neuroscience, and Narrative,* 2006. (RW 1723)

Thielmann, G. "Rumsfeld Reprise? The Missile Report that Foretold the Iraq Intelligence Controversy," *Arms Control Today,* July-August, 2003, pp. 3. (RW 1325)

Thomas, D. "US Military Intelligence Analysis: Old and New Challenges," in *Analyzing Intelligence: Origins, Obstacles, and Innovations*, eds. R.Z. George & J.B. Bruce, 2008, pp. 138. (RW 3101)

Thomas, J., Pennock, K., Fiegel, T., Wise, J., Pottier, M., Schur, A., Lantrip, D. & Crow, V. "The Visual Analysis of Textual Information: Browsing Large Document Sets", *DL '95 Conference,* Washington, DC, May 15-19, 1995 (RW 1199)

Thomas, J.J. & Cook, K.A. *Illuminating the Path: The Research and Development Agenda for Visual Analytics. Chapter 2. The Science of Analytical Reasoning.* 2007. (RW 2179)

Thomas, J.J. & Cook, K.A. *Illuminating the Path: The Research and Development Agenda for Visual Analytics. Executive Summary.* 2007. (RW 2178)

Thomas, S.T. "Assessing Current Intelligence Studies," *Intelligence and National Security,* Vol. 2, No. 2, 1988, pp. 239. (RW 1573)

Thomas, S.T. "Intelligence Production and Consumption: A Framework of Analysis," in *Intelligence: Policy and Process*, eds. A.C. Maurer, M.D. Tunstall & J.M. Keagle, Westview Press, Boulder, CO, 1985, pp. 125-139. (RW 1218)

Thomas, S.T. "A Political Theory of the CIA," *International Journal of Intelligence and Counterintelligence,* Vol. 11, No. 1, 1998, pp. 57-72. (RW 43)

Thomas, S.T. "Hidden in Plain Sight: Searching for the CIA's "New Missions"," *International Journal of Intelligence and Counterintelligence,* Vol. 13, No. 2, 2000, pp. 144-159. (RW 439)

Thompson, A. "Teachers' Beliefs and Conceptions: A Synthesis of the Research," in *Handbook of Research on Mathematics Teaching and Learning*, ed. D.A. Grouws, Macmillan, New York, 1992, pp. 127-146. (RW 4990)

Thompson, C. "Meet the Life Hackers," *New York Times Magazine,* October 16, 2003, 2003, pp. 40. (RW 1332)

Thompson, C. "Open-Source Spying," *New York Times,* December 3, 2006 (RW 1768)

Thompson, J.R., Hopf-Weichel, R. & Geiselman, R.E. *The Cognitive Bases of Intelligence Analysis,* Research Report 1362, U. S. Army Research Institute for the Behavioral and Social Sciences, Alexandria, VA, 1984. (RW 262)

Thompson, L.L., Levine, J.M. & Messick, D.M. *Shared Cognition in Organizations: The Management of Knowledge,* L. Erlbaum Associates, Mahwah, NJ, 1999. (RW 2119)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Thompson, L.L., Mannix, E.A. & Bazerman, M.H. "Group Negotiation: Effects of Decision Rule, Agenda, and Aspiration," *Journal of Personality and Social Psychology,* Vol. 54, No. 1, 1988, pp. 86-95. (RW 1929)

Thompson, L.B. *Pentagon Threat Matrix: Wrong again. Issue Brief*, Lexington Institute, Arlington, VA, 2004. (RW 618)

Thompson, P., Santos, E., Zhao, Q., Johnson, G. & Nguyen, H. "Counter Denial and Deception and Utility-Theoretic Information Retrieval for Intelligence Analysis," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 834)

Thompson, V.A., Newstead, S.E. & Morley, N.J. "Methodological and Theoretical Issues in Belief Bias: Implications for Dual-Process Theories," in *The Science of Reason: A Festschrift for Jonathan St. B.T. Evans*, eds. K.I. Manktelow, D.E. Over & S. Elqayam, Psychology Press, Hove, East Sussex, UK, 2011, pp. 309-337. (RW 5712)

Thomson, A. *Critical Reasoning: A Practical Introduction,* 2nd ed., Routledge, London, UK, 2002. (RW 3938)

Thong, J.Y.L., Hong, W.Y. & Tam, K.Y. "Understanding User Acceptance of Digital Libraries: What are the Roles of Interface Characteristics, Organizational Context, and Individual Differences?" *International Journal of Human-Computer Studies,* Vol. 57, No. 3, 2002, pp. 215. (RW 2356)

Thorne, S. "Data Analysis in Qualitative Research," *Evidence-Based Nursing,* Vol. 3, 2000, pp. 68. (RW 1774)

Thorne, S., Jensen, L., Kearney, M., Noblit, G. & Sandelowski, M. "Qualitative Metasynthesis: Reflections on Methodological Orientation and Ideological Agenda," *Qualitative Health Research,* Vol. 14, No. 10, 2004, pp. 1342. (RW 2237)

Thornlow, C.C. *Fusing Intelligence with Law Enforcement Information: An Analytic Imperative* 2005. (RW 2994)

Thornton, H. "Dispositions in Action: Do Dispositions make a Difference in Practice?" *Teacher Education Quarterly,* Vol. 33, No. 2, 2006, pp. 53-68. (RW 5177)

Thorson, M. *Content and Technology Integration [Powerpoint Presentation]* 2004. (RW 1508)

Thouless, R.H. *Straight and Crooked Thinking*, Pan Books Ltd., London, UK, 1953. (RW 4467)

Thuraisingham, B., Khan, L., Kantarcioglu, M., Chib, S., Han, J. & Son, S. "Real-Time Knowledge Discovery and Dissemination for Intelligence Analysis", *Proceedings of the 42nd Hawaii International Conference on System Sciences,* 2009 (RW 4243)

Thurn, M. "Semantics for Information Sharing and Discovery in the Intelligence Community", *Proceedings of the Third International Ontology for the Intelligence Community Conference OIC-2008,* Fairfax, VA, December 3-4, 2008, pp. 13-15. (RW 4825)

Tichy, G. *Over-Optimism among Experts in Assessment and Foresight,* ITA-02-05, Austrian Academy of Sciences, Vienna, Austria, 2002. (RW 1122)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Tidd, J.M. "From Revolution to Reform: A Brief History of US Intelligence," *SAIS Review*, Vol. 28, No. 1, 2008, pp. 5. (RW 3324)

Tidline, T.J. "Dervin's Sense-Making," in *Theories of Information Behavior*, eds. K.E. Fisher, S. Erdelez & L. McKechnie, Published for the American Society for Information Science and Technology by Information Today, Medford, N.J, 2005, pp. 113. (RW 3604)

Tidwell, W.A. "Horrible Thought," *Studies in Intelligence*, Vol. 2, No. 1, 1958, pp. 65-70. (RW 531)

Tierney, R.J., Soter, A., O'Flahavan, J.F. & McGinley, W. "The Effects of Reading and Writing upon Thinking Critically," *Reading Research Quarterly*, Vol. 24, No. 2, 1989, pp. 134-173. (RW 2846)

Tillers, P. *The Dynamic Evidence Page*, Available: http://tillers.net/home.html, Viewed: June 6, 2006. (RW 1501)

Tillers, P. & Schum, D. "A Theory of Preliminary Fact Investigation," *UC Davis Law Review*, Vol. 24, No. 4, 1991, pp. 931-1012. (RW 4116)

Tinapple, D. & Woods, D.D. "Message Overload from the Inbox to Intelligence Analysis: How Spam and Blogs Point to New Tools", *Human Factors and Ergonomics Society Annual Meeting Proceedings, Cognitive Engineering and Decision Making*, pp. 419-423. (RW 1945)

Tindale, R.S., Kameda, T. & Hinsz, V.B. "Group Decision Making," in *The Sage Handbook of Social Psychology*, eds. M.A. Hogg & J. Cooper, Sage, London; Thousand Oaks, CA, 2003, pp. 381. (RW 2048)

Tindale, R.S., Meisenhelder, H.M., Dykema-Engblade, A.A. & Hogg, M.A. "Shared Cognition in Small Groups," in *Blackwell Handbook of Social Psychology: Group Processes*, eds. M.A. Hogg & R.S. Tindale, Blackwell Publishers, Malden, Mass, 2003, pp. 1. (RW 2118)

Tinsley, C.H. "Social Categorization and Intergroup Dynamics," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, pp. 197-223. (RW 4778)

Tinsley, Y. *Juror Decision-Making: A Look Inside the Jury Room* 2001. (RW 2057)

Tishman, S., Jay, E. & Perkins, D.N. "Teaching Thinking Dispositions: From Transmission to Enculturation," *Theory into Practice*, Vol. 32, No. 3, 1993, pp. 147-153. (RW 2887)

Tishman, S. "What Makes a Good Thinker? A Look at Thinking Dispositions," *Harvard Graduate School of Education Alumni Bulletin*, Vol. 39, No. 1, 1994, pp. 7-9. (RW 4066)

Tishman, S. "Added Value: A Dispositional Perspective on Thinking," in *Developing Minds: A Resource Book for Teaching Thinking*, ed. A.L. Costa, 3rd ed., Association for Supervision and Curriculum Development, Alexandria, VA, 2001, pp. 72-75. (RW 5171)

Tishman, S. "Added Value: A Dispositional Perspective on Thinking," in *Developing Minds: A Resource Book for Teaching Thinking*, ed. A.L. Costa, 3rd ed., Association for Supervision and Curriculum Development, Alexandria, VA, 2001, pp. 72-75. (RW 5253)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Todd, P. & Bloch, J. *Global Intelligence: The World's Secret Services Today,* Bangladesh University Press, Bangkok, Thailand, 2003. (RW 1195)

Tollinger, I.V., Schunn, C.D. & Vera, A.H. "What Changes when a Large Team Becomes More Expert? Analyses of Speedup in the Mars Exploration Rovers Science Planning Process", *Proceedings of the 28th Annual Conference of the Cognitive Science Society,* July 26-29, 2006, pp. 840. (RW 1986)

Tomlinson, W.B. "Chinese Industry from the Air," *Studies in Intelligence,* Vol. 11, No. 2, 1967, pp. 37-50. (RW 525)

Tomme, E.B. "Emphasizing Effect Over Domain: Merging Three Organizations to Enhance the Efficacy of our Nation's Intelligence Production," *Air & Space Power Journal,* Spring, 2009 (RW 3428)

Tooby, J. & Cosmides, L. "Conceptual Foundations of Evolutionary Psychology," in *Handbook of Evolutionary Psychology,* ed. D.M. Buss, 2005, pp. 5. (RW 3348)

Topiak, M.E., West, R.F. & Stanovich, K.E. "The Cognitive Reflection Test as a Predictor of Performance on Heuristics-and-Biases Tasks," *Memory & Cognition,* Vol. 39, No. 7, 2011, pp. 1275-1289. (RW 5023)

Toplak, M.E., Sorge, G.B., Benoit, A., West, R.F. & Stanovich, K.E. "Decision-Making and Cognitive Abilities: A Review of Associations between Iowa Gambling Task Performance, Executive Functions, and Intelligence," *Clinical Psychology Review,* Vol. 30, No. 5, 2010, pp. 562-581. (RW 5423)

Toplak, M. & Stanovich, K.E. "The Domain Specificity and Generality of Disjunctive Reasoning: Searching for a Generalizable Critical Thinking Skill," *Journal of Educational Psychology,* Vol. 94, No. 1, 2001, pp. 197-209. (RW 3858)

Topping, D.M., Crowell, D.C. & Kobayashi, V.N. *Thinking Across Cultures,* L. Erlbaum Associates, Hillsdale, NJ, 1989. (RW 2412)

Torff, B. & Sternberg, R.J. "Changing Mind, Changing World: Practical Intelligence and Tacit Knowledge in Adult Learning," in *Adult Learning and Development: Perspectives from Educational Psychology,* eds. M.C. Smith & T. Pourchot, L. Erlbaum Associates, Mahwah, NJ, 1998, pp. 109. (RW 4266)

Torrance, H. "Systematic Reviewing - the 'Call Centre' Version of Research Synthesis. Time for a More Flexible Approach", *ESRC/RCBN Seminar on Systematic Reviewing,* University of Sheffield, June 24, 2004 (RW 2255)

Torrance, M. "Is Writing Expertise Like Other Kinds of Expertise?" in *Theories, Models and Methodology in Writing Research,* eds. G. Rijlaarsdam, H. van den Bergh & M. Couzijn, Amsterdam University Press, Amsterdam, 1996, pp. 3. (RW 2129)

Torrance, M. "Strategies for Familiar Writing Tasks: Case Studies of Undergraduates Writing Essays," in *Theories, Models and Methodology in Writing Research,* eds. G. Rijlaarsdam, H. van den Bergh & M. Couzijn, Amsterdam University Press, Amsterdam, 1996, pp. 283. (RW 2135)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Torrance, M. & Galbraith, D. *Knowing what to Write: Conceptual Processes in Text Production,* Amsterdam University Press, Amsterdam, 1999. (RW 1845)

Torrance, M., Thomas, G.V. & Robinson, E.J. "Finding Something to Write about: Strategic and Automatic Processes in Idea Generation," in *The Science of Writing: Theories, Methods, Individual Differences, and Applications*, eds. C.M. Levy & S.E. Ransdell, 1996, pp. 189. (RW 1824)

Torvik, V.I., Weeber, M., Swanson, D.R. & Smalheiser, N.R. "A Probabilistic Similarity Metric for MEDLINE Records: A Model for Author Name Disambiguation," *Journal of the American Society for Information Science & Technology,* Vol. 56, No. 2, 2005, pp. 140. (RW 2416)

Tough, P. *How Children Succeed: Grit, Curiosity, and the Hidden Power of Character,* Houghton Mifflin Harcourt, Boston, MA, 2012. (RW 5855)

Toulmin, S.E. *The Uses of Argument,* Cambridge University Press, Cambridge, UK, 2003. (RW 2806)

Train, E.L. "Naval Intelligence Training: Contributing to Today's Fight while Shaping for the Future," *American Intelligence Journal,* Vol. 26, No. 2, 2008/2009, pp. 18-24. (RW 3626)

Trautwein, U. & Luedtke, O. "Epistemological Beliefs, School Achievement, and College Major: A Large Scale Longitudinal Study on the Impact of Certainty Beliefs," *Contemporary Educational Psychology,* Vol. 32, No. 3, 2007, pp. 348-366. (RW 5332)

Travers, R. "The Coming Intelligence Failure," *Studies in Intelligence,* Vol. 40, No. 2, 1996 (RW 114)

Travers, R.E. "Failures, Fallacies, and Fixes: Posturing Intelligence for the Challenges of Globalization," in *The Intelligence Archipelago: The Community's Struggle to Reform in the Globalized Era*, eds. M.M.H. Gutjahr & Joint Military Intelligence College, 2005, pp. xi. (RW 1571)

Treffert, D.A. & Christensen, D.D. "Inside the Mind of a Savant," *Scientific American,* Vol. 293, No. 6, 2005, pp. 108. (RW 3146)

Treffinger, D.J., Isaksen, S.G. & Dorval, K.B. *Creative Problem Solving (CPS Version 6.1): A Contemporary Framework for Managing Change* (RW 2621)

Treffinger, D.J., Isaksen, S.G. & Dorval, K.B. "Creative Problem Solving: An Overview," in *Problem Finding, Problem Solving, and Creativity,* ed. M.A. Runco, Ablex Pub. Corp., Norwood, NJ, 1994, pp. 223. (RW 2745)

Treffinger, D.J., Isaksen, S.G. & Stead-Dorval, K.B. *Creative Problem Solving: An Introduction,* 4th ed., Prufrock Press, Waco, TX, 2005. (RW 2584)

Trent, S.A. *Team Cognition in Intelligence Analysis Training,* Ph.D. dissertation, Ohio State University, 2007. (RW 3582)

Trent, S.A., Grossman, J., Patterson, E., Scherbarth, M., Voshell, M., Schoenwald, J., Goldstein, S. & Tittle, J. *Federated Observational Research: A Unique Investigation Strategy for the Study of Distributed Cognition* 2007. (RW 2276)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Trent, S.A., Patterson, E. & Woods, D.D. *Challenges for Cognition in Intelligence Analysis* 2007. (RW 2277)

Trent, S., Voshell, M. & Patterson, E. "Team Cognition in Intelligence Analysis", *Proceedings of the Human Factors and Ergonomics Society 51st Meeting*, pp. 308. (RW 3578)

Treverton, G.F. *Approaches to "Outreach" for Intelligence,* Swedish National Defence College, Stockholm, Sweden, 2009. (RW 4604)

Treverton, G.F. "Estimating Beyond the Cold War," *Defense Intelligence Journal,* Vol. 3, No. 2, 1994, pp. 5-20. (RW 181)

Treverton, G.F. "9/11 Before & After: Asking what Government Can Do for Us," *San Francisco Chronicle,* December 30, 2001. (RW 1293)

Treverton, G.F. "Intelligence - a Scenario Too Far. Failure of American Imagination," *San Francisco Chronicle,* November 25, 2001. (RW 1251)

Treverton, G.F. "Intelligence Crisis", *Government Executive,* [Online], Available from: http://www.govexec.com/features/1101/1101s1.htm, 2001. (RW 333)

Treverton, G.F. *Reshaping National Intelligence for an Age of Information,* Cambridge University Press, Cambridge, UK, 2001. (RW 26)

Treverton, G.F. *Reshaping National Ntelligence for an Age of Information [Powerpoint Presentation]* 2001. (RW 1456)

Treverton, G.F. "Intelligence: The Achilles Heel of the Bush Doctrine," *Arms Control Today,* Vol. 33, No. 6, 2003, pp. 9-11. (RW 198)

Treverton, G.F. *Reshaping Intelligence to Share with "Ourselves",* Commentary No. 82, Canadian Security Intelligence Service, Ottawa, ON, 2003. (RW 605)

Treverton, G.F. "As the Third Anniversary of the 9/11 Attacks Approaches, it's Becoming Clear that the Fight Against Terrorism has been a Story of...Missed Opportunities. We Anticipate Enemy Moves with a Great Deal of Hype," *San Francisco Chronicle,* September 5, 2004. (RW 1294)

Treverton, G.F. "Intelligence - a Funhouse of Reflections," *San Francisco Chronicle,* February 15, 2004, (RW 1250)

Treverton, G.F. "Use History to Reshape Intelligence Gathering," *San Francisco Chronicle,* July 4, 2004, (RW 1252)

Treverton, G.F. *Emerging Threats to National Security,* CT-234, 2005. (RW 1373)

Treverton, G.F. *Making Sense of Transnational Threats. Workshop Reports,* RAND Corporation, Santa Monica, CA, 2005. (RW 1246)

Treverton, G.F. *The Next Steps in Reshaping Intelligence,* RAND Corporation, Santa Monica, CA, 2005. (RW 1131)

Treverton, G.F. "Risks and Riddles," *Smithsonian Magazine,* June, 2007 (RW 2444)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Treverton, G.F. "Intelligence Analysis: Between "Politicization" and Irrelevance," in *Analyzing Intelligence: Origins, Obstacles, and Innovations*, eds. R.Z. George & J.B. Bruce, 2008, pp. 91. (RW 3098)

Treverton, G.F. "Learning from Recent Best Practices and Spectacular Flops," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, 2008, pp. 283. (RW 3653)

Treverton, G.F. *Reorganizing U.S. Domestic Intelligence: Assessing the Options,* 2008. (RW 3321)

Treverton, G.F. *Intelligence for an Age of Terror,* Cambridge University Press, New York, NY, 2009. (RW 3448)

Treverton, G.F. *Making Policy in the Shadow of the Future,* RAND Corporation, Santa Monica, CA, 2010. (RW 4522)

Treverton, G.F. & Agrell, W. "Introduction," in *National Intelligence Systems: Current Research and Future Prospects*, eds. G.F. Treverton & W. Agrell, Cambridge University Press, New York, 2009, pp. 1. (RW 3524)

Treverton, G.F. & Gabbard, C.B. *Assessing the Tradecraft of Intelligence Analysis* 2008. (RW 2978)

Treverton, G.F. & Ghez, J.J. *Making Strategic Analysis Matter,* RAND Corporation, Santa Monica, CA, 2012. (RW 5509)

Treverton, G.F., Jones, S.G., Boraz, S. & Lipscy, P. *Toward a Theory of Intelligence. Workshop Report from June 15, 2005 Meeting.* 2006. (RW 1306)

Treverton, G.F. and O'Connell, K.M. "Reshaping Intelligence in an Era of Excess Information," *Los Angeles Times,* December 28, 1997. (RW 3185)

Treverton, G.F. & Wilson, P.A. "True Intelligence Reform is Cultural, Not just Organizational Chart Shift," *Christian Science Monitor,* Vol. 97, No. 35, 2005, pp. 9. (RW 222)

Triantaphyllou, E. *Multi-Criteria Decision Making Methods: A Comparative Study,* Kluwer Academic Publishers, Dordrecht, 2000. (RW 5438)

Trickett, S.B., Schunn, C.D. & Trafton, J.G. "Puzzles and Peculiarities: How Scientists Attend to and Process Anomalies during Data Analysis," in *Scientific and Technological Thinking*, ed. M.E. Gorman, L. Erlbaum Associates, Mahwah, N.J, 2005, pp. 97. (RW 2140)

Trim, P.R.J. "The Company-Intelligence Interface and National Security," *International Journal of Intelligence and Counterintelligence,* Vol. 13, No. 2, 2000, pp. 204-214. (RW 188)

Trinder, L. & Reynolds, S. *Evidence-Based Practice: A Critical Appraisal,* Blackwell Science, Oxford; Malden, MA, 2000. (RW 2223)

Trochim, W.M.K. & Donnelly, J.P. *Research Methods Knowledge Base,* 3rd ed., Thomson Custom Pub., Mason, OH, 2007. (RW 3117)

Troldahl, V.C. & Powell, F.A. "A Short-Form Dogmatism Scale for use in Field Studies," *Social Forces,* Vol. 44, No. 2, 1965, pp. 211-214. (RW 5340)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Trope, Y. "Identification and Inferential Processes in Dispositional Attribution," *Psychological Review,* Vol. 93, No. 3, 1986, pp. 239. (RW 1838)

Trope, Y. & Bassok, M. "Information Gathering Strategies in Hypothesis Testing," *Journal of Experimental Social Psychology,* Vol. 19, 1983, pp. 560-576. (RW 5239)

Trope, Y. & Liberman, A. "Social Hypothesis Testing: Cognitive and Motivational Mechanisms," in *Social Psychology: Handbook of Basic Principles,* eds. E.T. Higgins & A.W. Kruglanski, Guilford Press, New York, 1996, pp. 239. (RW 2897)

Trujillo, D.M. *Are Intelligence Failures Inevitable?* Available: http://www.e-ir.info/2012/11/08/are-intelligence-failures-inevitable/, Viewed: December 6, 2012. (RW 5870)

Tsai, C.C. "An Analysis of Scientific Epistemological Beliefs and Learning Orientations of Taiwanese Eighth Graders," *Science Education,* Vol. 82, No. 4, 1998, pp. 473-489. (RW 4646)

Tsai, C.C. ""Laboratory Exercises Help Me Memorize the Scientific Truths": A Study of Eighth Graders' Scientific Epistemological Views and Learning in Laboratory Activities," *Science Education,* Vol. 83, No. 6, 1999, pp. 654-674. (RW 4645)

Tsai, C.I., Klayman, J. & Hastie, R. "Effects of Amount of Information on Judgment Accuracy and Confidence," *Organizational behavior and human decision processes,* Vol. 107, No. 2, 2008, pp. 97-105. (RW 5295)

Tsitoura, N. & Stephens, D. "Development and Evaluation of a Framework to Explain Causes of Competitive Intelligence Failures," *Information Research,* Vol. 17, No. 2, 2012 (RW 5692)

Tsoukas, H. "Do we really Understand Tacit Knowledge?" in *The Blackwell Handbook of Organizational Learning and Knowledge Management,* eds. M. Easterby-Smith & M.A. Lyles, Blackwell Pub., Malden, MA, 2003, pp. 410. (RW 2047)

Tucker, N.B. "The Cultural Revolution in Intelligence: Interim Report," *The Washington Quarterly,* Vol. 31, No. 2, 2008, pp. 47-61. (RW 2976)

Tugend, A. "Shortcuts - Multitasking can make You Lose...Um...Focus," *New York Times,* October 24, 2008, (RW 3560)

Tukey, J.W. *Exploratory Data Analysis,* Addison-Wesley, Reading, MA, 1977. (RW 668)

Tuma, D.T. & Reif, F. *Problem Solving and Education: Issues in Teaching and Research,* L. Erlbaum Associates, Hillsdale, NJ, 1980. (RW 2582)

Turner, A., Hetzler, E., Cheney, B., Williams, L. & Zabriskie, S. "Method and System for Prospective Analysis of Alternative Futures," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 856)

Turner, M.A. "Issues in Evaluating US Intelligence," *International Journal of Intelligence and Counterintelligence,* Vol. 5, No. 3, 1991, pp. 275-285. (RW 1287)

Turner, M.A. "Setting Analytical Priorities in US Intelligence," *International Journal of Intelligence and Counterintelligence,* Vol. 9, No. 3, 1996, pp. 313-327. (RW 38)

Turner, M.A. "A Distinctive US Intelligence Identity," *International Journal of Intelligence and Counterintelligence,* Vol. 17, No. 1, 2004, pp. 42-61. (RW 64)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Turner, M.A. "Intelligence Reform and the Politics of Entrenchment," *International Journal of Intelligence and Counterintelligence*, Vol. 18, No. 3, 2005, pp. 383-397. (RW 921)

Turner, M.A. *Why Secret Intelligence Fails*, Potomac Books, Dulles, VA, 2005. (RW 1494)

Turner, S. "Intelligence for a New World Order," *Foreign Affairs*, Vol. 70, No. 4, 1991, pp. 150-166. (RW 87)

Turner, S., Hulnick, A.S. & Johnson, L.K. "Responses to Goodman's Revamping the CIA (Three Individual Letters)," *Issues in Science and Technology*, Vol. 18, No. 3, 2002, pp. 6-8. (RW 379)

Turnley, J.G. & Smrcka, J. *Terrorist Organizations and Criminal Street Gangs: An Argument for an Analogy*, SAND 2004-1104P, Sandia National Laboratories, Albuquerque, NM, 2002. (RW 487)

Tusikov, N. & Fahlman, R. "Threat and Risk Assessments," in *Strategic Thinking in Criminal Intelligence*, ed. J. Ratcliffe, 2nd ed., Federation Press, Sydney, 2009, pp. 147-164. (RW 5757)

Tversky, A. & Shafir, E. "The Disjunction Effect in Choice Under Uncertainty," *Psychological Science*, Vol. 3, 1992, pp. 305. (RW 2107)

Twardy, C.R. *Argument Maps Improve Critical Thinking*, Monash University, Melbourne, Victoria, Australia, [undated]. (RW 3145)

Tweney, R. "Scientific Thinking: A Cognitive-Historical Approach," in *Designing for Science: Implications from Everyday, Classroom, and Professional Settings*, eds. K.D. Crowley, C.D. Schunn & T. Okada, 2001, pp. 141. (RW 3941)

Twining, W. "Narrative and Generalizations in Argumentations about Questions of Fact," *South Texas Law Review*, Vol. 40, No. 2, 1999, pp. 351. (RW 4182)

Twining, W. "Taking Facts Seriously," *Journal of Legal Education*, Vol. 34, 1984, pp. 22. (RW 1383)

Twining, W. "Evidence as a Multi-Disciplinary Subject," *Law, Probability, & Risk*, Vol. 2, 2003, pp. 91. (RW 1364)

Twining, W. *Taking Facts Seriously - again* 2004. (RW 1366)

Twining, W. "Evidence as a Multi-Disciplinary Subject (2005)," 2005 (RW 1367)

Twining, W. "Taking Facts Seriously - again," *Journal of Legal Education*, Vol. 55, 2005, pp. 360. (RW 1384)

Twining, W. "Argumentation, Stories, and Generalizations: A Comment," *Law, Probability, & Risk*, Vol. 6, No. 1-4, 2007, pp. 169-185. (RW 4196)

Twining, W. "Moving Beyond Law: Interdisciplinarity and the Study of Evidence," in *Evidence, Inference and Enquiry*, eds. P. Dawid, W. Twining & M. Vasilaki, 2011, pp. 73-118. (RW 5629)

Twining, W.L. *Rethinking Evidence: Exploratory Essays*, Northwestern University Press, Evanston, IL, 1994. (RW 4185)

Twining, W.L. & Hampsher-Monk, I. *Evidence and Inference in History and Law: Interdisciplinary Dialogues*, Northwestern University Press, Evanston, IL, 2003. (RW 966)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Tynjälä, P. "Writing, Learning and the Development of Expertise in Higher Education," in *Writing as a Learning Tool: Integrating Theory and Practice*, eds. P. Tynjälä, L. Mason & K. Lonka, Kluwer Academic Publishers, Dordrecht Netherlands, 2001, pp. 37-56. (RW 4336)

Tynjälä, P., Mason, L. & Lonka, K. "Writing as a Learning Tool: An Introduction," in *Writing as a Learning Tool: Integrating Theory and Practice*, eds. P. Tynjälä, L. Mason & K. Lonka, Kluwer Academic Publishers, Dordrecht Netherlands; Boston, 2001, pp. 7. (RW 4262)

U.S. Central Intelligence Agency, Directorate of Intelligence. *Analysis: Directorate of Intelligence in the 21st Century (Strategic Plan)*, U.S. Central Intelligence Agency, Washington DC, 1996. (RW 4198)

U.S. Central Intelligence Agency, Directorate of Intelligence. *A Compendium of Analytic Tradecraft Notes: Volume I (Notes 1-10)*, U.S. Central Intelligence Agency, Washington DC, 1997. (RW 4194)

Ubell, R. *Virtual Teamwork: Mastering the Art and Practice of Online Learning and Corporate Collaboration*, Wiley, Hoboken, NJ, 2010. (RW 4594)

Uhlmann, M.M. "Approaches to Reform of the Intelligence Community," in *Intelligence Requirements for the 1980's*, ed. R. Godson, National Strategy Information Center, Washington, DC, 1979, pp. 9-19. (RW 152)

Undersecretary of Defense, US Department of Defense. *Reorganization of the Office of the Under Secretary of Defense for Intelligence* 2008. (RW 3194)

Unger, R.K. & Draper, R. "Personal Epistemology and Personal Experience," *Journal of Social Issues*, Vol. 42, No. 2, 1986, pp. 67-79. (RW 4921)

Unger, R.F. *Intelligence in Vietnam and Iraq: Lessons Unlearned*, M.S.S. thesis, U.S. Army War College, 2010. (RW 5597)

United Nations Office on Drugs and Crime. *Criminal Intelligence Training: Manual for Analysts* (RW 4109)

United States Commission on National Security/21st Century. *New World Coming: American Security in the 21st Century. Study Addendum*, 1999. (RW 365)

United States Commission on National Security/21st Century. *New World Coming: American Security in the 21st Century. Supporting Research and Analysis. the Phase I Report on the Emerging Global Security Environment for the First Quarter of the 21st Century*, 1999. (RW 364)

United States Commission on National Security/21st Century. *Seeking a National Strategy: A Concert for Preserving Security and Promoting Freedom. the Phase II Report on a U.S. National Security Strategy for the 21st Century.* 2000. (RW 367)

United States Commission on National Security/21st Century. *Road Map for National Security. Addendum on Implementation*, 2001. (RW 366)

United States Commission on National Security/21st Century. *Road Map for National Security. Addendum on Structure and Process Analyses. Volume 6 - Intelligence Community*, 2001. (RW 414)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

United States Commission on National Security/21st Century. *Road Map for National Security. Addendum on Structure and Process Analyses. Volume I - Key Observations and Overarching Processes,* 2001. (RW 455)

United States Commission on National Security/21st Century. *Road Map for National Security: Imperative for Change. the Phase III Report of the U.S. Commission in National Security/21st Century,* 2001. (RW 368)

United States Congress. House Permanent Select Committee on Intelligence. *IC21: Intelligence Community in the 21st Century: Staff Study,* US GPO, Washington, DC, 1996. (RW 1213)

United States Congress. House Permanent Select Committee on Intelligence. Subcommittee on Evaluation. *Iran: Evaluation of U.S. Intelligence Performance Prior to November 1978: Staff Report,* U.S. GPO, Washington, DC, 1979. (RW 1186)

United States Congress. Senate Select Committee on Intelligence. Subcommittee on Collection, Production, and Quality. *The National Intelligence Estimates A-B Team Episode Concerning Soviet Strategic Capability and Objectives: Report of the Senate Select Committee on Intelligence, Subcommittee on Collection, Production, and Quality, United States Senate, Together with Separate Views,* US GPO, Washington, DC, 1978. (RW 1187)

United States General Accounting Office. Program Evaluation and Methodology Division. *Prospective Evaluation Methods. the Prospective Evaluation Synthesis.* 1990. (RW 2274)

United States. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. *Report to the President of the United States,* Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, Washington, DC, 2005. (RW 920)

United States, Central Intelligence Agency & Office of Research and Development. *Intelligence Production Laboratory Conference Proceedings: Applications of Inference Theory and Analysis and of Artificial Intelligence to Problems in Intelligence Analysis, 15 November 1982 - 17 November 1982,* Analytic Methodology Research Division, Office of Research and Development, Central Intelligence Agency, Washington, DC, 1982. (RW 1473)

Uren, V., Motta, E. & Dzbor, M. "Browsing for Information by Highlighting Automatically Generated Annotations: A User Study and Evaluation", *K-Cap '05,* Banff, Alberta, Canada, October 2-5, 2005, pp. 75. (RW 1533)

Urhahne, D., Kremer, K. & Mayer, J. "Conceptions of the Nature of Science--are they General or Context Specific?" *International Journal of Science and Mathematics Education,* Vol. 9, No. 3, 2011, pp. 707-730. (RW 5204)

Urquhart, C. "Systematic Reviewing, Meta-Analysis and Meta-Synthesis for Evidence-Based Library and Information Science," *Information Research,* Vol. 15, No. 3, 2010 (RW 4372)

US Air Force. *Lead Turning the Future: The 2008 Strategy for United States Air Force Intelligence, Surveillance and Reconnaissance* 2008. (RW 3188)

US House of Representatives. Permanent Select Committee on Intelligence. *IC21 - the Intelligence Community in the 21st Century. Summary.* (RW 440)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

US National Commission on Libraries and Information Science. *A Comprehensive Assessment of Public Information Dissemination. Final Report, Volume 1. First Draft.* 2000. (RW 1457)

US National Commission on Libraries and Information Science. *A Comprehensive Assessment of Public Information Dissemination. Final Report, Volume 1.* 2001. (RW 1458)

US Senate Select Committee on Intelligence. *Joint Inquiry into Intelligence Community Activities before and After the Terrorist Attacks of September 11, 2001,* S. REPT. NO. 107- 351; H. REPT. NO. 107-792, 2002. (RW 4344)

US Senate. Select Committee on Intelligence. *Report on the US Intelligence Community's Prewar Intelligence Assessments on Iraq,* 2004. (RW 446)

US Senate. Senate Select Committee on Intelligence. *Explanatory Statement. Intelligence Reorganization Act of 1992* 1992. (RW 1226)

US Senate. Senate Select Intelligence Committee. *Report on CIA and National Security* 1996. (RW 1238)

Utts, J. "An Assessment of the Evidence for Psychic Functioning," *The Journal of Parapsychology,* Vol. 59, December, 1995, pp. 289-320. (RW 783)

Vakkari, P. "Relevance and Contributing Information Types of Searched Documents in Task Performance", *Proceedings of the 23rd Annual International ACM SIGIR Conference on Research and Development in Information Retrieval,* Athens, Greece, July 24-28, 2000, pp.22. (RW 4396)

Vakkari, P. "A Theory of the Task-Based Information Retrieval Process: A Summary and Generalisation of a Longitudinal Study," *Journal of Documentation,* Vol. 57, No. 1, 2001, pp. 44. (RW 4397)

Vakkari, P. "Trends and approaches in information behaviour research", *Information Research,* [Online], vol. 13, no. 4, paper 361. Available from: http://InformationR.net/ir/13-4/paper361.html, 2008, (RW 4787)

Vakkari, P. "Task Complexity, Problem Structure and Information Actions. Integrating Studies on Information Seeking and Retrieval," *Information Processing and Management,* Vol. 35, 1999, pp. 819. (RW 1770)

Vakkari, P. "Exploratory Searching as Conceptual Exploration", *HCIR 2010: Proceedings of the Fourth Workshop on Human-Computer Interaction and Information Retrieval,* New Brunswick, NJ, August 22, 2010, pp. 24. (RW 4323)

Vakkari, P. & Jaervelin, K. "Explanation in Information Seeking and Retrieval," in *New Directions in Cognitive Information Retrieval,* eds. A. Spink & C. Cole, Springer, Dordrecht, 2005, pp. 113. (RW 3592)

Valanides, N. & Angeli, C. "Effects of Instruction on Changes in Epistemological Beliefs," *Contemporary Educational Psychology,* Vol. 30, No. 3, 2005, pp. 314-330. (RW 5115)

Valanides, N. & Angeli, C. "An Exploratory Study about the Role of Epistemological Beliefs and Dispositions on Learners' Thinking about an Ill-Defined Issue in Solo and Duo Problem-

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Solving Contexts," in *Knowing, Knowledge and Beliefs: Epistemological Studies Across Diverse Cultures*, ed. M.S. Khine, Springer, Dordrecht, 2008, pp. 197-218. (RW 4352)

Valkenburg, R. & Dorst, K. "The Reflective Practice of Design Teams," *Design Studies*, Vol. 19, 1998, pp. 249. (RW 2685)

Vallee-Tourangeau, F. & Baker, A.G. "Attenuation of Belief Perseverance in a Covariation Judgment Task", *Proceedings of the 15th Annual Conference of the Cognitive Science Society*, June 18-21, 1993, pp. 1011. (RW 1997)

Vallone, D. & Pillar, N. (eds) *The Analyst's Cookbook, Volume II*, MCIIS Press, Erie, PA, 2011. (RW 5388)

Valtorta, M., Dang, J., Goradia, H., Huang, J. & Huhns, M. "Extending Heuer's Analysis of Competing Hypotheses Method to Support Complex Decision Analysis," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 303)

van Bruggen, J.M. & Kirschner, P.A. "Designing External Representations to Support Solving Wicked Problems," in *Arguing to Learn: Confronting Cognitions in Computer- Supported Collaborative Learning Environments*, eds. J. Andriessen, M. Baker & D. Suthers, Kluwer Academic Publishers, Dordrecht, The Netherlands, 2003, pp. 177-203. (RW 5289)

Van Cleave, M. "Remarks before the OPSEC Professionals Society," 2005 (RW 500)

Van Cleave, M. "Strategic Counterintelligence: What is it and what should we do about it?" *Studies in Intelligence*, Vol. 51, No. 2, 2007, pp. 1. (RW 2499)

Van Cleave, M.K. *Infrastructure Protection and Assurance*, Center for Information Policy Research. Harvard University, Cambridge, MA, 2000. (RW 1042)

van Creveld, M. *Twenty-Four Theses on Intelligence (Notes for OSS '02)* 2002. (RW 1444)

van Creveld, M. "Israel's Lebanese War: A Preliminary Assessment," *RUSI Journal*, Vol. 151, No. 5, 2006 (RW 1699)

van de Vall, M. "Sociological Practice: Problems, Theory, and Methods," *Knowledge & Policy*, Vol. 4, No. 3, 1991, pp. 3. (RW 2648)

van den Broek, P., Linze, B., Fletcher, C. & Marsolek, C. "The Role of Causal Discourse Structure in Narrative Writing," *Memory & Cognition*, Vol. 28, No. 5, 2000, pp. 711. (RW 2379)

van der Geest, T. "Studying "Real Life" Writing Processes: A Proposal and an Example," in *The Science of Writing: Theories, Methods, Individual Differences, and Applications*, eds. C.M. Levy & S.E. Ransdell, 1996, pp. 309. (RW 1825)

Van der Heijden, K. *Scenarios: The Art of Strategic Conversation*, 2nd ed., John Wiley & Sons, Chichester, West Sussex, 2005. (RW 3388)

Van der Henst, J. B., Politzer, G. & Sperber, D. "When is a Conclusion Worth Deriving? A Relevance Based Analysis of Indeterminate Relational Problems," *Thinking & Reasoning*, Vol. 8, No. 1, 2002, pp. 1. (RW 3183)

van der Sluijs, J., Risbey, J., Kloprogge, P., Ravetz, J., Funtowicz, S. & et al. "Guidance for Uncertainty Scanning and Assessment at RIVM," (RW 2611)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

van Dongen, K., Schraagen, J.M., Eikelboom, A. & te Brake, G. "Supporting Decision Making by a Critical Thinking Tool", *Proceedings of the Human Factors and Ergonomics Society 49th Annual Meeting,* Orlando, FL, September 26-30, 2005, pp. 517-521. (RW 3572)

Van Doren, P.H. "A Historic Failure in the Social Domain", *10th International Command and Control Research and Technology Symposium,* McLean, VA, June 13-16, 2005 (RW 474)

van Gelder, T. "How to Improve Critical Thinking using Educational Technology", *Meeting at the Crossroads: Proceedings of the Annual Conference of the Australasian Society for Computers in Learning in Tertiary Education (ASCILITE 2001),* Melbourne, Australia, December 9-12, 2001, pp. 539-548. (RW 3952)

van Gelder, T. "Enhancing Deliberation through Computer-Supported Argument Visualization," in *Visualizing Argumentation: Software Tools for Collaborative and Educational Sense-Making,* eds. P.A. Kirschner, S.J. Buckingham Shum & C.S. Carr, Springer, London, UK, 2002, pp. 97-116. (RW 3953)

van Gelder, T. "Critical Thinking: Lessons from Cognitive Science," *College Teaching,* Vol. 45, No. 1, 2005, pp. 1-6. (RW 3142)

van Gelder, T. *Bringing Visual Clarity to Complex Issues,* Available: www.timvangelder.com, Viewed: January 2, 2010. (RW 4065)

van Gelder, T., Bissett, M. & Cumming, G. "Cultivating Expertise in Informal Reasoning," *Canadian Journal of Experimental Psychology,* Vol. 58, No. 2, 2004, pp. 142-152. (RW 1925)

van Ginkel, W.P. *The use of Distributed Information in Decision Making Groups: The Role of Shared Task Representations* 2007. (RW 2032)

van Merrienboer, Joreoen J. G. & Boot, E.W. "Research on Past and Current Training in Professional Domains: The Emerging Need for a Paradigm Shift," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments,* ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 131-156. (RW 5139)

van Steenburgh, J.J., Fleck, J.I., Beerman, M. & Kounios, J. "Insight," in *Oxford Handbook of Thinking and Reasoning,* eds. K.J. Holyoak & R.G. Morrison, Oxford University Press, Oxford, UK, 2012, pp. 475-491. (RW 5503)

van Tulder, M.W., Koes, B.W. & Bouter, L.M. *The Importance of a Systematic Search Strategy* (RW 2272)

Van Vugt, M. & Hart, C.M. "Social Identity as Social Glue: The Origins of Group Loyalty," *Journal of Personality and Social Psychology,* Vol. 86, No. 4, 2004, pp. 585-598. (RW 1926)

van Woerkom, M. "The Relationship Betwen Coach and Coachee: A Crucial Factor for Coaching Effectiveness," in *Learning through Practice: Models, Traditions, Orientations, and Approaches,* ed. S. Billett, Springer, Dordrecht, 2010, pp. 256-267. (RW 4963)

Vance, C. *Letter Expressing Views regarding Senate 1003* 1991. (RW 1237)

Vandenberg, H.S. *Testimony before the Committee on Armed Services. US Senate. 80th Congress, First Session.* (RW 2784)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Vandepeer, C. *Rethinking Threat: Intelligence Analysis, Intentions, Capabilities, and the Challenge of Non-State Actors,* Ph.D. dissertation, University of Adelaide, 2011. (RW 5761)

Vanderbrook, M. "UNCTAD V: Intelligence Support at a Major International Economic Conference," in *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992*, ed. H.B. Westerfield, Yale University Press, New Haven, CT, 1995, pp. 357-376. (RW 892)

Vane, R., Griffith, D., Starr, C. & Schenaker, M. "Agent Augmented Structured Arguments," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 811)

VanGundy, A.B. *Techniques of Structured Problem Solving,* 2nd ed., Van Nostrand Reinhold Co., New York, 1988. (RW 2585)

VanLehn, K. *Discovering Problem Solving Strategies: What Humans do and Machines Don't (Yet),* ADA219008, 1989. (RW 1136)

VanLehn, K. "Cognitive Skill Acquisition," *Annual Review of Psychology,* Vol. 47, 1996, pp. 513. (RW 1961)

VanLehn, K. & van de Sande, B. "Acquiring Conceptual Expertise from Modeling: The Case of Elementary Physics," in *Development of Professional Expertise: Toward Measurement of Expert Performance and Design of Optimal Learning Environments*, ed. K.A. Ericsson, Cambridge University Press, New York, NY, 2009, pp. 356-378. (RW 5149)

Vannoy, J.S. "Generality of Cognitive Complexity-Simplicity as a Personality Construct," *Journal of Personality and Social Psychology,* Vol. 2, No. 3, 1965, pp. 385. (RW 4300)

Vedantam, S. "How the Brain Helps Partisans Admit no Gray," *Washington Post,* July 31, 2006, pp. A02. (RW 1617)

Vedantam, S. "Iraq War Naysayers may have Hindsight Bias," *Washington Post,* October 2, 2006, pp. A02. (RW 1645)

Vedantam, S. "Does Your Subconscious Think Obama is Foreign?" *Washington Post*, October 13, 2008, pp. A08. (RW 3347)

Verlinden, J. *Critical Thinking and Everyday Argument*, Thomson Wadsworth, Belmont, CA, 2005. (RW 4023)

Verplanken, B. "Need for Cognition and External Information Search: Responses to Time Pressure during Decision-Making," *Journal of Research in Personality,* Vol. 27, No. 3, 1993, pp. 238-252. (RW 4949)

Versteeg, N., Sanders, T. & Wijnen, F. "Knowing what's Going on. the Influence of Contextual Knowledge on the on-Line Resolution of Structural Ambiguity", *Proceedings of the 28th Annual Conference of the Cognitive Science Society,* July 26-29, 2006, pp. 852. (RW 1987)

Vertzberger, Y. *The World in their Minds: Information Processing, Cognition, and Perception in Foreign Policy Decisionmaking,* Stanford University Press, Stanford, CA, 1990. (RW 2554)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Vertzberger, Y. *Risk Taking and Decisionmaking: Foreign Military Intervention Decisions,* Stanford University Press, Stanford, CA, 1998. (RW 3593)

Vicens, Q. & Bourne, P.E. "Ten Simple Rules for a Successful Collaboration," *PLoS Computational Biology,* Vol. 3, No. 3, 2007 (RW 2295)

Vickers, M.G. "Intelligence Reform and the Next CIA Director," *CSBA Backgrounder,* 2004 (RW 273)

Vickers, R.D. "The Intelligence Reform Quandary," *International Journal of Intelligence and Counterintelligence,* Vol. 19, No. 2, 2006, pp. 356. (RW 1752)

Viens, M. "Five Forces Analysis," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 131-144. (RW 3619)

Vila-Matas, E. & Dunne, J. *Bartleby & Co.* New Directions, New York, 2004. (RW 1871)

Vincenti, W.G. *What Engineers Know and How They Know It: Analytical Studies from Aeronautical History,* Johns Hopkins University Press, Baltimore, 1990. (RW 2589)

Vinod, V.G., van den Eijkhof, J., Chandrasekar, R., Paradiso, A. & St. George, J. "News Sync: Three Reasons to Visualize News Better", *HCIR 2010: Proceedings of the Fourth Workshop on Human-Computer Interaction and Information Retrieval,* New Brunswick, NJ, August 22, 2010, pp. 45. (RW 4316)

Vinokur, A., Burnstein, E., Sechrest, L. & Wortman, P.M. "Group Decision Making by Experts: Field Study of Panels Evaluating Medical Technologies," *Journal of Personality and Social Psychology,* Vol. 49, No. 1, 1985, pp. 70. (RW 1942)

Vital, D. "Images of Other Peoples in the Making of Intelligence and Foreign Policy," *International Journal of Intelligence and Counterintelligence,* Vol. 16, No. 1, 2003, pp. 16-33. (RW 319)

Vogel, E.K. & Drew, T. *Why do we Forget Things?* 2008. (RW 3351)

Vollmeyer, R., Burns, B.D. & Holyoak, K.J. "The Impact of Goal Specificity and Systematicity of Strategies on the Acquisition of Problem Structure," *Cognitive Science,* Vol. 20, 1996, pp. 75. (RW 2163)

Volmink, J., Siegfried, N., Robertson, K. & Guelmezoglu, A.M. "Research Synthesis and Dissemination as a Bridge to Knowledge Management: The Cochrane Collaboration," *Bulletin of the World Health Organization,* Vol. 82, No. 10, 2004, pp. 778. (RW 2216)

von Schomberg, R. *Science, Politics, and Morality: Scientific Uncertainty and Decision Making,* Kluwer Academic Publishers, Dordrecht, 1993. (RW 2405)

Von Winterfeldt, D. & Edwards, W. *Decision Analysis and Behavioral Research,* Cambridge University Press, Cambridge Cambridgeshire, 1986. (RW 4212)

Voorhees, E.M. *Overview of TREC 2002* (RW 2853)

Voorhees, E.M. "Variations in Relevance Judgments and the Measurement of Retrieval Effectiveness," *Information Processing and Management,* Vol. 36, 2000, pp. 697. (RW 1482)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Voorhees, E.M. "I Come Not to Bury Cranfield, but to Praise it", *HCIR 2009: Proceedings of the Third Workshop on Human-Computer Interaction and Information Retrieval*, Washington, DC, October 23, 2009, pp. 13-16. (RW 4311)

Vosniadou, S. & Brewer, W. "Mental Models of the Earth: A Study of Conceptual Change in Childhood," *Cognitive Psychology*, Vol. 24, No. 4, 1992, pp. 535. (RW 1839)

Vosniadou, S. "The Conceptual Change Approach and its Reframing," in *Re-Framing the Conceptual Change Approach in Learning and Instruction*, eds. S. Vosniadou, A. Baltas & X. Vamvakoussi, Elsevier, Amsterdam, 2007, pp. 1-15. (RW 5102)

Vosniadou, S. "Personal Epistemology and Conceptual Change: An Introduction," in *Re-Framing the Conceptual Change Approach in Learning and Instruction*, eds. S. Vosniadou, A. Baltas & X. Vamvakoussi, Elsevier, Amsterdam, 2007, pp. 99-104. (RW 4922)

Vosniadou, S. "Conceptual Change Research: An Introduction," in *International Handbook of Research on Conceptual Change*, ed. S. Vosniadou, Routledge, New York, 2008, pp. xiii. (RW 3716)

Vosniadou, S., de Corte, E. & Mandl, H. *Technology-Based Learning Environments: Psychological and Educational Foundations*, Springer, Berlin, 1994. (RW 4265)

Voss, J.F., Kennet, J., Wiley, J. & Engstler-Schooler, T. "Experts at Debate: The use of Metaphor in the US Senate Debate on the Gulf Crisis," *Metaphor and Symbolic Activity*, Vol. 7, 1992, pp. 197. (RW 1616)

Voss, J.F., Wiley, J. & Carretero, M. "Acquiring Intellectual Skills," *Annual Review of Psychology*, Vol. 46, 1995, pp. 155-181. (RW 1884)

Voss, J.F. "On the Composition of Experts and Novices," in *Thinking, Reasoning, and Writing*, eds. E.P. Maimon, B.F. Nodine & F.W. O'Connor, Longman, New York, 1989, pp. 69. (RW 4350)

Voss, J.F. "On the Representation of Problems: An Information Processing Approach to Foreign Policy Decision Making," in *Problem Representation in Foreign Policy Decision Making*, eds. D.A. Sylvan & J.F. Voss, 1998, pp. 8-28. (RW 1615)

Voss, J.F. & Post, T.A. "On the Solving of Ill-Structured Problems," in *The Nature of Expertise*, eds. M.T.H. Chi, R. Glaser & M.J. Farr, L. Erlbaum Associates, Hillsdale, NJ, 1988, pp. 261. (RW 2656)

Vygotskii, L.S. & Cole, M. *Mind in Society: The Development of Higher Psychological Processes*, Harvard University Press, Cambridge, 1978. (RW 3894)

Vygotsky, L. *Thought and Language[by] L. S. Vygotsky*, MIT Press, Cambridge, MA, 1986. (RW 5894)

Vyshedskiy, A. *On the Origin of the Human Mind: Three Theories: Uniqueness of the Human Mind, Evolution of the Human Mind, and the Neurological Basis of Conscious Experience*, 2008. (RW 3430)

Wack, P. "Scenarios: Shooting the Rapids," *Harvard Business Review*, November-December, 1985 (RW 1728)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Wack, P. "Scenarios: Uncharted Waters," *Harvard Business Review*, September-October, 1985 (RW 1727)

Wactlar, H., Christel, M., Hauptmann, A. & Ng, T.D. "ENVIE: Extensible News Video Exploitation for Intelligence Analysis," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 839)

Wagenaar, W.A., van Koppen, P.J. & Crombag, H.F.M. *Anchored Narratives: The Psychology of Criminal Evidence*, Harvester Wheatsheaf, Hemel Hempstead, Hertfordshire, 1993. (RW 4223)

Wagman, M. *Cognitive Psychology and Artificial Intelligence: Theory and Research in Cognitive Science*, Praeger, Westport, CT, 1993. (RW 2553)

Wagman, M. *The Human Mind According to Artificial Intelligence: Theory, Research, and Implications*, Praeger, Westport, CT, 1999. (RW 2552)

Wailgum, T. "Inside the CIA's Extreme Technology Makeover, Part 1," *CIO*, 2008 (RW 3214)

Wailgum, T. "Inside the CIA's Extreme Technology Makeover, Part 2," *CIO*, 2008 (RW 3215)

Wailgum, T. "Inside the CIA's Extreme Technology Makeover, Part 3," *CIO*, 2008 (RW 3216)

Wailgum, T. "Inside the CIA's Extreme Technology Makeover, Part 4," *CIO*, 2008 (RW 3217)

Wainryb, C., Shaw, L.A., Langley, M., Cottam, K. & Lewis, R. "Children's Thinking about Diversity of Belief in the Early School Years: Judgments of Relativism, Tolerance, and Disagreeing Persons," *Child development*, Vol. 75, No. 3, 2004, pp. 687-703. (RW 5193)

Wakkary, R. "Framing Complexity, Design and Experience: A Reflective Analysis," *Digital Creativity*, Vol. 16, No. 2, 2005, pp. 65. (RW 2625)

Waldrop, M.M. "Innovation and Adaptation: IT Examples," in *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics*, ed. F. Fukuyama, Brookings Institution Press, Washington, DC, 2007, pp. 120-128. (RW 4701)

Walker, K. "A Model of the Future: Multi-Intelligence Tool is on Fast Track," *Intelligence, Surveillance and Reconnaissance*, September, 2004, pp. 40. (RW 238)

Walker, K. "Playing with FIRE: Modeling and Simulation Tool Pulls Everyone into the Intelligence Game," *Training and Simulation Journal*, August, 2004, pp. 34. (RW 237)

Walker, S.E. "Encouraging the Disposition to Critically Think," *Athletic Therapy Today*, Vol. 10, No. 2, 2005, pp. 42-44. (RW 5654)

Walker, S., Brownlee, J., Lennox, S., Exley, B., Howells, K. & Cocker, F. "Understanding First Year University Students: Personal Epistemology and Learning," *Teaching Education*, Vol. 20, No. 3, 2009, pp. 243-256. (RW 5232)

Waller, J.H. "In Search of Wisdom: When Estimates are Wrong and Actions Defy Logic," *Intelligencer*, Vol. 15, No. 3, 2007, pp. 39-41. (RW 4429)

Wallis, C. *Inferences and Human Inference Abilities*, California State University - Long Beach, Long Beach, CA, 2012. (RW 5776)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Wallsten, T.S. *Interpreting Qualitative Probability Expressions [Powerpoint Presentation]* (RW 1762)

Wallsten, T.S. *Issues in Forming, Revising, and Communicating Uncertain Judgments [Powerpoint Presentation]* 2007. (RW 3567)

Wallsten, T.S., Shlomi, Y. & Ting, H. *Exploring Intelligence Analysts' Selection and Interpretation of Probability Terms* (RW 3568)

Walsh, C.M. & Seldomridge, L.A. "Critical Thinking: Back to Square Two," *Journal of Nursing Education,* Vol. 45, No. 6, 2006, pp. 212-219. (RW 3967)

Walsh, C.M., Seldomridge, L.A. & Badros, K.K. "California Critical Thinking Disposition Inventory: Further Factor Analytic Examination," *Perceptual & Motor Skills,* Vol. 104, No. 1, 2007, pp. 141-151. (RW 5358)

Walsh, J.H. "Strategic Thinking and Air Intelligence," *Studies in Intelligence,* Vol. 2, No. 1, 1958, pp. 7-30. (RW 555)

Walsh, P.F. *Intelligence and Intelligence Analysis,* Routledge, Abingdon, UK, 2011. (RW 5738)

Walters, V.A. "Thirty Five Years in Intelligence," *Studies in Intelligence,* Vol. 20, No. 2, 1976, pp. 45-59. (RW 573)

Walton, D. "Dialogue Theory for Critical Thinking," *Argumentation,* Vol. 3, No. 2, 1989, pp. 169-184. (RW 4112)

Walton, D. *One-Sided Arguments: A Dialectical Analysis of Bias,* State University of New York Press, Albany, NY, 1999. (RW 3789)

Walton, D. & Macagno, F. "Common Knowledge in Legal Reasoning about Evidence," *International Commentary on Evidence,* Vol. 3, No. 1, 2005 (RW 1503)

Walton, G.M. & Cohen, G.L. "Stereotype Lift," *Journal of Experimental Social Psychology,* Vol. 39, No. 5, 2003, pp. 456. (RW 3156)

Walton, T. *Embodying Standards in a Textbook [Powerpoint Presentation]* Sherman Kent School of Intelligence Analysis, Washington, DC, [undated]. (RW 4499)

Walton, T.R. *Challenges in Intelligence Analysis,* Cambridge University Press, New York, NY, 2010. (RW 4500)

Walton, T. "Writing as Analysis: Using Writing to Challenge the Assumptions and Reframe the Analysis," in *A Handbook of the Psychology of Intelligence Analysis,* ed. R.L. Rees, 2008, pp. 405. (RW 3662)

Waltz, E. *Toward a MAUI NITE Intelligence Analytic Process Model,* Veridian Systems, Arlington, VA, 2003. (RW 630)

Waltz, E. *Knowledge Management in the Intelligence Enterprise,* Artech House, Boston, MA, 2003. (RW 1694)

Wang, P. "Methodologies and Methods for User Behavioral Research," *Annual Review of Information Science and Technology,* Vol. 34, 1999-2000, pp. 53-99. (RW 1126)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Wang, R., Kogut, P., Zhu, S., Leung, Y. & Yen, J. "Semantic Web Enabled Collaborative Agents for Supporting Analyst Teams," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 870)

Wang, Z., Chow, E. & Rohwer, R. "Experiments with Grounding Spaces, Pseudo-Counts, and Divergence Formulas in Association-Grounded Semantics," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 843)

Ward, D. "The Findability Quotient: Making Intel Accessible," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 876)

Ward, S.R. "Evolution Beats Revolution in Analysis," *Studies in Intelligence*, Vol. 46, No. 3, 2002, pp. 29-36. (RW 937)

Ward, T.B., Smith, S.M. & Vaid, J. "Conceptual Structures and Processes in Creative Thought," in *Creative Thought: An Investigation of Conceptual Structures and Processes*, eds. T.B. Ward, S.M. Smith & J. Vaid, 1997, pp. 1. (RW 1763)

Wark, D.L. "The Definition of some Estimative Expressions," *Studies in Intelligence*, Vol. 8, No. 4, 1964, pp. 67-80. (RW 518)

Wark, W. "The Study of Espionage: Past, Present, Future?" *Intelligence and National Security*, Vol. 8, No. 3, 1993, pp. 1-13. (RW 1572)

Wark, W.K. "Introduction: The Fin-De-Siecle Phenomenon," in *Security and Intelligence in a Changing World: New Perspectives for the 1990s*, eds. A.S. Farson, D. Stafford & W.K. Wark, F. Cass, London, UK, 1991, pp. 3-9. (RW 109)

Wark, W.K. "The Intelligence Revolution and the Future," *Studies in Intelligence*, Vol. 37, No. 5, 1994, pp. 9-16. (RW 68)

Warner, J. & Chang, L. *Brain Wired for Improv, Not Perfection*, Available: http://www.webmd.com/content/Article/130/117870.htm, (RW 2069)

Warner, J.S. "The Watchdog Committee Question," *Studies in Intelligence*, Vol. 10, No. 3, 1966, pp. 31-41. (RW 570)

Warner, M. *Cheating Fate: An Evolutionary Theory of Intelligence Systems* [undated]. (RW 2987)

Warner, M. "Wanted: A Definition of "Intelligence"," *Studies in Intelligence*, Vol. 46, No. 3, 2002, pp. 15-22. (RW 1369)

Warner, M. "Intelligence Transformation and Intelligence Liaison," *SAIS Review*, Vol. 24, No. 1, 2004, pp. 77-89. (RW 1142)

Warner, M. "The Divine Skein: Sun Tzu on Intelligence," *Intelligence and National Security*, Vol. 21, No. 4, 2006, pp. 483. (RW 2089)

Warner, M. "Searching Where the Light Shines? An American View of Methods for the Study of Intelligence," in *Strategic Intelligence. Volume 1: Understanding the Hidden Side of Government*, ed. L.K. Johnson, Praeger Security International, Westport, CT, 2007, pp. 109. (RW 2711)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Warner, M. "Sources and Methods for the Study of Intelligence," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 17. (RW 2453)

Warner, M. "Building a Theory of Intelligence Systems," in *National Intelligence Systems: Current Research and Future Prospects*, eds. G.F. Treverton & W. Agrell, Cambridge University Press, New York, 2009, pp. 11. (RW 3546)

Warner, M. "Intelligence as Risk Shifting," in *Intelligence Theory: Key Questions and Debates*, eds. P. Gill, S. Marrin & M. Phythian, 2009, pp. 16. (RW 3403)

Warner, M. "Cybersecurity: A Pre-History," *Intelligence and National Security*, Vol. 27, No. 5, 2012, pp. 781-799. (RW 5840)

Warner, M. "Fragile and Provocative: Notes on Secrecy and Intelligence," *Intelligence and National Security*, Vol. 27, No. 2, 2012, pp. 223-240. (RW 5614)

Warner, M. "Reflections on Technology and Intelligence Systems," *Intelligence and National Security*, Vol. 27, No. 1, 2012, pp. 133-153. (RW 5611)

Warner, M. & McDonald, J.K. *US Intelligence Community Reform Studies since 1947* 2005. (RW 4087)

Warren, J.B.E. *Determining Analyst Core Competencies using Experiential Learning Theory*, MSSI thesis, Joint Military Intelligence College, 2006. (RW 1657)

Warren, P., Thurlow, I., Davies, J., Dolinsek, I., Ruiz, C. & Gomez-Perez, J. "Context as a Tool for Organizing and Sharing Knowledge", *Second International Workshop on Context Information and Ontologies*, Lisbon, October 11, 2010 (RW 4861)

Warren, W. "Analysis of Analyses," *Periscope*, Vol. 26, No. 1, 2004, pp. 3-4. (RW 4449)

Wasserman, B. "The Failure of Intelligence Prediction," *Political Studies*, Vol. 8, No. 2, 1960, pp. 156-169. (RW 1260)

Wastell, C.A. "Cognitive Predispositions and Intelligence Analyst Reasoning," *International Journal of Intelligence and Counterintelligence*, Vol. 23, No. 3, 2010, pp. 449-460. (RW 4156)

Watanabe, F. "Fifteen Axioms for Intelligence Analysts," *Studies in Intelligence*, Summer, 1997, pp. 45-47. (RW 113)

Waterman, S. *US Intelligence on Iran*, Available: http://news.monstersandcritics.com/northamerica/printer_1217918.php, (RW 1729)

Wathen, C.N. "Believe it Or Not: Factors Influencing Credibility on the Web," *Journal of the American Society for Information Science & Technology*, Vol. 53, No. 2, 2002, pp. 134. (RW 5447)

Watkins, E. *Uncertainty* 1999 (?). (RW 1393)

Watson, G. & Glaser, E.M. *Watson-Glaser II Critical Thinking Appraisal Technical Manual and User's Guide*, NCS Pearson, Inc., San Antonio, TX, 2009. (RW 3766)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Watson, P. "The FBI's Changing Mission," in *U.S. Intelligence at the Crossroads: Agendas for Reform*, eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 146-153. (RW 643)

Watt, D.C. "The Historiography of Intelligence in International Review," in *Intelligence in the Cold War: Organisation, Role, International Cooperation*, eds. L.C. Jenssen & O. Riste, Norwegian Institute for Defence Studies, Oslo, Norway, 2001, pp. 173. (RW 3824)

Watt, D.C. "Intelligence and the Historian: A Comment on John Gaddis's "Intelligence, Espionage, and Cold War Origins"," *Diplomatic History*, Vol. 14, No. 2, 1990, pp. 199-204. (RW 122)

Watts, D. "So You Can't Pick the Hits. Neither Can Anyone Else", *Washington Post*, January 4, 2009, pp. B04. (RW 3375)

Watzlawick, P. *The Invented Reality: How Do We Know What We Believe We Know?: Contributions to Constructivism*, Norton, New York, 1984. (RW 3841)

Watzlawick, P., Weakland, J.H. & Fisch, R. *Change; Principles of Problem Formation and Problem Resolution*, Norton, New York, 1974. (RW 2913)

Waxman, M.C. "Emerging Intelligence Challenges," *International Journal of Intelligence and Counterintelligence*, Vol. 10, No. 3, 1997, pp. 317-331. (RW 59)

Wears, R.L. & Nemeth, C.P. "Replacing Hindsight with Insight: Toward Better Understanding of Diagnostic Failures," *Annals of Emergency Medicine*, Vol. 49, No. 2, 2007, pp. 206. (RW 2512)

Weaver, K., Garcia, S.M., Schwarz, N. & Miller, D.T. "Inferring the Popularity of an Opinion from its Familiarity: A Repetitive Voice can Sound Like a Chorus," *Journal of Personality and Social Psychology*, Vol. 92, No. 5, 2007, pp. 821. (RW 2794)

Weaver, L.E. "Social Network Analysis," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 103-116. (RW 3616)

Webb, E.J. *Unobtrusive Measures*, Sage Publications, Thousand Oaks, CA, 2000. (RW 2286)

Weber, E. & Hsee, C. "Culture and Individual Judgment and Decision Making," *Applied Psychology*, Vol. 49, No. 1, 2000, pp. 32-61. (RW 5475)

Webster, D.M. & Kruglanski, A.W. "Individual Differences in Need for Cognitive Closure," *Journal of Personality and Social Psychology*, Vol. 67, No. 6, 1994, pp. 1049-1062. (RW 4950)

Webster, P. "Breaking Down Information Silos: Integrating Online Information," *Online Magazine*, November/December, 2004, pp. 30. (RW 1419)

Webster-Wright, A. *Authentic Professional Learning: Making a Difference through Learning at Work*, Springer Verlag, Dordrecht; New York, 2010. (RW 5317)

Weed, M. "Meta Interpretation: A Method for the Interpretive Synthesis of Qualitative Research," *Forum: Qualitative Social Research*, Vol. 6, No. 1, 2005, pp. 37. (RW 2263)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Wegner, D.M. "Transactive Memory: A Contemporary Analysis of the Group Mind," in *Theories of Group Behavior*, eds. B. Mullen & G.R. Goethals, Springer-Verlag, New York, 1987, pp. 185. (RW 2880)

Wegner, D.M. *The Illusion of Conscious Will,* MIT Press, Cambridge, MA, 2002. (RW 5562)

Weick, K.E. *Sensemaking in Organizations,* Sage Publications, Thousand Oaks, 1995. (RW 3272)

Weick, K.E. *Making Sense of the Organization*, Blackwell Business, Oxford, UK, 2001. (RW 4579)

Weick, K.E. & Sutcliffe, K.M. *Managing the Unexpected: Assuring High Performance in an Age of Complexity*, Jossey-Bass, San Francisco, CA, 2001. (RW 4560)

Weick, K.E. & Sutcliffe, K.M. "Organizing and the Process of Sensemaking," *Organization Science*, Vol. 16, No. 4, 2005, pp. 409. (RW 1335)

Weinberg, J.M. "What is Evaluative Normativity, That We (Maybe) Should Avoid It?" *Behavioral and Brain Sciences,* Vol. 34, No. 5, 2011, pp. 274-275. (RW 5492)

Weinberger, D. *Too Big to Know: Rethinking Knowledge Now that the Facts Aren't the Facts, Experts are Everywhere, and the Smartest Person in the Room is the Room,* Basic Books, New York, 2011. (RW 5641)

Weinberger, S. *Spies to use Twitter as Crystal Ball*, Available: http://stratrisks.com/geostrat/2073, Viewed: August 22, 2012. (RW 5786)

Weinberger, S. *The Spy Who Tweeted Me: Intelligence Community Wants to Monitor Social Media,* Available: http://www.wired.com/dangerroom/2011/09/social-media-spies/, Viewed: January 19, 2012. (RW 5406)

Weinberger, S. *Intelligence Agencies Turn to Crowdsourcing*, Available: http://www.bbc.com/future/story/20121009-for-all-of-our-eyes-only/1, Viewed: October 12, 2012. (RW 5830)

Weiner, T. "How to make a Spy," *Foreign Policy,* September/October, 2007 (RW 2819)

Weinstein, C.E. "A Look to the Future: What we might Learn from Research on Beliefs," in *Beliefs about Texts and Instruction with Text*, eds. R. Garner & P.A. Alexander, L. Erlbaum Associates, Hillsdale, NJ, 1994, pp. 295. (RW 2657)

Weinstein, M. & Oxman-Michelli, W. "Critical Thinking: Language and Inquiry Across the Disciplines", *Proceedings of the Annual Conference of the Institute for Critical Thinking*, Upper Montclair, NJ, (RW 4081)

Weinstock, M. *Epistemological Understanding and Argumentive Competence as Foundations of Juror Reasoning Skill*, Ph.D. dissertation, Columbia University, 1999. (RW 5121)

Weinstock, M. & Cronin, M.A. "The Everyday Production of Knowledge: Individual Differences in Epistemological Understanding and Juror-Reasoning Skill," *Applied Cognitive Psychology*, Vol. 17, No. 2, 2003, pp. 161-181. (RW 5192)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Weisberg, D.S., Keil, F.C., Goodstein, J., Rawson, E. & Gray, J.R. "The Seductive Allure of Neuroscience Explanations," *Journal of Cognitive Neuroscience,* Vol. 20, No. 3, 2008, pp. 470. (RW 3377)

Weisberg, R.W. "Modes of Expertise in Creative Thinking: Evidence from Case Studies," in *The Cambridge Handbook of Expertise and Expert Performance*, ed. K.A. Ericsson, Cambridge University Press, Cambridge, UK, 2006, pp. 761-788. (RW 5741)

Weiss, C. "Communicating Uncertainty in Intelligence and Other Professions," *International Journal of Intelligence and Counterintelligence,* Vol. 21, No. 1, 2008, pp. 57. (RW 2912)

Weiss, D.J. & Shanteau, J. "The Vice of Consensus and the Virtue of Consistency," in *Psychological Investigations of Competence in Decision Making*, eds. K. Smith, J. Shanteau & P.E. Johnson, Cambridge University Press, Cambridge, U.K.; New York, 2004, pp. 226. (RW 2385)

Weitzman, E.A. "Software and Qualitative Research," in *Handbook of Qualitative Research*, eds. N.K. Denzin & Y.S. Lincoln, 2nd ed., Sage Publications, Thousand Oaks, CA, 2000, pp. 803. (RW 2749)

Welburn, A.C.G. "The Application of False Principles and the Misapplication of Valid Principles: A Trap for the Unwary," *Australian Defence Force Journal*, 124, 1997, pp. 25-36. (RW 231)

Welch, B. *The Analyst's Style Manual* 2008. (RW 3236)

Welch, W.J. *Is China Stable? An Intelligence Analysis Perspective on the Question of Stability in China in the Next Five to Ten Years,* M. S. thesis, Mercyhurst College, 2006. (RW 3421)

Weldon, C. *Letter from Weldon to Gates* 1997. (RW 465)

Welgan, J.R. *The Effect of Labels on Analysis,* M.S. Applied Intelligence thesis, Mercyhurst College, 2009. (RW 3934)

Welgan, J.R. "The Terrorist Label and its Effect on Analysis", *ISA's 50th Annual Convention "Exploring the Past, Anticipating the Future",* New York, NY, Feb. 15, 2009. (RW 4491)

Wellman, H. "The Origins of Metacognition," in *Metacognition, Cognition, and Human Performance*, eds. G.E. MacKinnon, T.G. Waller & D. Forrest-Pressley, Academic Press, Orlando, FL, 1985, pp. 1-31. (RW 5324)

Wells, L. & Horowitz, B. "A Methodology for the Ranking of Suicide Bomber Recruitment Preferences using Multiple Sources of Data," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 803)

Wen, M.L., Kuo, P.-., Tsai, C.-. & Chang, C.-. "Exploring High School Students' Views regarding the Nature of Scientific Theory; a Study in Taiwan," *Asia Pacific Education Researcher,* Vol. 19, 2010, pp. 161-178. (RW 5059)

Wend, H.B. *Pearl Harbor and the 11th of September: Some Historical Parallels,* Boston University, Boston, MA, (RW 503)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Wendt, A. *Social Theory of International Politics*, Cambridge University Press, Cambridge, UK, 1999. (RW 1653)

Wermter, J. & Hahn, U. "Finding New Terminology in Very Large Corpora", *K-Cap '05*, Banff, Alberta, Canada, October 2-5, 2005, pp. 137. (RW 1535)

Wertheimer, M.A. "Crippling Innovation — and Intelligence," *Washington Post*, July 21, 2004, p. A19. (RW 480)

Wertsch, J.V. "Is it Possible to Teach Beliefs, as Well as Knowledge about History," in *Knowing, Teaching, and Learning History: National and International Perspectives*, eds. P.N. Stearns, P. Seixas & S. Wineburg, New York University Press, New York, 2000, pp. 38. (RW 3797)

West, M.A. *Effective Teamwork: Practical Lessons from Organizational Research*, 2nd ed., BPS Blackwell, Malden, MA, 2004. (RW 2031)

West, N. "Cold War Intelligence Defectors," in *Handbook of Intelligence Studies*, ed. L.K. Johnson, 2007, pp. 229. (RW 2470)

West, R.F., Meserve, R.J. & Stanovich, K.E. "Cognitive sophistication does not attenuate the bias blind spot", *Journal of Personality and Social Psychology*, [Online], pp. June 19, 2012. Available from: http://dx.doi.org/10.1037/a0028857, 2012, (RW 5693)

West, R.F. & Stanovich, K.E. "The Incidental Acquisition of Information from Reading," *Psychological Science*, Vol. 2, No. 5, 1991, pp. 325. (RW 2438)

West, R.F., Toplak, M.E. & Stanovich, K.E. *Heuristics and Biases as Measures of Critical Thinking: Associations with Cognitive Ability and Thinking Dispositions* [undated]. (RW 3333)

Westbury, C. *Bayes' for Beginners* (RW 3599)

Westerfield, H.B. *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992*, Yale University Press, New Haven, CT, 1995. (RW 702)

Westerfield, H.B. "America and the World of Intelligence Liaison," *Intelligence and National Security*, Vol. 11, No. 3, 1996, pp. 523-559. (RW 134)

Westerfield, H.B. "Inside Ivory Bunkers: CIA Analysts Resist Managers' 'Pandering'-Part I," *International Journal of Intelligence and Counterintelligence*, Vol. 9, No. 4, 1996-97, pp. 407-424. (RW 1067)

Westerfield, H.B. "Inside Ivory Bunkers: CIA Analysts Resist Managers' "Pandering" - Part II," *International Journal of Intelligence and Counterintelligence*, Vol. 10, No. 1, 1997, pp. 19-55. (RW 42)

Wharton, C.M., Holyoak, K.J., Downing, P.E., Lange, T.E., Wickens, T.D. & Melz, E.R. "Below the Surface: Analogical Similarity and Retrieval Competition in Reminding," *Cognitive Psychology*, Vol. 26, No. 1, 1994, pp. 64. (RW 1806)

Wharton, C.M. & Lange, T.E. "Analogical Transfer through Comprehension and Priming", *Proceedings of the 16th Annual Conference of the Cognitive Science Society*, August 13-16, 1994, pp. 934. (RW 1809)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Wheaton, K.J. & Beerbower, M.T. "Towards a New Definition of Intelligence," *Stanford Law and Policy Review*, Vol. 17, No. 2, 2006, pp. 319-330. (RW 3174)

Wheaton, K. *Top 5 Intelligence Analysis Methods (List),* Available: http://sourcesandmethods.blogspot.com/2008/12/top-5-intelligence-analysis-methods.html, (RW 3368)

Wheaton, K. *Top 5 Intelligence Analysis Methods: Analysis of Competing Hypotheses (#1)* 2008. (RW 3370)

Wheaton, K. *Top 5 Intelligence Analysis Methods: Bayesian Analysis (#5)* 2008. (RW 3374)

Wheaton, K. *Top 5 Intelligence Analysis Methods: Intelligence Preparation of the battlefield/environment (#4)* 2008. (RW 3373)

Wheaton, K. *Top 5 Intelligence Analysis Methods: Multi-Criteria Decision Making matrices/multi-Criteria Intelligence Matrices (#2)* 2008. (RW 3371)

Wheaton, K. *Top 5 Intelligence Analysis Methods: Social Network Analysis (#3)* 2008. (RW 3372)

Wheaton, K. *Top 5 Intelligence Analysis Methods: What Makes a Good Method? (List, Part 2)* 2008. (RW 3369)

Wheaton, K.J. *The Revolution Begins on Page Five: The Changing Nature of the National Intelligence Estimate and its Implications for Intelligence* (RW 3030)

Wheaton, K.J. *What do Words of Estimative Probability Mean? an Exercise in Analyst Education* (RW 3028)

Wheaton, K.J. "Analytic Tools and Methods: New Parables for New Challenges," in *A Handbook of the Psychology of Intelligence Analysis*, ed. R.L. Rees, CENTRA Technology, Burlington, MA, [in press], pp. 342-372. (RW 3656)

Wheaton, K.J. *The Warning Solution: Intelligent Analysis in the Age of Information Overload,* AFCEA International Press, Fairfax, VA, 2001. (RW 146)

Wheaton, K.J. *Analytic Confidence Defined...Finally! (Original research),* Available: http://sourcesandmethods.blogspot.com/, (RW 3059)

Wheaton, K.J. *Conceptual Modeling and its Role in Intelligence Analysis,* Available: http://sourcesandmethods.blogspot.com/, (RW 3054)

Wheaton, K.J. *Part 2 -- what is a Wiki and Why is it so Different? (A Wiki is Like a Room...),* Available: http://sourcesandmethods.blogspot.com/, (RW 3037)

Wheaton, K.J. *Part 3 -- the Origins and Scope of the Data (A Wiki is Like a Room...),* Available: http://sourcesandmethods.blogspot.com/, (RW 3038)

Wheaton, K.J. *Part 4 -- some Broad Metrics (A Wiki is Like a Room...),* Available: http://sourcesandmethods.blogspot.com/, (RW 3039)

Wheaton, K.J. *Part 5 -- A Few Comparisons (A Wiki is Like a Room...),* Available: http://sourcesandmethods.blogspot.com/, (RW 3040)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Wheaton, K.J. *Part 6 -- "...and the Survey Says!" (A Wiki is Like a Room...),* Available: http://sourcesandmethods.blogspot.com/, (RW 3041)

Wheaton, K.J. *Part 7 -- what the Decisionmakers Thought (A Wiki is Like a Room...),* Available: http://sourcesandmethods.blogspot.com/, (RW 3042)

Wheaton, K.J. *Part 8 -- Final Thoughts (A Wiki is Like a Room...),* Available: http://sourcesandmethods.blogspot.com/, (RW 3043)

Wheaton, K.J. *What is Intelligence?* Available: http://sourcesandmethods.blogspot.com/, (RW 3178)

Wheaton, K.J. *A Wiki is Like a Room and Other Lessons Learned from 15 Wiki-Based, Open Source, Intelligence Analysis Projects (Part 1: Introduction),* Available: http://sourcesandmethods.blogspot.com/, (RW 3036)

Wheaton, K.J. *Evaluating Intelligence* 2009. (RW 3477)

Wheaton, K.J. "Teaching Strategic Intelligence through Games," *International Journal of Intelligence and Counterintelligence,* Vol. 24, No. 2, 2011, pp. 367-382. (RW 4598)

Wheaton, K.J. *The Top 6 Skills for Entry-Level Intelligence Analysts,* Available: http://sourcesandmethods.blogspot.com/2011/08/top-6-skills-for-entry-level.html, (RW 5090)

Wheaton, K.J. "The Revolution Begins on Page Five: The Changing Nature of NIEs," *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 2, 2012, pp. 330-349. (RW 5616)

Wheaton, K.J. & Chido, D.E. "Structured Analysis of Competing Hypotheses," *Competitive Intelligence Magazine,* Vol. 9, No. 6, 2006, pp. 12. (RW 2935)

Wheaton, K.J., Lee, J. & Deshmukh, H. *Bayesian Statistics in the Real World of Intelligence Analysis: Lessons Learned* 2007. (RW 2985)

Wheaton, K. & Chido, D. "Evaluating Intelligence," *Competitive Intelligence Magazine,* Vol. 10, No. 5, 2007, pp. 19. (RW 3365)

Wheeler, W. "Naval Intel must (Re)Acquire Core Skills," *Proceedings of the United States Naval Institute,* Vol. 130, No. 2, 2004, pp. 42-47. (RW 358)

Wheelon, A.D. "Technology and Intelligence," *Technology in Society,* Vol. 26, No. 2-3, 2004, pp. 245-255. (RW 1143)

Whitaker, E.T., Valtorta, M.G. & Huhns, M.N. "Building and Evaluating Analytical Models using Case-Based Reasoning for Knowledge Discovery and Bayesian Evidence Management", *NIMD PI Meeting,* 18 -20 April, 2006 (RW 1760)

Whitaker, E., Simpson, R., Burkhart, L., MacTavish, R. & Lobb, C. ""Cognitive Factors in Homeland Defense". Reusing Intelligence Analysts' Search Plans", *HFES 2004: Proceedings of the Human Factors and Ergonomics Society. 48th Annual Meeting.* September 20-24, 2004, pp. 367. (RW 2873)

White, A. "The use of Concept Mapping in Ecological Management: A Case Study Involving Grassland Ecosystems in Victoria, Australia," in *Applied Concept Mapping: Capturing,*

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Analyzing, and Organizing Knowledge, eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 151-168. (RW 4970)

White, H.D. "Scientific Communication and Literature Retrieval," in *The Handbook of Research Synthesis*, eds. H.M. Cooper & L.V. Hedges, Russell Sage Foundation, New York, 1994, pp. 41. (RW 2154)

White, R.W., Kules, B., Drucker, S.M. & Schraefel, M.C. "Supporting Exploratory Search," *Communications of the ACM,* Vol. 49, No. 4, 2006, pp. 37. (RW 1516)

White, R.W. & Roth, R.A. *Exploratory Search: Beyond the Query-Response Paradigm*, Morgan & Claypool Publishers, San Rafael, CA, 2009. (RW 4342)

Whitehead, M. & Costantino, T. "Understanding the Research Process of Experienced Online Information Researchers to Inform Development of a Scholars Portal," *Evidence Based Library and Information Practice,* Vol. 4, No. 2, 2009, pp. 120-132. (RW 4804)

Whitelaw, K. "Getting it Dead Wrong," *US News and World Report,* Vol. 138, No. 13, 2005, pp. 32. (RW 754)

Whitelaw, K. "The Eye of the Storm," *US News and World Report,* Vol. 141, No. 17, 2006, pp. 48. (RW 1705)

Whitelaw, K. & Ragavan, C. "A Good Spy is Hard to Find," *US News and World Report,* Vol. 137, No. 18, 2004, pp. 59. (RW 755)

Whitelaw, K., Ragavan, C. & et al. "What's Known, What's Needed," *US News and World Report,* Vol. 137, No. 3, 2004, pp. 34. (RW 756)

Whitfield, J. "Group Theory," *Nature,* Vol. 455, 2008, pp. 720. (RW 3291)

Whiting, M.A., Haack, J. & Varley, C. "Creating Realistic, Scenario-Based Synthetic Data for Test and Evaluation of Information Analytics Software", *Beliv '08,* April 5, 2008 (RW 3267)

Whitman, J. "On Estimating Reactions," *Studies in Intelligence,* Vol. 9, No. 3, 1965, pp. 1-6. (RW 545)

Whitmire, E. "The Relationship between Undergraduates' Epistemological Beliefs, Reflective Judgment, and their Information-Seeking Behavior," *Information Processing & Management,* Vol. 40, No. 1, 2004, pp. 97. (RW 5554)

Whittaker, S. & Hirschberg, J. "The Character, Value, and Management of Personal Paper Archives," *ACM Transactions on Computer-Human Interaction,* Vol. 8, No. 2, 2001, pp. 150. (RW 3280)

Wiant, J.A. *The Anthropology of Intelligence: Ethnographic Notes Form the Field. A Discussion Paper.* (RW 2986)

Widick, C. *An Attribute-Treatment Interaction Model of Instruction Based on Cognitive Developmental Theory,* 1975. (RW 4696)

Wigfield, A., Zusho, A. & De Groot, E.V. "Introduction: Paul R. Pintrich's Contributions to Educational Psychology: An Enduring Legacy," *Educational Psychologist,* Vol. 40, No. 2, 2005, pp. 67-74. (RW 4982)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Wilbert, C. *Children Learn to Share by Age 7 Or 8,* (RW 3230)

Wilcox, F. "Intelligence Reform: Winning the "for Keeps" Game," *American Intelligence Journal,* Vol. 25, No. 1, 2007, pp. 51. (RW 3223)

Wilensky, H.L. *Organizational Intelligence: Knowledge and Policy in Government and Industry,* Basic Books, New York, NY, 1967. (RW 929)

Wilkinson, B.J. *Panel Discussion: Metrics and Measures for Intelligence Analysis Task Difficulty. 2005 International Conference on Intelligence Analysis. Powerpoint Presentation Briefing Notes* 2005. (RW 3869)

Wilkinson, B.J. "Panel Discussion: Metrics and Measures for Intelligence Analysis Task Difficulty. Powerpoint Presentation," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2-6 May 2005 (RW 1113)

Wilkinson, M. "The Battle of Stalingrad, Biological Weapons, and the Expert Witness: Challenging Single-Source Evidence in Intelligence Studies," *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 4, 2012, pp. 795-813. (RW 5836)

Willey, R.J. "Audience Awareness: Methods and Madness", *37th Annual Meeting of the Conference on College Composition and Communication,* New Orleans, LA, March 13-15, 1986 (RW 4497)

Williams, A.V. & Peot, G. *Intelligence and Responsibility: A Study on Intelligence and Responsibility in Modern Democracies. Investigations on Three Case Studies,* Lund University, Lund, Sweden, [undated]. (RW 495)

Williams, C.H. "Doing Critical Thinking Together: Applications to Government, Politics, and Public Policy," *PS: Political Science and Politics,* Vol. 24, No. 3, 1991, pp. 510-516. (RW 3970)

Williams, J.P. "The Importance of Examining Beliefs about Text," in *Beliefs about Texts and Instruction with Text,* eds. R. Garner & P.A. Alexander, L. Erlbaum Associates, Hillsdale, NJ, 1994, pp. xi. (RW 2815)

Williams, K. & Patman, F. "Personal Entity Extraction Filtering using Name Data Stores," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 863)

Williams, M.A. "Best Practices for Technology Support to Analytic Best Practices [Powerpoint Presentation]", *Global Intelligence Forum 2010,* Dungarvan, Ireland, July 11-13, 2010 (RW 4234)

Williams, P. "Intelligence Requirements for Transnational Threats: New Ways of Thinking, Alternative Methods of Analysis and Innovative Organizational Structures", *New Frontiers of Intelligence Analysis: Shared Threats, Diverse Perspectives, New Communities,* Rome, Italy, 31 March - 2 April, 2004, pp. 35-62. (RW 4666)

Williams, P. "21st Century Challenges to Warning: The Rise of Non-State Networked Threats", *Global Futures Forum: Emerging Threats in the 21st Century,* Zurich, Switzerland, November 9-11, 2006, pp. 10-12. (RW 5671)

Williams, W.M. & Sternberg, R.J. "Group Intelligence: Why Some Groups are Better than Others," *Intelligence,* Vol. 12, No. 4, 1988, pp. 351. (RW 2093)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Williams, W.M. "Blissfully Ignorant," *Psychological Science in the Public Interest*, Vol. 5, No. 3, 2004, pp. i-ii. (RW 1074)

Williams-Taliaferro, E.L. "Timeline Analysis," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press; Mercyhurst College Institute of Intelligence Studies Press, Erie, PA; Erie, PA, 2006, pp. 63-70. (RW 3611)

Willingham, D.T. "Inflexible Knowledge: The First Step to Expertise," *American Educator*, Winter, 2002, [unpaged]. (RW 3690)

Willingham, D.T. "Students Remember...What They Think About," *American Educator*, Summer, 2003, [unpaged]. (RW 3691)

Willingham, D.T. "Critical Thinking: Why is it so Hard to Teach?" *American Educator*, Vol. 31, No. 2, 2007, pp. 8-19. (RW 3677)

Willis, J.T. *Affective Dispositions and Cognitive Skills in Critical Thinking: Implications for Measurement, Training, and Team Performance*, Master of Arts thesis, University of South Florida, 2004. (RW 5017)

Wilson, E.O. *The Social Conquest of Earth*, Liveright Pub. Corp., New York, 2012. (RW 5908)

Wilson, J.Q. "Thinking about Reorganization," in *U.S. Intelligence at the Crossroads: Agendas for Reform*, eds. R. Godson, E.R. May & G.J. Schmitt, Brassey's, Washington, DC, 1995, pp. 28-35. (RW 639)

Wilson, M. *Toward an Ontology of Integrated Intelligence and Conflict. A Primer*, Decision Support Systems Inc., Reno, NV, 2001. (RW 245)

Wilson, M. *Continual and Complete Intelligence. A 21st Century Approach*, Decision Support Systems, Inc., Reno, NV, 2002. (RW 478)

Wilson, S.V. "American Intelligence and the Tricentennial," *Studies in Intelligence*, Vol. 20, No. 3, 1976, pp. 1-7. (RW 521)

Wilson, T.D. "The Nonsense of 'Knowledge Management'," *Information Research*, Vol. 8, No. 1, 2003 (RW 4374)

Wilson, T.R. *Asymmetric Approaches to Joint Vision 2020*, Center for Information Policy Research, Harvard University, Cambridge, MA, 2001. (RW 1152)

Wilson, T.D. *Strangers to Ourselves: Discovering the Adaptive Unconscious*, Belknap Press of Harvard University Press, Cambridge, MA, 2002. (RW 2167)

Wilson, T.D. & Bar-Anan, Y. "Psychology: The Unseen Mind," *Science*, Vol. 321, No. 5892, 2008, pp. 1046. (RW 3242)

Windschitl, M. & Andre, T. "Using Computer Simulations to Enhance Conceptual Change: The Roles of Constructivist Instruction and Student Epistemological Beliefs," *Journal of Research in Science Teaching*, Vol. 35, No. 2, 1998, pp. 145-160. (RW 4648)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Windschitl, P.D. & Chambers, J.R. "The Dud-Alternative Effect in Likelihood Judgment," *Journal of Experimental Psychology: Learning, Memory, & Cognition,* Vol. 30, No. 1, 2004, pp. 198-215. (RW 1923)

Wineburg, S. "Reading Abraham Lincoln: An Expert/Expert Study in the Interpretation of Historical Texts," *Cognitive Science,* Vol. 22, No. 3, 1998, pp. 319. (RW 5095)

Wineburg, S.S. "Historical Problem Solving: A Study of the Cognitive Processes used in the Evaluation of Documentary and Pictorial Evidence," *Journal of Educational Psychology,* Vol. 83, No. 1, 1991, pp. 73. (RW 3997)

Wing, I.G.R. "Chaos Theory and Intelligence Analysis," *Australian Defence Force Journal,* 115, 1995, pp. 21-26. (RW 83)

Winks, R.W. *Cloak & Gown: Scholars in the Secret War, 1939-1961,* 2nd ed., Yale University Press, New Haven, 1996. (RW 2960)

Winn, A.C. "The Future of US Intelligence," *Parameters,* Summer, 2006, pp. 120. (RW 1422)

Winn, A.C. "Strategic Intelligence," *Parameters,* Spring, 2008, pp. 91. (RW 3074)

Winne, P.H. & Jamieson-Noel, D. "Exploring Students' Calibration of Self Reports about Study Tactics and Achievement," *Contemporary Educational Psychology,* Vol. 27, No. 4, 2002, pp. 551. (RW 5304)

Winston, P.H. & Horn, B. *The Psychology of Computer Vision,* McGraw-Hill, New York, 1975. (RW 2533)

Wippl, J.W. "Intelligence Exchange through InterIntel," *International Journal of Intelligence and Counterintelligence,* Vol. 25, No. 1, 2012, pp. 1-18. (RW 5397)

Wirtz, J. "Hiding in Plain Sight: Denial, Deception and the Non-State Actor," *SAIS Review,* Vol. 28, No. 1, 2008, pp. 55-63. (RW 4363)

Wirtz, J.J. *The Tet Offensive: Intelligence Failure in War,* Cornell University Press, Ithaca, NY, 1991. (RW 4891)

Wirtz, J.J. "The "Unlessons" of Vietnam," *Defense Analysis,* Vol. 17, No. 1, 2001, pp. 41-57. (RW 508)

Wirtz, J.J. "DejaVu? Comparing Pearl Harbor and September 11," *Harvard International Review,* Vol. 24, No. 3, 2002, pp. 73-77. (RW 294)

Wirtz, J.J. "Theory of Surprise," in *Paradoxes of Strategic Intelligence: Essays in Honor of Michael I. Handel,* eds. M.I. Handel, R.K. Betts & T.G. Mahnken, Frank Cass, London, UK, 2003, pp. 101-116. (RW 215)

Wirtz, J.J. "Miscalculation, Surprise, and U.S. Intelligence," in *Intelligence and the National Security Strategist: Enduring Issues and Challenges,* eds. R.Z. George & R.D. Kline, National Defense University Press, Washington, DC, 2004, pp. 389-398. (RW 697)

Wirtz, J.J. "The American Approach to Intelligence Studies," in *Handbook of Intelligence Studies,* ed. L.K. Johnson, 2007, pp. 28. (RW 2455)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Wirtz, J.J. "The Intelligence-Policy Nexus," in *Strategic Intelligence. Volume 1: Understanding the Hidden Side of Government*, ed. L.K. Johnson, Praeger Security International, Westport, CT, 2007, pp. 139. (RW 2713)

Wirtz, J.J. "Theory of Surprise," in *Intelligence Theory: Key Questions and Debates*, eds. P. Gill, S. Marrin & M. Phythian, 2009, pp. 73. (RW 3406)

Wirtz, J.J. & Rosenwasser, J.J. "From Combined Arms to Combined Intelligence: Philosophy, Doctrine, and Operations," *Intelligence and National Security,* Vol. 25, No. 6, 2010, pp. 725-743. (RW 4572)

Wise, J.C., Lee, S.H., Litzinger, T., Marra, R.M. & Palmer, B. "A Report on a Four-Year Longitudinal Study of Intellectual Development of Engineering Undergraduates," *Journal of Adult Development,* Vol. 11, No. 2, 2004, pp. 103-110. (RW 5570)

Witlin, L. "Mirror-Imaging and its Dangers," *SAIS Review,* Vol. 28, No. 1, 2008, pp. 89. (RW 3328)

Wittenbaum, G.M. & Stasser, G. "The Reevaluation of Information during Discussion," *Group Processes and Intergroup Relations,* Vol. 1, 1998, pp. 21. (RW 2151)

Wittenbaum, G.M. & Park, E.S. "The Collective Preference for Shared Information," *Current Directions in Psychological Science,* Vol. 10, 2001, pp. 70. (RW 1880)

Wobensmith, J.C. & Smith, J. "Reinvigorating Intelligence," *Journal of International Security Affairs,* 12, 2007 (RW 2955)

Wohlstetter, A. "Is there a Strategic Arms Race?" *Foreign Policy,* 15, 1974, pp. 3-20. (RW 748)

Wohlstetter, A. "Optimal Ways to Confuse Ourselves," *Foreign Policy,* 20 (Fall), 1975, pp. 170-198. (RW 719)

Wolfberg, A. *To Transform into a More Capable Intelligence Community: A Paradigm Shift in the Analyst Selection Strategy*, National Defense University, Washington, DC, 2003. (RW 766)

Wolfberg, A. "The Challenges of Creating a New Analytical Culture," *American Intelligence Journal,* Vol. 22, Spring/Summer, 2004, pp. 11-20. (RW 690)

Wolfberg, A. "Investing in the Social Capital of Knowledge," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2-6 May 2005 (RW 610)

Wolfberg, A. "Full Spectrum Analysis: A New Way of Thinking for a New World," *Military Review,* July-August, 2006, pp. 35. (RW 1622)

Wolfberg, A. & Dixon, N. "Speaking Truth to Power: Nurturing a Reflective Culture at the U.S. Defense Intelligence Agency," *Reflections,* Vol. 10, No. 4, 2011, pp. 12. (RW 5415)

Wolfberg, A. & Pelley, B. "The Role of Innovation: Creating a Culture of Improvement," *American Intelligence Journal,* Vol. 26, No. 2, 2008/2009, pp. 30. (RW 3628)

Wolfe, F. *Scientific Method* 1930. (RW 4735)

Wolfinger, N.H. "On Writing Fieldnotes: Collection Strategies and Background Expectancies," *Qualitative Research,* Vol. 2, No. 1, 2002, pp. 85. (RW 2120)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Wolverton, M., Harrison, I., Lowrance, J., Rodriguez, A. & Thomere, J. "Supporting the Pattern Development Cycle in Intelligence Gathering," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 872)

Wong, B.L.W., Xu, K. & Attfield, S. "Provenance for Intelligence Analysis using Visual Analytics", *CHI 2011: Workshop on Analytic Provenance,* Vancouver, BC, May 7-8, 2011, [unpaged]. (RW 5511)

Wong, B., Khine, M.S. & Sing, C.C. "Challenges and Future Directions for Personal Epistemology Research in Diverse Cultures," in *Knowing, Knowledge and Beliefs: Epistemological Studies Across Diverse Cultures,* ed. M.S. Khine, Springer, Dordrecht, 2008, pp. 445-456. (RW 4359)

Wong, J.N. "The Progress of Pinyin," *Studies in Intelligence,* Vol. 5, No. 1, 1961, pp. A35-A52. (RW 567)

Wong, K.W.J. *Development of Selection Evaluation and System Intelligence Analytic Models for the Intelligent Building Control Systems,* PH.D. dissertation, Hong Kong Polytechnic University, 2007. (RW 4543)

Woocher, L. *Conflict Assessment and Intelligence Analysis,* Special Report 275, United States Institute of Peace, Washington, DC, 2011. (RW 5514)

Wood, J.V., Perunovic, W.Q.E. & Lee, J.W. "Positive Self Statements: Power for some, Peril for Others," *Psychological Science,* Vol. 20, No. 7, 2009, pp. 860-866. (RW 3490)

Wood, P. & Kardash, C. "Critical Elements in the Design and Analysis of Studies of Epistemology," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing,* eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 231. (RW 4334)

Wood, P., Kitchener, K. & Jensen, L. "Considerations in the Design and Evaluation of a Paper-and-Pencil Measure of Epistemic Cognition," in *Personal Epistemology: The Psychology of Beliefs about Knowledge and Knowing,* eds. B.K. Hofer & P.R. Pintrich, L. Erlbaum Associates, Mahwah, NJ, 2002, pp. 277. (RW 4391)

Woodard, N. "Tasting the Forbidden Fruit: Unlocking the Potential of Positive Politicization," *Intelligence and National Security,* Vol. 28, No. 1, 2013, pp. 91-108. (RW 5915)

Woods, D.D. "Visual Momentum: A Concept to Improve the Cognitive Coupling of Person and Computer," *International Journal of Man Machine Studies,* Vol. 21, 1984, pp. 229. (RW 1597)

Woods, D.D. "The Cognitive Engineering of Problem Representations," in *Human-Computer Interaction and Complex Systems,* eds. G.R.S. Weir & J.L. Alty, Academic Press, London; San Diego, California, 1991, pp. 169. (RW 1598)

Woods, D.D. "The Price of Flexibility in Intelligent Interfaces," *Knowledge-Based Systems,* Vol. 6, 1993, pp. 1. (RW 1599)

Woods, D.D. "Cognitive Demands and Activities in Dynamic Fault Management: Abduction and Disturbance Management," in *Human Factors in Alarm Design,* ed. N. Stanton, Taylor & Francis, London, 1994, pp. 63. (RW 1589)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Woods, D.D. "The Alarm Problem and Directed Attention in Dynamic Fault Management," *Ergonomics*, Vol. 38, No. 11, 1995, pp. 2371. (RW 1600)

Woods, D.D. "Towards a Theoretical Base for Representation Design in the Computer Medium: Ecological Perception and Aiding Human Cognition," in *Global Perspectives on the Ecology of Human-Machine Systems*, ed. J. Flach, 1995, pp. 157. (RW 1602)

Woods, D.D. "Steering the Reverberations of Technological Change on Fields of Practice: Laws that Govern Cognitive Work." (RW 1587)

Woods, D.D. & Dekker, S.W.A. "Anticipating the Effects of Technological Change: A New Era of Dynamics for Human Factors," *Theoretical Issues in Ergonomics Science*, Vol. 1, No. 3, 2000, pp. 272. (RW 1588)

Woods, D.D. & Patterson, E. "How Unexpected Events Produce an Escalation of Cognitive and Coordinative Demands," in *Stress, Workload, and Fatigue*, eds. P.A. Hancock & P.A. Desmond, L. Erlbaum Associates, Mahwah, N.J, 2001, pp. 290. (RW 1595)

Woods, D.D., Patterson, E.S. & Roth, E.M. "Can We Ever Escape from Data Overload?" *Cognition, Technology, and Work*, Vol. 42, 002, pp. 22-36. (RW 1469)

Woods, D.D. & Sarter, N. "Learning from Automation Surprises and Going Sour Accidents," in *Cognitive Engineering in the Aviation Domain*, eds. N.B. Sarter & R.I. Amalberti, L. Erlbaum Associates, Mahwah, N.J, 2000, pp. 327. (RW 1590)

Woods, D.D. & Watts, J.C. "How Not to Have to Navigate Through Too Many Displays," in *Handbook of Human-Computer Interaction*, eds. M. Helander, T.K. Landauer & P.V. Prabhu, 2nd ed., Elsevier, Amsterdam, 1997, pp. 617. (RW 1591)

Woods, D.D. *Chapter 14 - Failure as System Information. Draft from Behind Human Error. Author's Copy* [undated]. (RW 2005)

Woods, D.D. *Chapter 15 - Fundamental Surprise. Draft from Behind Human Error. Author's Copy* [undated]. (RW 2006)

Woods, D.D. *Behind Human Error*, 2nd ed., Ashgate, Burlington, VT, 2010. (RW 4593)

Woods, D.D. & Cook, R.I. "Perspectives on Human Error: Hindsight Biases and Local Rationality," in *Handbook of Applied Cognition*, eds. F.T. Durso, R.S. Nickerson & J.D. Schvaneveldt, John Wiley & Sons, New York, NY, pp. 141-171. (RW 1944)

Woods, D.D. & Hollnagel, E. *Joint Cognitive Systems: Patterns in Cognitive Systems Engineering*, CRC, Taylor & Francis, Boca Raton, FL, 2006. (RW 4725)

Woods, D.D., Johannesen, L.J., Cook, R.I. & Sarter, N.B. *Behind Human Error; Cognitive Systems, Computers, and Hindsight*, Crew Systems Ergonomics Information Analysis Center, Wright-Patterson Air Force Base, Ohio, 1994. (RW 1594)

Woods, D.D., Patterson, E.S. & Roth, E.M. *Aiding the Intelligence Analyst in Situations of Data Overload. A Diagnosis of Data Overload*, ERGO-CSEL 98-TR-03, Ohio State University, Columbus, OH, 1998. (RW 200)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Woods, D.D., Patterson, E.S. & Roth, E.M. *Can We Ever Escape from Data Overload? A Cognitive Systems Diagnosis,* AFRL-HE-WP-TR-1999-0195, Ohio State University and Roth Cognitive Engineering, Columbus, OH, 1998. (RW 199)

Woods, D.D., Pople, H.E., Roth, E.M., *The Cognitive Environment Simulation as a Tool for Modeling Human Performance and Reliability,* NUREG/CR-5213 ed., Division of Systems Research, Office of Nuclear Regulatory Research, U.S. Nuclear Regulatory Commission, Washington, DC, 1990. (RW 1596)

Woolley, A.W., Hackman, J.R., Jerde, T.E., Chabris, C.F., Bennett, S.L. & Kosslyn, S.M. "Using Brain-Based Measures to Compose Teams: How Individual Capabilities and Team Collaboration Strategies Jointly Shape Performance," *Social Neuroscience,* Vol. 2, No. 2, 2007, pp. 96. (RW 3730)

Woolley, A.W., Gerbasi, M.E., Chabris, C.F., Kosslyn, S.M. & Hackman, J.R. *What Does it Take to Figure Out What is Going On? How Team Ability Composition and Work Strategy Jointly Shape Analytic Effectiveness,* The Group Brain Project, technical report no. 4, 2007. (RW 3014)

Woolley, A.W. & Hackman, J.R. *Defining Analytic Zones in Organizations,* The Group Brain Project, technical report no. 3, 2006. (RW 3013)

Woolley, A.W., Hackman, J.R., Jerde, T.E., Chabris, C.F., Bennett, S.L. & Kosslyn, S.M. *Using Brain-Based Measures to Compose Teams: How Individual Capabilities and Team Collaboration Strategies Jointly Shape Performance,* The Group Brain Project, technical report no. 1, 2006. (RW 3011)

Woolley, A.W., Gerbasi, M.E., Chabris, C.F., Kosslyn, S.M. & Hackman, J.R. "Bringing in the Experts: How Team Composition and Collaborative Planning Jointly Shape Analytic Effectiveness," *Small Group Research,* Vol. 39, No. 3, 2008, pp. 352. (RW 3729)

Woolsey, R.J. *Statement for the Record. Hearings of the Senate Select Committee on Intelligence.* 1996. (RW 458)

Wooster, H. "The Zoo and the Jungle - a Comparison of the Information Practices of Intelligence Analysts and of Scientists," in *Information System Science and Technology: Papers Prepared for the Third Congress,* eds. D.E. Walker, Thompson Book Co., Washington, DC, 1967, pp. 307. (RW 1475)

Worth, S. "Narrative Knowledge: Knowing through Storytelling", *MIT4: The Work of Stories. Fourth Media in Transition Conference,* May 6-8, 2005. (RW 3564)

Worthen, H. & Berchman, M. "Apprenticeships: What Happens in Onthe-the-Job Training (OJT)?" in *Learning through Practice: Models, Traditions, Orientations, and Approaches,* ed. S. Billett, Springer, Dordrecht, 2010, pp. 222-239. (RW 4962)

Wortman, P.M. "Judging Research Quality," in *The Handbook of Research Synthesis,* eds. H.M. Cooper & L.V. Hedges, Russell Sage Foundation, New York, 1994, pp. 97. (RW 2488)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Wozny, J.L. "Alternative Thinking Techniques," in *The Analyst's Cookbook. Volume I.*, eds. K.J. Wheaton, E.E. Mosco & D.E. Chido, Mercyhurst College Institute of Intelligence Studies Press, Erie, PA, 2006, pp. 29-34. (RW 3607)

Wright, A. *Glut: Mastering Information through the Ages,* Joseph Henry Press, Washington, DC, 2007. (RW 3184)

Wright, D.P. "Instruction in Critical Thinking: A Three Part Investigation", *Annual Meeting of the American Educational Research Association,* New York, NY, April 3-6, 1977 (RW 4465)

Wright, R. *The Moral Animal: Evolutionary Psychology and Everyday Life,* 1st Vintage books ed., Vintage Books, New York, 1995. (RW 2409)

Wright, W., Schroh, D., Roulx, P., Skaburskis, A. & Cort, B. "Advances in nSpace - the Sandbox for Analysis," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 810)

Wright, W., Schroh, D., Roulx, P., Skaburskis, A. & Cort, B. "The Sandbox for Analysis - Concepts and Methods", *CHI 2006 Proceedings*, Montreal, Quebec, Canada, April 22-27, 2006, pp. 801. (RW 1524)

Wu, Y. & Tsai, C. "High School Students' Informal Reasoning regarding a Socio-Scientific Issue, with Relation to Scientific Epistemological Beliefs and Cognitive Structures," *International Journal of Science Education,* Vol. 33, No. 3, 2011, pp. 371-400. (RW 5230)

Wuchty, S., Jones, B.F. & Uzzi, B. "The Increasing Dominance of Teams in Production of Knowledge," *Science,* Vol. 316, No. 5827, 2007, pp. 1036. (RW 2401)

Wurdinger, S.D. & Carlson, J. *Teaching for Experiential Learning: Five Approaches that Work,* Rowman & Littlefield Education, Lanham, MD, 2010. (RW 4882)

Yan, P., Chen, H. & Zeng, D. "Syndromic Surveillance Systems," *Annual Review of Information Science and Technology,* Vol. 42, No. 1, 2008, pp. 425-594. (RW 4432)

Yang, S. "Information Seeking as Problem-Solving using a Qualitative Approach to Uncover the Novice Learners' Information-Seeking Process in a Perseus Hypertext System," *Library and Information Science Research,* Vol. 19, No. 1, 1997, pp. 71. (RW 2147)

Yang, Y., Yoo, S., Zhang, J. & Kisiel, B. "A Cross-Benchmark Evaluation of Adaptive Filtering Methods," 2005 *International Conference on Intelligence Analysis,* McLean, VA, 2 - 6 May 2005. (RW 799)

Yeaton, W.H., Langenbrunner, J.C., Smyth, J.M. & Wortman, P.M. "Exploratory Research Synthesis: Methodological Considerations for Addressing Limitations in Data Quality," *Evaluation and the Health Professions,* Vol. 18, 1995, pp. 283. (RW 2197)

Yee, S.H., Rogers, J.E., Harvey, J., Fisher, W., Russell, M. & Bradley, P. "Cocnept Mapping Ecosystem Goods and Services," in *Applied Concept Mapping: Capturing, Analyzing, and Organizing Knowledge*, eds. B.M. Moon, R.R. Hoffman, J.D. Novak & A.J. Canas, CRC Press, Boca Raton, FL, 2011, pp. 193-214. (RW 4972)

Yeh, P.F. "Using Prediction Markets to Enhance US Intelligence Capabilities," *Studies in Intelligence,* Vol. 50, No. 4, 2006 (RW 1971)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Yeh, S.S. "Tests Worth Teaching to: Constructing State-Mandated Tests that Emphasize Critical Thinking," *Educational Researcher,* Vol. 30, No. 9, 2001, pp. 12-17. (RW 4113)

Yetiv, S.A. "Groupthink and the Gulf Crisis," *British Journal of Political Science,* Vol. 33, No. 3, 2003, pp. 419-439. (RW 220)

Yi, Y. "The Effects of Contextual Priming in Print Advertisements," *Journal of Consumer Research,* Vol. 17, No. 2, 1990, pp. 215-222. (RW 5688)

Yore, L.D., Florence, M.K., Pearson, T.W. & Weaver, A.J. "Written Discourse in Scientific Communities: A Conversation with Two Scientists about their Views of Science, use of Language, Role of Writing in Doing Science, and Compatibility between their Epistemic Views and Language," *International Journal of Science Education,* Vol. 28, No. 2-3, 2006, pp. 109. (RW 2327)

Yore, L.D., Hand, B.M. & Florence, M.K. "Scientists' Views of Science, Models of Writing, and Science Writing Practices," *Journal of Research in Science Teaching,* Vol. 41, No. 4, 2004, pp. 338. (RW 2330)

Youn, I. "The Culture Specificity of Epistemological Beliefs about Learning," *Asian Journal of Social Psychology,* Vol. 3, No. 1, 2000 (RW 5532)

Young, G. *Reasoning Backwards: Sherlock Holmes' Guide to Effective Problem Solving,* Young Associates Inc., Midland, MI, 2011. (RW 4550)

Young, J.T. "US Intelligence Assessment in a Changing World: The Need for Reform," *Intelligence and National Security,* Vol. 8, No. 2, 1993, pp. 127-139. (RW 1065)

Young, J.T. "Reengineering US Intelligence," in *Brassey's Mershon American Defense Annual. Current Issues and the Asian Challenge*, eds. W. Murray & A.R. Millett, Ohio State University, Columbus, OH, 1996, pp. 28-57. (RW 149)

Young, N.S., Ioannidis, J.P.A. & Al-Ubaydli, O. "Why Current Publication Practices may Distort Science," *PLoS Medicine,* Vol. 5, No. 10, 2008, pp. e201. (RW 3288)

Yussen, S.R. "The Role of Metacognition in Contemporary Theories of Cognitive Development," in *Metacognition, Cognition, and Human Performance*, eds. G.E. MacKinnon, T.G. Waller & D. Forrest-Pressley, Academic Press, Orlando, FL, 1985, pp. 253-283. (RW 5367)

Zaccaro, S.J. *The Nature of Executive Leadership: A Conceptual and Empirical Analysis of Success,* American Psychological Association, Washington, DC, 2001. (RW 3049)

Zadarecky, J. *The Role of Air Force in U.S. Counternarcotics Policy,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1991. (RW 1043)

Zak, P.J., Borja, K., Matzner, W.T. & Kurzban, R. "The Neuroeconomics of Distrust: Sex Differences in Behavior and Physiology," *American Economic Review,* Vol. 95, No. 2, 2005, pp. 360. (RW 2051)

Zechmeister, E.B. & Johnson, J.E. *Critical Thinking: A Functional Approach,* Brooks/Cole Publishing Co., Pacific Grove, CA, 1992. (RW 3862)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Zegart, A. "Implementing Change: Organizational Challenges," in *Intelligence Analysis: Behavioral and Social Scientific Foundations*, eds. B. Fischhoff & C. Chauvin, National Academies Press, Washington, DC, 2011, pp. 309-329. (RW 4782)

Zegart, A.B. *Through the Looking Glass: September 11th and the Adaptation Failure of American Intelligence Agencies. Draft* 2004. (RW 510)

Zegart, A.B. *Written Remarks for the Record. The Senate Select Committee on Intelligence* 2004. (RW 312)

Zegart, A.B. "September 11 and the Adaptation Failure of US Intelligence Agencies," *International Security*, Vol. 29, No. 4, 2005, pp. 78-111. (RW 447)

Zegart, A.B. "An Empirical Analysis of Failed Intelligence Reforms before September 11," *Political Science Quarterly*, Vol. 121, No. 1, 2006, pp. 33. (RW 2266)

Zegart, A.B. “Cloaks, Daggers, and Ivory Towers: Why Academics Don’t Study U.S. Intelligence,” in *Strategic Intelligence*, ed. L.K. Johnson, Praeger Security International, Westport, CT, 2007, pp. 21. (RW 2710)

Zegart, A.B. ""CNN with Secrets:" 9/11, the CIA, and the Organizational Roots of Failure," *International Journal of Intelligence and Counterintelligence*, Vol. 20, No. 1, 2007, pp. 18. (RW 1755)

Zegart, A.B. *Spying Blind: The CIA, the FBI, and the Origins of 911*, Princeton University Press, Princeton, NJ, 2007. (RW 3007)

Zegart, A.B. ""Spytainment": The Real Influence of Fake Spies," *International Journal of Intelligence and Counterintelligence*, Vol. 23, No. 4, 2010, pp. 599. (RW 4310)

Zegart, A.B. *Eyes on Spies: Congress and the United States Intelligence Community*, Hoover Institution 2011. (RW 5043)

Zegart, A. & Quinn, J. "Congressional Intelligence Oversight: The Electoral Disconnection," *Intelligence and National Security*, Vol. 25, No. 6, 2010, pp. 744-766. (RW 4573)

Zeigler, M., Danay, E., Heene, M., Asendorpf, J. & Buhner, M. "Openness, Fluid Intelligence, and Crystallized Intelligence: Toward an Integrative Model," *Journal of Research in Personality*, [draft], 2012. (RW 5427)

Zeitz, P. *The Art and Craft of Problem Solving*, 2nd ed., John Wiley, Hoboken, NJ, 2007. (RW 2651)

Zelenko, D., Aone, C. & Tibbetts, J. "Trainable Evidence Extraction System (TEES),” 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 880)

Zelik, D.J., Patterson, E.S. & Woods, D.D. *Judging Sufficiency: How Professional Intelligence Analysts Assess Analytical Rigor* (RW 2981)

Zelik, D., Patterson, E.S. & Woods, D.D. "Supporting the Assessment of Rigor: Representing Analysis to Create Process Insight", *2nd Annual Workshop on Meta-Information Portrayal*, Washington, DC, August 21-23, 2007 (RW 3131)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Zelik, D., Patterson, E.S. & Woods, D.D. *When is Analysis Sufficient? A Study of How Professional Intelligence Analysts Judge Rigor* 2007. (RW 2991)

Zelik, D., Patterson, E. & Woods, D.D. "Understanding Rigor in Information Analysis", *Proceedings of the 8th International NCM Conference.* (RW 2279)

Zelikow, P. "American Economic Intelligence: Past Practice and Future Principles," in *Eternal Vigilance? 50 Years of the CIA*, eds. R. Jeffreys-Jones & C. Andrew, F. Cass, London, UK, 1997, pp. 164-177. (RW 8)

Zelikow, P. "The Evolution of Intelligence Reform, 2002-200," *Studies in Intelligence,* Vol. 56, No. 3, 2012, pp. 1-20. (RW 5901)

Zelniker, T. "Cognitive Style and Dimensions of Information Processing," in *Cognitive Style and Cognitive Development*, eds. T. Globerson & T. Zelniker, Ablex Publishing, Norwood, NJ, 1989, pp. 172-191. (RW 5251)

Zemirli, W.N., Tamine-Lechani, L. & Boughanem, M. "A Personalized Retrieval Model Based on Influence Diagrams", *Proceedings of the 2nd International Workshop on Context-Based Information Retrieval*, Roskilde University, Denmark, August 21, 2007. (RW 4869)

Zenhausern, R. "Imagery, Cerebral Dominance, and Style of Thinking: A Unified Field Model," *Bulletin of the Psychonomic Society,* Vol. 12, 1978, pp. 381. (RW 2432)

Zetik, D.C. & Stuhlmacher, M.F. "Goal Setting and Negotiation Performance: A Meta-Analysis," *Group Processes & Intergroup Relations,* Vol. 5, No. 1, 2002, pp. 35. (RW 2568)

Zhang, L.F. & Sternberg, R.J. "Intellectual Styles and Creativity," in *Routledge Companion to Creativity* 2009, pp. 256. (RW 3053)

Zhang, L., Sampson, M. & McGowan, J. "Reporting of the Role of the Expert Searcher in Cochrane Reviews," *Evidence Based Library and Information Practice,* Vol. 1, No. 4, 2006, pp. 3-16. (RW 4800)

Zhang, L. "A Comparison of U.S. and Chinese University Students' Cognitive Development: The Cross-Cultural Applicability of Perry's Theory," *Journal of Psychology,* Vol. 133, No. 4, 1999, pp. 425. (RW 5571)

Zhang, L. & Sternberg, R.J. *The Nature of Intellectual Styles,* L. Erlbaum Associates, Mahwah, NJ, 2006. (RW 3051)

Zhang, L. & Guan, Y. "Topology-Aware Single Message Attack Traceback," 2005 *International Conference on Intelligence Analysis*, McLean, VA, 2 - 6 May 2005. (RW 878)

Zhang, T. "Self-Identity Construction of the Present China," *Comparative Strategy,* Vol. 23, No. 3, 2004, pp. 281-301. (RW 385)

Zhu, C., Valcke, M. & Schellens, T. "The Relationship between Epistemological Beliefs, Learning Conceptions, and Approaches to Study: A Cross-Cultural Structural Model?" *Asia Pacific Journal of Education,* Vol. 28, No. 4, 2008, pp. 411-423. (RW 5235)

Zimmerman, C. "The Development of Scientific Reasoning Skills," *Developmental Review,* Vol. 20, No. 1, 2000, pp. 99. (RW 1883)

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

Zimmerman, C. *The Development of Scientific Reasoning Skills: What Psychologists Contribute to an Understanding of Elementary Science Learning* 2005. (RW 2186)

Zimmermann, D. "The Security Intelligent Enterprise," *International Journal of Intelligence and Counterintelligence,* Vol. 24, No. 3, 2011, pp. 569-574. (RW 5404)

Zimper, A. & Ludwig, A. "On Attitude Polarization Under Bayesian Learning with Non-Additive Beliefs," *Journal of Risk and Uncertainty,* Vol. 39, No. 2, 2009, pp. 181-212. (RW 4621)

Zinner, C. "Intelligence must Plan to Develop Tomorrow's Analyst," *Signal,* Vol. 63, No. 8, 2009, pp. 69-73. (RW 4547)

Zlotnick, J. *National Intelligence,* Industrial College of the Armed Forces, Washington, DC, 1964. (RW 777)

Zlotnick, J. "A Theorem for Prediction," *Studies in Intelligence,* Vol. 11, No. 4, 1967, pp. 1-12. (RW 4211)

Zlotnick, J. "Bayes' Theorem for Intelligence Analysis," *Studies in Intelligence,* Vol. 16, No. 2, 1972, pp. 43-52. (RW 526)

Zraket, C.A. *Four Vital Issues in C3I,* Center for Information Policy Research. Harvard University, Cambridge, MA, 1990. (RW 1044)

Zukas, A. & Price, R.J. "Document Categorization using Latent Semantic Indexing", *2003 Symposium on Document Image Understanding Technology,* Greenbelt, MD, April 9-11, 2003, pp. 87-91. (RW 893)

Zuniga-Brown, T. "Mind on Minds: Education and National Security," *International Journal of Intelligence and Counterintelligence,* Vol. 24, No. 2, 2011, pp. 352-366. (RW 4597)

Zyzanski, S.J., McWhiney, I.R., Blake, R., Crabtree, B.F. & Miller, W.L. "Qualitative Research: Perspectives on the Future," in *Doing Qualitative Research*, eds. B.F. Crabtree & W.L. Miller, Sage Publications, Thousand Oaks, Calif, 1992, pp. 231. (RW 2779)

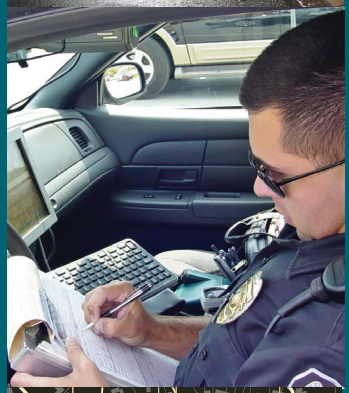
Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

LIST OF ACRONYMS

ACH	Analysis of Competing Hypotheses
AFRL	Air Force Research Laboratory
FAC	Framework for Analytic Cognition
IC	Intelligence Community
IQ	Intellectual Ability
PCASS	Preliminary Credibility Assessment Screening System
WMD	Weapons of Mass Destruction

Distribution A: Approved for public release; distribution unlimited;
88ABW-2013-5245; Cleared 12 December 2013

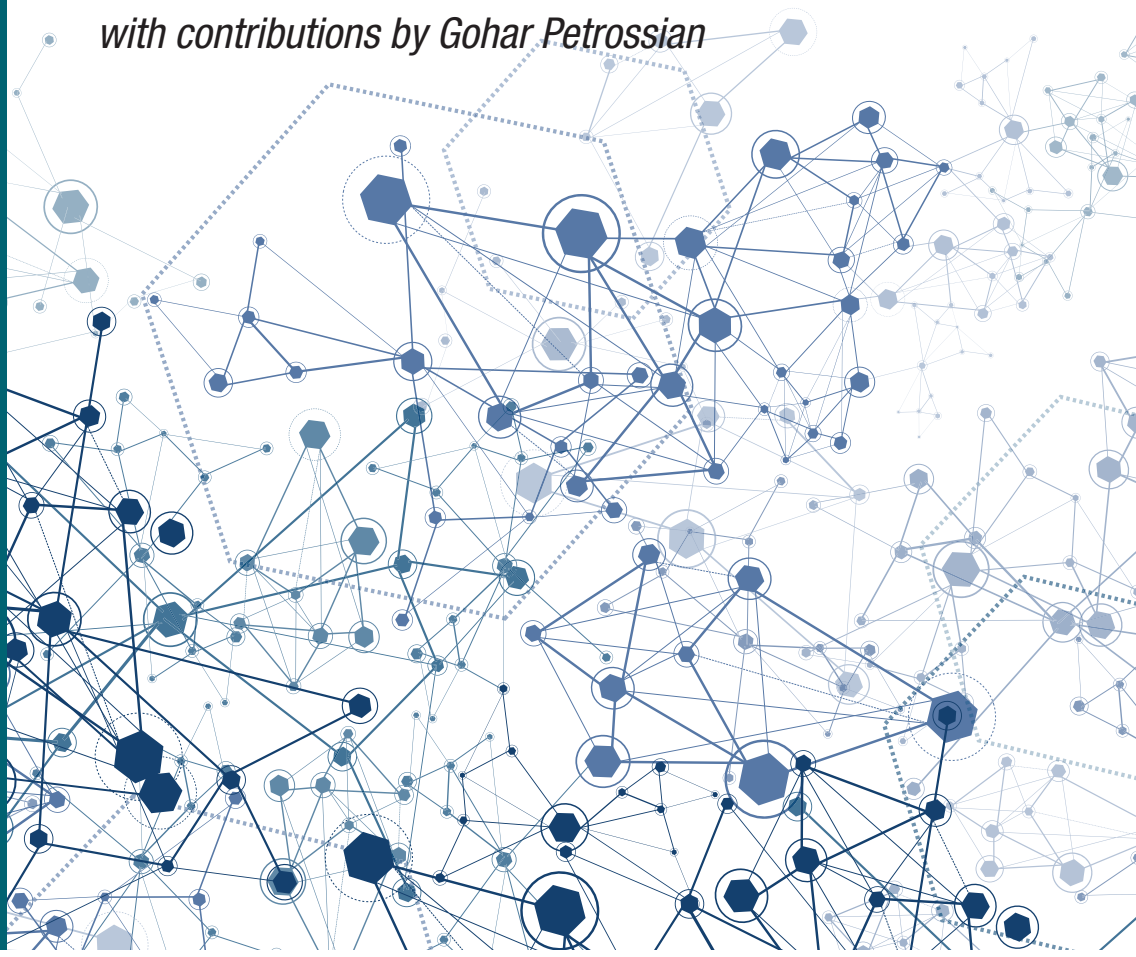
This Page Is Intentionally Left Blank



Intelligence Analysis for Problem Solvers

John E. Eck and Ronald V. Clarke

with contributions by Gohar Petrossian



COPS
Community Oriented Policing Services
U.S. Department of Justice

Center for
Problem-Oriented Policing

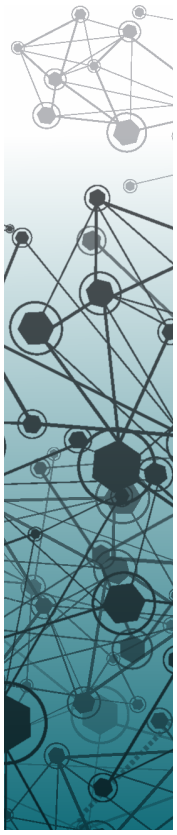
This project was supported by cooperative agreement # 2008CK-WX-K004 awarded by the Office of Community Oriented Policing Services, U.S. Department of Justice. The opinions contained herein are those of the author(s) and do not necessarily represent the official position or policies of the U.S. Department of Justice. References to specific agencies, companies, products, or services should not be considered an endorsement of the product by the author(s) or the U.S. Department of Justice. Rather, the references are illustrations to supplement discussion of the issues.

The Internet references cited in this publication were valid as of the date of this publication. Given that URLs and websites are in constant flux, neither the author(s) nor the COPS Office can vouch for their current validity.

© 2013 Center for Problem-Oriented Policing, Inc. The U.S. Department of Justice reserves a royalty-free, nonexclusive, and irrevocable license to reproduce, publish, or otherwise use, and authorize others to use, this publication for Federal Government purposes. This publication may be freely distributed and used for noncommercial and educational purposes.

ISBN: 978-1-935676-55-3

Published 2013



Intelligence Analysis for Problem Solvers

John E. Eck and Ronald V. Clarke
with contributions by Gohar Petrossian

Acknowledgments

We are grateful to the Office of Community Oriented Policing Services (COPS Office) for commissioning this manual, which is intended to be a companion volume to our earlier publication, *Crime Analysis for Problem Solvers: In 60 Small Steps*, which was also commissioned and published by the COPS Office. We thank our many colleagues and friends on whose work we have drawn. Special thanks are due to those who supplied material for inclusion: Christopher Bruce (Step 41), Mangai Natarajan (Step 20), Jerry Ratcliffe (Step 4), and Rashi Shuhkla (Step 43). Daryn Beauchesne, Leonard Miranda, Kristen Miggins, Andy Mills, Nanci Plouffe, Karin Schmerler, John Stedman, and Julie Wartell took part in a meeting, graciously hosted by the Chula Vista Police Department, to discuss our plans for the manual. Finally, we are grateful to Christopher Bruce and Andy Mills for their detailed commentary on the first draft of the manual.

John E. Eck

Ronald V. Clarke

Contents

Acknowledgments 1
Read This First 5
What is this manual about and who is it for? 5
How is the manual organized? 6
Part 1: Intelligence Analysis for Solving Problems 9
Understand the Role of Intelligence Analysis 10
1. Know What Intelligence Analysis Comprises 10
2. Know That Intelligence Analysis Must Look Beyond Enforcement 12
3. Understand the Intelligence Analysis Process 14
4. Recognize How Intelligence Analysis Fits Into Crime Analysis 16
5. Appreciate How Intelligence Fits in Policing Strategies 19
Know the Fundamentals of Criminal Groups 22
6. Recognize that Offenders Choose to Commit Crime 22
7. Pay Attention to How Crime Opportunities Arise 24
8. Distinguish between Criminal Groups and Problem Gatherings 26
9. Tell Apart Organized Crime and Organized Criminals 28
10. Modify the Conditions that Facilitate Organized Crimes 30
11. Study the *Modus Operandi* Step-by-Step 32
12. Look for Convergent Settings 35
13. Disrupt Recruitment and Replacement 37
Assemble the Key Information 40
14. Interview Offenders 40
15. Tap the Knowledge of Officers 43
16. Work with Businesses, Private Security, and the City 45
17. Work the Community 47
Produce Intelligence 49
18. Create Intelligent Maps 49
19. Use Network Analysis to Connect the Players 52
20. Undertake Conversational Analysis of Wire Tap Data 56
21. Compare Competing Hypotheses 59
22. Find Ways to Share Vital Information with Other Jurisdictions 61

Create Effective Actions 63
23. Diagram the Crime Process 63
24. Apply Situational Prevention to Each Stage of The Crime. 66
25. Work with Gatherings and Crowds. 69
26. Pull Levers. 72
Never Compromise Ethics and Integrity 74
27. Be Accountable 74
28. Do Not Delude Yourself 77
29. Be Principled in Your Work 80
30. Don't Unnecessarily Beat Yourself Up. 82
Part 2: Case Studies of Criminal Groups and Problem Gatherings 85
31. How to Read the Case Studies 86
Criminal Groups 88
32. Retail Drug Dealers 88
33. Terrorists 91
34. White Supremacists 93
35. Animal Rights Extremists 96
36. Internet Pedophile Rings 99
37. Graffiti Crews. 102
38. Outlaw Motorcycle Gangs 105
39. Street Gangs 108
40. Auto-Accident Fraud Rings 111
41. Organized Shoplifters 114
42. Organized Car Thieves 117
43. Clandestine Methamphetamine Labs. 121
Problem Gatherings 124
44. Cruising. 124
45. Illegal Street Racing 126
46. Spring Breaks 129
47. Political Demonstrations 131
48. Student Party Riots. 134
About the Authors 137

Read This First

The 9/11 Commission famously criticized the country's intelligence agencies for failing to "connect the dots" before the attack—that is, for failing to detect a pattern in the scattered items of information about the hijackers that had come to the attention of various federal and state agencies. The resulting calls for intelligence reform were at first confined to the nation's security agencies, the FBI and the CIA. Soon police leaders began to argue that their agencies, too, had a vital role in addressing terrorism and that they must be included in the loop.

Terrorism may have raised the profile of police intelligence, but it is not the main reason for improving its use. Police intelligence has a far wider role in public safety, crime reduction, and order maintenance. This wider role is explored throughout this manual. Unfortunately, the word "intelligence" also raises public fears that secretly collected police information will be used to subvert individual liberties and democratic institutions. We will touch on these concerns later; here, we should explain why we wrote the manual, who it is for, and what it covers.

What is this manual about and who is it for?

As we discuss in Step 1, intelligence analysis is "a process for making sense of a diverse array of information about crime problems created by offender groups, with the goal of reducing crime." Numerous books and manuals for crime analysts are available that describe how to process data to guide police anti-crime tactics and strategies. In contrast, most writing on police intelligence focuses on data gathering and sharing, administration, and legal requirements. These are all important topics, but they do not help the analyst **analyze**, i.e., make sense of the data in order to glimpse behind the veil of a criminal enterprise.

Our manual fills this gap by providing a practical guide to intelligence analysis, much like our earlier manual on crime analysis written for the Center for Problem-Oriented Policing. In writing this manual, it soon became clear that police intelligence has a much larger mission than simply finding out who is up to no good, who they hang out with, what they are about to do, and where they can be found. These are the sorts of questions we normally expect police intelligence to address. However, there are other questions that intelligence analysis can effectively address, such as: How do offenders commit their crimes? What circumstances help them commit their crimes? And, what countermeasures might prevent them from doing so? In short, we look beyond the "who" to address "how," "when," "where," and "what."

This manual fuses aspects of intelligence analysis with Problem-Oriented Policing**.** The links between the two have been ignored in the past, with the exception of Jerry Ratcliffe's book referenced below. However, knowing how intelligence analysis can help solve problems and how problem solving can improve the effectiveness of intelligence analysis will aid any police practitioner interested in reducing crime or disorder.

This manual is not intended to serve the entire law enforcement community. Nor does it describe all facets of intelligence. Rather it focuses on the **analysis** of intelligence, and we wrote it for three groups in local policing agencies: (1) intelligence officers and analysts, (2) crime analysts who might need to use intelligence information and, (3) police managers who supervise crime and intelligence analysts. If you are such a manager, and you find that the work of analysts is something of a mystery, then we hope this manual can demystify their work and help you make better use of your analysts.

The coverage of this manual

The central focus of this manual is the analysis of data: making sense of the variety of bits of information describing criminal groups or problem gatherings. This manual does not cover:

- Federal, state, and local intelligence organizations, groups, and networks
- How to set up or manage an intelligence unit within a police organization
- All the sources of data and information available
- Security requirements for those with access to intelligence data
- Legal requirements for obtaining and sharing intelligence information

There are other documents, books, and resources that cover these topics.

Three key assumptions

1. In preparing to write this manual, it quickly became apparent that (1) there is considerable overlap in the analytic techniques employed and the skills needed by intelligence analysts and crime analysts and, (2) most police agencies would have insufficient resources to employ separate groups of both specialists. We have therefore assumed that intelligence analysis and crime analysis are broadly similar and will generally be undertaken by the same group of analysts.
2. In our early discussions with crime and intelligence analysts, they were able to identify only one important difference between their roles: That intelligence analysis focuses mainly on criminal groups and problem gatherings. Examples of the former would be terrorists, street gangs, outlaw motorcycle gangs, and organized shoplifters, and of the latter would be illegal street races, political demonstrations by extremist groups, and student crowds at spring break. Consequently, this manual focuses on analyzing information about criminal groups and problem gatherings.
3. The third assumption derives from our backgrounds in community policing and problem-oriented policing. The purpose of intelligence analysis should be to find ways of altering the "facilitating conditions" that permit these groups and gatherings to create harm. In other words, intelligence analysis can contribute both to long-term and immediate reductions in crime.

How is the manual organized?

The first part of the manual consists of 30 "Steps" organized under six sections. Each step covers a discrete topic and each one stands on its own. So there is no need to read the manual straight through from beginning to end; you can dip into it at any point. Nevertheless, topics do connect with each other and follow a logical order. Where these connections are vital, we reference other steps. At the end of most steps, we include some references to written materials that give more details about the topic.

The second part of the manual contains case studies of various criminal groups and problem gatherings that we undertook in order to assist our thinking about the uses of intelligence analysis. These case studies provide useful examples of the kinds of information that might be collected and ways in which it might be used.

Policing agencies and law enforcement

- Throughout this manual, we use the term "police agencies" to refer to agencies of local government whose primary business is policing. As well as municipal and town agencies, this includes sheriff agencies that provide police services to county residents and businesses, but not those that only provide correctional, warrant, or court services. We do not include federal agencies, such as the Federal Bureau of Investigation (FBI), Drug Enforcement Administration (DEA), and Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF).
- We use the term "law enforcement" to refer to a procedure or tactic that police agencies can use, but we do not use the term "law enforcement agency" because law enforcement is only one of many tools police can use. Intelligence analysis should help police decision makers choose among the available tools.

READ MORE:

Jerry Ratcliffe. 2008. *Intelligence-Led Policing.* Cullompton, Devon: Willan Publishing.

Ronald V. Clarke and John E. Eck. 2005. *Crime Analysis for Problem Solvers. In 60 Small Steps.* Washington, D.C.; U.S. Department of Justice, Office of Community Oriented Policing Services.

Part 1

Intelligence Analysis for Solving Problems

01 KNOW WHAT INTELLIGENCE ANALYSIS COMPRISES

TERRORIST THREATS HAVE DRAWN ATTENTION TO THE VITAL ROLE OF INTELLIGENCE. However, the threats have also promoted inflated expectations and confusion regarding this role. This is particularly true in local policing. One source of confusion is that "intelligence" is used to refer both to raw information collected from some source and to the result of systematically analyzing this information. Many writings on intelligence analysis do little to clarify the term because they provide limited guidance as to what actions comprise analysis and the purposes these actions are supposed to serve.

National intelligence and criminal intelligence

While there are substantial differences between national intelligence (as conducted by federal agencies involved in international affairs) and criminal intelligence, we found Robert Clark's book (referenced below) on national intelligence helpful in defining the scope and objectives of police intelligence analysis. Clark asserts that intelligence analysis has five characteristics: orientation, target, goals, inputs, and methods. For policing, the first three characteristics are far more important and we discuss orientation, targets, and goals below.

Orientation – proactive

Intelligence analysis has a future orientation. It tries to determine what criminal activity is likely to happen if police do nothing to prevent it. In short, intelligence analysis is proactive. Consequently, reactive uses of information, such as to solve crimes that have already occurred, are not generally included in intelligence analysis. Solving crimes helps to redress past events, and though vital, this is not designed principally to prevent future incidents. Investigative information can be converted to intelligence when it is analyzed for the purpose of preventing future crimes.

Targets – groups

Intelligence analysis is directed against offenders operating in groups. Groups may facilitate offending, thus making them more serious than individual offenders acting alone. More importantly, intelligence can exploit the special vulnerabilities of groups, which are as follows:

- **Keeping Secrets.** Benjamin Franklin said, "Three can keep a secret if two are dead." While this is rather extreme, it illustrates an important point: the more people who need to keep a secret, the less likely it is that the secret will be kept. This is why criminal groups often enforce secrecy with threats, and perhaps it is also the reason the Hell's Angels quote Benjamin Franklin. But, offender groups are not necessarily good at keeping their members compliant.
- **Visibility.** A related vulnerability is that the larger the group of offenders, the greater the difficulty of keeping a low profile. The danger is especially great when group members gather. Establishing secret meeting places helps them overcome this difficulty. But establishing such a place often requires group members to work with non-offenders (e.g., landlords) and this also increases their risk of detection. Groups that ostentatiously promote themselves create more information that intelligence analysis can exploit.
- **Coordination**. Unlike individual offenders operating alone, groups of offenders have to coordinate their activities with one another. Coordination difficulties rise as the group increases in size. Consequently, while groups have greater capacities than individuals, they are also less flexible, which, at least in the short run, makes them more predictable. In the long run, groups may have a greater chance to innovate than individuals, but this takes time.

In short, groups leak information that can be gathered and analyzed and, as we note below, the variety of information sources makes analysis mandatory.

Goal – prevention

The fundamental purpose of intelligence analysis is to prevent group crimes from occurring. This is consistent with the first two elements: a future orientation and

group offending. Intelligence analysis targets groups in order to reduce crime. To serve this purpose, the detection, arrest, and prosecution of group offenders are important, but intelligence analysis is not limited to these actions. Going beyond law enforcement is critical to achieving crime reduction goals. Consistent with community and problem-oriented policing strategies, intelligence analysis can serve a wide range of preventive activities. In subsequent steps, we describe how intelligence analysis can expand the range of prevention activities by applying principles derived from environmental criminology.

Inputs – many

Intelligence analysis uses information from a wide variety of sources. It is not restricted to covert sources. Standard police records, available to the public, and other data collected by private and public agencies are often extremely useful. We examine some of the most obvious sources in this manual, but the sources available are only limited by imagination, resources, and technology. If intelligence analysis were restricted to a single source, the need for analysis would be much reduced. It is the need to make sense of multiple information sources, including data from other jurisdictions (see Step 22), each with its own strengths and weaknesses, that makes analysis important. Consequently, we do not define intelligence analysis by the type of information used: variety is what is important.

Methods – varied

Intelligence analysis methods involve processes to sort, interpret, and compare information from multiple sources in order to determine what offending groups are likely to be operating, how they commit crimes, and what can be done to keep these groups from being successful. Just as there are many sources of information, police can use many analytical methods. We will discuss some of the most important. We do not define intelligence analysis by the use of any particular method; any systematic approach that helps provide an accurate assessment can be part of intelligence analysis.

Lone wolves

What about the threat of "lone wolf" terrorists? Are their actions not susceptible to intelligence analysis? Practically speaking, no. Although the harm they can do is extreme, this does not mean that intelligence analysis can do any more for the lone wolf terrorist than it could do for the lone wolf bank robber, the isolated drug dealer, or the stand alone fraudster. If individual offending creates patterns, crime analysis can help. Controlling access to explosive materials, for example, helps thwart isolated terrorists as well as organized ones. However, without a group or a pattern of behavior, police have to rely on isolated and unpredictable reports of community members, chance encounters, and investigative work. This might happen when lone wolves "reach out" to others for assistance (e.g., obtaining weapons, information, or other support). When they mistakenly reach out to individuals with connections to police, this presents the police with an opportunity to identify and remove them.

In summary, *intelligence analysis is just a specialized form of crime analysis that focuses on problems created by groups of offenders*. It is a process for making sense of a diverse array of information about crime problems created by offender groups, with the goal of reducing crime. Intelligence is just a form of information that describes groups. Sources and methods do not define it.

READ MORE:

Robert M. Clark. 2007. *Intelligence Analysis: A Target-Centric Approach.* 2nd Edition. Washington, D.C.: CQ Press.

02 KNOW THAT INTELLIGENCE ANALYSIS MUST LOOK BEYOND ENFORCEMENT

WE HAVE SAID THE GOAL OF INTELLIGENCE ANALYSIS IS TO REDUCE THE PROBLEMS CREATED BY OFFENDER GROUPS. Gathering, analyzing, and sharing data might assist in making arrests and prosecutions and could result in breaking up a group. However, this can only be considered effective action if the problems created by the group decline.

For example, breaking up a group that steals catalytic converters may not be productive, under the following circumstances:

1. The group was never responsible for an important proportion of the problem
2. The wrong members of the group are removed
3. Those arrested are quickly replaced by others, thus reestablishing the group
4. Other groups move in to take advantage of the now vacant opportunity

Unless there is a reduction of theft of catalytic converters, the actions were not effective. To ensure that they are effective, intelligence analysis should focus on the complete problem. In our example, the analysis should examine the catalytic converter theft process from beginning to end—from the characteristics of vehicles and victims to the reentry of the stolen converters into the legitimate market. In short, the problem is not the group stealing the catalytic converters, but the entire theft process, of which the group is an integral part.

These points can be illustrated by police attempts to disrupt street drug dealing, particularly in the late 1980s through the early 1990s when police targeted the most highly visible drug groups. Unfortunately, the most visible were not necessarily the most active in dealing or the most violent. In addition, informants sometimes directed police operations to serve their own needs; a difficulty that is made worse when there is little or no effort to gather systematic information on the problem so the informant's data can be evaluated in a larger context. Even when the group was a major contributor to the problem, the enforcement sometimes focused on those most easily replaced—retail dealers. Such easily replaced individuals are not critical to the functioning of the organizations.

Several randomized experiments conducted in the 1990s show the difference between an enforcement approach and an intelligence, problem-focused approach. (All these studies are reviewed in the National Research Council book referred to below.) First, let us consider Sherman and Rogan's experiment to determine the effectiveness of crack house raids in Kansas City. Possible raid targets were randomly allocated to receiving a raid and not receiving a raid. Though some crime reductions were observed at the raided houses relative to the other houses, these reductions were relatively minor.

Now, consider another experiment designed to look at the effectiveness of going beyond enforcement. In San Diego, Eck and Wartell looked at what happens if, after a raid, the landlord was compelled to improve apartment management practices. Raided addresses were randomly assigned to three groups: those that received no further treatment (control group); addresses where police sent the landlord a letter describing the raid and offering assistance (letter group); and addresses where police compelled the landlord to meet with narcotics detectives and city code inspectors and form a plan to improve the property (meeting group). All places had less drug dealing after the raid than before, but the meeting group places had a 60 percent reduction in crime relative to the control group (the letter group had outcomes between the control and meeting groups).

Finally, let us consider another drug experiment comparing problem-solving efforts at drug hot spots with enforcement crackdowns. Weisburd and Green randomly assigned street drug markets hot spots in Jersey City to either of these conditions. The problem solving approach showed far greater reductions in drug dealing and other forms of disorder than the standard enforcement approach.

These and other studies point to a consistent picture of the kinds of police strategies that work to reduce crime. In 2004, a National Research Council report described four policing strategies and their relative effectiveness (see Figure 1). The more focused the strategy and the wider array of tactics used, the more effective the strategy. In the lower left of Figure 1, the standard model of policing (relying predominately on random patrol, follow-up investigations, and rapid response) is the least effective strategy. It does not focus on specific places, people, or times and uses a predominately law enforcement approach.

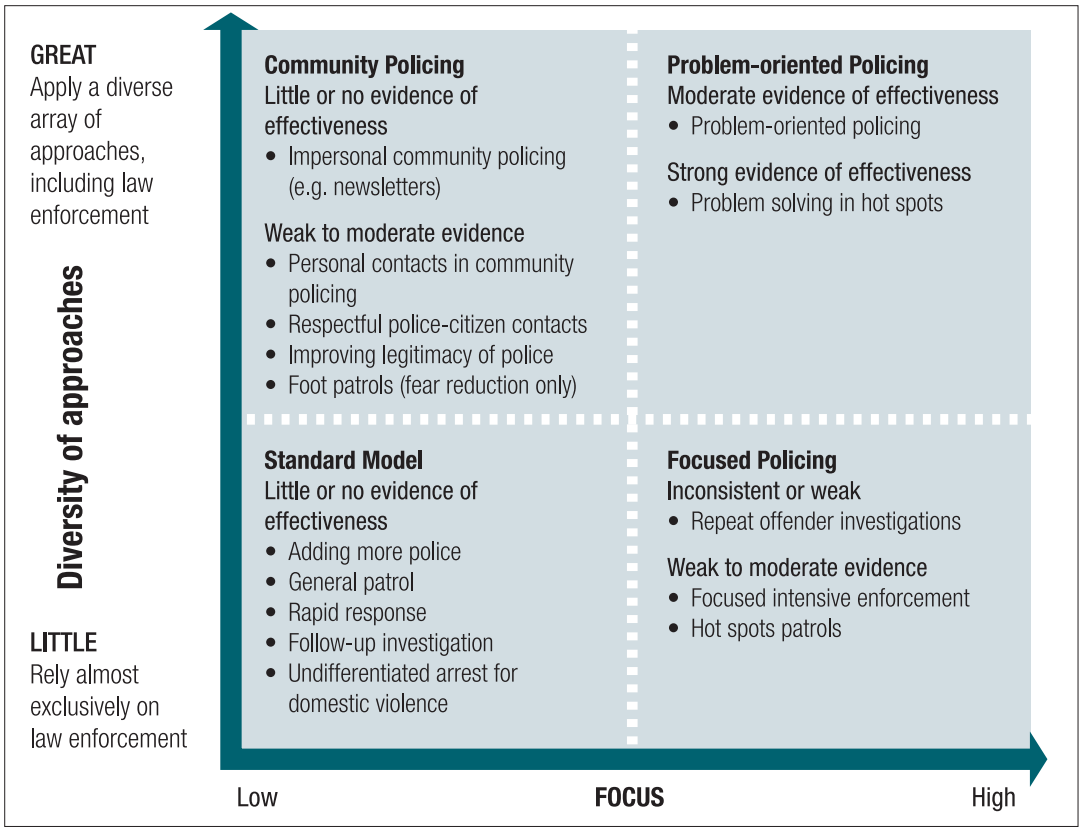
Somewhat more effective is community policing (in the absence of problem solving). Community policing gains effectiveness by adding considerably more tactics, but it is still relatively unfocused. Focused policing, on the lower right in Figure 1, is far more effective than standard policing, because it narrows policing efforts to "hot" people, places, or times. Instead of spreading resources thinly, like standard policing, it concentrates resources. Intelligence analysis fits very well into this strategy. Evidence and theory suggest that combining the focus with a wider array of tactics improves police effectiveness more. That is the form of policing in the upper right part of Figure 1. The three experiments described above illustrate this point. All experiments involved focusing on hot places, but when police coupled law enforcement with other tactics they further increased their effectiveness at reducing crime and disorder.

The role of intelligence analysis in addressing problems is to shed light on how offenders behave so police can craft a solution. In short, intelligence analysis is an integral part of Problem-Oriented Policing. Often this will involve some sort of enforcement, but the enforcement will be highly targeted to have the greatest impact on the problem, and will often be part of a larger set of actions designed to make it harder for any remaining or new offenders to perpetuate the problem.

READ MORE:

National Research Council. 2004. *Fairness and Effectiveness in Policing.* Washington, D.C.: National Academies Press.

Figure 1. Policing strategy effectiveness



03 UNDERSTAND THE INTELLIGENCE ANALYSIS PROCESS

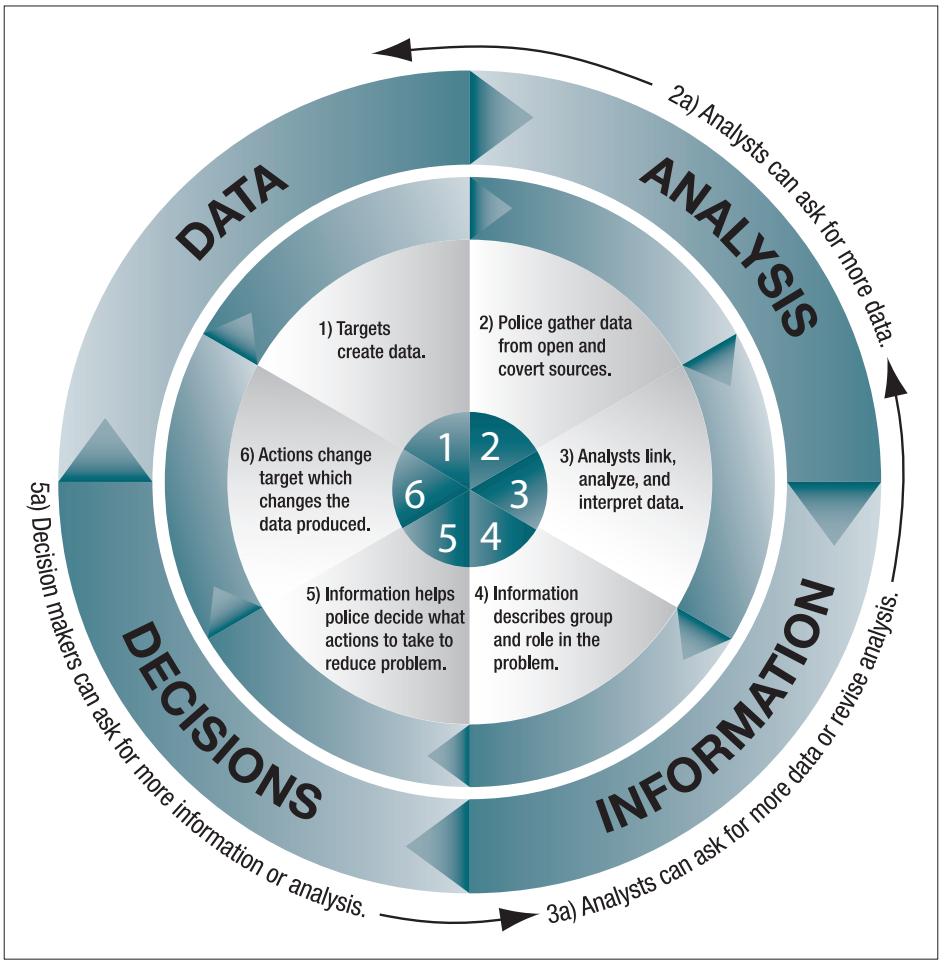
INTELLIGENCE ANALYSIS IS NOT SIMPLY THE COLLECTION OF COVERT DATA, nor is it making sure it is shared appropriately. Although collection and sharing receive considerable attention, and for very good reasons, this attention has obscured the simple fact that they are merely parts of a larger process illustrated by Figure 2. Our discussion of the process follows the numbered stages in the diagram.

1. **Targets create data.** Offender groups are the targets. Citizens might see them. They might act in ways that provoke police stops and arrests. They might write graffiti or create social network pages. They may have bank accounts. They may be recorded by closed circuit television (CCTV). In each of these examples, a person or machine captures data describing group members. In isolation and in these raw forms, these data are relatively meaningless.
2. **Police gather data.** Data from an informant, or on a digital recording device, or in a database needs to be collected to be analyzed. There are data capture processes that are obvious (e.g., police databases of offenders or CCTV footage from cameras near a crime site, confederates of members of an offender group) while other data capture processes require some creative thinking to recognize (see Steps 6–13).
3. **Analysts interpret data** and 4. **Analysts produce information**. Once police or others collect the data, analysts need to combine it with other data and interpret it to produce useful information. An important part of the analysis is determining the validity of the data (for example, is one piece of data consistent with other pieces of data from other sources). Another important aspect of analysis is organizing valid data into a coherent story. Organizing data requires analysts to use two sets of tools. One set of tools comprise analytical techniques: maps, network charts, statistical programs, and so forth. However, theories of groups and how they produce crime are more important than analytical techniques. Theories suggest what data is important and how it should fit with other data. Theories also provide hypotheses that you can test with the data (see Step 21). All good analysts have one or more theories of how they can organize the data to produce a meaningful and valid story. We will discuss several such theories in later Steps 6 through 13. This analysis—with techniques and theories—creates information.
5. **Information helps police to decide what to do.** Information assists decision makers who choose actions. Decisions based on this information create actions whose purpose is to alter that target (for example, arresting members of the group) or the environment in which the target operates (for example, preventing group members from having access to key places, denying them weapons or other tools, or freezing their assets).
6. **Actions change the target and produce new data.** If your analysis has accurately described the offending group and its behaviors, and if the decision maker has used this information, then the actions will change the target. They may remove members of the group, or force the group to alter its behaviors. Ideally, this results in less crime or disorder. Such outcomes are known because the data emitted by the group changes—there are fewer attacks, less graffiti, less drug dealing, and so forth. The new data enters the cycle and helps police adjust their understanding of the group.

In fact, the cycle is more complex than just these six stages described. An intelligence process also consists of a series of feedback loops (2a, 3a, 5a) dependent on the target, information, and the decisions being considered.

- 2a. **Analysts can seek more data** and 3a. **Analysts can revise their initial analysis.** As an analyst, you should not passively accept any data that comes your way. You can request the collection of additional data—for example asking that

Figure 2. Intelligence analysis process



new questions be put to an informant. This new data might help test the reliability of previously collected data. It might fill in critical gaps about a group; it might be used to determine how the group makes use of its environment; or the new data may be needed to help determine which of several alternative hypotheses is more likely to be true (see Step 21). New data might require further analysis or the original analysis may have produced contradictory results so further analysis is needed, for example. The additional data would then have to be analyzed in light of the earlier information.

- 5a. **Decision makers can ask for more information or analysis.** While decisions are being formulated you might be asked for additional information that could help refine the choice of actions. If the information is readily available, you can pass it on to other decision makers. This might require going back further and conducting additional analysis. Or it might even require obtaining additional data.

The analysis process does not end with action against a target. You still need to determine if the actions had the desired effect. Does the group still exist? Have the group's criminal activities slowed down or stopped? Has the group changed its tactics to circumvent police actions? Have other groups moved in to replace the original group? Were there unintended consequences from the actions? Evaluating actions helps decision makers decide whether they should move on to other targets, make adjustments in how they handle this target, or whether their actions failed and they need to start over.

04 RECOGNIZE HOW INTELLIGENCE ANALYSIS FITS INTO CRIME ANALYSIS

CRIME ANALYSTS USE THE TERM "ANALYSIS" TO REFER TO SPECIFIC TECHNIQUES THEY USE, SUCH AS GEOGRAPHIC analysis (i.e., crime mapping) or statistical analysis (to explore relationships among the variables in a data set). But the police use "analysis" in many other ways as well. This creates confusion about the meaning of the term and how "intelligence analysis" fits with other forms of analysis. Here we describe how intelligence analysis is related to other kinds of analysis used by local police agencies.

Perhaps the commonest use of the term by police relates to the type of decision it serves. **Strategic analysis** typically describes enquiries conducted to help long-term broad decisions—such as determining the appropriate approach for addressing repeat offenders. **Tactical analysis** serves shorter term decisions, having a narrower scope. So patrol commanders might ask for a tactical analysis of how best to allocate officers to handle a political demonstration. Intelligence analysis can be used at either level.

Analysis is also sometimes used by police to describe the "customers" for the analytical work, as in the following:

- **Investigative analysis** helps investigators solve particular crimes, or a pattern of crimes.
- **Patrol analysis** is designed to serve the needs of patrol officers and supervisors.
- **Traffic analysis** helps police focus resources on vehicle traffic (though sometimes the term is used to describe drug trafficking or communications traffic).
- **Problem analysis** is used by police and others involved in problem-oriented policing projects to reduce specific forms of crime and disorder.

A crime analysis unit may conduct any combination of these forms of analysis. As we will describe below, intelligence analysis overlaps investigative analysis and problem analysis.

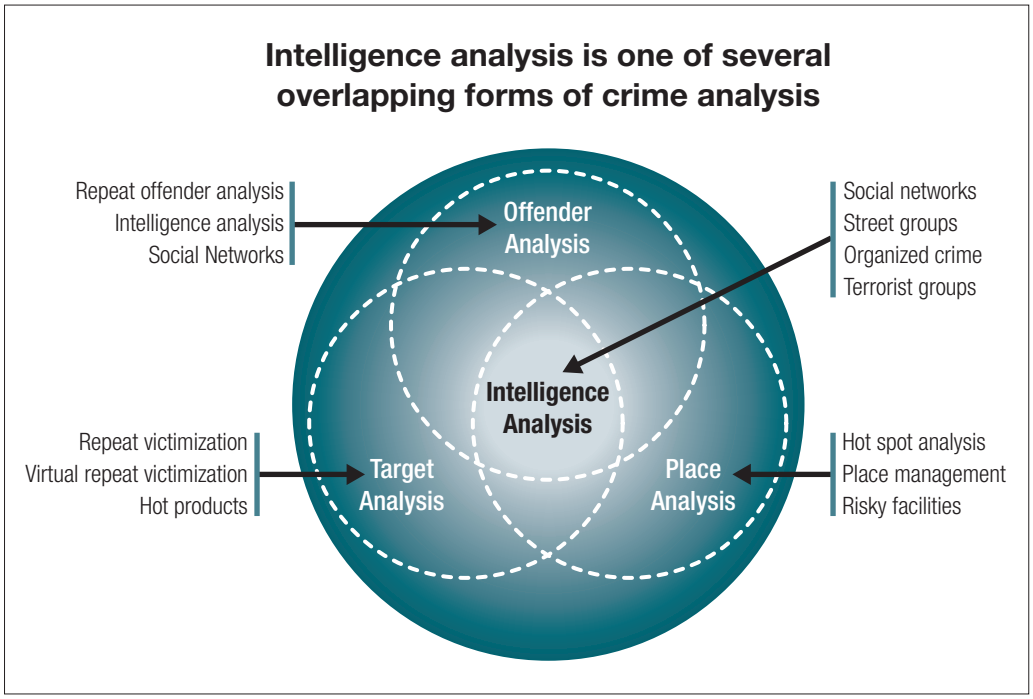
Since crimes involve offenders, targets, and places, there can be analysis that focuses on all three of these elements. **Offender analysis** focuses on offenders, and is closely related to investigative analysis. In contrast, **place and geographic analysis** focuses on various geographic concentrations of crime—such as crime hot spots, repeat crime places, and risky facilities (see the POP Center's *Risky Facilities Guide* for more details). And **target analysis** focuses on the people or things offenders attack. Forms of target analysis include repeat victim analysis, virtual repeat victim analysis, and hot product analysis. These and other forms of target analysis are used in problem analysis.

As shown in Figure 3 on page 17, target, place, and offender analysis overlap and all are forms of crime analysis (the examination of information to help prevent crime). For example, Joe Combs, a detective for the Cincinnati Police Department, discovered that a single apartment complex had an extraordinarily high number of burglaries (both compared to its previous history, and compared to other apartment complexes). Within the complex, several households were burgled multiple times, and most burglaries during this spike in crimes were committed by a small group of offenders (the burglaries declined following their arrest). He had discovered a combination of repeat places, repeat victimization, and repeat group offending.

It is useful to link forms of analysis to the types of problems the analysis is supposed to examine. That is why we define police intelligence analysis as focused on problems created by groups of offenders. Intelligence analysis is related to offender analysis (and investigative analysis) because of its focus on offender groups. Intelligence analysis also overlaps both place and target analysis. Consequently, intelligence analysis is a form of crime analysis as well.

Another way to see how intelligence analysis fits within crime analysis is to compare analysis used in reacting to crime patterns and those forms of analysis that attempt to understand the causes of crime patterns and to develop prevention initiatives. The first we will call reactive and the second proactive. We can also distinguish between analysis focusing on offenders and

Figure 3. Overlapping forms of crime analysis



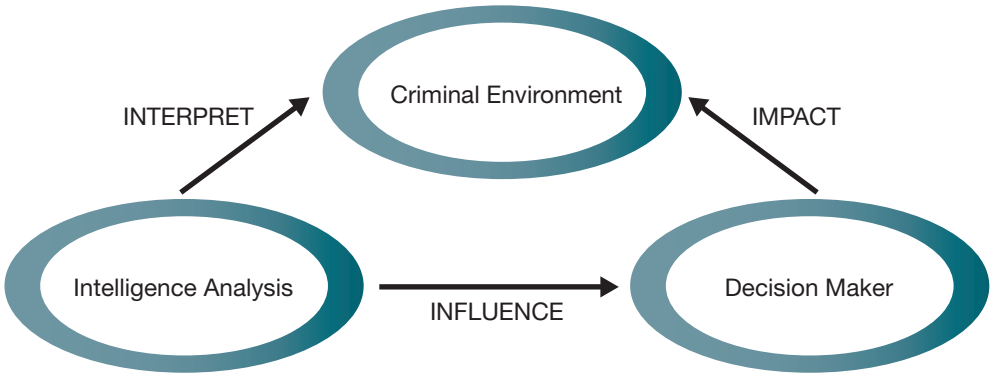
those focusing on crime patterns (such as geographic analysis). This gives us a simple way of organizing some of the most important forms of analysis (see Table 1). Intelligence analysis is a proactive form of offender analysis. It shares this proactive status with place analysis. Both place analysis and intelligence analysis are forms of problem analysis. Also, they stand in contrast to reactive analysis of crime patterns, such as simple hot spot detection and other forms of geographic analysis. This view of intelligence analysis underpins Jerry Ratcliffe's 3-i model, which portrays the role of intelligence analysis as an essential, action-oriented, decision support function (see *The 3-i Model* on page 18).

In conclusion, there is no standard way of classifying analysis types and many forms of analysis overlap. Intelligence analysis shares many features with many types of crime analysis. We believe that the distinguishing feature of intelligence analysis concerns not techniques but the fact that intelligence analysis focuses attention on offender groups.

Table 1. Reactive and proactive forms of crime analysis

REACTIVE AND PROACTIVE FORMS OF CRIME ANALYSIS		
	Reactive	Proactive
Offenders	Investigative analysis – the analyst examines databases to assist investigators solve a crime or crime series.	Intelligence analysis – the analyst pulls together information on problems created by offender groups to help craft methods for reducing that problem.
Locations	Patrol analysis – the analyst examines databases to help determine when and where police should allocate patrol resources.	Place-analysis – the analyst pulls together information from databases, targeted information gathering and other sources to reduce problems at particular locations.

The 3-i model



Jerry Ratcliffe's **3-i model** redefines the role of analysis in an intelligence-led policing environment. Instead of viewing intelligence analysis as simply understanding the criminal environment, the **3-i model** demands that intelligence analysts also identify decision makers and influence their thinking. Decision makers are people who have the power and resources to have an impact on the criminal environment. Thus, intelligence analysts have a leadership role within policing, guiding priorities, and resource decisions.

Ratcliffe's **3-i model** begins with an arrow from analysis to the criminal environment. This emphasis is deliberate. Analysts can't wait for data to come to them: they have to actively seek out the information they need. Creating and disseminating an intelligence product is not a sufficient outcome in the **3-i model**. Instead analysts must identify a decision-making framework they can influence and actively work to help decision makers have a direct impact on the criminal environment. Making recommendations to guide decision makers (both inside and outside policing) to prevent, disrupt or reduce criminal activity is a vital role of the analyst. Learning the theory and practice of what works to reduce crime is crucial.

Ratcliffe's **3-i model** challenges analysts and decision makers to work closely together. It rethinks the role of intelligence analysis as an essential, action-oriented, decision support function.

Source: Ratcliffe, J. H. (2008) Intelligence-Led Policing, Willan Publishing. For further information see www.jratcliffe.net.

05 APPRECIATE HOW INTELLIGENCE FITS IN POLICING STRATEGIES

AS MENTIONED IN STEP 2, IN 2004 THE NATIONAL RESEARCH COUNCIL PUBLISHED A COMPREHENSIVE ASSESSMENT of police research and policy. It showed how all policing strategies fall into four groups, depending on the degree to which they focus on specific crime problems and the range of tactics they employ. These four groups are standard policing, community policing, focused policing, and problem-oriented policing (see Table 2). Intelligence analysis plays somewhat different roles in each strategy.

Standard policing makes the least use of intelligence analysis. Standard policing is relatively unfocused and employs a limited number of law enforcement tactics generically across a wide variety of circumstances. The principal tactics are patrolling, reactive follow-up investigations, and rapid response to calls. To improve effectiveness, the main approach is to add more police and do more of the same. Research has shown that at best this has very limited effects on crime, fear of crime, or disorder. Standard policing uses very little information and makes little use of crime analysis to assist in making critical decisions. Intelligence analysis, when used, is the province of highly specialized units that often communicate poorly with standard patrol operations.

Standard policing is ineffective for several reasons. First, it does not use information to focus resources on the relatively few people, places, and circumstances that need the most attention. Consequently, it spreads its resources too thin where they are most needed. Further, the lack of information makes it difficult to develop innovative tactics that exploit the vulnerabilities of offenders. Finally, standard policing puts more emphasis on following routine law enforcement and arrest practices than on preventing crime.

Community policing seeks to bridge the gap between police and community. It places far less emphasis on law enforcement and uses a wider repertoire of policing tactics. However, community policing is relatively unfocused unless it includes a strong component of problem solving. Research evidence suggests that it can be somewhat more effective at reducing crime than standard policing, but the results are ambiguous. Like standard policing, most community policing makes limited use of information technology, crime analysis, and intelligence.

The strength of community policing is that it provides the foundation for the two-way exchange of information between members of the public and the police. This is particularly critical in neighborhoods suffering from high levels of crime and when dealing with crime groups hidden within communities, or

Table 2. Intelligence in policing strategies

	LOW FOCUS	HIGH FOCUS
Limited tactics Mostly Law Enforcement	Standard policing Very little influence on crime Very little use of intelligence analysis	Focused policing Strong influence on crime Intelligence data from limited sources which is used to target enforcement on crime groups
Wide variety of tactics Including Some Law Enforcement	Community policing Modest influence on crime Improves the flow of intelligence data from community members	Problem-oriented policing Highly effective against crime Intelligence from variety of sources is used to craft interventions that curtail crime group activities

intimidating community members. In the absence of community policing, developing intelligence on these groups can be extremely difficult. For these reasons community policing is a necessary condition for effective intelligence analysis. It is a foundation strategy on which other strategies can be built.

Focused policing strategies are a collection of approaches that build on the law enforcement tactics used in standard policing by making much greater use of information. Information is used to identify offenders and places that are disproportionately involved in crime. There is strong evidence that targeting very high crime *places* can reduce crime considerably, but evidence about the usefulness of targeting persistent *offenders* is much less clear. This can increase the chances of arresting the most prolific offenders, but existing studies have failed to examine whether crime declined as a result of such targeting.

Because focused policing places information analysis at the forefront of policing, intelligence is more important for this strategy than for the standard policing or community policing. However, in the absence of community support, only limited intelligence is available. Furthermore, when limited to law enforcement tactics, focused policing does not address the facilitating conditions that allow criminal groups to operate. So focused policing, like community policing, is a foundation for effective use of intelligence. But neither is sufficient on its own and we need to combine community and focus.

Problem-oriented policing, which was developed to address the limitations of standard policing, succeeds in combing community and focus. It was specifically designed to be highly focused—thus capturing the advantages of focused policing—and to use a variety of tactics with the community—thus building on community policing. It addresses any and all aspects of crimes, including the places involved, the targets and victims affected, and the offenders.

Research into problem-oriented policing practices has shown that it is highly effective at reducing crime and disorder. Though there are few head-to-head comparisons between focused policing and problem-oriented policing, the research that is available shows that following a problem-oriented approach has greater benefits than simply focusing on crime hotspots.

The basic principles of problem-oriented policing are simple to state. First, problem-oriented policing places far greater emphasis on what the police are to accomplish—the ends of policing—than on the means of policing. As long as the policing practices are constitutional and legal, are acceptable to the community, are affordable, and have a high likelihood of being effective, problem-oriented policing does not specify what should be done. Instead, problem-oriented policing states that the goals of police are to reduce community problems. Second, problem-oriented policing claims that information needs to be examined to determine how specific problems arise and to determine what sorts of actions can be done to reduce or eliminate these problems. Third, problem-oriented policing calls for a thorough search for solutions to the problem, not limited to law enforcement options. Finally, since the goal of problem solving is to solve the problem, problem-oriented policing requires evaluation of the outcomes of the intervention.

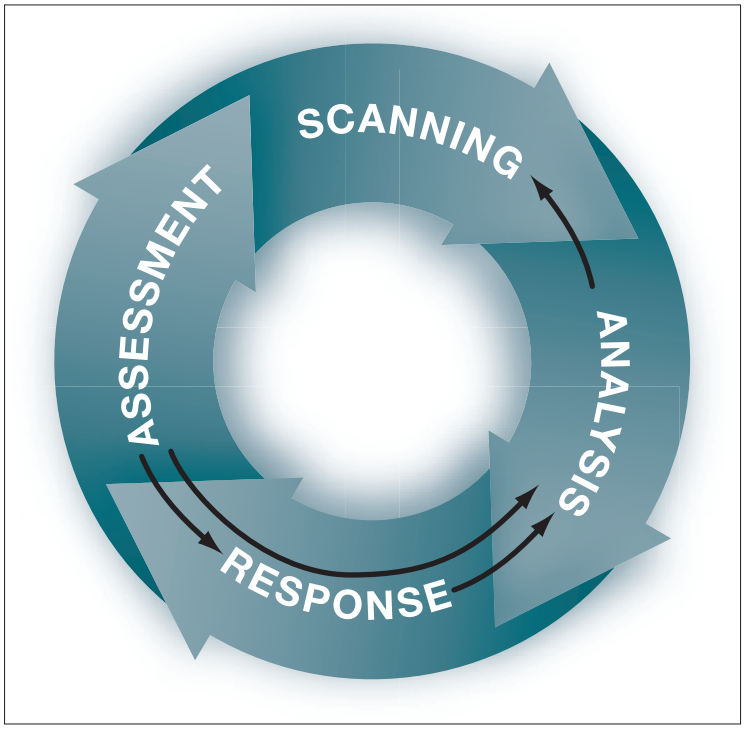
These principles have been codified in the well-known SARA process (see Figure 4). SARA stands for Scanning, Analysis, Response, and Assessment. This is a cyclical model that starts with the identification and definition of a problem (Scanning), followed by detailed analysis (Analysis). Intelligence analysts can play important roles at these initial stages by helping to identify groups that are generating serious crime problems and producing information that describes how they operate. Response is the third stage, where solutions are developed and implemented. Intelligence analysis can help identify possible interventions based on information describing group vulnerabilities.

The last stage (Assessment) is the evaluation of the intervention. Again, intelligence analysis can help determine if the interventions worked by looking at the impact on the targeted group and whether their crimes have declined. In Figure 4, the large clockwise arrows show the standard cycle. The smaller, inner arrows indicate that often a problem-solving process needs to revisit earlier stages as new questions arise or evidence suggests that interventions are not working as expected.

READ MORE:

David Weisburd and John Eck. 2004. "What Can Police Do to Reduce Crime, Disorder and Fear?" *The Annals of the American Academy of Political and Social Science* 593:42–65.

Figure 4. Stages of the SARA process



06 RECOGNIZE THAT OFFENDERS CHOOSE TO COMMIT CRIME

A USEFUL STARTING POINT FOR APPROACHING INTELLIGENCE ANALYSIS is to assume that offenders choose to take advantage of limited crime opportunities. They take advantage of situations where crime is easy, low risk, rewarding, socially encouraged, or provoked. There is considerable evidence that focusing on offender choices can reduce crime, and there are many ways to address crime by blocking opportunities.

"Choice" means that offenders select actions they think will help them achieve their purposes. In making these choices, offenders have limited and sometimes confusing information. They also often have limited time and competing objectives. To address these limits, they use rules of thumb and habit to reduce the information they need and to increase the speed of their decisions. "Do what others in my group do," is one such rule of thumb. "Do what worked before," is another such rule.

Understanding offender choice is critical to intelligence analysis. This is because the principle method of reducing crime is to change these choices. We do this by manipulating the physical and social environment surrounding offenders. There are five choice criteria offenders use: effort, risk, reward, excuses, and provocations. The less effort or risk, the greater the likelihood the offender will commit a crime. The more reward, greater the excuses, or higher the provocations, the more likely the offender will choose crime.

These five criteria influence all people—not just offenders—in all choices—not just offending. Features of the immediate environment signal the individual as to whether a particular set of actions will be useful or counterproductive. The individual then makes a choice. This environment includes the physical setting and the social arrangements. One very important social environment for intelligence is the offenders' group.

An offender in a group may make a very different choice than the same offender outside a group but facing the same circumstances. Groups provide a context that influences individual choice (see Table 3 on page 23):

1. Group members can make crime **easier** by supplying tools, providing transportation, sharing information, and taking on some of the work. A crime that one person cannot do, may be feasible with a group.
2. Groups can make it **safer** (fewer risks) by mutual protection and sharing information about possible risks. Identifying suspects may become harder if witnesses cannot distinguish among several confederates.
3. Groups also make crime **excusable** for their members by justifying the behavior and providing stories as to why the crime is "really necessary."
4. Groups make crime **enticing** to their members through peer pressure, and by providing examples to follow.
5. Groups make crime **rewarding** by giving individual members a sense of belonging, providing an audience to celebrate successful crimes, and other intangible, but important, psychological rewards, in addition to the more familiar tangible rewards of crime.

These attributes, which we collectively call **ESEER**, correspond to standard choice criteria we all use when selecting actions: effort, risk, excuses, provocations, and rewards. These are so critical to understanding crime and its prevention, we will return to them repeatedly throughout this manual.

To an outsider, considering the individual offender in the abstract, the choice may seem inexplicable and even irrational. When examined in the context of a group of offenders, the same choice appears reasonable (even though objectionable). However, groups do not inevitably increase crime. Offender groups can control their members' behaviors so that individuals only choose crimes when it is more likely to aid the group. As we will discuss later (Step 26), it is sometimes possible to exploit the group to reduce offending.

Because individuals seldom have complete knowledge about other members of their group, they may misinterpret the circumstances. One example is called "pluralistic ignorance." This describes circumstances where each member of a group believes other members value something when in fact few if any other members actually value it. However, to please the others, each group member professes that they too hold that value, thus justifying what the others believed. As a result, the group members express a preference that no individual alone would prefer. Within an offender group, no individual may want to get involved in a fight with another group, but thinking that the other members do want to get into a fight, and believing they will lose face if they refuse, all members of the group jump into the fight.

A commonly held misconception is that people in large crowds lose their self-identity and become "irrational." However, considerable research on crowds shows that this is not the case. People make choices in crowds just as they do outside of crowds. The difference is that within a crowd, an individual will also take into account what other people are doing and what is happening to them. From an outsider's perspective, the crowd may seem as a single entity that transcends the individuals that make it up. However, from inside it is clear that a crowd, of any size, comprises individuals and small groups, often with very different interests. Intelligence analysis can play an important role in helping to maintain orderly crowds by providing information on the diversity of interests within a crowd and helping to separate the few troublemakers from the many other individuals.

While offenders take advantage of existing opportunities for crime, they can also manipulate situations to extend opportunities and make new ones. An organized crime group that bribes a local politician creates opportunities for taking public funds. A terrorist group that infiltrates a member into security forces opens up opportunities for further terrorist activities that did not exist before. Street gang intimidation of witnesses expands the ability of the gang to engage in criminal activity. Intelligence analysis should look at how offending groups manipulate their environments to extend their opportunities.

READ MORE:

Ronald Clarke. 2008. "Situational Crime Prevention." In *Environmental Criminology and Crime Analysis*, ed. Richard Wortley and Lorraine Mazerolle. Cullompton, Devon: Willan Publishing.

Table 3. How groups influence choices

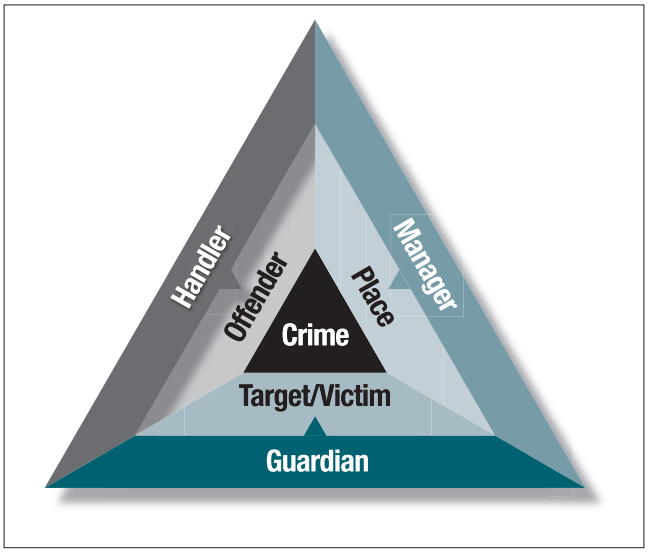
CHOICE CRITERIA	INFLUENCE OF GROUP	EXAMPLES
Effort	Makes crime **easier**	Dividing a complex task or spreading effort among several offenders
Risks	Makes crime **safer**	Providing protection, sharing information, or intimidating witnesses
Excuses	Makes crime more **excusable**	Claiming crimes are permissible or desirable, and denigrating victims
Provocations	Makes crime more **enticing**	Pressuring, encouraging, or guiding members
Rewards	Makes crime more **rewarding**	Providing an audience, status, and reputation

07 PAY ATTENTION TO HOW CRIME OPPORTUNITIES ARISE

THE MOST ESSENTIAL REQUIREMENT FOR CRIME IS OPPORTUNITY. Regardless of a person's motivations, if there is no opportunity there can be no crime. Further, a tempting opportunity may entice a person to commit a crime they would not ordinarily consider. Offender groups can develop to exploit specific opportunities. Human traffickers and smugglers take advantage of two opportunities: the desire of people to leave impoverished countries and the demand for cheap human labor in other countries. Internet commerce created the opportunities that cyber gangs exploit. Drunken bar patrons provide opportunities for youth groups to commit robberies.

Opportunities are situations that offenders can exploit for their gain (e.g., material reward, social dominance, revenge, relief from threat, and so forth). The basic structure of opportunities is often depicted by the problem analysis triangles (see Figure 5). The inner triangle shows the three elements required for a crime to occur: a ready **offender** or group of offenders, a desirable **target** (person, animal, or thing), and a **place** for the two to interact. At minimum, crime opportunities occur when offenders are at places with desirable targets. Removing any one of these three required elements can eliminate the opportunity. Standard law enforcement focuses on offender removal. This can be useful, if the offenders are not easily replaced (Step 13), but there are other ways to reduce crime that also must be considered, either for use with enforcement or as stand-alone options.

Figure 5. The problem analysis triangles



There is more to crime opportunities than these three basic elements: a crime opportunity also requires absence or ineffectiveness of any of the three outer elements of the triangle.

- **Guardians** are people who protect the target—owners of things the offender wants to take or damage, friends of people the offender would like to attack, or security guards hired to protect buildings from terrorist attack.
- **Handlers** are people who try to keep the potential offender out of trouble. They can be parents, siblings, spouses, friends, coworkers, teachers, clergy, and others with whom the potential offender is positively socially connected. They can even be other offenders.
- Finally, **managers** are people who control spaces: owners of locations (private or public), hired employees who work at the location, or others to whom the owner has delegated authority to regulate conduct at the place.

Collectively, we call handlers, guardians, and managers **controllers**, as they control their corresponding elements on the inner triangle. Consequently, in addition to removing one or more of the inner elements, adding one or more controllers helps to reduce crime.

The convergence of offenders with targets at accessible places, in the absence of controllers, makes crime possible. When this happens repeatedly, a crime pattern emerges. Why does this occur? The normal routines of everyday life create most crime opportunities. These include commuting and school schedules. Street drug dealers often locate near commuter routes and when they do so their daily activity patterns follow the routines of commuters

and students. Armed robbery groups can exploit the regular patrons of entertainment districts and drinking routines. The routines of the internet allow fraudsters to exploit users. Natural disasters disrupt some routines, but create other routines that offenders can exploit, including the routines of insurance companies and government aid agencies. Car and suicide bombings by terrorist groups are feasible because people routinely gather at particular places: markets, hotels, and transportation hubs, for example. A peaceful political march creates a routine that small groups of offenders can exploit to create disturbances. Driving routines leave some stretches of highway largely vacant for periods, thus allowing street racing groups to use them. Knowing the spatial and temporal patterns of crime is not just important for allocating law enforcement, it is critical for identifying the routines the crime group is exploiting so that sustainable prevention can be introduced.

Opportunity is in the eye of the offender. Offenders, singly or in groups, judge reward, effort, risk, excuses, and provocations (see ESEER in Step 6) by the presence and absence of the six elements described by the problem triangle. The presence of a target at a place reduces effort while suggesting reward and perhaps providing a provocation. Guardians and managers influence risk and effort. Other offenders can increase excuses and provocations as well as reduce effort and risk. Handlers reduce excuses and provocations, and sometimes rewards.

Offenders, however, can manipulate situations to increase the crime opportunities. Manipulation of opportunities—creating new ones or improving existing ones—is easier for offenders in groups than those operating singly.

Targets and their guardians

Groups enhance the ability of offenders to manipulate targets. A group of offenders has an easier time finding targets because they have more people looking. Sheer numbers can overwhelm a target's defenses and overcome guardians. A group of offenders has greater ability to intimidate victims, thus reducing the chances of effective police involvement. Specialization within a group allows it to undertake complex offenses, from con games to terrorist attacks. A large group, with sufficient resources, can bribe guardians to gain access to targets. Similarly, it can infiltrate a legitimate organization.

Offenders and their handlers

Groups promote offending through recruitment of members and allies. A large group can isolate its members, thus reducing outside influences—such as from parents—and increasing the influence of other group members. In this way, they replace outside handlers with inside handlers. Groups can also promote offender learning. Members of the group learn about what works and what does not to successfully pull off a crime. This information can be disseminated throughout the group and passed down to future members. Importantly, groups produce both excuses and provocations for committing crimes. However, in some circumstances you may be able to take advantage of how offenders in groups handle each other to reduce group violence (Step 26).

Places and their managers

Offender groups can seize control of places that an individual offender cannot. A drug-dealing group can hold a street corner against other dealers more easily than a dealer can on his own, for example. Terrorist organizations in some countries hold large swaths of territory. Offender groups can use places for meetings; for stashing weapons, drugs, and other goods; for prostitution and other human exploitation; for safe houses; and other purposes. Whether seized or purchased, once a place is controlled by the group it can organize the physical space to facilitate its activities. These methods can result in reduced risk or effort, or increased rewards.

Even if the group does not completely take over a location, they can bribe, intimidate, or replace managers so that the group can be sure that the place operates in a manner that helps their activities.

READ MORE:

Marcus Felson. 2008. "Routine Activity Theory." In *Environmental Criminology and Crime Analysis,* ed. Richard Wortley and Lorraine Mazerolle. Cullompton, Devon: Willan Publishing.

Marcus Felson and Ronald V. Clarke. 1998. *Opportunity Makes the Thief.* Police Research Series Paper 98. London: Home Office.

08 DISTINGUISH BETWEEN CRIMINAL GROUPS AND PROBLEM GATHERINGS

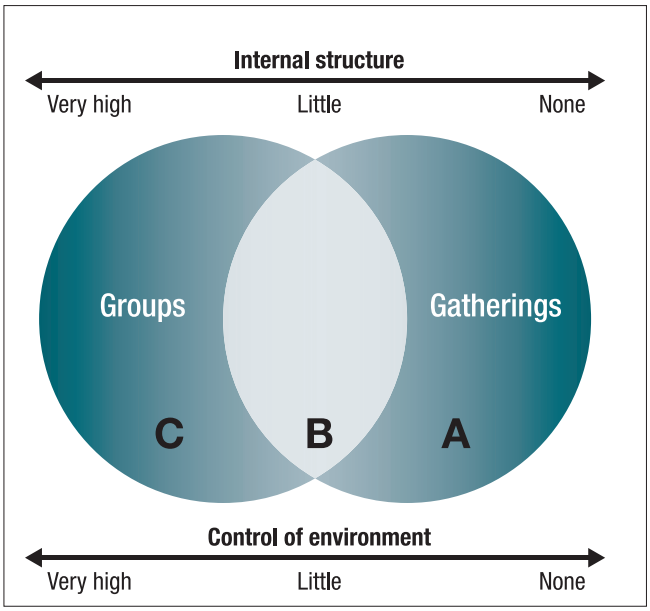
YOU SHOULD DISTINGUISH CRIMINAL GROUPS (such as pedophile rings and outlaw motorcycle gangs) from problem gatherings (such as juveniles involved in cruising or who meet for street racing). In both cases, you need to analyze the conditions that permit them to operate in your jurisdiction and ultimately work to remove these conditions. An important distinction between groups and gatherings concerns their internal structure:

- Groups are composed of offenders connected by some form of internal structure. Examples of structure include routine communications links, hierarchy, chains of command, and recruitment and expulsion practices. These and other forms of structure can be clear, strong, and enduring (area C in Figure 6), but often they are vague, weak, and transitory (Step 9).
- Gatherings are collections of individuals at particular places and time. Gatherings have little or no structure. Many gatherings are only collections at a place and time of separate individuals with no other connections (area A), but some gatherings have weak internal structures, thus overlapping with groups (area B). Typically, many participants have no intent to offend.

Here are three examples illustrating these distinctions:

1. A local bus system efficiently transports students to and from their schools by routing busses through a downtown hub where passengers can transfer. Students from many different schools congregate at the transit hub. If there are no other connections among the students, this is an example of a gathering. Within this gathering, a few individual students may bully and steal from other students, but they do not coordinate their activities in any way. Some of the non-offending students, nevertheless, may provide cover for the offenders. Here, the environment (the school, bus systems, the transit hub, gathering of students) provides an external structure and a set of crime opportunities for individual offenders.
2. Some youths from the same school may travel together so they can intimidate and steal from other students at the transit hub. They target students from a rival school waiting for particular busses at particular times. Here we see the overlap of gathering and group: the offending students have a rudimentary internal structure that helps them exploit their environment, but the environment is still providing most of the structure.
3. A neighborhood street gang robs pedestrians and runs a protection racket for merchants. It has a leader, rules for entry and conduct, and a hierarchy. Members use vehicles to get around and find likely targets. The internal structure here is strong, and allows the group to make use of the environment. Further, the group members can manipulate the environment to further their criminal activities. For example, they may alter the physical environment by using a meeting place and adapting it to their use (e.g., destroying streetlights). Intimidation alters the social environment to reduce their risks of apprehension.

Figure 6. Groups and gatherings



While participants in a gathering are extremely dependent on the physical and social environment, members of a criminal group use their internal structure to control their environment. Internal structure can protect a group's core members from the physical and social environment within which it operates. This means that leaders of criminal groups are exposed to fewer risks from the police and from rival groups. The downside of a group organization is that it is costly—senior members need to compensate junior members and others for the risks they run. Further, as groups become more organized they are likely to grow, and the larger they become, the greater attention they attract from the police. Finally, a tightly organized criminal group is less flexible in adapting to changes in the environment.

Sometimes it will be difficult for you to determine if you are dealing with an organized group or an unstructured gathering. If individual offenders perceive the physical and social environment in the same way, these offenders may behave in the same way and appear more organized than they really are. Here are some hypothetical examples of how this confusion can arise:

- Copper thieves can independently learn that vacant buildings in a particular neighborhood are good targets. Here thieves take advantage of the environment provided. Since each thief sees the same environment, each behaves the same way, even though they are not coordinating their actions. In contrast, an owner of a recycling business might recruit thieves, direct them to vulnerable targets, provide transportation, settle disputes among thieves, and provide guarantees that they are paid. In this case, the owner is creating an organization that is not completely dependent on the environment. To you, the two scenarios may look the same. You could mistakenly believe that in the first instance the thefts were organized or in the second instance that the thieves were disorganized individuals merely taking advantage of an obvious opportunity. Your intelligence analysis can help avoid such mistakes.
- Speeding may be highly concentrated along a particular stretch of highway at particular times, because each driver perceives the same opportunity to speed. Drivers only take into account the road in front of them and the cars in their immediate vicinity, but do not follow instructions from a "head" driver. The stable environment creates recurrent patterns of congestion and speeding. Intelligence analysis is not helpful with such collections (though crime analysis is). Let us contrast this speeding example to illegal road racing. An illegal road-racing gathering needs some organization, but not much because the relevant environment—the street system—is highly predictable and well understood by its members. Members know that on certain nights, particular stretches of road will be highly suitable for racing. The gathering only needs to be organized enough for members to know that others will show up at advantageous times and places and will obey the same rules of conduct. Such a gathering can operate because the environment provides much of the information necessary to coordinate activities. Such a group is highly dependent on this environment—if it changes then the group may have difficulty adapting. Nevertheless, a rudimentary organization facilitates the races.
- A group must be organized if it is to export stolen cars on a routine basis. The environment still produces opportunities (e.g., being near a port city), but to select the types of vehicles the export market wants, in the volume necessary, and coordinate the thefts with the shipping, the offenders must be far more organized than the street racers. Though these offenders are exercising more control over their environment, changes in the environment (e.g., tighter controls over who is allowed into the port facilities) can reduce the ability of this organization to function.

You can reduce the ability of organized groups to commit crimes by breaking them up or by changing the physical or social environment on which they rely. The importance of these two approaches will vary by the internal structure of the organization you are analyzing. The rare extremely organized crime groups will require far more law enforcement effort, though changing the environments can help undermine their capabilities. The more frequently encountered loosely structured organizations will be more vulnerable to environmental changes and less responsive to enforcement. Problematic gatherings, being more dependent on their environments, are best addressed by altering these environments.

09 TELL APART ORGANIZED CRIME AND ORGANIZED CRIMINALS

THE POPULAR IMAGE OF "ORGANIZED CRIME" IS THAT OF LARGE, ENDURING MAFIA-TYPE SYNDICATES, often with international reach, which are involved in a variety of criminal enterprises including extortion, racketeering, drug sales, and human trafficking. These syndicates have strict hierarchies of authority and demand extreme loyalty from their members, who might perform specialist roles. When necessary, they will seek to corrupt officials and they will use violence to enforce obedience from those they exploit or victimize.

While such organizations still exist, their prominence has faded and they now comprise only a minority of organized criminal groups. Far more common are small, organized networks of entrepreneurial offenders, often transitory in nature, that develop to exploit particular opportunities for illegal profit. These groups vary from temporary associations created to commit a time-limited series of offenses, to enduring businesses that invest in on-going criminal activities (see Table 4).

The formal definitions of organized crime recently adopted by the national police forces in the U.K. and Germany, as well as by the European Union, reflect this new reality. In all cases, the definitions try to include the entrepreneurial groups, principally by stating that the organized group can be composed of as few as two individuals. For example, the German federal crime intelligence office, the Bundeskriminalamt (or BKA), defines organized crime as follows:

"The planned violation of the law for profit or to acquire power, where offences are each, or together, of a major significance, and are carried out by more than two participants who co-operate within a division of labor for a long or undetermined time span using: a) commercial or commercial-like structures, or b) violence or other means of intimidation, or c) influence on politics, media, public administration, justice and legitimate economy."

Many of the crimes committed by organized criminals—for example; human smuggling, drug trafficking, sex trafficking, and money laundering—depend on overseas contacts. Opportunities for these crimes have expanded in line with increased globalization and developments in technology. Thus, the growth in international trade has made it easier to import drugs and to export stolen motor vehicles. The rise of the Internet and cell phone technology has made it easier to coordinate transnational crimes. The expansion of air travel has facilitated migration, legal and illegal, which brings with it increased opportunities for crime.

Table 4. Types of criminals

ORGANIZED CRIME SYNDICATES	NETWORKS OF CRIMINAL ENTREPRENEURS
Few in number	Many
Large	Small
Regional/national	Local
Stable, enduring	Unstable, temporary
Outside normal society	Integrated in society
Structured	Loosely knit
Hierarchical	"Flat" organization
Static membership	Fluid membership
Differentiated roles	Undifferentiated roles
Entrenched leadership	Changing leadership
Formal rules/regulations	Informal agreements
Criminal identity	Business identity
Full-time illegal operations	Part-time operations
Ties of loyalty	Business relationships
Use of violence	Avoidance of violence
Crime generalists	Crime specialists
Abundant resources	Limited resources
Sophisticated technology	Everyday technology
Seek opportunities	Respond to opportunities

Source: Bullock, Tilley, and Clarke 2010.

This is because recent immigrants still have ties in their home countries, which enable those so inclined to find the partners needed for transnational crime.

Given the wider definition of organized criminal groups, it is likely that several such groups, involved in quite different crimes, might independently be operating within your jurisdiction. One group might be specializing in home invasions, another in carjacking, a third in sex trafficking, and so forth. This considerably complicates the role of your department in respect of organized crimes and also provides difficult challenges for you in helping your police colleagues deal with the groups.

The purposes of intervention

In subsequent steps of the manual, we discuss in detail a number of organized groups. We will show that each group is different, that you must acquire different data about each one, and you will need to create tailor-made interventions. The purpose of intervening will vary with the nature of the group, as follows:

1. Some of the criminal groups, terrorist cells for example, are so dangerous that the principal objective of police action must be to remove them—i.e., identify and arrest the group members as soon as possible. As in the case of terrorists, this task would often be handed over to the federal authorities.
2. In many other cases, say an organized burglary ring, the prime responsibility for identifying and arresting the group would fall to your department, using largely the same approach when identifying and arresting individual criminals.
3. In a third group of cases, taking out the group might not be realistic or even particularly desirable. In dealing with street gangs, for example, the principal objective will usually be to restrict their capacity, or opportunity, to engage in behavior that is harmful to them or to the community. In other words, when dealing with organized groups, local police will often be involved in preventive action.
4. Even when the primary objective is to identify and arrest a dangerous group, an important additional objective should always be to prevent the formation of new groups to take the place of those arrested. Essentially, this involves applying principles of situational crime prevention to identify and modify the opportunities, or "facilitating conditions," favorable to the formation or operation of these groups. This task, discussed in the next step, puts intelligence analysts in a central role.

Marcus Felson has applied his routine activity theory to develop the following *"Rules for Understanding and Reducing Organized Crimes"*

1. Divide organized crimes into very specific types.
2. Focus on the acts, not the group engaged in them.
3. Expect considerable variation among groups in organization.
4. Assume that such crime is seldom ingenious.
5. Monitor and thwart the opportunity for small-time crime
6. Closely study the *modus operandi* in committing the crimes
7. Find out how crime feeds off legitimate and marginal activities.
8. Tease out the sequence of events for ongoing criminal cooperation.
9. Interfere with that sequence, access to the customer, or *modus operandi*.
10. Use situational prevention to reduce crime opportunities that feed organized crime, directly and indirectly.

Adapted from: Felson 2006

READ MORE:

Karen Bullock, Ronald V. Clarke, and Nick J. Tilley. 2010. *Situational Prevention of Organized Crimes.* Cullompton, Devon: Willan Publishing.

Marcus Felson. 2006. *The Ecosystem for Organized Crime,* United Nations European Institute for Crime Prevention and Control (HEUNI), Paper No. 26.

10 MODIFY THE CONDITIONS THAT FACILITATE ORGANIZED CRIMES

THE FACILITATING CONDITIONS THAT ALLOW A PARTICULAR ORGANIZED GROUP TO FORM AND OPERATE include both the physical conditions of the immediate situations in which the offenses occur and the wider social arrangements that make the crime possible. We can illustrate these by assuming that your jurisdiction harbors a group involved in stealing cars for export. Some of the facilitating conditions in your jurisdiction might include the following:

1. You are close to the Mexican border, to a deep-water port, or to a ferry terminal that serves Caribbean or South American countries.
2. You have substantial immigrant communities with ties to these countries, or temporary immigrant workers from these countries.
3. Local businesses trade with these countries.
4. The SUVs and pick-ups favored by local residents fetch high prices in these countries.
5. Young immigrant men have been thrown out of work by the recession and have become involved in crime.
6. Nearby border crossings are very busy and vehicles are subject to minimal checks. Ditto for the ports.
7. Too few officers in your department have the language skills to police the immigrant communities effectively.
8. Senior officers do not assign a high priority to vehicle theft.

Not all of these facilitating conditions can be modified—you cannot change the geographic location of your town—but you should focus on those conditions that are potentially modifiable. For example, your department could assign a higher priority to vehicle theft and could recruit more bilingual officers to allow more effective community policing of immigrant neighborhoods. Or your chief could lobby for more effective vehicle checks at border crossings. Not only should you be identifying the scope for these kinds of actions, but you should be arguing the case for their adoption.

How facilitating conditions make crime ESEER

Like much of the guidance in this manual, the framework for analyzing facilitating conditions is drawn from the field of situational crime prevention, specifically from the five principal techniques of opportunity reduction. These consist of techniques that:

1. Increase the effort needed to commit a particular kind of crime
2. Increase the risks of the crime
3. Reduce the rewards
4. Remove excuses for committing the crime
5. Remove specific temptations or provocations

These opportunity-reducing techniques correspond to five categories of facilitating conditions described in Step 6—those that make crime **E**asy, **S**afe, **E**xcusable, **E**nticing, and **R**ewarding, or **ESEER**. With regard to the list of facilitating conditions for theft of cars for export laid out above, it could be said that: 1–3 make it easy; 7 and 8 make it safe; 5 makes it excusable; 6 makes it tempting; and 4 makes it rewarding. ESEER should make it easier for you to think about and identify the facilitating conditions for any kind of crime.

Police efforts to prevent the repetition of a tragic drowning of illegal immigrants in the U.K.

In February 2004, a group of 23 illegally trafficked Chinese nationals drowned while digging for cockles (a shellfish) in Morecambe Bay, Lancashire. The resulting police investigation took 18 months. It required evidence to be collected in China and from European cockle processing plants, it accumulated 1.5 million pages of documentation (many in Mandarin, Spanish, and French), and it involved many different

government agencies in the U.K. and elsewhere. The six-month trial led to manslaughter convictions of three individuals responsible for illegally bringing the Chinese workers to the U.K. and for putting them to work in hazardous conditions.

Despite the enormous cost and effort of prosecuting the case, the Lancashire Constabulary realized that the conditions for a repeat of the tragedy were still in place:

- The scope for vast profits remained. The price of cockles had increased by 400 percent in the four years prior to the tragic drowning.
- Harvesting cockles is simple and relies only on the availability of cheap labor. Chinese networks were still open for recruitment and transportation.
- Illegal immigrants were willing to pay organized criminals up to £20,000 to enter the U.K., this money being deducted weekly from their pitiful wages. Profits were increased by accommodating them in cramped housing and giving them minimal safety equipment.
- Numerous ways to access the vast shoreline provided anonymity to cocklers and their controllers.
- The official permit scheme for harvesting cockles was still lax. On a single day, eight months after the tragedy, 61 Chinese nationals were working illegally on the sands, 48 with fraudulently obtained permits.
- The enforcement of safety regulations had also remained lax. The organized crime group had little interest in the safety of their workers of whom only about 10 percent carried lifejackets, GPS devices, or flares.
- About 100 vehicles transporting as many as 400 cocklers visited the shoreline daily and 80 percent of the vehicles were un-roadworthy, overloaded, or carried roof-riding passengers.
- An estimated 30 percent of cocklers were fraudulently claiming welfare benefits, at an estimated cost per year of £1,200,000.
- U.K. Border controls remained open to exploitation, and the risk of deportation was low. Immigration authorities had insufficient resources to detain potential illegal immigrants, who were released and asked to report to the immigration office at a later date.

Fearing a repeat of the tragedy, the Lancashire Constabulary decided to modify as many of these facilitating conditions as possible. An important priority was to reduce the anonymity of the organized crime group and the exploited workers. The permit scheme was strengthened, but the real innovation was to use existing legitimate workers to assist in identifying illegal workers. This was accomplished through the provision of a "muster point" (a catering van) in a safe location on the sands to communicate legal, procedural, and safety issues. A notice board displayed vehicle and contact details of workers on the sands, tide times, cockle bed information, as well as agency details.

This brought various benefits. Twelve hundred regulated workers were recorded in the new permit scheme and fraudulent unemployment benefit claims were reduced by 20 percent in the first year. Un-roadworthy vehicle usage reduced by 84 percent, with roof-riding eradicated. All workers started to carry personal life-saving equipment. Sea rescue deployments to save cocklers dropped from 34 in 2004 to 1 in 2005. The workforce went on to form their own shellfish association which met weekly and performed a self-policing function.

Detectives uncovered new information about migrant trafficking between China and the U.K., including who were the criminals and associates, how the profits were made, and how money was laundered. This information was insufficient to prosecute offenders, but shining a spotlight on them meant that they were operating in a more hostile environment with associates becoming worried that police attention might be drawn to their businesses. This helps explain why the criminals involved could not simply displace their illegal cockling activities elsewhere in England.

READ MORE:

Stuart Kirby. 2010. "Policing Mobile Criminality: Towards a Situational Crime Prevention Approach to Organised Crime." In *Situational Prevention of Organised Crimes*, ed. Karen Bullock, Ronald V. Clarke, and Nick Tilley. Cullompton, Devon: Willan Publishing.

11 STUDY THE MODUS OPERANDI STEP-BY-STEP

CRIMINOLOGISTS HAVE BEEN PREOCCUPIED BY THE QUESTION OF CRIMINAL MOTIVATION—why is that certain people, or kinds of people, become involved in crime and delinquency? In trying to answer this question, they have used hundreds of studies to probe into the backgrounds of offenders and have identified a vast range of possible contributory factors of upbringing, biology, personality, and social circumstances.

These theories are of limited practical value in your work as a crime analyst. This is because police can do nothing to alter an offender's history and little to change society. In any case, at a more down to earth level, motives for crime generally derive from common human failings such as greed, anger, covetousness, and the wish for such things as excitement, revenge, respect, and sexual release. Although some understanding of these commonplace motives may be helpful in analyzing particular categories of crime, knowing *why* crimes are committed is usually less useful than knowing *how* they are committed. This is because a detailed understanding of the *modus operandi* for a specific category of crime reveals many points for opportunity-reducing interventions. This is evident from Table 5, adapted from an analysis by Derek Cornish, formerly of the London School of Economics, showing steps in stealing a car from a parking lot and associated interventions.

Apart from showing a range of possible interventions, the table reveals a little appreciated fact: even a crime as simple as taking a car from a parking lot is not over in a flash, as we tend to think. In fact, it can take quite long to plan, prepare for, and execute—and this table does not even show what happens after the car is taken, how it might be used, sold, or concealed.

If we assume the car has been stolen to order for export, we would need to include, as a preliminary; receiving the instructions about which kind of car to steal, where best to find such a car, and where to deliver it. After the car has been removed from the lot, we would need information about the subsequent stages in getting the car to the ultimate buyer in another country. These include:

1. Bringing the car to a secure location where its identity may be changed and it might be disassembled
2. Storing it until ready to transport across border
3. Loading it in a sealed container onto a ship, either whole or disassembled
4. Or simply driving it across the border
5. At the destination handing it over to a local contact

Table 5. Stealing a car from a parking lot and possible interventions

STEPS	POSSIBLE INTERVENTIONS
Hook-up with co-offender	Use informants in convergent settings (see Step 12)
Get tools (screwdriver, slide-hammer, duplicate keys)	Control sales of duplicate keys and slide-hammers
Enter parking lot	Parking lot barriers; attendants; few entrances
Loiter unobtrusively	Cameras and/or regular patrols to deter loiterers
Reject alarmed cars Choose suitable vehicle	Visible protection of tempting vehicles
Enter car (duplicate keys, use screwdriver)	Cameras to monitor suspicious behavior; improve natural surveillance of lot
Break ignition lock (slide-hammer) or hot-wire ignition	Vehicle alarm to alert security; vehicle immobilizer
Exit parking lot in car	Attendants or other exit barriers; Vehicle-tracking system activated

Source: Cornish 1994.

6. Or having it collected at the dock by such person
7. If necessary having it reassembled
8. Legally registering it if necessary
9. Selling it on the open market or to private buyer

A detailed understanding of these stages would reveal many other possible interventions, though you might be interested primarily in the first four of them because they occur locally and you might therefore be in a better position to impede them, than stages 5–9 that take place overseas.

Laying out the sequence of stages for a problematic gathering can also reveal many intervention points. This is illustrated in Table 6, taken from a POP Guide on dealing with five sequential stages of student party riots: Initial planning; Preassembly preparation; Assembly; Assembled gathering; and Dispersal. The several steps falling under each of these stages yield many possible points of intervention.

READ MORE:

Derek Cornish. 1994. "The Procedural Analysis of Offending and its Relevance for Situational Prevention." Vol. 3 of *Crime Prevention Studies*, 151–196. Monsey, New York: Criminal Justice Press.

Table 6. Intervening to prevent a student party riot

	INTERVENTION	HOW IT WORKS
Stage 1: Initial planning		
1	Create a multiagency task force	Assembles community resources, and clarifies the roles and responsibilities of the groups involved
2	Require students to obtain a permit	Gives advance notice of a gathering, sets standards for the event, and holds hosts responsible for meeting the standards
3	Assign police to assist the hosts	Officers help students to meet legal requirements for a gathering
4	Increase penalties for rioting	Deters students from destructive behavior at the gathering
5	Partner with the media to influence student and community perceptions	Increases positive perceptions of the event and perceptions of risk for those interested in causing a disturbance
6	Work with landlords to ensure renter compliance	Creates more risk for hosting disruptive gatherings on rented property; encourages landlords to assist in preventing these
7	Control alcohol distribution	Reduces student alcohol consumption, underage drinking and purchasing of alcohol, and drunken driving
8	Provide alternative entertainment	Reduces the number of people at a single gathering; provides alternative recreation in a more controlled setting
Stage 2: Preassembly preparation		
9	Ask students to form "student patrols"	Reduces the need for official interventions
10	"Sanitize" the gathering location	Removes objects that can become a safety hazard
11	Monitor ads for gatherings	Notifies authorities of large gatherings in advance
12	Limit parking	Increases the effort needed to attend; removes targets that may be vandalized; clears exits in case of an emergency
13	Close or control traffic flow	Reduces pedestrian injuries; prevents students from bringing in large, dangerous objects

	INTERVENTION	HOW IT WORKS
Stage 3: Assembling		
14	Provide transportation to the event	Facilitates orderly arrival; reduces the number of cars; prevents attendees from bringing large quantities of alcohol
15	Establish a positive police presence	Reduces anonymity and facilitates communication
16	Establish and control perimeters	Prevents the gathering from spreading into the surrounding areas
Stage 4: Assembled gathering		
17	Use alternative deployment methods	Gives officers a tactical advantage over car patrols
18	Use visual deterrents to misconduct	Reminds those attending of the consequences of rioting
19	Videotape the assembled gathering	Reduces anonymity; assists in subsequent investigations
20	Site the media around the gathering	Breaks-up the cohesion of large groups
21	Watch for flashpoints	Immediate intervention can prevent a violent outbreak
22	Standardize the procedure to deal with disturbances	Helps stop violence as soon as it begins
Stage 5: Dispersal		
23	Provide transport from the event	Controls dispersal; reduces drunken driving
24	Facilitate orderly dispersal	Breaks up the gathering before a disturbance begins

Source: Tamara Madensen and John E. Eck. 2006. *Student Party Riots*. Problem Specific Guides No 40. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

12 LOOK FOR CONVERGENT SETTINGS

IN STEPS 8 AND 9 WE NOTED THAT MOST OFFENDER GROUPS ARE LOOSE KNIT AFFILIATIONS OF INDIVIDUALS, rather than tightly controlled hierarchical organizations. How do these groups form, how do they persist, and how do new loose knit groups reform when other groups are broken up?

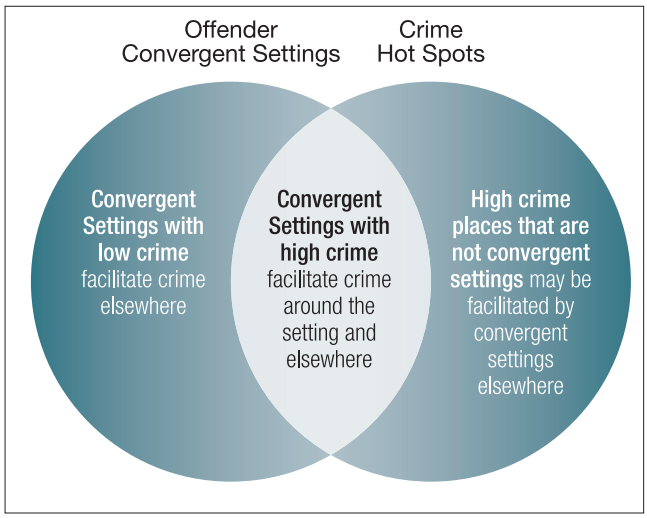
Convergent settings play an important role in these processes. Marcus Felson describes an offender convergent setting as a stable and predictable place where offenders, or potential offenders, can meet and form alliances. A place may be a convergent setting only at particular times. For example, a nightclub may offer a variety of performances throughout the week, but on Friday nights, the management caters to a particular crowd by providing music they find appealing. Potential offenders in this crowd know that if they show up on Friday nights they will find others with the same criminal interests.

The parking lot of a street corner convenience store may provide another example of a convergent setting. The store serves as an anchor for offenders by providing food and shelter for those hanging out. It also provides a ready excuse to be at the location, should a police officer stop the offender.

Convergent settings serve offenders in five ways:

1. **They bring together offenders and potential offenders who would not meet otherwise.** So they provide a spawning ground for offender groups. Many legitimate settings do this. High schools, for example, bring juveniles together who would not meet in other circumstances. The vast majority of these youth do not get into serious trouble, but a few students band together to commit crimes. Any youth gathering spot can serve as a convergent setting that can create groups that would not form in the absence of the convergent setting. Entertainment zones also serve such functions. A few mosques have served as convergent settings that allow Islamic extremists to meet and recruit potential new terrorists. Institutions for offenders—such as drug rehabilitation centers, half-way houses, and prisons—can become convergent settings.
2. **They provide a venue for strangers to observe each other and build sufficient trust and knowledge that they can work together.** If the setting only brings people together for very short intervals, then group formation is difficult. The ability to hang out and talk without looking suspicious is important.
3. **They provide convenient ways for offenders who already know each other to meet.** If an offender knows a bar to be a place where other offenders are likely to be present on a Saturday night, then he just needs to show up. He does not have to make specific plans with other offenders.
4. **They help groups replace members.** Without a replacement process, groups disappear. This is very common. With a convergent setting, it is easy for groups to recruit new members. When group members know that others at the setting are potential offenders this allows easy recruiting. Offenders who want to join a group know that if they routinely show up at a convergent setting, they have a good chance of becoming a member of a group.
5. **In private places they allow group members to meet without scrutiny.** Such places supply venues for initiation rituals, planning of complex offenses, and social support. Whereas public convergent settings are usually created for legitimate reasons and exploited for illegitimate reasons, private offender convergent settings are usually created to serve illegitimate ends.

Figure 7. Convergent settings are sometimes crime hot spots



Convergent settings may also be crime hot spots (see Figure 7). A bar that is a convergent setting for offenders attracts offenders who might take advantage of targets in the area. The opposite is also true. An active drug dealing location may become a convergent setting because it attracts people who want to become part of the drug trade. These wannabe members can provide a temporary labor pool—for carrying messages, serving as look outs, steering customers, or holding guns, drugs, or money—and while doing this can be evaluated for recruitment as permanent members of the group.

Analysts can detect convergent settings that are also crime hot spots through crime mapping. Convergent settings that are not crime hot spots will require you to find other methods of detection. Informants, offender surveillance and tracking, and other techniques will be more helpful than crime maps.

Convergent settings are not always physical places. For example, terrorists can use Internet websites as **virtual** convergent settings. Such websites allow people from around the world to meet and exchange information. Child pornography can be distributed through virtual convergent settings that accelerate the formation of pornography rings.

What should you do about offender convergent settings?

The most important thing is to look for them and exploit them for purposes of collecting data about offenders. Convergent settings can be a rich source of intelligence data describing active offenders: how they are organized, and what they may be doing.

Changing the setting so it does not facilitate offender groups is another important option. This is particularly true if the convergent setting is also a crime hot spot. Since many such settings are public places used by non-offenders, you should give preference to finding ways the place can continue to function without aiding offenders. This is possible if the owners of the place are not involved in crime. If the owner is aligned with the offender group, then regulatory or civil court action may be required to seize control of the place and keep it from being used by offenders.

There can be a conflict between using the offender convergent setting as a source of intelligence data and disrupting offender convergence. Allowing an offender convergent setting to operate in order to gain intelligence data also allows the offender group to continue committing crimes. This may be worthwhile if either a) many non-offenders legitimately use the setting, b) if closing the place simply displaces the convergent setting, or c) the offender group disrupted by the setting's closure is highly likely to be replaced by some other offender group.

On the other hand, altering a convergent setting to reduce crime may cut off vital intelligence and make it difficult to keep track of offender groups. If closing the setting reduces crime, and limits offender groups from reestablishing, then the loss of intelligence is probably a reasonable cost. This seems likely when the convergent setting is the locus of a crime hot spot.

Consequently, before making a decision about how to address a convergent setting, police should consider who else, besides offenders, uses the place; the availability of alternative convergent settings that offenders can displace to; and the chances that another offender group will exploit the situation.

READ MORE:

Marcus Felson. 2003. "The Process of Co-Offending." In *Theory for Practice in Situational Crime Prevention,* ed., Martha Smith and Derek B. Cornish. Vol. 16 of *Crime Prevention Studies.* Monsey, New York: Criminal Justice Press.

13 DISRUPT RECRUITMENT AND REPLACEMENT

POLICE WILL OFTEN TRY TO REMOVE KEY MEMBERS OF A CRIMINAL GROUP on the grounds that the broken up group will no longer be a problem. If its members are not replaced, or replacement takes a very long time, then disruption can work.

Before looking at the different forms of replacement, let us examine a generic recruitment process used to varying extent by most offender groups that can replace their members:

- The group must make contact with a potential new member. Convergent settings are useful at this stage and networks of offenders can refer potential recruits to group members.
- Screening or conducting the equivalent of a background check must be undertaken. This may be limited—such as checking on the potential recruit's reputation—or it might be extensive—for example, designed to weed out police operatives or informants.
- Screening may be coupled with testing or testing may be done separately. Testing might involve carrying out simple tasks to see how the subject performs, initiation rites, or even training. Screening and testing will depend on the risks associated with recruiting the wrong person, and on the skill level needed to carry out the tasks.
- Finally, the recruit might be employed as a peripheral member to carry out some minor tasks. Depending on the size and nature of the group, the subject may be promoted.

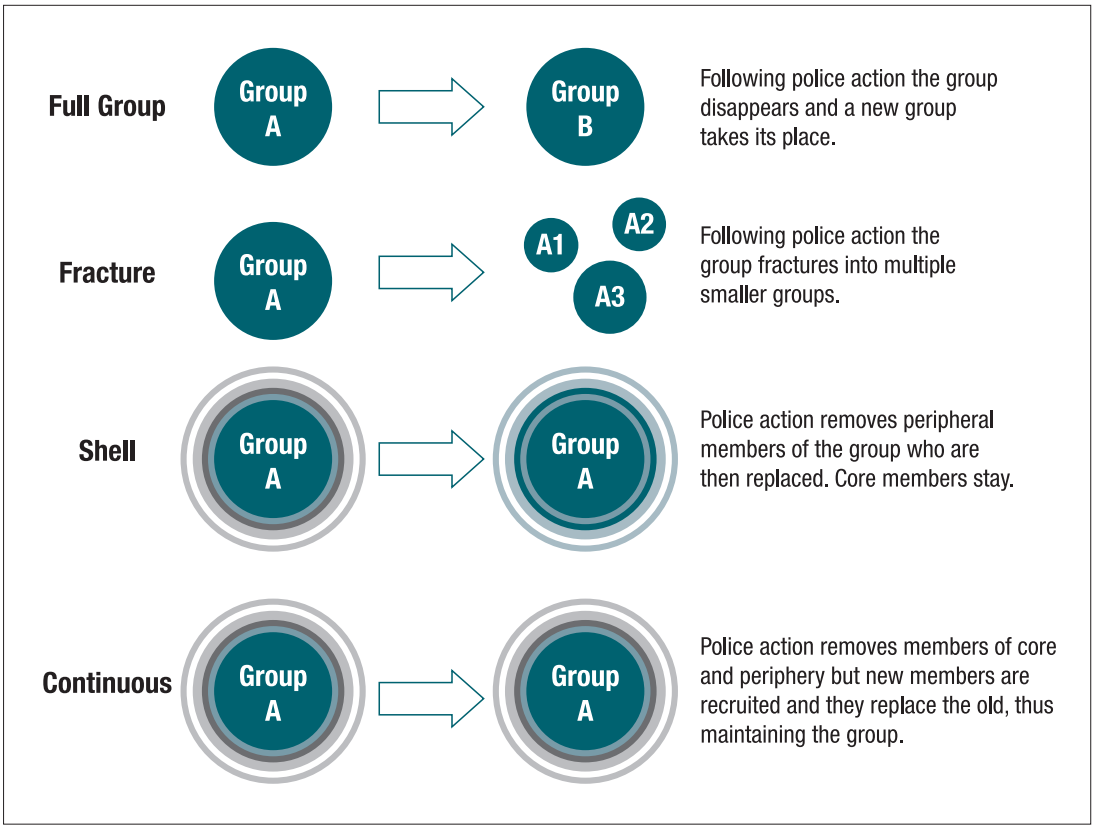
These stages assume varying importance for different forms of replacement.

Forms of group replacement

There are four forms of replacement (as illustrated in Figure 8) that you need to be concerned with:

1. **Full group replacement.** This occurs if the targeted group is incapacitated and totally replaced by another group. Many offender groups have limited ability to replace members, or even desire to do so. A group of young men on a street corner may have formed because they grew up near each other and have known each other for a long time. The members trust each other. Arresting and incarcerating most of them may disband the group, but the remaining members may have little interest in recruiting new members. However, another group of similarly situated young men may then move into the criminal niche that the first group has vacated. While this may not occur immediately, it is likely to occur if the conditions that fostered the first group are still present. Full replacement may also come after groups fight it out for who will take the territory or businesses of the disrupted group.
2. **Fracturing a group.** Removing members of a group may incapacitate the targeted group, but the remaining members may start up several smaller groups and continue the criminal behavior of the now defunct first group. The cottage industry theory of midlevel drug dealing suggests that this is common. According to this theory, many midlevel trafficking groups are loose knit marriages of convenience that form and reform. It could be that fracturing such a group facilitates recruitment of new crime participants because those offenders left on the street might seek out new partners. Fracturing can generate new groups if the conditions that facilitate group crime persist; the remaining members continue to take advantage of these conditions.
3. **Replacement of peripheral members.** If the group is made up of a core set of members surrounded by peripheral participants, then replacement of these peripheral members is possible when police remove peripheral members. The shell of disposable members, who undertake the riskiest activities, protects the core. This is common in retail drug trafficking—core distributors hire locals to sell the drugs and take the risk. It is also used in fraud groups,

Figure 8. Forms of group replacement



where the core players use disposable agents (who might not know the core members' names) to do the dirty work. In these circumstances, unlike continuous replacement, there is no expectation that members in the shell will ever advance to the core.

4. **Continuous replacement.** Some groups have recruitment practices that allow them to bring in new members and promote them. Enforcement may remove members from the core and periphery but the recruitment and promotion processes allow the group to continue its criminal activities. Continuous replacement requires the criminal group to have sufficient size that it can continuously suffer losses and maintain its basic structure. Any criminal group that is large and has existed for many years while under law enforcement pressure has probably mastered this strategy. Outlaw motorcycle gangs may be a good example of this: some have existed for decades with turnover at all levels of the organization.

Conditions for recruitment and replacement

The environmental opportunity structure within which the group operates creates two conditions necessary for recruitment and replacement:

1. The group cannot persist if the environment does not facilitate the particular criminal behavior the group carries out. The environment must provide a set of conditions—the opportunity structure—that permits the group to function. The group is adapted to this opportunity structure. Radical changes in the opportunity structure will limit all four forms of replacement discussed above.
2. There must also be an opportunity structure for recruitment and replacement. One example is convergent settings that we discussed in Step 12. Convergent settings allow offenders to meet other potential partners and permit group members to routinely meet potential new members.

Intelligence analysis needs to focus on the group's environment to understand these two conditions.

Replacement of peripheral members

A police official we interviewed described the following example of the use of shell replacement. In the 2000s, police agencies in eastern Massachusetts took dozens of reports from victims of the "Big Carrot" scam. Victims were called at work by someone claiming to be "Jim, your UPS driver." "Jim" divulged that his brother worked at Sears, Best Buy, or a similar "big box" store that was overstocked on big-screen TVs, or other high-end electronics, and the victims could get a great deal if they would pay cash. The victims met "Jim's brother" outside the store, turned over the cash, and got a handwritten receipt and instructions to pick up their merchandise at the loading dock. By the time they discovered there was no merchandise, Jim's brother had fled.

While many departments arrested dozens of men, they were unable to crack the core group who made the initial calls. They were never the ones to meet victims, collect the money, and hand over the "receipts." Instead, they hired ex-cons to serve as the "runners," who were the ones arrested. None of them knew the names of their bosses, and they were simply replaced with new stooges for the next round of scams. Although police did develop some intelligence on the ringleaders, as of 2010, police still occasionally received reports of these crimes, with no change in *modus operandi*.

14 INTERVIEW OFFENDERS

INTERVIEWING OFFENDERS CAN GIVE YOU USEFUL INFORMATION ABOUT WHY THEY COMMIT THEIR CRIMES, how they decide to commit them, and how they carry them out. You do not need to interview a "representative" or even a large sample to gain considerable insight into the group you are examining. You can sometimes conduct the interviews with offenders who are temporarily in custody, awaiting a court appearance. You might be able to get officers handling the case to ask the questions on your behalf, but you will have to brief them very carefully about the information you want and why. Even after release from jail or prison, you may find it useful to see if offenders are willing to talk about how they and others committed crimes.

Cooperation depends critically on the content of the questions. Make it clear that you are not looking for information about specific crimes they have committed or information about specific co-offenders. Treat the offender as an expert whose insights you are seeking. If you make clear that you are interested in generalities about the crimes in question—how targets are selected, how crimes are committed, ways of recruiting members, etc.—you can get much useful information. Offenders are often willing to talk openly about their crimes if they see no risks for themselves in doing so. This has been shown in many research studies, with different kinds of offenders. If you have little experience with such interviews, seek out an investigator with a reputation for putting offenders at ease and gaining useful information.

It is sometimes important to obtain information from a larger, more representative group. You might also feel it is important to interview active offenders who have not been caught. In such cases, your department may need to contract with a private research firm to conduct the interviews or with a university researcher. Such interviews are commonly undertaken by researchers studying a particular problem (see both Boxes for examples).

Where there is no need to talk with active offenders, they can be interviewed in prison. Again, if you use outside researchers to conduct such interviews, you must brief them carefully about what you need to know. Your agency will have to work out confidentiality and nondisclosure agreements with the researcher so they do not have to report which offenders said what.

Interviewing procedures

Professor Scott Decker of Arizona State University, who has conducted many interviews with offenders, breaks up the task into the eight steps discussed below:

1. *Establish the goal of the interviews before you start.* What gap would the interviews fill and how will that help in your analytic efforts? Do you need to understand the offender's motives, co-offending strategies, and target selection techniques? How will you use this information? It is important to devise a questionnaire to guide your interview.
2. *Decide who to interview.* Interviewing just any member of the group might not be worthwhile. High-rate offenders would usually be more knowledgeable about the operations of the group, other members' involvement, group objectives, and organizational structure. Seeking out the right person for the interview is therefore important.
3. *Determine who should conduct the interview.* This is mostly a matter of who has the skill and the access to the offenders. As mentioned above, if the offender is in police custody, a skilled officer might be able to interview the offender if you provide the questions that need answering. If you have the interviewing skills then you can do it. Interviewing active offenders who have not been caught poses greater difficulties. Locating them and interviewing them 'on their own turf' will require advance intelligence about where these groups operate. In most cases, someone from the police could conduct the interviews, again, with your guidance, but it might be possible to enlist the help of skilled researchers in this task.

4. *Convince offenders to participate.* This is sometimes difficult, although research suggests that many convicted offenders are willing to talk about their own feats. You should consult your local legal counsel to find out what inducements can legally be offered to these offenders in return for their participation, which do not violate policies and professional ethics.
5. *Record the answers.* Use of a tape recorder will allow the information to be transcribed and analyzed in detail. On the other hand, using a tape recorder may jeopardize cooperation.
6. *Analyze interview results.* This can be helped by using hypertext analysis software packages, such as Folio Views or Ask Sam, which allow you to quickly sort through the interview results and identify patterns.
7. *Sort out the truth.* This can be done by repeated questioning to look for consistency, interviewing different offenders about the same issue, or comparing what they say to what is already known through other sources. If you already have some knowledge about the group whose member you are interviewing, that knowledge will help sort truth from fiction.
8. *Use the interview results in problem solving.* Successful interviews will dictate response strategies that you can suggest to your police department. The Boston Operation Ceasefire, for example, used interviews with active gang members to learn about their preferences for guns and the gang's dependence on drug dealing. The results from these interviews led to the use of directed patrol against gang drug sales whenever there were shootings.

Theft of supplies and medicines in hospitals: What nurses said…

Dean Dabney interviewed 25 registered nurses in three hospitals to find out more about the theft of supplies and medicines. Almost all the nurses said that they took supplies from hospital stock, and claimed that this was accepted behavior among nurses who generally believed it was 'kind of compensation.' Thefts of over-the-counter drugs, including painkillers, were very common and were never reported to the hospital authorities. Thefts of non-narcotic prescription medicine was also common; in these cases, nurses take advantage of the lag between the pharmacists realizing that the patient is no longer taking the medicines and when they quit sending them. Thefts of narcotic medicines by nurses, although rare, also occur, but are much more likely to be reported by other nurses.

Source: Dean Dabney. 2000. Neutralization and deviance in the workplace: Theft of supplies and medicines by hospital nurses. In *Deviance and Deviants,* ed. Richard Tewksbury and Patricia Gagne. Los Angeles: Roxbury Publishing.

Incorporating offender interviews in problem solving

The Cincinnati Police Department and researchers at the University of Cincinnati worked together to use offender and victim interviews to reduce street robberies. Police were interested in whether groups of offenders were involved, if the robbers targeted Hispanic victims, and several other questions. Police and researchers developed a set of questions. Two detectives interviewed robbery arrestees and victims, and taped the interviews. At the university, the tapes were transcribed, the transcriptions coded so they could be analyzed, and then the coded date was analyzed. The results showed that the offenders were probably not operating in stable groups, but they had a distinct preference for Hispanic victims who robbers rightfully believed were unlikely to report the robberies. Police used these results to inform members of the Hispanic community in the area.

READ MORE:

Scott Decker. 2005. *Using Offender Interviews to Inform Police Problem Solving*. Problem-Oriented Guides for Police. Problem-Solving Tools Series, No. 3. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

15 TAP THE KNOWLEDGE OF OFFICERS

PATROL OFFICERS AND INVESTIGATORS ARE IMPORTANT SOURCES OF INTELLIGENCE DATA and tapping their knowledge can be extremely helpful to you. This point is often addressed by developing better procedures for information sharing. Data sharing procedures can help, but they do not go far enough. This is because information sharing can only help when two conditions are met: someone has data of potential use for intelligence, and someone knows that the data is potentially valuable. Former U.S. Secretary of Defense, Donald Rumsfeld, has developed a classification based on these conditions, which we apply in the four cells of Table 7.

If the data is known to be of value to address an offender group, and an officer has the information, then the emphasis should be placed on data sharing (cell 1). However, when police have the data, but do not know its value, then intelligence analysts need to spend more time briefing patrol officers and investigators about what sorts of data is useful. This is sharing information about targets (cell 2).

When no one in the police department has the data, then information or target sharing will not help. If intelligence analysts can identify specific gaps in their knowledge (they know the value of the data, but do not have it), then focused efforts to gain the data can be designed and launched (cell 3).

The most difficult circumstance is that no one knows that the data is of value (though it is), and no one in the police department has the data (cell 4). There is no satisfactory solution to this problem, but there are three practices that can help:

1. If patrol officers or investigators have diverse experiences with a group of offenders, bringing them together to exchange ideas and experiences may be useful. Discussions among police who have very different experiences with the group may challenge some basic assumptions about the group and reveal potential knowledge gaps. The purpose of the discussion is to explore disagreements; consensus and agreement is not the goal.

Table 7. Four problems with using the knowledge of police officers

FOUR PROBLEMS WITH USING THE KNOWLEDGE OF POLICE OFFICERS		
	Data's value is known	Data's value is unknown
Data is known to police	Cell 1 Someone within the police agency has the data, and they know it is useful for intelligence. Improvement in information sharing may help.	Cell 2 Someone within the police agency has the data, but the value of this data is unknown. Sharing target information may help.
Data is unknown to police	Cell 3 No one in the police agency has the data, but it is known that if the data were available, it would be valuable. Targeted data collection may be helpful.	Cell 4 No one in the police agency has the data, and even if that data was collected its value would not be known. Discussions among police familiar with the problem, surveys of police personnel, or theory driven data collection may help.

2. Data may be dispersed among many individuals so that no individual understands that they have useful data. Surveys of officers and investigators can identify: (a) patterns of knowledge that no one was aware of; (b) hidden differences in police understanding; and (c) knowledge gaps that can be targeted for additional data collection. In the late 1990s, the Washington/Baltimore High Intensity Drug Trafficking Area (W/B HIDTA) conducted an annual survey of its many squads to assess commonalities and differences among the offender groups being investigated. The surveys suggested that for the most part, the groups being addressed by the investigative squads were small to moderate in size, not hierarchically organized, and not long lived. This was useful strategic intelligence for the W/B HIDTA.
3. Training officers, investigators, and intelligence analysts in environmental criminology theories may help them understand the problem being addressed. Discussing ways to address offender groups (based on research and experience) can also reduce the circumstances under which police do not know the data they need to collect.

Barriers to information sharing

Patrol officers and investigators may sometimes be unwilling to share information for reasons discussed below. Here we use the familiar framework of risks, effort, rewards, excuses, and provocations.

Risks of Sharing. If officers feel there is greater risk for sharing information than not sharing, then little sharing will take place. Have clear policies and procedures for sharing and hold people accountable for sharing, when sharing is legally permitted. Hold supervisors accountable for assuring adequate sharing.

Effort of sharing. If information sharing is easy, more information will be shared. Reducing the effort necessary to pass information along can be facilitated by making it convenient. If two units routinely need to share information, this will happen more readily when they are located in close physical proximity. Reducing the paperwork burden can also reduce the effort, though this may interfere with holding supervisors accountable for sharing.

Rewards for not sharing. If officers or their units get more rewards for holding on to data than for sharing it, they will not share. Look for ways of crediting officers for sharing. If officers do not learn how the data they provided helped, then they are less likely to share in the future. Giving feedback on the utility of the data increases rewards for sharing. Further, if officers are only asked to give data, but seldom receive data, then they will have less incentive to share. Look for opportunities to provide them with useful data.

Excuses for not sharing. There are four common excuses officers use to avoid sharing intelligence data: it is not my job; there is no one to tell; others already know this; and, I did not know it was useful. Policies and procedures, training, and supervision can address the first excuse. Ensuring that intelligence analysts are known to officers can address the second. Holding discussions with officers and investigators about targets can address the last two excuses.

Provocations for not sharing. If officers and investigators have bad relationships with intelligence analysts, then they are more likely to withhold data than if they have good relationships. While policies, procedures, training, and supervision are necessary, they are not sufficient to assure information sharing. Good personal relationships are essential.

16 WORK WITH BUSINESSES, PRIVATE SECURITY, AND THE CITY

DISASTER PREPARATION ALREADY REQUIRES YOUR DEPARTMENT TO WORK CLOSELY WITH THE MAYOR OR CITY manager, as well as with other city agencies such as fire, emergency medical, hospitals, and schools. Make use of this partnership when gathering intelligence about criminal groups that you may be investigating. In addition, forming partnerships with private security and businesses in your city can help your department in gathering intelligence about criminal groups. This is especially important for dealing with suspected terrorist groups.

Businesses are an important source of information about the activities of criminal groups. For example, banks, check-cashing establishments, and money-transfer stations, such as Western Union, can tell you about suspicious financial transactions or financial transactions of suspect groups; car rental agencies, motels, and real estate agents can give you information about newcomers and transients; and private security practitioners can inform you about organized fraud that might be funding terrorism. Your department should take charge of the partnership, but to obtain full cooperation it should give private sector colleagues public credit for their contributions.

In the United States, private security employees outnumber the police by three to one. They are responsible for the security of most of your jurisdiction's infrastructure and provide visible crime control in the places where people spend much of their daily lives: at work, on public transport, in educational facilities, in shopping malls, and even in gated communities. One of the best ways to approach the larger businesses in your community is through their corporate security officers, but there are many other security professionals in your community who could provide you with valuable help. These include local security consultants, the suppliers of guard services, and installers of security hardware and systems.

You might think you already have good informal contacts with this group, facilitated by the many retired police officers employed within their ranks. However, the Department of Homeland Security recommends that, to serve the goal of preventing terrorism, police chiefs in larger jurisdictions should consider formalizing relationships with private security through coordination agreements or memorandums of understanding. Formalization shows employees from both sides that the partnership is an organizational priority. Specifically, it will help your department do the following:

- Safeguard the critical infrastructure in your community that is protected by private security and ensure rapid recovery in the event of an attack
- Obtain effective help from private security in emergencies
- Improve the flow of information—in both directions. Partnering will allow you to communicate threat information to the private sector efficiently and, conversely, it will allow the private sector direct access to the right people when they need help or want to report information.
- Make use of private-sector knowledge on topics that your department might know little about, such as organized fraud or cybercrime
- Obtain access to private-sector resources and facilities that will help you meet training and operational needs

Perhaps the most critical issue concerns the handling of sensitive information. Your department may be uncomfortable sharing information—especially about terrorist groups—with companies owned by foreign entities and it may not be legally permitted to share information that private security requests, such as criminal histories. For their part, private security may fear that proprietary business information could become public as a result of Freedom of Information Act requests. They might avoid speaking candidly at partnership meetings because competitors could learn about their problems, or because they might be charged with antitrust violations if they discuss inappropriate topics. Finally, they might not report instances of cybercrime because your department might then seize their records and computers. In a word, this all boils down to mutual trust which takes time and patient negotiation to develop.

Getting started

- Clarify the purpose of the partnership and set goals for improved collaboration and coordination
- Spell out what the partnership must do to accomplish its mission
- Identify the resources the partnership will need to meet its goals and find ways to secure these materials
- Find a physical and logistical home for the partnership and appoint a police officer to coordinate its activities
- Decide how the partnership members will communicate, both routinely and in emergencies
- Create an identity for the partnership through the use of a logo, brochure, or website, and use this identity to obtain funds and recruit members

READ MORE:

John Dempsey. 2008. *Introduction to Private Security.* Thomson Higher Education.

Graeme Newman and Ronald Clarke. 2008. *Policing Terrorism: An Executive's Guide*. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

The Law Enforcement-Private Security Consortium. 2009. *Operation Partnership: Trends and Practices in Law Enforcement and Private Security Collaboration.* Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services. www.cops.usdoj.gov/Publications/e08094224-OpPartnership.pdf.

17 WORK THE COMMUNITY

YOU CANNOT OVERESTIMATE THE IMPORTANCE OF THE COMMUNITY: it is the source of most police knowledge about offender groups. Offender groups will attempt to control what community members know about them and what they pass on to police. So, if there is friction between community members and the police, offender groups will exploit this weakness.

By community, we mean people who live, work, study, or play in the area. There are four main ways that the community can assist police in addressing offender groups, corresponding to the four stages of SARA (Step 5).

Identifying concerns and problems (scanning)

Community members are the first to encounter offender groups, if not as victims then as neighbors, acquaintances, customers, or tenants. Before police are aware of a new offender group, people in the community have often detected its presence. This may be one of the greatest values of community policing—taking community concerns seriously and allowing the police to learn early about developing problems.

While police should pay close attention to the community, you should not take all views expressed by the public as equally valid. You should treat expressions of concern regarding offender groups as hypotheses that you need to test (Step 21). Table 8 illustrates this point. Community members may express no concern about some group behaviors—because they do not find these troublesome; they are intimidated; they gain from the behaviors; or they are unaware of them. Police enquiries may indicate that this lack of concern is valid (cell 1) or that there is a serious problem but the public is not expressing concern (cell 2). In contrast, the community may find some group behaviors very troublesome. Analysis may indicate that these concerns are misdirected (cell 3) or that they are fundamentally sound (cell 4). Distinguishing between cells 3 and 4 is often difficult. Community members may have important insights that go beyond data available to the police, but they can also misperceive situations and demand actions that are inappropriate, costly, or violate civil liberties.

Table 8. Community concerns and community problems

	NO EVIDENCE OF A PROBLEM	EVIDENCE OF A PROBLEM
No expressed community concern	1. Issues that can be ignored. But you cannot rule out the possibility of a deeply hidden problem.	2. Determine why the community is unconcerned with the problem and consider expanding work with the community to address the problem.
Expressed community concern	3. Seek data to determine if the concern is valid, or if evidence is negative, determine why some members of the public believe there is a problem. The public's concerns may need redefining. This may not be an issue intelligence analysis can address.	4. Some community members may be in a good position to assist with gathering intelligence.

Knowledge about offender groups (analysis)

The most obvious way community members can help is by providing data on the offender group. You can expect four groups of people to have useful knowledge of the group:

1. **Co-offenders** are community members who are members of the group or knowingly assist the group in its activities.
2. **Victims** are people directly harmed by the group's criminal behaviors. (Many of these victims, especially of group violence, may be co-offenders.)
3. **Place managers** are the owners and managers of businesses, residences, and other facilities that the group uses. These managers may be unaware of the group's activities, they may know what is going on but choose to ignore it, or they may knowingly work with the group.
4. **Others** include neighbors, businesses, delivery workers, and government workers who frequent the area and encounter the group.

The value of the information will depend on how well these people know the group, their physical proximity to the group's area of operation, and the degree to which the group's behavior influences their lives. If the group is well integrated into the community, this might limit the information you can expect to get from the public

Possible ways to address group (response)

Just as community members vary in their knowledge of a group, so does their ability to assist in dealing with the group. Those most knowledgeable may not be those who can do the most about the group. Those who can provide the greatest assistance in addressing problems may not be those who know most about the group. Residents of an apartment building, for example, may know a lot about a gang that uses the building, but they may not be able to do much about it. On the other hand, the owner of the building, who may know the least about the group, has the power to change lease conditions and alter the building's physical environment.

There are three ways members of the public can assist:

1. They have resources and legal powers that can be used against the group. Place managers provide a good example, particularly if the group relies on specific locations for their activities.
2. They have expertise that can be applied to the solution. Such expertise can vary from the ability to help remove an abandoned building or clean up a vacant lot used by a gang, to having computer training sufficient to create a database and website for a community group.
3. They create community and political support for actions against the group. This can be particularly important if the offender group is networked with elected officials, or there is a need to put pressure on business or property owners who facilitate the group's activities. At minimum, you do not want substantial community antagonism to the police efforts, so winning and maintaining public support can be important for solving crime problems. Selling a solution to a community after it has been decided on behind closed doors is often more difficult than including community members in problem solving from the beginning—even if this raises concerns about how much intelligence information can be shared with participating community members.

Perceptions of effectiveness (assessment)

The final way community members can assist intelligence analysis is the evaluation of police actions. If public perceptions are important, then poll community members after police actions to determine if they perceive a reduction in the problem. This can be as simple as informal discussions with members of the public or as rigorous as randomly sampling the public and interviewing them about how they view the problem. For example, if the police take action against an offender group shaking down business owners for protection money, it would be useful to have covert conversations with business owners to determine if they are still receiving threats.

Even if such data is not used to evaluate effectiveness, sharing evaluation results with the community is useful. It may be that while there is strong quantitative evidence of a reduction in the group crime problem, members of the public can point to exceptions that you need to address.

18 CREATE INTELLIGENT MAPS

GEOGRAPHIC INFORMATION SYSTEMS (GIS) CAN ASSIST THE ANALYSIS OF CRIMINAL GROUPS AND PROBLEMATIC gatherings. Geographic analysis allows you to think and communicate "visually" about the problem you are investigating. This can be very helpful in your process of research, analysis, and presentation of the intelligence you have gathered. It can help you provide your police department with timely and accurate intelligence, and also with advice on tactics and deployment strategies.

The questions you might seek to answer using GIS include the following:

- Where are these groups concentrated geographically?
- How dispersed are they in your jurisdiction, state, nationally, or even internationally?
- Can the environmental characteristics of the place where these groups are found give you any additional clues about the group?
- Which kinds of urban areas or cities are these groups more likely to operate in?
- Are there any unique geographic features of the area that hold some special meaning for the groups who live there?
- Have there been geographic shifts in the groups' movements throughout years? If so, what dictates these geographic shifts?
- Can you identify any geographic patterns about the movements or distributions of these groups throughout your jurisdiction, the state, or the nation?
- What targets are most at risk? Where are these targets located?

Geographic analysis and problem-oriented policing

The analysis needed for problem-oriented policing under SARA (Step 4) can also be applied in geographic analysis (see Vann and Darson listed below).

Scanning. Maps can quickly identify crime clusters and hot spots by location, time of day, type of crime, etc. For example, you can use GIS to identify types of crimes committed by the group you are studying. But be cautious. Some problems are not strongly geographical, and will not show up on maps. So do not rely exclusively on maps to detect problems.

Analysis. Maps can be used to relate crime to other spatial variables, such as street layout, transportation arteries, land use categories, locations, and so on. It can also be used to profile crimes that have been committed by the group you are studying, which will give you valuable information on offenders and their characteristics. GIS can also be used to map at-risk targets and locations where these groups operate. In addition, GIS can be used to understand the reasons why the groups commit the crime and how location affects their decision.

Response. Maps can be used strategically (e.g., identifying crime patterns) and tactically (e.g., extrapolating serial crimes to predict anticipated targets). If you have identified at-risk targets and locations, for example, GIS can be used to map the response strategy you are proposing to your department, thus allowing for well-planned resource allocation.

Assessment. Maps can be used as before and after overviews depicting the effects of the intervention proposed. Such examination will allow you to make an assessment of the success or the failure of the intervention implemented.

Cracking down on gangs with GIS

The Akron (Ohio) Police Department's Gang Unit incorporated mapping in their efforts to address the gang problem in the city. The unit used graffiti markings throughout the city to identify the active gangs and to record gang boundaries and track gang activity. Gang Unit officers began by visiting the sites and taking pictures of the graffiti, which were marked with the graffiti's location. The data was then entered into a GIS database to map the boundaries of more than 30 gangs in Akron. Apart from allowing officers to describe the areas where gang activity was present,

this also enabled them to identify overlapping space—"hot zones" or "conflict zones"—where gang conflict was most common. These areas were identified through graffiti portraying insults between the rival gangs. The map of these territories is shown in Figure 9 on page 51.

Tracking gang activity in Orange County, California

Recognizing that gang activity crossed jurisdictional boundaries, the Orange County Chiefs and Sheriffs Association created a countywide Gang Strategy Steering Committee to address the shared problem of gang violence. The committee comprised 22 law enforcement agencies, as well as researchers, local government agencies, the community, and businesses. It created a Gang Incident Tracking System (GITS), which was used, in conjunction with GIS, for mapping and spatial analysis of gang activity in the county. GITS and GIS were used not only for monthly statistics and information management, but also for personnel deployment, strategic planning, and resource management. The data gathered through these systems was used to evaluate gang prevention strategies, and intervention and suppression activities for each individual department, as well as for the county.

Geospatial analysis of terrorist activities

Researcher Brent Smith and colleagues used GIS to examine incidents of terrorism in the United States during the past 25 years. Specifically, the research focused on the planning processes and behaviors that the terrorists engaged in while preparing their attacks. A strong spatial relationship was found between terrorist incidents, terrorists' preparatory behaviors, and where they resided. Fifty percent of incidents happened within 30 miles from where they resided, and this was most apparent among international, left-wing, and single-issue terrorists. The analysis also found, for example, that in the case of environmental terrorists, antecedent activities took place very close to the incident location, with a median distance of about 5.3 miles. For international terrorists, this distance ranged between 271 and 810 miles, implying a quite different planning strategy.

The **Crime Mapping and Analysis Program (CMAP)** provides training to law enforcement agencies in the use of GIS, as well as crime and intelligence mapping. The program is funded by the National Institute of Justice's Office of Science and Technology. CMAP provides useful resources including a crime analysis unit developer kit, free software downloads, publications, and free crime mapping and analysis manuals. Their website is www.justnet.org/Pages/cmap.aspx.

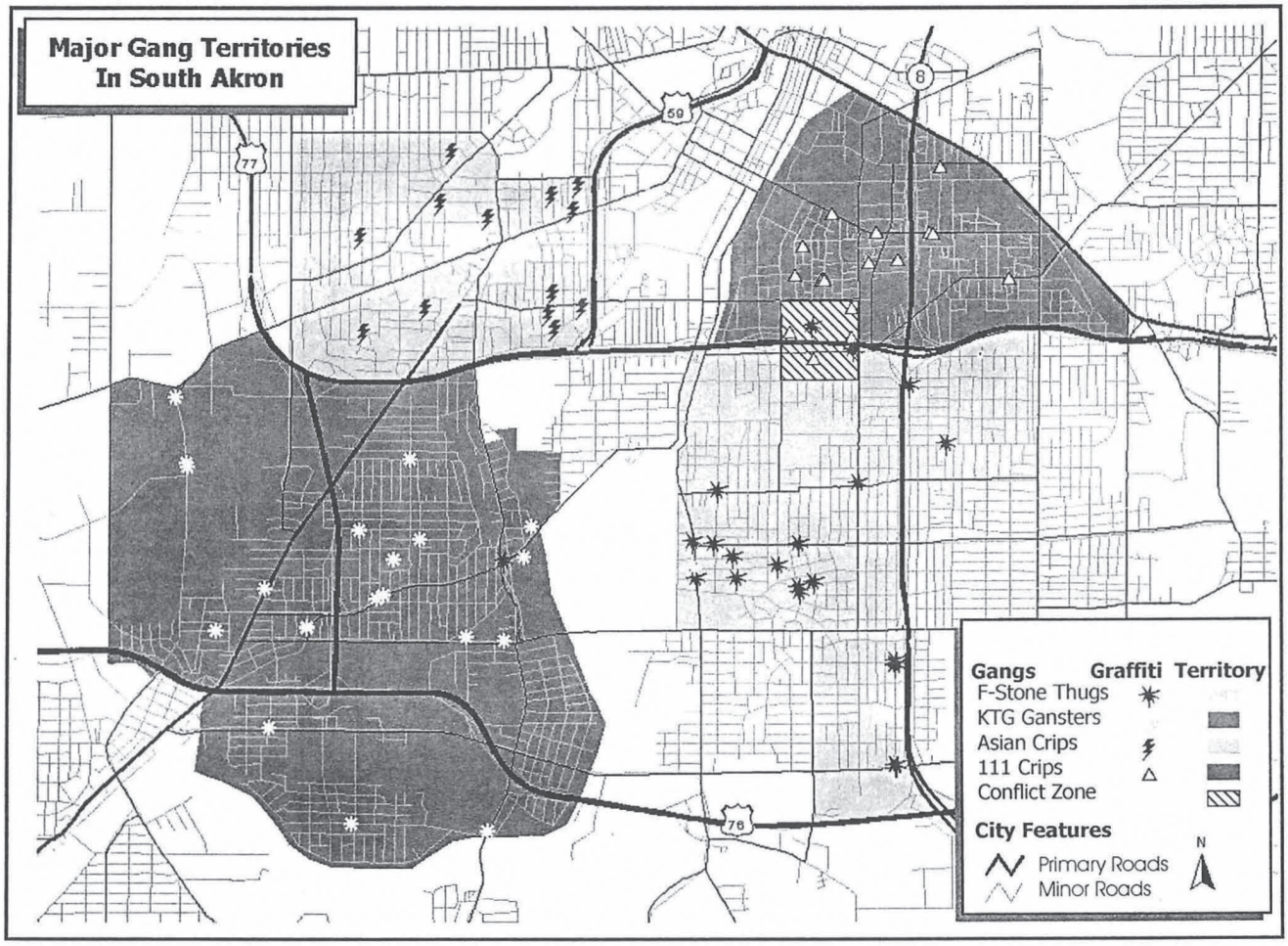
READ MORE:

Spencer Chainey and Jerry Ratcliffe. 2005. *GIS and Crime Mapping.* New York: Wiley.

Brent L. Smith, Jackson Cothren, Paxton Roberts, and Kelly R. Damphousse. 2008. *Geospatial Analysis of Terrorist Activities: The Identification of Spatial and Temporal Patterns of Preparatory Behavior of International and Environmental Terrorists.* Report published by the U.S. Department of Justice under Grant #2005-IJ-CX-0200. www.ncjrs.gov/pdffiles1/nij/grants/222909.pdf.

Irvin Vann and David Garson. 2003. *Crime Mapping: New Tools for Law Enforcement.* New York: Peter Lang Publishing.

Figure 9. Major gang territories in South Akron



Source: Otto et al. n.d. *Cracking Down on Gangs with GIS.* Akron (Ohio) Police Department. (Available at faculty.uml.edu/apattavina/44.594/GISGangs.pdf.)

19 USE NETWORK ANALYSIS TO CONNECT THE PLAYERS

NETWORK ANALYSIS ALLOWS YOU TO EXAMINE LINKS BETWEEN MEMBERS OF A GROUP AND RELATIONSHIPS among groups and organizations. It has been applied to investigations of organized crime groups and street gangs, and in uncovering terrorist networks.

It is often important to determine each individual's role within the group. For example, when investigating an organized crime group, you can integrate information from other sources, such as crime incident data, telephone records, and surveillance reports to determine who the leader is; who is responsible for drug supply, distribution, sales, smuggling; who handles money laundering; and so on.

Types of network analysis

Researchers categorize network analysis into three generations according to the degree of complexity:

1. The first generation is a manual approach. It creates a link chart showing criminal associations based on raw data on relationships. This might not be difficult to do when the group is small and the relationships among its members are not complex.
2. Second generation network analysis uses software, such as Analyst's Notebook, Netmap, XANALYS Link Explorer, and COPLINK. These programs can handle large groups and large amounts of relationship data. They permit a visual analysis of relationships among members of the groups and are helpful in determining whether the group is loosely or tightly organized.
3. Third generation social network analysis provides a graphic representation of social networks (also known as a sociogram) and can reveal subgroups, discover patterns of interaction, identify central individuals, and uncover network organization and structure. Because it uses mathematical computations to identify these patterns, it allows less subjectivity on the part of the analyst and reduces the risk of omitting important details. This type of network analysis is becoming widely used by researchers and analysts.

Elements of social network analysis

Key elements to analyze when performing social network analysis include actors, network positions, network structure, network density, and connectedness.

Actors

When studying particular actors or individuals, you should concentrate on gathering information on connections among individuals, places, vehicles, phone numbers, and other things. Personal characteristics of actors are far less important. The fact that Fred often calls Gene's phone, and Gene was seen driving a car owned by Trisha is more important than the fact that Fred is 25 and Gene is 27, and that no one knows Trisha's age.

Network position

Three major concepts in network analysis—degree centrality, closeness centrality, and betweenness centrality—will help you identify the position of actors in the network:

1. Actors with many direct ties to others have high scores on **degree centrality**. They may play an active role in the network, making them more critical.
2. Actors who are physically closer to more actors in the network will have high scores on **closeness centrality**. They are able to easily coordinate tasks and transfer resources within the network.
3. Lastly, those actors who connect many other actors have high scores on **betweenness centrality**. Their removal may prevent contacts between other actors; effectively fracturing the network.

The Royal Canadian Mounted Police use a *Target Profile Sheet* to gather information about actors involved in serious and organized crime.

Personal Data:

- Personal details
- Information on the target's affiliations (e.g., geographic scope of criminal activity, memberships, or addictions)

Criminal History:

- Target's criminal history
- Target's criminal reputation (e.g., position, influence, and importance in the criminal network)

Criminal Roles:

- The criminal capacity of the actor (e.g., crime projects the actor facilitated)
- The current role or primary function of the actor within the network, and how easily replaced

Skills and Experience:

- The expertise and skills that distinguish this actor from others in the group

Finances:

- Known fixed assets and income of the actor and his/her deemed nominees

Vulnerabilities:

- What personal, behavior, status, or relationship aspects make the actor vulnerable or attractive to law enforcement

Social Ties:

- Connections (including family ties), specified by:
  a. The type of the relationship
  b. Frequency of interaction
  c. Degree of criminal association
  d. Degree of licit professional association
  e. The nature of the social relation

The Investigative Research:

- The investigation itself (previous and ongoing efforts)

Network structure

When analyzing the relationships between two or more actors in the group, you are interested in not only the relationships among them, but also cliques or groups of close ties between these actors. That is, you are examining the structure of the entire network—for example, whether it is loosely or tightly organized. This could be important when devising a response strategy. For instance, more open or widely spread networks are more vulnerable to disruption by removing key members.

Network density

The density of a network allows you to determine how close knit or loose knit it is. Figure 10 gives a simple formula for density and applies it to three networks. The first network has less than a third of the maximum possible connections. The second network has all possible connections. Networks that are fully connected (density of 100 percent) are called cliques. The third network is called a cluster because it is at least 80 percent connected. Note that in the first network, three members (E, F, and G) form a clique. In a clique it may be difficult to distinguish between critical and peripheral members.

Connectedness

You may find it useful to determine the degree of connectedness among members, especially when it is vital for you to determine the flow of communication or authority. Connectedness is determined by the direct and indirect ties among the network members (count the connections between two members). In network 1 of Figure 10, one link connects individuals A and B. Two links connect A to D and three to C or E. Four links are needed to get to the other three members.

Network analysis and Operation Ceasefire

David Kennedy and his colleagues made important use of network analysis during Boston's Operation Ceasefire. Members of various criminal justice agencies identified violent gangs and provided information on the gang members. More importantly, they provided information on conflicts among different street gangs, which were translated into sociograms that laid out the gang conflict network (see Figure 11). Gangs not in conflict with other gangs are in the upper right, but are not part of the network.

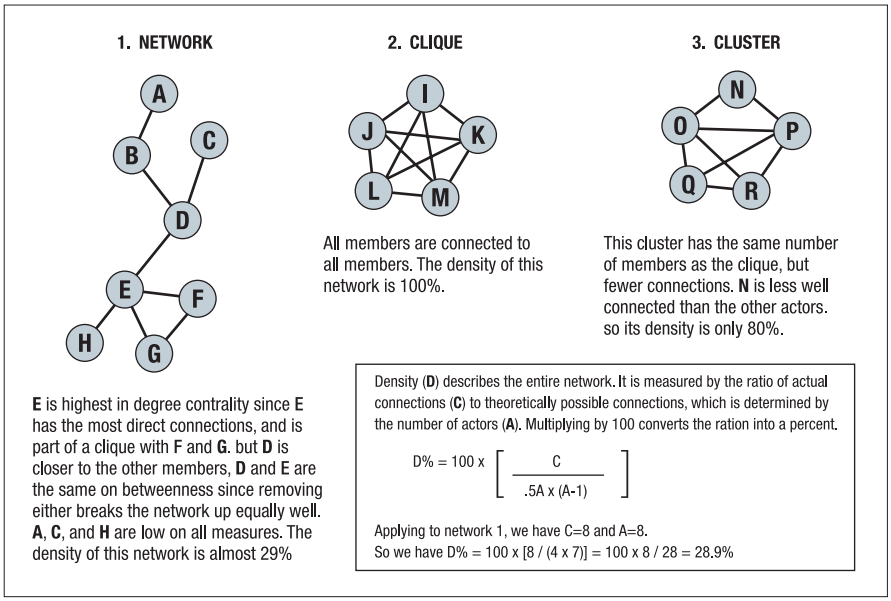
This seemingly simple information illustrated why particular geographic areas were experiencing high levels of violence. It also revealed which street gangs were most connected within the network and which therefore merited an intervention focus. Finally, it helped to anticipate consequences of interventions by highlighting rival gangs that might attempt to take advantage of law enforcement focus on a particular street gang.

READ MORE:

F.A.J. Ianni, and E. Reuss-Ianni. 1990. "Network Analysis." In *Criminal Intelligence Analysis,* ed. Paul Andrews and Marilyn Peterson, 67–84. Loomis, California: Palmer Enterprises.

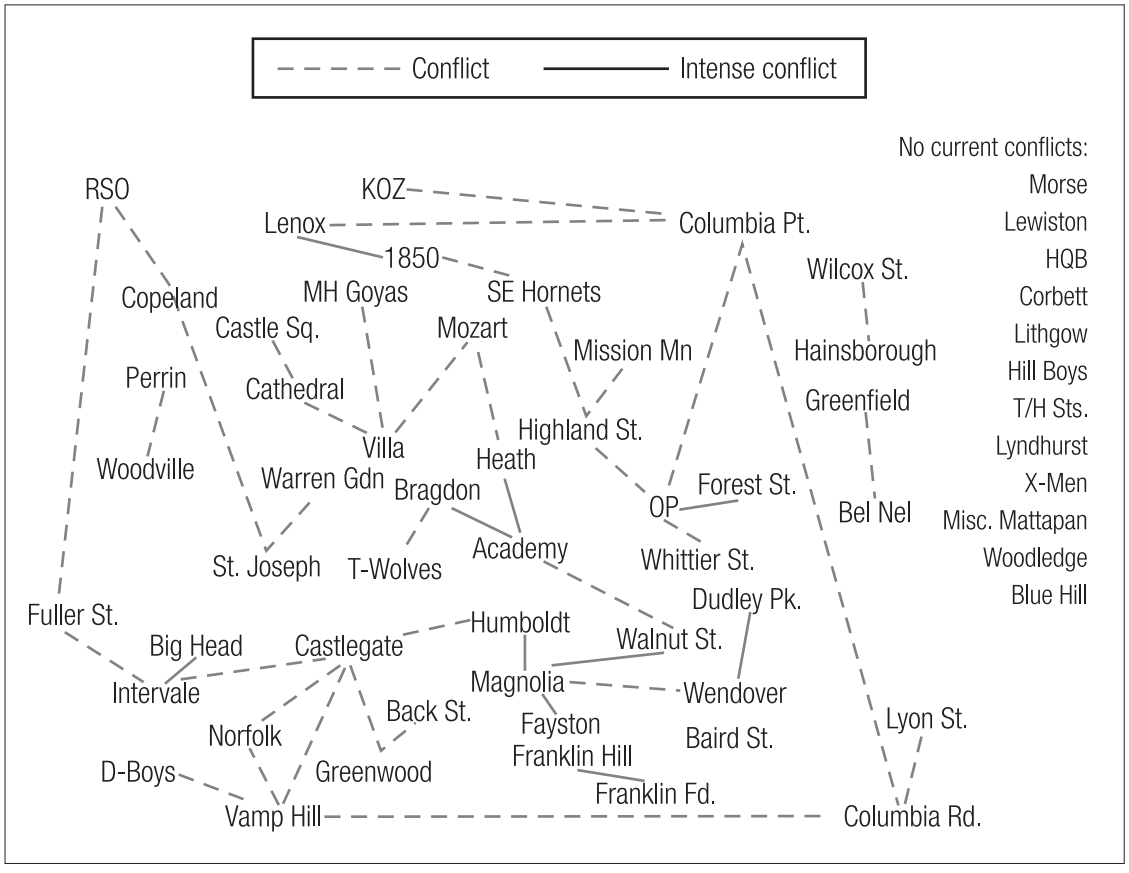
David Kennedy, Anthony Braga, and Anne Morrison Piehl. 1997. "The (Un)Known Universe: Mapping Gangs and Gang Violence in Boston." In *Crime Mapping and Crime Prevention,* ed. D. Weisburd and T. McEwen, 219–262. Monsey, New York: Criminal Justice Press.

Figure 10. Density and other measures of networks



Source: Ianni and Reuss-Ianni 1990.

Figure 11. Gang conflict network



Source: Kennedy, Braga, and Piehl 1997.

20 UNDERTAKE CONVERSATIONAL ANALYSIS OF WIRE TAP DATA

CONVERSATIONAL ANALYSIS IS USED TO INVESTIGATE CRIMINAL NETWORKS AND PROSECUTE CRIMINAL CASES. It involves compiling and reviewing telephone conversations between two or more people in a criminal conspiracy. It reveals relationships between these people, the key players in crimes, and each member's role in the network.

Procedures

Conversational analysis has three main stages: (1) collecting and transforming the data; (2) analyzing the data; and (3) reporting findings.

In more complex investigations you might find it helpful to analyze the conversations using an Ask Sam or Folio Views—hypertext software programs that allow for storing, sorting, retrieving, and analyzing textual data (see Mangai Natarajan's study described below). In other cases, it can be helpful to produce a written transcript to aid in the detailed analysis of conversations: looking at what is said, and what is merely implied but left unsaid. There are two types of analysis for this situation.

Micro analysis

This consists of two forms of analysis, phonological analysis and syntactic analysis.

Phonological Analysis examines the sounds used by those speaking and is necessary when recordings are not clear—for example, if you have to clarify whether someone said "I wouldn't take a bribe, would you?" or "I would take a bribe, wouldn't you?"

Syntactic Analysis examines sentence structure and helps to clarify grammatical relationships. For example, when a speaker says "I want you to do it," the 'you' maybe ambiguous, since it can refer to the other party involved in that part of the conversation, or it might include other people as well. When someone says "I want *you* to do it" he is most likely referring to the primary respondent in the conversation.

Discourse analysis

Discourse analysis is used to analyze the linguistic aspects of conversations. It comprises a variety of sub-analyses.

Topic Analysis seeks to identify who introduces which topics and whether or not the topics are recycled or reintroduced later in the conversation. This information is useful when establishing the speaker's intentions. Topic analysis is also used to establish conversational dominance. For example, when one person introduces 80 percent of the topics in a conversation, this is indicative of an asymmetrical relationship between the participants, and signifies the person is a leader, or an instigator who is trying to get others to do his will.

Project Caviar

The Caviar network was a criminal enterprise engaged in international drug trafficking. Police in Canada, Europe, and South America ran a two-year investigation that led to the dismantling of hashish and cocaine distribution chains spanning these countries. The primary data submitted as evidence in the trials of 22 members of the network was electronically monitored telephone conversations. These were used to identify primary participants and determine how deeply each person was involved in the trafficking operations.

Response Analysis involves examining the responses to topics introduced by others. Topic response options listed below summarize the most common strategies used by listeners when they have been introduced to a topic. They may:

1. Resolve the topic
2. Resolve part of topic
3. Request clarification or amplification of topic
4. Provide off-topic responses
5. Change or redirect the topic
6. Provide vague, ambiguous, or no response
7. Provide clarification that denies or changes the premise of the topic
8. Deny the topic's premise

For example, if the respondent in the conversation says 'uh-huh,' he is not carefully agreeing to whatever has been introduced. Or when a person does not respond, it generally indicates negativity.

Topic-flow analysis organizes topics sequentially, noting the conversational movement among speakers, and marking the success or failure of the speakers in their efforts to achieve their goals. Topics of discussion are generally put into three categories: substantive topics (the goal of the conversation), corollary topics (ways of achieving or arriving at the substantive topics), and transitional topics (formulaic aspects of a conversation, such as greetings and in-between 'small talk' that often provides psychological breaks from the heavier conversation).

Language function analysis identifies functions of the words used. For example, speakers promise, deny, report facts, complain, give opinions, advise, order, and thank, and they use different linguistic tools to achieve these functions—i.e., using language to get things done.

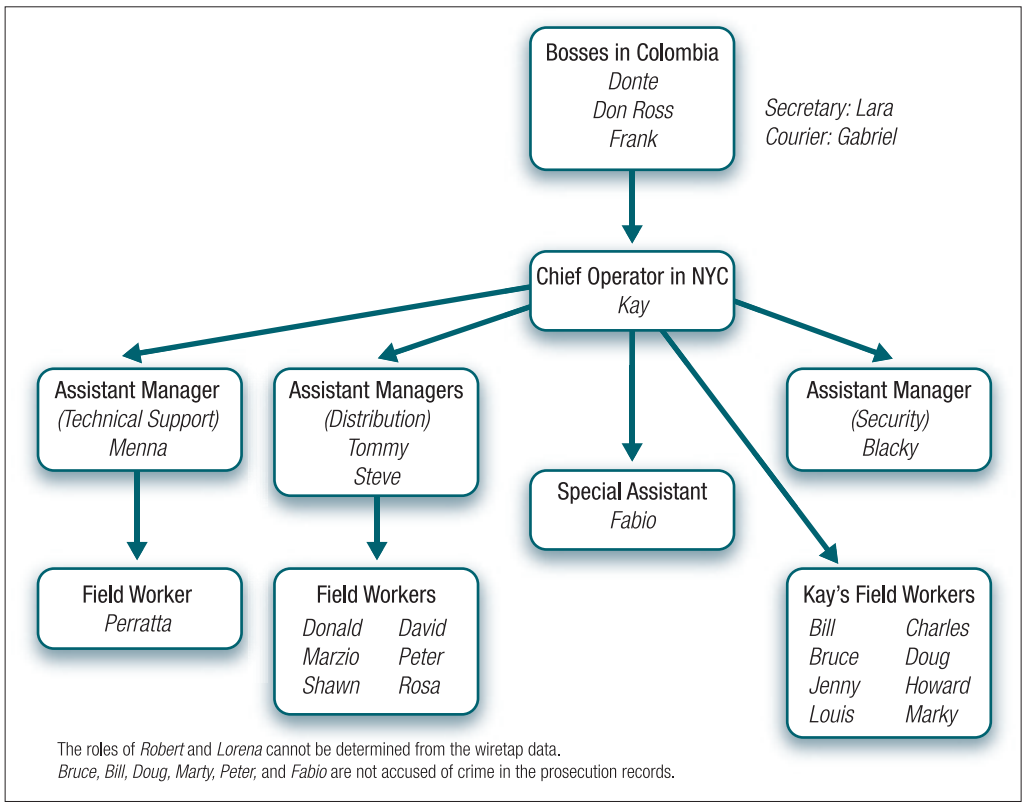
Contrastive analysis compares phrases used in the conversation analyzed—for example, in an investigative report compiled by police officers. Officers commonly paraphrase the suspect's words so that quite a different message is conveyed from what was actually said. Contrastive analysis will, therefore, allow you to compare and contrast these distinctly different sources of data pertaining to the same people.

Uncovering a drug trafficking organization in New York

Mangai Natarajan of John Jay College of Criminal Justice conducted an analysis in 2000 of wiretap records and other prosecution materials to uncover the structure of a large drug trafficking organization in New York City. She sought to determine the roles and status of the individuals within the organization and to chart the hierarchy among its members. She scanned 600 pages of transcripts of 151 telephone conversations, ranging in duration from 2 to 10 minutes, into "Folio Views." Her analysis consisted of five distinct stages:

1. *Conversational count by individuals.* This yielded a count of the number of conversations each individual was involved in, as well the number of other people with whom he or she had telephone contact.
2. *Status analysis.* This involved the use of a coding guide to determine the relative status of individuals. The guide was used to distinguish between people of higher and lower status, and included such indicators as requesting information, expressing satisfaction, providing information, giving orders, clarifying orders, and use of 'sir.'
3. *Task analysis.* This involved identifying the major tasks performed by each individual by inspecting the content of the conversations. The individuals were identified as bosses, assistant managers, field workers reporting to the assistant managers, and field workers reporting to the chief operator.
4. *Network analysis.* This involved establishing links between individuals (Step 19).
5. *The organizational chart.* This involved developing an organizational chart by using the information obtained from stages 1-4. This is shown in Figure 12 on page 58.

Figure 12. Structure of the drug trafficking organization according to wiretap database



Source: Natarajan 2000.

READ MORE:

Roger Shuy. 1990. "The Analysis of Tape Recorded Conversations." In *Criminal Intelligence Analysis,* ed. Paul Andrews and Marilyn Peterson, 117–147. Loomis, California: Palmer Enterprises.

Mangai Natarajan. 2000. "Understanding the Structure of a Drug Trafficking Organization: A Conversational Analysis." In *Illegal Drug Markets: From Research to Prevention Policy,* ed. Mangai Natarajan and Mike Hough, 273–298. Monsey, New York: Criminal Justice Press.

21 COMPARE COMPETING HYPOTHESES

UNFORTUNATELY, YOUR BEST INTELLIGENCE INFORMATION IS ALWAYS INCOMPLETE, often riddled with errors, sometimes contradictory, and typically ambiguous. This is mostly because you are trying to predict the behaviors of people who are trying to conceal their actions from the police. If your best efforts have a high chance of being wrong, how can you improve your intelligence information?

The answer is to consider alternatives and systematically compare these alternatives. Morgan Jones describes an eight-stage approach, developed by the CIA, called Analysis of Competing Hypotheses (ACH). We will follow his description here.

Stage 1: Generate hypotheses. Typically, there is more than one way to interpret data. So it is better to package the information produced from the data as a set of competing hypotheses: a range of plausible alternative interpretations of the data. Sometimes a single analyst can imagine multiple interpretations. But it is often useful to have several people consider the data and come up with alternatives.

Stage 2: Construct a matrix for comparing the hypotheses. Examples are given in Tables 9, 10, and 11. While you can examine any number of hypotheses, it may be more practical to restrict consideration to the most plausible ones, or to the most contrasting ones (that is, minor variations of the same basic hypotheses are lumped together).

Stage 3: List evidence along the left side. Evidence comes from the data already collected. Focus only on significant evidence, rather than many minor details that could be distracting and irrelevant. Also, if the absence of information is important, then this too, is evidence. This will be particularly significant if a hypothesis asserts that certain information should be available, but it cannot be found. Also ask, "What evidence not in the matrix would overturn the hypothesis, if it were available?" Looking for this evidence can help evaluate these hypotheses.

Stage 4: Test evidence for consistency with each hypothesis. Once you list all the evidence, work across (row by row) and determine if each piece of evidence is consistent with each hypothesis. If the evidence is consistent with a hypothesis, put a **C** in the cell for the hypothesis. If it is inconsistent, put an **I** in the cell. And enter **?** in the cell if it is unclear whether the evidence is consistent or inconsistent with a hypothesis. If you wish, you can give degrees of consistency or inconsistency using numbers, symbols, or colors.

Stage 5: Refine the matrix. You may find new hypotheses that had not been considered. These should be added. New evidence may be uncovered and this should be added. Block out any piece of evidence that is consistent with all hypotheses (as is the case with evidence one in Table 10: Matrix 2). Evidence that is consistent with all hypotheses cannot help you determine which hypotheses are the most likely to be true. Do not discard this evidence, as it may turn out to be useful later.

Stage 6: Evaluate each hypothesis. Now, work down and consider each hypothesis separately. Block out any hypothesis for which there is considerable inconsistent evidence. Before making a final decision, consider the quality of the evidence involved. In Table 11: Matrix 3, we have blocked out hypotheses **A** and **C** because three of the four relevant pieces of evidence are inconsistent with them.

Table 9. Matrix 1

MATRIX 1: Testing each piece of evidence for consistency				
	Hypotheses			
Evidence	A	B	C	D
1.	C	C	C	C
2.	I	C	I	C
3.	I	?	I	I
4.	I	C	C	C
5.	I	C	I	I

Based on Morgan 1998

Stage 7: Rank the remaining hypotheses. The hypothesis that is rated the highest has the *least inconsistent evidence*. Hypothesis **B** appears superior to hypothesis **D** in Matrix 3, because it has no inconsistent evidence, though one piece of evidence is ambiguous. Because the data on which the evidence is built can be subject to alternative interpretations, different analysts may have different interpretations. The advantage of the ACH process is that it forces everyone involved to look at all the hypotheses and evidence systematically. It can eliminate the hypotheses that are least likely and narrow the discussion to a few hypotheses. If, at this step, you determine that specific types of data could break the deadlock, then commission additional data collection. When new evidence is available, go back to step 5 and compare the remaining hypotheses with the old and new evidence.

Stage 8: Perform a sanity check. Morgan advocates reviewing the findings to make sure no mistakes were made and that those involved are comfortable with the decision.

Table 10. Matrix 2

MATRIX 2: Eliminating evidence consistent with all hypotheses				
	Hypotheses			
Evidence	A	B	C	D
1.	C	C	C	C
2.	C	C	I	C
3.	I	?	I	I
4.	I	C	C	C
5.	I	C	I	I

Based on Morgan 1998

Table 11. Matrix 3

MATRIX 2: Eliminating evidence consistent with all hypotheses				
	Hypotheses			
Evidence	A	B	C	D
1.	C	C	C	C
2.	C	C	I	C
3.	I	?	I	I
4.	I	C	C	C
5.	I	C	I	I

Based on Morgan 1998

Though you can conduct the ACH process with paper and pencil, the Palo Alto Research Center (PARC) has developed a simple and free downloadable software program. The PARC software has several additional features. It allows you to describe the type of evidence, rate the credibility of the evidence, and rate the relevance of the evidence. It also allows you to give a score to the evidence for each hypothesis and come up with a numerical score for each hypothesis. Finally, though the PARC software has somewhat different steps, the underlying logic is the same as the steps described here.

It is important to remember that ACH relies on the logic of refutation rather than support. In other words, *ACH systematically eliminates the worst hypotheses* (those which are the least consistent with the evidence). In this way it narrows the field of plausible hypotheses. It does not prove a hypothesis is true. The hypotheses remaining are the least inconsistent; least bad.

Though ACH cannot assure that intelligence information is always correct, by forcing a systematic rigorous approach to using data it reduces the chances of error.

READ MORE:

Morgan Jones. 1998. *The Thinker's Tool Kit: 14 Powerful Techniques for Problem Solving.* New York: Three Rivers Press.

Palo Alto Research Center. 2006. *$ACH_{2.0.3}$ Download Page—Analysis of Competing Hypotheses.* www2.parc.com/istl/projects/ach/ach.html.

Michael Townsley, Monique Mann, and Kristian Garrett. 2011. The Missing Link of Crime Analysis: A Systematic Approach to Testing Competing Hypotheses. *Policing* 5(2): 158–171.

22 FIND WAYS TO SHARE VITAL INFORMATION WITH OTHER JURISDICTIONS

RIGHT AT THE BEGINNING OF THIS MANUAL, WE MENTIONED THAT THE 9/11 COMMISSION CRITICIZED INTELLIGENCE agencies for failing to "connect the dots" and that this criticism focused attention on the need to find ways of sharing critical information. As former CIA director, R. James Woolsey, noted in testimony to Congress, "the flow of information sharing is likely to be more from localities to Washington, rather than the other way around." The fact that local police came face-to-face with three of the 9/11 hijackers in traffic stops before the attack is often cited as an example of an opportunity that was lost because an integrated information sharing system was not in place.

We are still struggling with the difficulties of putting such a system in place. The regional Joint Terrorism Task Forces established by the FBI throughout the country before 9/11, represent one attempt to find a solution to this problem. Fusion in many states represents another information-sharing initiative. Information from multiple jurisdictions is pooled and made available to participating police. A center's mission can be limited to antiterrorism, but it often includes other significant crimes, such as insurance fraud, money laundering, and armed robbery. Therefore, these fusion centers can serve as a valuable resource for your department.

Joint Terrorism Task Forces

There are now more than 100 JTTFs throughout the country, including the 56 FBI field offices. Their mission is to coordinate federal, state, and local law enforcement efforts to detect, prevent, and respond to terrorist attacks. Primarily investigative and analytic agencies, JTTF are staffed by FBI investigators, agents from federal agencies—such as the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) and the Bureau of Immigration and Customs Enforcement (ICE)—and detectives from local police and sheriff's departments. Several successes have been credited to the JTTF, including the arrest and conviction of the terrorists who mounted the first attack on the World Trade Center in 1993 and of the so-called shoe bomber, Richard Reid.

Impediments to information sharing

In Step 15 we discussed some of the impediments to sharing information among the personnel of a single police department. Here we list six important impediments to sharing information among different departments and jurisdictions:

1. There are more than 17,000 state and local law enforcement agencies in the United States, very few of which have staff trained in a common intelligence curriculum and technology to collate, analyze, and exploit raw intelligence data. Even within the same force, there might be little interconnectivity among existing computer systems.
2. Secrecy is the stock-in-trade of intelligence agencies; historically, protecting sources and preventing leaks has been of great importance. This is why the need-to-know doctrine drives policy on information sharing. Unfortunately, in practice this doctrine inhibits information sharing and, therefore, inhibits new insights that sometimes occur when new eyes examine old information.
3. Particularly in the early stages of an inquiry, it is likely that investigators will guard their information jealously. There are two reasons for this:
   a. Investigators may be wary of leaks that would jeopardize the investigation. They may know that officers in other forces might benefit from the information, but who might also treat it carelessly or misuse it. Consequently, they might not share information when they should have done.

   b. Investigators (understandably) wish to reap the kudos that will result from successfully apprehending the criminals they have been investigating. Sharing the information with some other enforcement agency, particularly one higher in prestige, could result in that agency taking over the investigation, making the arrests, and gaining all the glory.

4. Some crimes, such as terrorism, are rare and it is hard for people to remain vigilant when nothing seems to be happening, and hard to maintain the morale of those doing the watching. Added to this is that useless information is vastly more common than information that is useful. While we often hear stories of intelligence successes, resulting from tips received or surveillance undertaken, we do not hear about the work that leads nowhere. This lack of success can result in a "why bother" attitude and a reluctance to expend the effort needed in pursuing investigations. It also can mean that investigators are reluctant to lose face by sharing information that could prove to be useless.

5. The essence of prevention is stopping something from happening. It can be hard to demonstrate that such efforts have been successful when the agency that collects the relevant information is not the agency that takes the action to prevent the thing from happening. Once again, this fact works against the intelligence function and more specifically against the sharing of information.

6. Finally, there is much misunderstanding of laws and regulations governing the sharing of intelligence. In discussions on this topic someone is sure to bring up 28 C.F.R. Part 23, which only applies to federally-funded multi-jurisdictional intelligence systems, and even then only has very general rules about data access and storage. Many police and analysts seem to think that it prohibits them from sharing data or requires them to do certain things it does not actually require. So try to clarify legal/regulatory impediments that do and do not apply in your particular case.

What, then, should you do to promote information sharing? There are two principles that should guide your approach:

1. Identify key individuals within in or near your jurisdiction, who could be a continuing source of useful information, and cultivate a relationship with them so that they get to know and trust you.

2. When a dealing with a specific problem (for example, one of a criminal motorcycle gang or a pedophile ring) you should identify specific stakeholders with a direct interest in reducing the problem, who would be likely to help you with your investigation.

READ MORE:

Graeme Newman and Ronald Clarke. 2008. *Policing Terrorism: An Executive's Guide.* Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

23 DIAGRAM THE CRIME PROCESS

OFFENDING IS NOT AN INSTANTANEOUS EVENT THAT OCCURS WITHOUT A PAST OR A FUTURE. It is a process that offenders must complete for their crime to be successful. This step and the following one will show you how to diagram such processes so you can disrupt them.

Follow a four-stage procedure for linking the process that offender groups follow in committing crimes to a set of interventions designed to thwart the group's abilities.

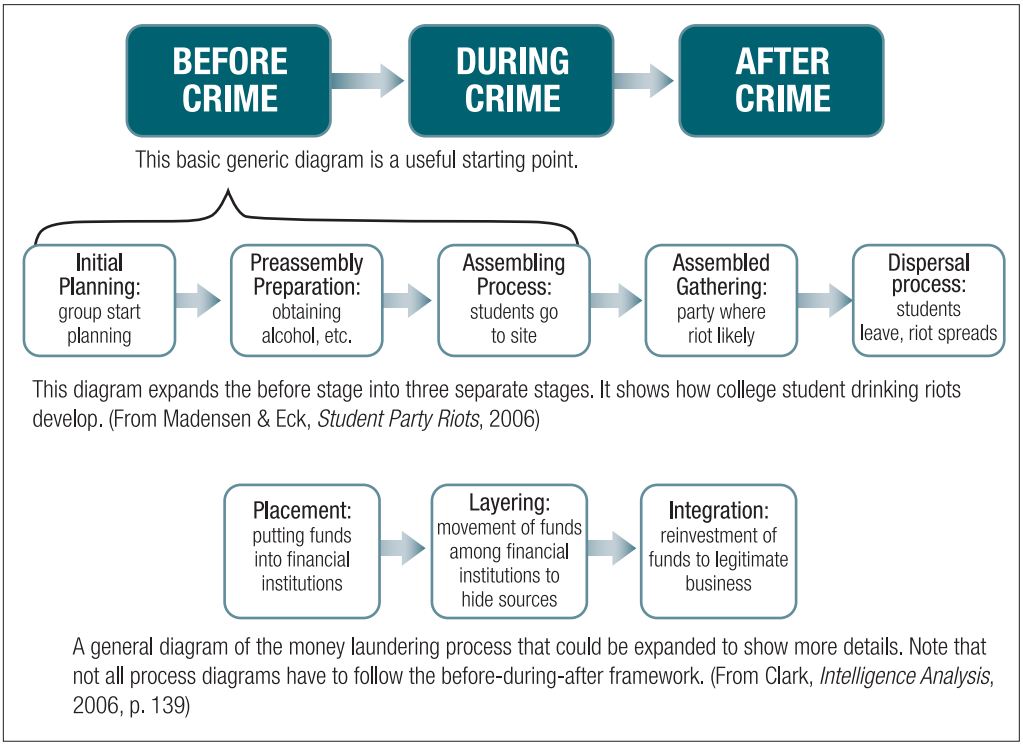
1. Describe the process offenders follow to commit crimes.
2. Add other actors and describe their actions that facilitate the crime.
3. Develop possible prevention interventions at each process stage, for each actor.
4. Select a comprehensive set of actions from these possible actions.

Describe the process

The simplest crime process diagram has three stages that describe what the offenders do before they can commit a crime, during the commission, and afterwards (top row in Figure 13). All preparatory actions, such as finding crime targets, planning, finding weapons and other tools, organizing confederates, and so forth, are in the before stage. In the during stage are all the actions the offenders must take while directly carrying out the crime, including overwhelming victims, gaining access to the site, providing security, and securing valuables. The last stage includes activities such as escaping, disposing of stolen items, threatening witnesses, and laundering money.

Any of the stages can be divided into multiple sub-stages to show the process in greater detail (see second row of Figure 13, and for more detail see Step 11).

Figure 13. Crime process diagrams



This basic generic diagram is a useful starting point.

This diagram expands the before stage into three separate stages. It shows how college student drinking riots develop. (From Madensen & Eck, *Student Party Riots*, 2006)

A general diagram of the money laundering process that could be expanded to show more details. Note that not all process diagrams have to follow the before-during-after framework. (From Clark, *Intelligence Analysis*, 2006, p. 139)

Table 12. Adding details to the model

INTELLIGENCE SUMMARY GRID				
	ACTORS			
WHEN	Group A	Group B	Targets	Place managers
Long Before				What place managers are doing at this stage
Just Before		What this group is doing at this stage		
During	What this group is doing at this stage			
After			What targets are doing at this stage	
Comments:				
In this example, there are two interacting offender groups, their crime targets, and people who own or manage locations critical for the crime. Other combinations of actors are possible, as are different stages of the process. In each cell, describe what the actor is doing at that stage, based on intelligence. For groups, describe what they do to carry off the crime successfully. For targets, describe what they do, or fail to do, to protect themselves. If a cell is empty there is a lack of data.				

The before-during-after framework is useful, but it does not fit all crimes. Money laundering, for example, follows a different process. The model of money laundering in the bottom of the figure is very general. A model for a specific money laundering operation would describe sub-stages within each major stage.

If the offender group has several ways to commit the crime, then you should create multiple models: one for each way.

Add other actors

Since all crimes involve actors other than offenders, a comprehensive process model should account for their actions, too. In Step 7 we introduced the various actors we should be concerned with: offenders, handlers, targets, guardians, and place managers. During the before stage, what are potential victims doing that the offenders can take advantage of? What is being done by the owners and managers of places where the crimes occur? At the during stage, what are all the actors doing? And afterwards, what are all the relevant actors doing?

Table 12 shows how this additional data can be included. The relevant actors depend on the crime problem, as does the number of stages. Empty cells indicate where there is too little intelligence data to determine what a particular actor is doing. If understanding what is going on at this stage is important, then you need to focus data gathering on this cell.

Develop possible interventions

Table 13 on page 65 describes possible prevention actions associated with the actors and stage. Ideally, every cell in the grid would have multiple possible actions. But some cells will be blank indicating that you cannot identify a good preventive action due to a lack of information.

Table 13. Developing responses

INTELLIGENCE SUMMARY GRID				
WHEN	ACTORS			
	Group A	Group B	Targets	Place managers
Long Before	Preventive actions			Preventive actions
Just Before		Preventive actions		
During			Preventive actions	
After	Preventive actions			
Comments:				
In each cell create a list of actions involving that actor who could disrupt the crime process at that stage. Ideally, the entire grid would be filled, but this requires intelligence for each cell. Blank cells indicate where no prevention will be implemented because of lack of intelligence. Once a comprehensive list of actions has been developed, select the combination of actions most likely to be implemented and most likely to have an impact on the problem.				

Select a set of interventions

Having created a list of possible prevention actions, organized by actor and stage, it is time to select the combination of actions that are most productive. The characteristics of a good set of interventions can be described by the acronym EAGLE. The parts are:

- Effective
- Acceptable to the community
- Go well together
- Legal
- Expected to be implemented

To create a comprehensive set of prevention actions; 1) address each stage of the process, and 2) address at least two actors at each stage. This provides a layered attack on the offender group's capabilities that has built-in redundancy. Should some actions fail, or should the offender group attempt to thwart the prevention, other parts of the plan can take up the slack.

READ MORE:

Derek Cornish. 1994. "The Procedural Analysis of Offending and its Relevance for Situational Prevention." Vol. 3 of *Crime Prevention Studies*. Monsey, New York: Criminal Justice Press.

24 APPLY SITUATIONAL PREVENTION TO EACH STAGE OF THE CRIME

COMPLETELY REMOVING THE OFFENDER GROUP MAYBE DESIRABLE, BUT NOT BE POSSIBLE because of offender replacement (Step 13). If members of the group are arrested, new members may replace them. Or new groups can spring up to continue the offending. This is often the case with violent street groups and retail drug dealing organizations. It is also the case with large-scale international criminal organizations. Another circumstance under which removal strategies may be inadequate occurs when removal can provoke violence. Consequently, you need to use other approaches that are complementary with a removal strategy but help thwart replacement and violent competition.

Situational Crime Prevention can be very useful for influencing offender behavior, particularly when offender removal is difficult, replacement is likely, or removal creates additional violence. As we described in Step 6, offenders make choices based on the local context of crime opportunities; they exploit the environment, taking advantage of circumstances that encourage crime. Recall ESEER: if crime is easy, safe, excusable, enticing, and rewarding there will be more crime. Situational Crime Prevention changes the incentives. It alters the social and physical context of crime to make crime harder or riskier, or by removing rewards, excuses, and provocations.

Because different crimes are encouraged by different features of the environment, you need to analyze local circumstances to determine exactly how to influence offenders. To aid the selection of appropriate interventions, a classification of 25 situational techniques has been developed, which is reproduced in Figure 14. We will briefly summarize the 25 techniques below.

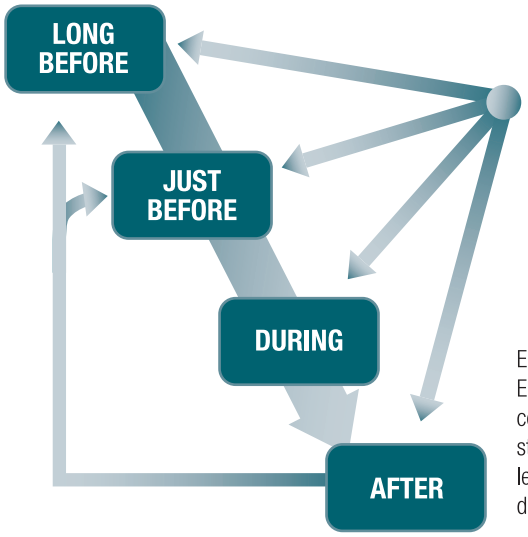
Increase the Effort. Target hardening involves securing targets. Access control makes it difficult for the offender to get to the target. Exit screening makes it difficult to escape with the target, or from the target site. Deflection (for example, through street closures) steers offenders away from targets. Controlling tools makes the crime harder by denying critical resources (e.g., explosive materials) to the offender group.

Figure 14. 25 Techniques of situational crime prevention

Increase EFFORT	Increase RISK	Reduce REWARDS	Reduce EXCUSES	Reduce PROVOCATIONS
Harden targets	Extend guardianship	Conceal targets	Set rules	Reduce frustration and stress
Control access	Assist natural surveillance	Remove targets	Post instructions	Avoid disputes
Screen exits	Reduce anonymity	Identify property	Alert conscience	Reduce arousal and temptation
Deflect offenders	Engage place management	Disrupt markets	Assist compliance	Neutralize peer pressure
Control tools/ weapons	Strengthen formal surveillance	Deny benefits	Control drugs and alcohol	Discourage imitation

Source: R.V. Clarke. 2008. "Situational Crime Prevention." In *Environmental Criminology and Crime Analysis*, ed. Wortley and Mazerolle. Cullompton, UK: Willan.

Figure 15. Applying situational prevention to the entire crime process



Increase EFFORT	Increase RISK	REWARDS	Reduce EXCUSES	Reduce PROVOCATIONS
Harden targets	Extend guardianship	Conceal targets	Set rules	Reduce frustration and stress
Control access	Assist natural surveillance	Remove targets	Post instructions	Avoid disputes
Screen exits	Reduce anonymity	Identify property	Alert conscience	Reduce arousal and temptation
Deflect offenders	Engage place management	Disrupt markets	Assist compliance	Neutralize peer pressure
Control tools/ weapons	Strengthen formal surveillance	Deny benefits	Control drugs and alcohol	Discourage imitation

Each stage in a crime process involves decisions. Each of these can, in principle, be influenced by consideration of offender incentives. The AFTER stage can be particularly important if offenders learn (i.e., outcomes of one crime influence decisions in the next).

Increase the Risks. Extending guardianship involves having citizens do more to protect each other. Assisting natural surveillance is related to this; it makes it easier for citizens to watch an area. Reducing anonymity reduces the ability of offenders to hide by being unknown. Place management involves a wide variety of practices to engage owners of locations in prevention. Formal surveillance employs dedicated security personnel or electronic monitoring.

Reduce Rewards. Concealing targets attempts to hide them from offenders. Removing targets takes this a step further and takes the targets away completely. Property identification involves marking targets so they have less value at resale. Disrupting markets also makes it difficult to sell stolen merchandise or illegal substances and services. Finally, denying benefits entails taking the value out of the behavior (for example by using ink tags in clothing stores that spoil stolen items).

Remove Excuses. Rule setting removes ambiguity for misbehavior and allows early intervention. Posting instructions serves as a reminder about rules. Awakening conscience appeals to offenders' sense of justice. Assisting compliance makes good behavior more likely. Finally, controls on drugs and alcohol make it harder to overcome inhibitions about committing crime.

Reduce Provocations. Reducing frustration and stress makes it harder for offenders to justify their actions. Avoiding disputes keeps conflicts from arising or getting out of hand. Curtailing emotional arousal also reduces temptations to offend. Neutralizing peer pressure keeps offenders from encouraging each other to commit crimes. Discouraging imitation limits information to offenders so they are less likely to copy criminal behaviors of others.

Some techniques may work better together than separately. Thus, rule setting is typically accompanied by posted instructions that serve as veiled threats to an offender. And rules that require people to reveal their identities both removes anonymity and increases the offenders' perceived risk. No technique works in all circumstances for all crimes. Thus, rule setting and instructions alone may be of little importance to a determined offender, but they may deter the more casual, opportunistic offenders. However, all the techniques have an important role in controlling particular crimes in some circumstances.

As we have discussed, intelligence data can be used to determine the process that the offender group uses to exploit crime opportunities. At each stage of the process a situational analysis should be conducted to determine the best ways to keep the group from successfully executing that part of the process. This is illustrated in Figure 15. While it is obvious that curtailing early stages of the process can prevent the group from committing crimes, it is less obvious why

dealing with the final stage is productive. The reason is that it is this stage when the group gets its reward. Whether it is the sales of stolen goods, an enhanced reputation for a killing, or publicity for a terrorist attack, most rewards come at the end. Situational interventions at this stage can substantially reduce the incentive for further crime.

A comprehensive strategy for preventing a group from producing crimes will contain a set of actions at each stage of the group's crime process. While planning a strategy for preventing the group's activities you should describe the situational techniques used at each stage of the process. To provide assurance that the overall strategy will be effective, it is useful to employ at least two different types of techniques (e.g., increasing risks and reducing rewards, or removing excuses and increasing effort) at each stage.

READ MORE:

Ronald Clarke. 2008. "Situational Crime Prevention." In *Environmental Criminology and Crime Analysis,* ed. Richard Wortley and Lorraine Mazerolle. Cullompton, Devon: Willan Publishing.

Marcus Felson and Ronald Clarke. 1998. *Opportunity Makes the Thief.* Police Research Series. Paper 98. London: Home Office

25 WORK WITH GATHERINGS AND CROWDS

IN STEP 17, WE DISCUSSED THE IMPORTANT ROLE THAT COMMUNITY MEMBERS PLAY IN ADDRESSING CRIME. This is particularly true when dealing with large gatherings of individuals, though many of these gatherings are not serious problems for the police. Special events, large block parties, celebrations, and daily commuter crowds typically need the police only to provide traffic regulation, offer directions to citizens, and ensure security against minor crimes. However, demonstrations to protest government policy, to push social or economic agendas, to voice opposition to other political or cultural positions, or to take stands against corporate practices may require active police intelligence analysis before, during, and after the events.

Covert gathering of data about the organizers of the gathering, their intentions, and their plans is tempting, but highly risky because it puts personal liberty in jeopardy. Once revealed, or even suspected, covert gathering of data can undermine the public support for the police.

When dealing with gatherings, intelligence analysis must be considered within an overall police strategy for facilitating individuals' abilities to make their opinions known and carry out constitutionally protected actions, while at the same time preventing violence and other harmful behaviors. Spying on individuals to determine who holds what legitimate beliefs and belongs to what legitimate organization is not permissible in most western democracies. Identifying violent individuals, or individuals who facilitate violence, is a legitimate police activity. The boundary between these two actions is grey, and keeping police actions to the correct side of this boundary is often difficult.

One way to keep police away from this boundary is to get the participants in the gathering to keep order, ostracize troublemakers, and not obstruct focused police actions to remove troublemakers. This may be difficult, but is often easier than imagined because of some basic characteristics of gatherings and crowds, including:

- **Individuals in crowds are rational.** Individuals do not surrender their rationality when in crowds nor do they lose their capacity to make decisions.
- **Large gatherings are diverse.** They contain people with many different perspectives and intentions.
    1. In most cases, only a tiny fraction is seeking to create trouble. This group will use the larger gathering for their purposes and may attempt to provoke the police into taking forceful actions against the larger gathering, and thus gain the support of the other members of the gathering.
    2. Another slightly larger fraction may be willing to facilitate the troublemaking, or join in once it is started. But they are unlikely to act unless the first group provokes the police to over-react.
    3. A much larger proportion of the gathering will stand-by, either confused or puzzled, but if seriously provoked may provide tacit support for the first two groups.
    4. The greatest number of participants in the gathering will try to distance themselves from the troublemakers by leaving the scene once trouble starts.
- **People in gatherings have limited information.** They often know little about what is going on around them. Even with a cell phone and text messages, a person in the middle of a gathering is unlikely to know what is going on at the edges, and those at the head of a march will know little about what is going on at the tail.

Table 14. Dialogue policing before, during, and after a demonstration

BEFORE	DURING	AFTER
Ensure police statements to the media build trust with demonstrators	Check that agreements are kept and facilitate new agreements	Avoid potentially provocative statements in media by the police
Create agreements between demonstration organizers and police	Establish active communication links between police and demonstration organizers	Get feedback on police operations from demonstration organizers
Exchange information between police commanders and demonstration organizers	Prevent hazardous incidents or reduce their seriousness	Explain police actions during the demonstration to demonstrators
Create scenarios for the commander	Read mood in crowds and among police	Give feedback to police on behavior of demonstrators
Involve and inform third parties affected by the demonstration	Inform third parties affected by the demonstration	Exchange information with third parties affected by the demonstration

Adapted from: Holgersson and Knutsson 2010

- **People in gatherings influence each other.** Probably the most important influences on members of a gathering are the people in their immediate vicinity. These are often people who accompany them to the gathering, or who they knew before the gathering.
- **Crowd members and police influence each other.** You cannot understand what the crowd will do without considering what the police will do. And much bad behavior by individuals in crowds is in reaction to police actions, and vice versa. When things go very wrong, it is often because some police and some crowd members co-produced disorder.

To the maximum extent possible, police should facilitate legitimate goals of the gathering. This requires building trust with the leaders of the gathering so their help can be enlisted in policing the gathering. Explaining police actions before, during, and after the gathering is critical. So is having an agreed on plan for the event. Also, because few plans can be implemented without changes, there needs to be a way for police and members of the gathering to communicate.

Overt and bidirectional intelligence is important. The Swedish Police have developed a strategy involving "dialogue policing." Trained officers, dressed in civilian clothes, but clearly identified as police officers, work directly with leaders of the gathering. They pass information about the leaders' intents and concerns to the police commander, and the commander's concerns and intent back to the leaders. They do not spy on individuals in the crowd or report specific illegal behavior—that is the job of others in the police. They seek to dispel rumors and provide a way for the police to negotiate with the gathering's leaders, thereby reducing the anxiety of both the police and members of the gathering. If the police need to take forceful action against specific individuals or a small group, the dialogue officer can explain what is taking place and why.

Dialogue policing is an overall strategy of negotiation and discussion that begins at the earliest stages of planning the gathering (see Table 14). In this context the police can learn a great deal about the gathering without resorting to covert actions.

The dialogue officers are not the only way that information is communicated to the gathering by the police, or that the police gather information about the crowd. Throughout the gathering, police assess the mood of the crowd and modify their actions accordingly. Many of their actions are intended to remove excuses for misbehavior, and to not provoke. At the same time police communicate a specific risk to the few individuals who may be intent on violence, and deny them the rewards of being supported by the vast majority of the crowd. By socially separating those intent on violence from the rest of the crowd, the police make it harder for them to use violence to gain their objectives.

READ MORE:

Stefan Holgersson and Johannes Knutsson. 2010. "Dialogue Policing—A Means for Less Crowd Violence?" In *Preventing Crowd Violence,* ed. Johannes Knutsson and Tamara Madensen, 191–216. Boulder, Colorado: Lynne Rienner Publishers.

26 PULL LEVERS

IDENTIFYING HIGHLY ACTIVE OFFENDERS AND THEN GIVING THEM A DIRECT CREDIBLE THREAT OF LEGAL SANCTIONS can substantially reduce their offending. However, offenders working in a group are more difficult to influence because the group's members can exert strong counter pressure. David Kennedy pioneered a three-pronged approach to reducing group violence, called "Pulling Levers," that not only overcomes this group effect, but also turns it to an advantage. It has been successfully applied in a variety of cities and to problems of street level drug dealing.

Much of the violence in poor neighborhoods is the result of disputes between rival street gangs. The dispute may be over a drug transaction, or a real or imagined slight. Group members encourage each other to violence because they believe that this is expected of them by the other members of the group. In fact, it may be that few if any group members prefer violence, but all believe the others do. In Step 6 we described this as "pluralistic ignorance." Group members also justify their behavior by taking an oppositional stance to legitimate authority, particularly the police, and believe wrongly that they are standing up for the community and have their community's support.

Pulling Levers exploits these mistaken beliefs in order to get group members to regulate each other's conduct. It seeks to accomplish this goal in three ways, all requiring direct communication with offenders:

1. **Providing a direct credible threat.** The objective is to hold the entire group responsible for the violent actions of each member. Standard police practice after a killing is to arrest and prosecute only the offenders directly responsible. Other group members who provide a supporting role are left untouched. Also left untouched are group members not directly involved who have outstanding warrants, are in violation of parole conditions, or in other ways vulnerable to criminal justice sanctions. There is an incentive for those not touched by the investigation to provoke other group members to violence. If one group member takes the fall for a killing, then the other group members achieve higher status. Under Pulling Levers, legal pressure is placed on all group members if one of their members is involved in a killing. The risk is thereby spread to the entire group so there is less incentive for members to provoke each other to violence.

   To accomplish this, two sets of data are needed:

   a. All violent street groups in an area need to be identified and the relationships among these groups need to be established. Some groups will be allied with each other, some will be fighting with others, and some groups may have no contact with others. This information needs to be updated regularly.
   b. All members of each group should be identified: who they are, their descriptions, their criminal histories, where they can be found, and other similar information. This information, too, needs to be routinely updated.

   The network of group members and the network of groups are used when communicating with offenders. This addresses the problem of violence created by pluralistic ignorance by giving all group members a face saving way of backing away from violent encounters.

2. **Providing a way out of street life.** Whereas the first purpose is to convey a direct deterrent threat, the second is to offer a way out of the gang through job training, substance abuse treatment, and other help. This not only affords a way out for individual members of the group, but it also threatens the integrity of the group itself because the real possibility of a positive exit undermines the shared belief that legitimate society is a source of the group's troubles. So even if relatively few group members take advantage of the offer, the possibility of a way out reinforces the law enforcement threat of the first message.

3. **Demonstrating that the community is against violence.** The third objective is to provide the community with a forum for expressing their strong dislike of violent behavior. Community members, particularly those closest to the group members—family members, former group members, and people working in the streets—communicate a dual message: "You are part of the community and we want you safely back. But we strongly disapprove of your violence which is destroying our community and if you do not change we will support the actions of the police to make you stop." Socially isolating the group removes the excuse that they are acting on the part of the community.

The call out session

"Call out sessions" are widely used. Group members are summoned to a meeting, held in a safe venue in which all three messages are conveyed. While it is impossible to get all of them to attend, the objective is to get some members from each group who can then bring the word back to those who did not attend. In Cincinnati, most call outs were held in a courtroom so members in jail, as well as those on parole or probation could get the message.

The police deliver the first message, often supported by federal and local prosecutors and other criminal justice agencies. Outreach workers who can guide group members into job training, rehabilitation, or educational services deliver the second message. Community members deliver the third message.

The first meeting seldom achieves a reduction in violence, but the police and other criminal justice agencies must swiftly carry out their threat when the next killing occurs. Then a second call out meeting is held and the results of the investigation are used to demonstrate that the consequences are real. The other two messages are reinforced and the successes of anyone who took advantage of the exit services are highlighted. This cycle sometimes needs to be repeated several times.

It is important to track the progress of these efforts. Much of the analytical support needed to develop network diagrams and track progress for the Cincinnati Initiative to Reduce Violence (CIRV) is provided by the University of Cincinnati's School of Criminal Justice, which routinely monitors shootings and killings in the city and uses group related homicide trends as a method of monitoring effectiveness.

READ MORE:

Anthony Braga, David M. Kennedy, Anne M. Piehl, and Elin J. Waring. 2001. "Measuring the Impact of Operation Ceasefire." In *Reducing Gun Violence: The Boston Gun Project's Operation Ceasefire.* Washington, D.C.: National Institute of Justice. www.ncjrs.gov/pdffiles1/nij/188741.pdf.

University of Cincinnati Policing Institute. 2009. *Implementation of the Cincinnati Initiative to Reduce Violence (CIRV): Year 2 Report.* Cincinnati, Ohio: University of Cincinnati Policing Institute. www.cincinnati-oh.gov/police/pages/-32719-/.

27 BE ACCOUNTABLE

IT IS OFTEN DIFFICULT TO DETERMINE IF INTELLIGENCE WORK IS PRODUCTIVE, particularly when it serves a long-term initiative to address criminal groups. Its particular contribution as part of such an initiative is also hard to determine. Like all police functions, however, accountability is critical and all intelligence-driven operations should have clear goals and defined outcomes that can be measured.

The single biggest difficulty is that long-term initiatives tend to lose sight of their goals and begin to focus on their activities. When addressing criminal gangs, for example, the emphasis tends to be on numbers of arrests and disrupting the gangs, rather than reducing the harms the gangs are producing. Intelligence analysts can play an important role in keeping the initiative focused on its goals by measuring outcomes and results. This step examines how to incorporate effectiveness measures into the planning of an intelligence-driven initiative. The principles we describe here are not unique to intelligence, but are, in fact, good practice for all policing.

Setting clear goals and developing measures of effectiveness begins early in the planning of any initiative designed to address group-related crime. Intelligence has an important role to play in both setting goals and developing measures of success. That is, you need to determine how you and others will know whether or not the initiative obtained its objectives.

Table 15 lists four minimal requirements for planning an initiative to address a criminal group. Next to each is its accountability measure. The first thing to be decided is what the initiative is supposed to achieve. These are the goals of the initiative. Goals should be described relative to the harms the group produces. **Goals can be stated in terms of absolute numbers or in percent reductions from current levels.** For example, the Cincinnati Initiative to Reduce Violence

Table 15. Planning and measuring

PLAN	MEASURE	WHAT THE MEASURE SHOWS	WHAT THE MEASURE DOES NOT SHOW
Goals: desired level of problem	**Outcomes:** degree of goal achievement	Whether the initiative is effective in curbing the problems created by the criminal group	Whether the benefit is worth the costs **Efficiency:** To measure efficiency divide outcomes by expenditures or by activities
Objectives: anticipated impacts on the group or their environments	**Results:** degree to which objectives were achieved	Whether the initiative is altering the groups' functioning	Problem reduction effectiveness Compare outcomes to results to see if results are productive
Actions: activities planned	**Activities:** actions carried out	What the initiative is doing	Whether the initiative is achieving anything Compare activities to results to determine achievements
Resources: personnel, equipment, information systems, and money needed	**Expenditures:** resources consumed	The costs of the initiative	Whether these costs are "buying" anything of value See efficiency measurement above

(CIRV, as described in Step 26) set goals in terms of percent reductions in group-related homicides to be achieved over a 12-month period.

An intelligence initiative addressing possible violence associated with a political demonstration could set the goal in terms of property damage, injuries, or other harms that should be minimized. The goal ought to be achievable and meaningful. While completely eliminating group-related homicides is certainly desirable, it may not be achievable. A very small reduction may be achievable, but is less meaningful. The expression, "do not let the perfect be the enemy of the good" applies here. An unattainable perfect goal may prevent the achievement of a very good goal.

The outcome of the initiative is the actual measured reduction in harm. **Outcomes are measures showing how close you came to achieving the planned goals.** It would be the actual number of homicides (or actual percent reduction) in the CIRV example. It would be the actual number of injuries or level of property damage in the example of the political demonstration. Outcomes do not describe the efficiency of the initiative. To determine the "bang for the buck" or "value for money," you need to divide the outcome (e.g., crimes reduced) by the resources used (e.g., money expended). Ideally, each unit of the outcome (e.g., homicide prevented) is associated with a low cost.

Objectives describe the impact of the initiative on the group or the facilitating environment. The initiative seeks to change either the group itself—e.g., break up the group, impede its ability to recruit new members, and so forth—or it seeks to change the environment that facilitates the group's crimes—e.g., deny the group access to specific locations, keep the group's members from intimidating community members, and so forth. The theory of your initiative is that if these objectives can be obtained, then this will lead to achieving your goals.

Results are measures of the degree to which these objectives have been obtained. Because group functioning might not be easily observed, results are often documented through interviews with arrested group members, discussions with community members, informant reports, and from similar sources. Regardless of how successful the initiative is in obtaining desirable results, the impact on the group only matters if the harm from the group's activities can be reduced (outcomes). Results do not measure initiative effectiveness (that is what the outcomes measure), but they show possible progress in that direction.

The next stage down from objectives is actions. The planned **actions are the steps necessary to produce the desired objectives.** Examples of such actions are drug buys, surveillance of group members, interviews with victims, and meetings with community members.

Counting the actions carried out, or measuring the time expended on actions produces measures of activities. Activity measures show what you did (but not what you accomplished). Knowing what the initiative does is important so activities can be linked to results, and then outcomes. But activities consume resources so it is not desirable to maximize activities unless they produce commensurate results and outcomes. Ideally, you would have very few activities and produce great results and major outcomes.

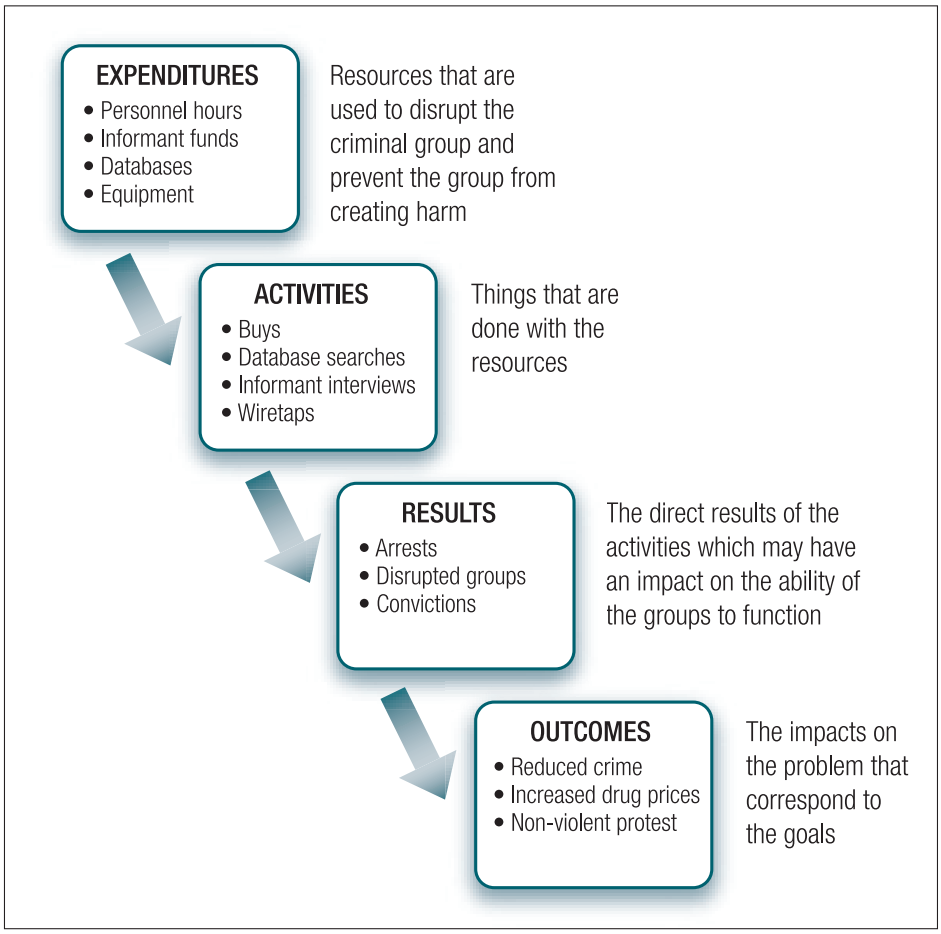
Having determined what actions are necessary to carry out the initiative, the final step is to determine the resources needed to carry out the actions. **Resources are the raw inputs into the initiative.** Typically, the personnel constitute the bulk of resources, while specialized equipment and databases are also often needed.

Expenditures measure resources used, such as personnel time spent on various tasks, informant payments, and fees for access to proprietary databases. It is often useful to monetize expenditures so you can create efficiency measures by dividing outcomes by money expended. A highly efficient initiative achieves large outcomes with little expenditure, while an inefficient initiative costs a great deal and gains little.

In short, expenditures buy activities, which produce results, which create outcomes. This is depicted in Figure 16. While the planning process starts with goals, moves to objectives, then to actions, and ends with resources, the measurement process tracks the actual implementation of the initiative, and works in the opposite direction: from expenditures, to activities, to results, and ends with outcomes.

Tracking these four types of measures over time is critical for ensuring that the initiative is doing what it is supposed to do. If the outcomes are not improving then changes need to be made in the planned objectives and actions.

Figure 16. Measurement schema



28 DO NOT DELUDE YOURSELF

IT IS EASY TO DECEIVE YOURSELF, BUT THIS CAN BE DANGEROUS IN INTELLIGENCE ANALYSIS. When self-deceptions are due to thinking mistakes they are called *cognitive traps;* when due to how the intelligence function is organized, they are called *groupthink*.

Cognitive traps

Richard Heuer shows how intelligence failures result from three limitations of our thinking:

1. When our minds have too much information to process they discard data they judge to be irrelevant.
2. When facts are missing or the quality of data is in doubt, our minds often fill in gaps.
3. When there is limited time available to assess the data, our minds jump to conclusions.

These limitations result in our minds using short cuts, or **heuristics**, to speed up thinking. Heuristics are helpful in everyday situations when they fit the situation, and when the costs of being wrong are small. **Cognitive traps** arise when the heuristics do not fit the situation.

Table 16 on page 78 and 79 lists common heuristics and related cognitive traps in the first three columns. The fourth column describes situations where the heuristics can be useful. The last column describes ways of avoiding traps when the heuristic does not apply.

Groupthink

Groupthink is the tendency of a team to reach a conclusion that reduces internal conflict, rather than addresses the problem. It is most prevalent when the team: (a) lacks diversity; (b) is isolated from groups that may have alternative points of view; and (c) has no clear rules for decision making that make it safe to voice conflicting opinions. Groupthink becomes worse when the team's decision making is dominated by a single person or faction. In the extreme, a senior police executive or elected official dictates a party line that constrains the team's analysis.

Groupthink can be reduced; (a) by increasing the diversity of backgrounds and experience of participants; (b) by creating explicit rules for discussion that require airing opposing viewpoints; and (c) by promoting values of getting the story right and reducing the problem, rather than creating a consensus and focusing on enforcement.

Judge the strength and weight of evidence. *Strength refers to the role the evidence plays in confirming or falsifying a hypothesis. Weight refers to the degree that the evidence can be trusted.* An informant may report that leaders from two rival gangs recently met to plan an attack on a third gang. This confirms analysis about the changing relationships among gangs. If the informant has a history of spreading false rumors or it is doubtful that the informant could have firsthand knowledge of the meeting, then the weight of the evidence is small, though the strength may be high.

Guard against inflating a problem

Christopher Bruce has reminded us that police and analysts tend to equate their own self-worth with the seriousness of the crimes and the danger posed by the criminal groups they are investigating. Consequently, officers, analysts, and, on occasion, entire police agencies exaggerate certain crime problems. This is largely unintentional, though it might play well in the media and might help garner more resources for the department. However, it can have more pernicious effects. Relatively harmless groups of kids may get treated like gangs, immigrant communities harboring nothing more serious than a few illegal immigrants may be treated like havens of terrorism, and every gathering of motorcycle enthusiasts is policed as if the Hell's Angels are mobilizing for war.

Table 16. Heuristics and cognitive traps in intelligence analysis

HEURISTIC	EXPLANATION	EXAMPLE	WORKS IF…	COUNTERMEASURES
Anchoring	The initial guess strongly influences the final estimate.	An initial estimate that a biker gang has 100 members influences later estimates. If this first guess is wrong, so will be later estimates.	The people making the first estimate have a good track record for accuracy.	Consider multiple first guesses that are very different.
Tunnel vision	Focus on a narrow range of alternatives, often just one.	Only enforcement is considered for addressing an offender group. Other tactics might work better.	There is strong evidence supporting the narrow range of alternatives.	Use evidence-based approaches, when available. When not, seek out a range of alternatives, including unusual ones.
Select the first	Choose the first alternative as being good enough.	The first explanation of the group's behavior that fits the data is chosen. Alternative explanations that might also fit are not considered.	The cost of a mistake is small and speed of decision is critical.	Even when a good explanation is available, brainstorm plausible alternatives that might fit the facts.
Availability	Decisions are based on what comes to mind most easily.	Following media reports of a notorious group, analysts label their group as similar.	Prominence of an idea is linked to its validity.	Use brainstorming or other techniques that expand ideas. (See "Select the first.")
Framing	The answer is strongly influenced by how the question is asked.	"How will we break up the group?" points to enforcement; "How will we reduce the harms this group creates?" suggests a wider range of tactics.	The way of asking the question has a track record of leading to success.	Make sure the decision-making group is diverse in background and experience. Invite in outsiders who might ask different questions

Make hypotheses explicit. The more explicit your team is about its assumptions, the more likely it can test its assumptions and avoid costly mistakes. Searching for alternative hypotheses helps reveal hidden assumptions (Step 21). It is much easier to find hidden assumptions when the group places two or more explanations in fair competition and the team engages in systematic searches for data that can falsify one or more of the explanations.

Debrief. Whether the intelligence operation was successful or not, and particularly when it was not, analysts and others involved should systematically go over the experience to document lessons learned.

READ MORE:

Richard Heuer. 2007. *Psychology of Intelligence Analysis*. Hauppauge, New York: Novinka Books.

Kim Rossmo. 2009. *Criminal Investigative Failures*. Boca Raton, Florida: CRC Books.

HEURISTIC	EXPLANATION	EXAMPLE	WORKS IF…	COUNTERMEASURES
Representa-tiveness	Base a judgment on another group that shares some characteristics.	Both groups dealing drugs leads to the conclusion that meth sellers operate like crack dealers.	The characteristic is important and genuinely diagnostic of the problem.	Keep in mind variation. Look for differences as well as similarities.
Identity	Big events must have big causes.	A multiple shooting suggests a planned attack by several shooters, when in fact one shooter acted impulsively when threatened.	The only causes possible are big.	Consider that small, perhaps seemingly inconsequential things, initiated the causal chain.
Correlation	Two events that occur close in time and space must be related.	Analysts conclude that two shootings in one neighborhood in one week are due to gang disputes.	The association has been established by research and it is strong.	Coincidence and randomness are always possible. Look for other evidence beside association.
Confirmation	Look only for evidence that supports a hypothesis.	Having decided that all members of a group come from one neighborhood, only evidence supporting this conclusion is examined.	Evidence in support contradicts all the alternative hypotheses.	Look for contradictory evidence. Consider evidence supporting alternative hypotheses (Step 21).

Adapted from: Rossmo 2009

29 BE PRINCIPLED IN YOUR WORK

THE PUBLIC ARE OFTEN SKEPTICAL OF CLAIMS FOR THE UTILITY OF INTELLIGENCE ANALYSIS AND CONCERNED ABOUT threats it may pose to personal liberty and democratic values. Others in the police and public feel that it is useful, essential, and poses little threat to democracies or liberty. Examples can be found to support both sets of views. In short, police intelligence is controversial and the controversy will not be resolved any time soon.

Despite this, there can be consensus around specific issues. Most people would agree that certain police intelligence operations are useful and promote democratic values. Excellent examples of this are the directed deterrence projects, based on "Pulling Levers" (Step 26), that have been used across the United States to combat street group-related homicides and street drug dealing. These projects focus police attention on high-violence individuals and groups, and high-volume drug markets. Police implement these projects in collaboration with community groups, and can field them without threatening civil liberties. Focusing reduces the number of individuals brought under police scrutiny and community collaboration provides some transparency. And, it reduces crime.

Protecting individual liberties and constitutional principles is fundamental to policing. There is no debate over this. Because this is so important, it bears repeating, largely because there have been failures in the past to adhere to these standards. Such failures are not simply the fault of individuals; they are the failings of the agencies that employ the individuals. Agencies that rely heavily on law enforcement (and overlook alternatives), employ broad sweeping campaigns (instead of focusing on the most harmful people and places), and measure activities (rather than outcomes) facilitate such failures.

An important way to ensure that intelligence analysis lives up to high ethical standards is to focus on harmful target groups and measure success by outcomes. When success is measured by arrests, seizures, disrupted criminal organizations, and other means, then there is an incentive to produce arrests and seizures, and to announce that criminal groups have been fractured (whether they have been or not).

Shifting the focus to outcomes makes it easier to take the more principled path, but it does not guarantee ethical behavior. When we call for a focus on goals and outcomes we are not claiming that "the ends justify the means." But by stating that there are many means to select among, we are claiming that in most, if not all, circumstances there will be good means that can help achieve the ends desired; it is not a choice between effective bad means, and ineffective good means.

There are 10 principles that if followed will help assure ethical results. Except for the first, they are in no particular order. Indeed, they overlap and are mutually supporting.

1. **Reinforce democratic values.** Open discussion and debate is the foundation of democracy. Many of the principles that follow have their foundation in this principle. Conduct intelligence analysis in a manner that facilitates open discussion and debate. However, know that you cannot divulge all data. In fact, divulging some data will undermine democratic values. Still, to the extent possible, be open about information. Look for ways that allow for open discussion with the public that do not compromise individual liberties, sources of data, or methods for obtaining data. At the very minimum, do not use your position to undermine democratic institutions and processes.
2. **Tell the truth.** Better to say nothing than to give false reports. Though deceiving offenders can produce short-term gains, in the long term they learn about the deceptions. Importantly, the public is also likely to be deceived. In either case, gaining future cooperation from the public or from offenders becomes more difficult.
3. **Tell as much as possible.** You might not be able to tell all, but it is possible to tell much. You do not have to tell it all at one time; some information can be kept secret for a time. Definitely convey the uncertainty in the information shared with the public.

4. **Focus on behaviors, not characteristics.** As much of your intelligence is uncertain, protecting the anonymity of individuals is important. Focus on the behavior of groups, not the characteristics of their members. Do not generalize beyond the specific offenders in question. Do not hold individuals up for public ridicule.
5. **Demonstrate progress.** Focus on the harms done by groups and measure your progress by the reduction in these harms, not by your activities. Focusing on progress toward achieving goals reduces the need to discuss sources, methods, and other things that should be kept confidential. When you describe actions and activities, link them directly to goals and outcomes. Admit setbacks and explain them.
6. **Be truthful to yourself.** Conduct self-assessments of your work. When successful, discover why it worked and how it can be repeated. Acknowledge that some successes were due to good fortune, and may not be repeatable. When unsuccessful, find out why you did not succeed and what you can do to avoid repeats. Identify unforeseen circumstances that impeded success and determine how these can be addressed in the future.
7. **Recognize limits.** Acknowledge that when it comes to crime, all data is suspect, and this is even more the case when dealing with offender groups. Understand that as much as you think you know about a group, or your effect on the group, you probably do not know enough. Appreciate the limits of human cognition and develop ways to reduce their negative impact. Recognize that you are likely to be wrong and that humility is a requirement.
8. **Focus.** Police resources are scarce and the public is most concerned about broad use of police powers. For both reasons, target groups that produce the most harm. Use criminal justice sanctions precisely, and convey credible deterrent threats to group members. When seeking to address locations that facilitate group crimes, pick the exact places that aid the groups, rather than larger areas. Focusing not only expends fewer resources and poses less of a threat to civil liberties, but it is also the most effective approach.
9. **Be wary of false consensus.** The uncertainty inherent in understanding group criminal behavior means that it is highly unlikely that any group of police agents has a full understanding of what is going on. There will always be surprises. Consequently, it is important to create an environment that encourages new ideas, innovative ways of doing things, alternative view points, and dissenting opinions.
10. **Test ideas.** Hypothesis testing is seldom viewed as a moral imperative, but when the truth is uncertain and the stakes are high, it is critical that ideas be put to strong tests. A strong test seeks out information that could falsify the idea. Testing is quintessentially democratic, because it does not rely on the status of the person with the idea, or how many followers that idea has. The idea must survive assault by facts and logic.

30 DON'T UNNECESSARILY BEAT YOURSELF UP

WE HAVE REPEATEDLY ARGUED IN THIS MANUAL THAT ARRESTING GROUP MEMBERS IS RARELY ENOUGH to solve a crime problem and, in line with the principles of problem-oriented policing, you should work to change the conditions that make the group's crimes possible. However, we are not blind to the difficulties of doing this. Arresting offenders is seen as the prime duty of the police, and a clear legal and procedural framework exists to guide you. On the other hand, changing the facilitating conditions for crime is a much less familiar role for police and you can expect it to be resisted. Furthermore, compared with traditional policing, which has been around since the London Metropolitan Police was founded in 1829, experience in the use of problem-oriented policing is comparatively recent and you can expect its procedures to be less well-defined, if not outright murky.

Our manual has been written to help you, but you can expect to run into roadblocks of two kinds that can delay and discourage you. These are: (1) objections to the idea of reducing opportunities for offenders, and (2) difficulties of changing critical facilitating conditions.

Objections

The source of many objections you might encounter is **the fundamental attribution error**. Psychologists use this term to describe the human tendency to ignore the role of situation and environment in causing behavior. For psychologists, behavior results from the interaction between the organism and the environment. Translated for police, this means that crime results from the interaction of a motivated offender with a crime opportunity. Traditional policing focusses on "taking out" the offender from the equation, while problem-oriented policing seeks also to remove the opportunities for crime. The difficulty is that the public have little understanding that opportunities play a large part in causing crime. They think that crime is solely the result of immorality, selfishness, and greed. As a consequence, you will likely encounter many objections and even accusations as you seek to change the facilitating conditions for the problem you are addressing, such as these below:

1. **You are not doing your job.** That is to say, you are not arresting offenders and bringing them to justice. This argument may be made when you are trying to persuade some individuals—for example shopkeepers, apartment complex managers, owners of pubs and clubs—to change their premises or practices to make crime less likely to occur.
2. **You are blaming the victim and inconveniencing the law-abiding.** Those who accuse you of not doing your job might also claim that you are blaming them for the crime problem, and inconveniencing them with burdensome requirements, when all they are trying to do is run a successful business that provides a service to the public.
3. **You are ignoring displacement.** People tend to believe that offenders will always find a way to commit crime whatever the impediments thrown up against them. It is not only the public that believes this—many police do as well. But there is now ample evidence from research that displacement is a much less common result of reducing opportunities for crime than usually believed. You should be ready to counter the displacement argument by becoming familiar with *Analyzing Crime Displacement and Diffusion*, Problem-Solving Tool Guide No. 10.

Facilitating conditions may be too difficult to change

You can usually deal with the objections listed above through patient explanation (another skill required of those engaged in problem-oriented policing). However, your efforts to change facilitating conditions might run into a more intractable roadblock—some of these conditions just cannot be changed. We are not referring here to obvious facts of geography, such as the proximity to the Mexico border that facilitates

theft of cars for export. Instead, we are referring to the limits of local police to persuade key stakeholders to make changes. We identify three sources of these limits below, together with illustrative examples:

1. **Action is needed at regional or national levels.** For example, a facilitator of most varieties of car theft—whether joyriding, theft for resale, or theft for export overseas—is the lack of in-built vehicle security. Only in recent years has effective security, such as electronic ignition immobilizers and central door and window locking, been built-in at manufacture. But the vehicle fleet in the United States now averages more than 10 years in age and, assuming your jurisdiction is typical, most of the cars it encompasses provide easy pickings for thieves. In the long-run, this situation will change as manufacturers increasingly adopt more built-in security, perhaps in response to federal regulation or to meet public demand. Meanwhile, your hands are tied.
2. **Stakeholders may be unable or unwilling to act.** It might be thought that the best way to reduce theft for export to Mexico would be to tighten vehicle inspection at the border. Leaving aside that many stolen cars cross the border before they have been reported stolen, there are several reasons why this is difficult to achieve. First, border security is more heavily focused on incoming than outgoing traffic. Second, number plate recognition devices are prone to malfunction, so their warnings are often ignored. Third, increasing inspection times by just a minute or two will rapidly result in lengthy queues and unacceptable delays. Finally, organized thieves are well-practiced in deceiving hurried inspection procedures. Consequently, what seems to be an obvious and effective way to deal with the problem cannot be implemented.
3. **Changes are too expensive or too disruptive of business models.** Research has clearly shown that two clerks on duty in convenience stores, particularly at slow times, substantially reduce the risks of robbery. Nevertheless, legislation mandating this measure was strenuously resisted in Florida and elsewhere, on grounds that it was too costly. In fact, all businesses, from corner stores to national banks, always compare the costs of crime prevention with the costs of crimes that might be prevented. When the risks of crime are low, the businesses often prefer to run these risks and call in the police when a crime occurs. They may also resist a crime prevention measure when it requires them to make difficult changes in their usual operations. For example, new home builders in Charlotte resisted police advice, based on solid research, that site burglaries could be reduced if appliances were installed in new homes immediately before the purchasers took up residence rather than weeks before. This was because builders found it was administratively easier to arrange for appliances for a particular housing development to be delivered together and installed all that same time instead of arranging for them to be installed just before each house was occupied.

It may be problems such as these that undermine your problem-oriented policing project. But you should always remember there is never just one way to solve a problem. If you run into a roadblock, turn your attention to another key facilitating condition that you might be able to change. Who knows, you might therefore enjoy the considerable satisfaction of bringing about a lasting reduction in crime.

READ MORE:

Ronald V. Clarke and Herman Goldstein. 2002. "Reducing Theft at Construction Sites." In *Analysis for Crime Prevention.* Vol. 13 of *Crime Prevention Studies.* Monsey, New York: Criminal Justice Press.

Part 2

Case Studies of Criminal Groups and Problem Gatherings

31 HOW TO READ THE CASE STUDIES

IN WRITING THIS MANUAL, WE DISCOVERED THAT WHEREAS CRIME ANALYSIS COVERS THE GENERALITY OF CRIME, intelligence analysis is mostly focused on offending by groups. We had not seen this point made before, but it soon arose in our discussions about intelligence analysis with police analysts—in fact, they mostly took the point for granted.

At first, we treated this idea as a hypothesis, but we gradually became more confident that it does indeed represent the reality of intelligence analysis, at least in the policing field. Consequently, we thought it important to test the idea by undertaking a closer study of a variety of groups and gatherings in order to learn more about:

1. The kinds of information needed to understand them sufficiently well to identify possible points of intervention for problem-oriented policing
2. The guidance provided by the literature about ways to analyze the information that might exist
3. The existing information on the range of measures that have been deployed by police and others to prevent the crimes committed, to apprehend the offenders, and generally to reduce the harms resulting from the actions of the groups and the activities associated with the gatherings

For these purposes, we did not have to cover every kind of criminal organization and problem gathering; indeed, it would have been impossible to do so in the limits of time and pages available. Rather, we sought to include a variety of groups and gatherings, some familiar (e.g., street gangs, retail drug dealers, and street racing) and some less so (Internet pedophile rings, organized insurance fraudsters, and animal rights extremists). In making our selections, we chose not to include groups and gatherings for which published information was sparse. The first eleven case studies describe a wide variety of crime groups and the final five case studies describe a diverse selection of problem gatherings.

While our original objective in assembling this information was to test the ideas we present in the body of the manual, we thought it could be helpful to present summaries of the assembled information in the form of the case studies. If you happen to be dealing with any of the groups or gatherings included here, you might find the relevant case studies to be of direct value in your own intelligence work. More generally useful to you, however, might be the examples they provide of the kinds of intelligence that could be collected for other groups and gatherings, and the kinds of preventive interventions that might be considered. This would be the main benefit of looking through all the case studies once you have finished reading the body of the text.

The goal of these case studies is to provide a general way of approaching criminal groups, rather than provide an encyclopedia of what is known and unknown. This can change rather swiftly, and there is some debate over a number of issues. At the end of each case, we provide a few readings. These are the sources we found most useful. We choose not to provide detailed citations to all the things written on each group. If you find yourself directly addressing one of the types of groups in these case studies, you should do additional research to come up with useful approaches. *Researching a Problem*, one of the Guides from the Center for Problem-Oriented Policing, could help you get started.

The case studies were mostly written by our colleague, Gohar Petrossian. They follow a reasonably standard format adjusted somewhat to the topic and to the available information. They begin with a general overview of the problem, followed by the discussion of the facilitating conditions or factors promoting the problem. Some case studies include sections explaining how these groups are organized. Examples of domestic or international response strategies are presented either in the body of the text or in separate boxes. Lastly, suggestions as to what you might contribute as an intelligence analyst and what your agency can do are provided at the end of each case study. Be aware that these examples are not intended to be exhaustive and, unfortunately, few have been rigorously evaluated. They are included merely to help you and your agency get started!

READ MORE:

Ronald Clarke and Phyllis Schultze. 2004. *Researching a Problem*. Problem-Oriented Guides for Police. Problem-Solving Tool Series No. 2. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

32 RETAIL DRUG DEALERS

MANY, PERHAPS MOST, POLICE IN THE UNITED STATES HAVE GROUPS OF DRUG DEALERS OPERATING ILLICITLY in their city. The variety of drugs sold makes it difficult to describe the role of intelligence in addressing local drug markets, and we will stick to some broad principles that must be adapted to your local conditions.

Forms of retail drug dealing

Drug markets are where the supply of drugs meets the demand for drugs. They are of two general types:

- **Closed markets.** These operate through social networks. To buy drugs you must know a seller in the network who trusts you, or you need someone who knows a seller. The advantage to all participants is that closed markets offer security from the police, and from robbery by other offenders. For buyers, they can also provide some assurance of product quality because information circulates among the insiders who routinely interact with each other.
- **Open markets.** Participants in these markets may not know each other. Street markets tend to be geographically fixed so that customers can find them. For sellers, the advantage is that they can get more customers, but there are major risks from police and from robbery. Open markets tend to be more violent than closed markets because they are less secure. Open markets can become convergent settings (Step 12) and thereby foster criminal activity in their surroundings.

Open markets are a much more serious problem for communities than are closed markets: not only are they more violent, but they cater to larger numbers of people and they are more visible to the public.

What are the facilitating conditions?

- **Consumers.** A relatively few high-volume consumers and many small-time users are needed.
- **Supply.** The dealer must be connected with people who can supply drugs. Suppliers are often organized in a "cottage industry" style where small groups form and disband as necessary. They may travel from small cities to larger metropolitan areas to secure drugs to supply their local dealers. Such suppliers are easily replaced.
- **Financing.** There are two ways drug dealing can be financed:
  1. The dealer uses his own money to purchase drugs. The supplier gets paid up front and the dealer pockets the proceeds from the sales. Small-scale operations can function this way.
  2. The supplier provides the drugs on credit, and the dealer pays him back from the proceeds. This requires either trust or an enforcement mechanism. This increases the risks of violence.

Though these are the dominant financing arrangements, others are possible. For example, a dealer might provide enforcement services to a supplier in exchange for drugs, or pay for drugs with stolen goods or firearms.

- **Social networks of buyers and sellers.** For closed markets the minimal requirement is a social network of individuals, some of whom want drugs and others who have drugs to sell. This may be the dominant form of drug sales as it has the fewest requirements.
- **Neighborhoods.** Open drug markets require locations that are easily accessible to customers and where their operations will not be disrupted by property owners. Low-income neighborhoods are ideal locations because much of the property is owned by absentee landlords who have little incentive to intervene because of the low economic return on their properties. Once established, drug sellers tend to congregate near each other, just like legitimate businesses, if the area suitable for drug dealing is big enough to accommodate them without conflict.

- **Streets.** Large open markets need ready access to customers. So these tend to be on or near major arterial routes or highways, within vulnerable neighborhoods. Street patterns that permit circular cruising give customers the ability to locate dealers quickly and leave.
- **Places.** These are open markets where people can legitimately hang out and where owners will not interfere. Corner convenience stores are useful because dealers and customers can blend in. Nearby rental apartments where landlords are not scrupulous about tenant management provide locations for stashing drugs, meeting suppliers, and resting places. Lax place management is critical in all circumstances.

What is being done?

There has been a shift in attention from policing drug networks to policing drug places. The rise of hot spots policing has led to intensive patrolling of small areas with high crime concentrations. If these concentrations are close to drug markets, the markets suffer from these patrols. Problem-oriented approaches have been found to be effective in suppressing open drug markets, and superior to hot spots policing alone. Most successful problem solving has engaged the owners of properties—landlords, retailers, bar owners, and so forth—in making their locations unsuitable for dealing. Typically, these place managers cooperate. But when they do not, public pressure and the threat of civil sanctions can be helpful. Many landlords are woefully ignorant about crime and drug dealing, so landlord training can be helpful.

Street closures and other traffic manipulations can also be helpful in specific circumstances. When dealers and users take advantage of easy access to market sites, then altering traffic flow by changing street access can be helpful.

What can you do?

Differentiate between open and closed markets, but recognize that some markets may use aspects of each.

Keep a current list of open and closed markets in your area.

Rank markets by the three Vs:

- Violence—killings, shootings, and assaults
- Volume—number of dealers, sellers, and transactions
- Visibility—how noticeable to the public

Determine how dealers in the most problematic markets either finance their supplies or get protection for their operations.

Know who the dealers are and who they associate with.

For open markets you could identify places critical for market operation and their owners/managers; study street patterns that allow buyers to meet sellers; or identify facilitating conditions that can be altered at the place, street, and in the immediate area.

For closed markets you could gather intelligence on how these develop and interact; and identify those which are most problematic using the three Vs—violence, volume, visibility.

What can your agency do?

Set priorities. Put high-violence markets (usually open markets) at the top of the list for closing down.

Drive illicit drug use underground. Drug dealing cannot be eliminated, but it can be reduced. Displacing open markets to closed can reduce each of the three Vs: violence, volume, and visibility.

Engage place owners. Involve owners and managers of locations at risk of drug dealing. This will include apartment owners and managers, bar owners and employees, entertainment venue owners and employees, and others.

Address street patterns and traffic flow. Alter street patterns that assist open drug dealing. Gain the active participation of local residents and businesses to minimize collateral damage to legitimate activities.

Communicate directly with the dealers. Creating a credible direct deterrent threat to dealers has been shown to reduce open drug dealing. This approach operates very much like "pulling levers" (Step 26).

READ MORE:

Alex Harocopos and Mike Hough. 2005. *Drug Dealing in Open-Air Markets*. Problem-Oriented Guides for Police. Problem-Specific Guides Series, No. 31. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

Rana Sampson. 2001. *Drug Dealing in Privately Owned Apartment Complexes.* Problem-Oriented Guides for Police. Problem-Specific Guides Series, No. 4. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

Ronald V. Clarke. 2005. *Closing Streets and Alleys to Reduce Crime: Should You Go Down This Road?* Problem-Oriented Guides for Police. Response Guides Series, No. 2. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

33 TERRORISTS

UNTIL 2001, YOUR CHIEF MIGHT RARELY HAVE THOUGHT ABOUT THE THREAT OF TERRORISM, but 9/11 changed that. However remote the threat of an attack may be, the consequences can be so horrific that police must now spend precious resources on prevention and preparation.

Apart from being an act of unparalleled evil, 9/11 was unusual because its perpetrators were foreign terrorists. This might have signaled an increase in foreign attacks, though until then the great majority of attacks had been perpetrated by domestic terrorists, such as eco-terrorists, anti-abortionists, hate groups, and militias. The most lethal attack by domestic terrorists was the 1995 car bombing of the federal building in Oklahoma by Timothy McVeigh.

Domestic terrorists have not been able to conduct repeated attacks, with the relatively minor exceptions in the 1960s of the black power movement, and the bombings carried out by the Puerto Rican Liberation movements in the 1960s and 1970s. Could repeated terrorist attacks again happen here? These are some possible sources of risk:

- A long history of violence among Latino and other gangs in large U.S. cities, some of whom are composed of former paramilitary extremists such as the Mara Salvatrucha deriving from El Salvador.
- Deportation of illegal immigrant gang members back to their home country, thus creating the opportunities to establish international networks.
- Existence of well-established immigrant communities that provide cultural cover for potential terrorists.

What can your department do to avert an attack?

The most important things to do are to strengthen community policing, particularly of immigrant communities, and develop links with fusion centers and the FBI Joint Terrorism Task Force.

What can you do, as an intelligence analyst, to support your chief? You should:

- Learn about terrorism so that you know what kind of intelligence to assemble. Start with *Policing Terrorism*, listed in "Read more." (Since terrorism myths abound, *Myths about terrorism* on page 92 includes those discussed in *Policing Terrorism*.)
- While accepting that the risk of attack for most cities is very low, try to determine which factors could increase the risk for your city (see Brief 8 in *Policing Terrorism*).
- Develop local intelligence by analyzing reports from police officers, particularly community officers in areas where potential terrorists might feel comfortable, and from businesses such as motels, banks, and car rental agencies (see Step 16). The San Diego Police Department routinely monitors reports of the theft of propane canisters from suppliers and e-mails the information to its investigators and analysts.
- Identify possible targets for attack in your jurisdiction. Begin by drawing up three lists:
  1. A short list of the most obvious targets to be protected as soon as possible. (For guidance, see Briefs 29 and 30 of *Policing Terrorism*.)
  2. A prioritized list of other targets that require extensive target hardening and a timetable for ensuring that this is done.
  3. A longer list of all possible targets that should be protected by some basic target hardening measures that your department should work to get put in place.

READ MORE:

Graeme Newman and Ronald Clarke. 2008. *Policing Terrorism: An Executive's Guide*. Washington D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

Myths about terrorism

1. *Anyone might be a terrorist.* A white-haired grandmother from the Midwest, even if behaving suspiciously, is very unlikely to be a terrorist. More likely is that she is confused or ignorant of the rules, and that should be the assumption when police approach her. They should reserve their suspicions for those who most closely fit the terrorist profile.
2. *Every immigrant is suspect.* Those who fit the terrorist profile best (for the present at least) are young male immigrants of Arab appearance. Among this group, only a tiny minority are wannabe terrorists or even terrorist sympathizers. Assume in your dealings with immigrant groups that they are as opposed to terrorism as anyone else.
3. *Terrorists are crazed fanatics.* However much we disagree with their reasoning and condemn their cruelty, cold rationality guides much of their behavior. Like all organized criminals, they carefully plan their acts, they try to avoid being caught, and they are determined to succeed.
4. *Terrorists are eager to die.* As we know, some terrorists are willing to die for their cause, but many are careful with their lives. They have the same ambitions for success and happiness as everyone else, and they would prefer to escape and strike again rather than fail and die.
5. *Terrorists are evil geniuses.* Not every terrorist has the mind attributed to Osama bin Laden. Most are ordinary, fallible individuals. They might carefully plan their acts, but they cannot anticipate every eventuality and they will be forced to improvise and take chances. This will sometimes result in failure and perhaps in being killed.
6. *Terrorists might strike anywhere.* Only in theory they might; in practice they must conserve their resources and strike for the greatest effect. If we think like terrorists we can anticipate their choices and act accordingly to protect the most vulnerable targets.
7. *Terrorists are unstoppable.* Most groups of terrorists last only one or two years before falling apart. There are also many examples of terrorism being substantially reduced. For example, the Israelis have reduced suicide bombings by installing border fences.
8. *We can win the war on terrorism.* We can hinder the terrorists and make them less successful, but we can never eliminate terrorism from our world. That is about as unlikely as winning the war on crime.
9. *If it can happen in London (Israel, Delhi…), it can happen here.* Do not assume that a form of terrorism that occurs overseas can easily be reproduced here. Each form of terrorism depends crucially on the opportunities provided by the environment in which it is committed. This environment is rarely the same from country to country. For example, the routine suicide bombings that used to be committed in Israel were made possible by the close proximity of Palestine, the relative ease of entering Israel, and the steady supply of willing bombers. Such conditions do not exist here.
10. *We must prepare for nuclear attack.* Most experts agree that the logistics of building or stealing, and delivering a nuclear bomb make it unlikely terrorists would attack us in this way. Planting a "suitcase bomb" (a radiological dispersal device) in any of our large cities would be much easier. That this would lead to mass casualties is unlikely, though it might result in widespread panic.
11. *Fighting terrorism is a job for the feds.* The FBI and the CIA cannot defeat terrorism on their own. They must garner the support of the public, the private sector, and above all, police agencies. Local police have a key role in gathering intelligence about terrorists, in helping to protect vulnerable targets, and in responding to any attack.
12. *Sharing intelligence is the key to defeating terrorism.* However much we improve intelligence we could never rely on it alone. We also need systematically to reduce the opportunities for terrorism by protecting the most vulnerable targets. Local police might be excused for failing to unearth a terror plot; but there is no excuse for failing to protect key targets or fumbling the response in the event of an attack.

34 WHITE SUPREMACISTS

MEMBERS OF WHITE SUPREMACIST GROUPS BELIEVE THAT WHITES SHOULD DOMINATE SOCIETY because they are superior to other races. They hold in contempt not only other races, ethnicities, and non-protestant religions, but also gays and lesbians. Sometimes they commit hate crimes against these groups. They share a common ideological focus to clean up "cultural pollution" in the United States.

Group members tend to be middle-aged males, average in terms of income, occupation, and level of education. Since 9/11, some white supremacist groups have actively sought to recruit current and former members of the U.S. Armed Services in order to exploit their access to restricted areas and intelligence, or to apply their specialized training in weapons, tactics, and organizational skills.

More than 500 white supremacist groups are thought to exist in the United States, with an overall membership of 100,000 to 200,000. They publish more than 50 periodicals and have established about 2,000 different hate sites on the Internet. They now increasingly rely on the Internet to express their views, recruit new members, and sell their products. Five main groups of white supremacists are as follows:

1. **The Identity Church** incorporates some of the most active and violent organizations, including "Aryan Nations," "Covenant and Sword," and "Arm of the Lord." They seek to justify their racist and anti-Semitic beliefs in a scriptural reading that posits white Christians as God's "chosen" people. They see Jews, defined as non-white, as the greatest enemy, whose ultimate plan is to "race mix" the white race out of existence by brainwashing white women into the arms of black men. On the other hand, they view Blacks as "pre-adamic," a race incapable of creativity and intellectual labor and of constructing a "civilization" or "culture." Followers of the Identity Church ideology believe in the inevitability of a global war between races, which they see as the only way to create a white homeland.
2. **Neo-Nazis** such as the "National Socialist White People's Party" and the "National Alliance," use tracts of Germany's Third Reich to inform their "Americanism" and "White-power" rhetoric.
3. **Skinheads** share neo-Nazi rhetoric and ideology in a somewhat less orderly and consistent manner. According to the Anti-Defamation League (www.adl.org), their numbers may be increasing. They tend to be younger, more loosely organized, but also more violent than some other hate groups.
4. The **Ku Klux Klan**, though once powerful and prominent, is currently in a state of fragmentation. In its contemporary form, it addresses problems like AIDS, crime, welfare, or immigration "solely through the prism of race and offers not solutions but a license to hate." (June A. Marlin. 1992. *Klan's Invisible Empire is Alive and Active in Northeast*. Available at http://alb.merlinone.net/mweb/wmsql.wm.request?oneimage&imageid=5618828.)
5. The ***Posse Comitatus*** (Latin for 'power of the county') shares the anti-Semitism of other hate groups, alongside the anti-statism of the militia groups. The only legitimate form of government for the Posse Comitatus exists at the local level, since the federal government is dominated by Jewish financial interests.

Conditions that promote the emergence of white supremacist groups or facilitate their actions

Such conditions include the following:

- Uncertain economic times, farm crises, and perceived threats to rural industries
- Social changes, such as the rise of the women's movement, the civil rights movement, and gay and lesbian movements
- High rates of non-white immigration
- A volatile political atmosphere, such as that surrounding the wars in Iraq and Afghanistan
- The election, in 2008, of America's first African American president

- The existence of radical churches in rural states
- Lax gun controls in these states
- Internet providers that tolerate hate messages on web pages

It is immediately obvious that very little can be done to change these societal conditions, although the House of Representatives passed the Local Law Enforcement Hate Crimes Prevention Act 2007 to provide federal assistance to state and local jurisdictions to prosecute hate crimes. In fact, local and state police are perhaps in the best position to take action against such groups.

What can you do?

Learn about hate groups and identify those active in your area. Gather intelligence about their ideologies and their backgrounds, and identify possible targets of these groups.

Gather intelligence about the leaders of the hate groups. Where legal grounds for arrest exist, removing the leader will significantly impact the functional capability of the group.

Use analysis to identify possible target locations and select areas at risk. Inform your department about possible future attacks.

Identify and monitor websites operated by hate groups active in your jurisdiction.

Study the *modus operandi* in hate crimes. This may help prevent future attacks on similar targets.

What can your agency do?

Form a task force trained to recognize and properly respond to hate crime if and when it occurs in your jurisdiction.

Warn the leaders of organizations targeted by hate groups to watch out for possible signs of hate crimes and encourage them to contact your agency if alarmed.

Encourage the community to report hate crimes and employ its assistance in investigating and responding to hate crime incidents, and in apprehending the perpetrators.

Seek help from state and federal law enforcement if the groups' operational outreach is beyond your jurisdiction and more sophisticated investigative tools are necessary to support your current operations.

Identify and disrupt any gatherings that use racial slogans, anti-Semitic themes, or any other white supremacist ideology to carry out their activities and recruit new members.

Identify and remove (if possible) the possible financial sources of these groups.

Four characteristics of enduring white supremacist groups

1. Strong leaders with a clear ideological agenda as, for example, in the cases of the Aryan Nations and the National Alliance.
2. Consistent pursuit of activities to expand their goals and acquire the necessary finances. Most groups have perpetrated serious crimes on a regular basis, which has contributed to group stability.
3. Strategic advantage taken of political opportunities. The broader political atmosphere feeds these groups with the opportunities to further their ideologies.
4. Internal cohesion. Organizational instability is seen as a major threat to the survival of these groups. This can result from conflict among its leaders, loss/removal of leadership or the inner core, and the loss of funds.

Source: Freilich, Chermak, and Caspi 2009.

Operation Lone Wolf

In 1998, the San Diego P.D. began to investigate a hate crime case where several prominent members of the community and religious locations were targeted. The two-year investigation resulted in the arrest and prosecution of Alex Curtis, a well-known white supremacist leader. Curtis had been involved for many years in promoting and fostering racial violence through his website, telephone hotlines, and newspaper (*The Nationalist Observer*). He targeted businesses owned and operated by Jewish people, as well as elected officials or known public figures who either openly spoke against white supremacist activities, or who helped minorities. The investigation also led to the arrest of Curtis' cell members. Following the arrests, San Diego experienced a dramatic decrease in hate crimes.

Source: San Diego P.D. 2001. Herman Goldstein Award. Available at www.popcenter.org/library/awards/goldstein/2001/01-60.pdf.

READ MORE:

Neil Chakraborti and Jon Garland. 2009. *Hate Crime: Impact, Causes and Responses.* Thousand Oaks, California: Sage Publications, Ltd.

Joshua D. Freilich, Steven M. Chermak, and David Caspi. 2009. Critical events in the life trajectories of domestic extremist white supremacist groups. *Criminology and Public Policy* 8(3): 497–530.

35 ANIMAL RIGHTS EXTREMISTS

ANIMAL RIGHTS EXTREMISTS, AND MEMBERS OF GROUPS ENGAGED IN THIS KIND OF CRIMINAL ACTIVITY, are generally young to middle-aged, white, and well-educated. Thus, they draw from the same pool of individuals who are attracted to organizations that work peacefully for animal rights, such as Greenpeace, the Wilderness Society, and People for the Ethical Treatment of Animals.

SHAC (Stop Huntingdon Animal Cruelty) is an extremist animal rights group. In 1999, it almost succeeded in shutting down Huntingdon Life Sciences, a British company that conducts product safety testing on animals. SHAC employed a combination of intimidation and violent protests and, since then, extremist groups have become increasingly violent and are said to have caused millions of dollars' worth of damage.

How are they organized?

The best-known animal rights extremist group is the Animal Liberation Front (ALF). It was established in Great Britain in the 1970s as an outgrowth of groups such as Greenpeace and the Sea Shepherd Conservation Society. It consists of an unknown number of individual cells made up of a few people who act autonomously. The activists remain largely anonymous to both the public and each other, which is done purposefully to maximize the security and fluidity of the movement. The ALF operates in more than a dozen countries, including France, New Zealand, Poland, Italy, and Slovakia.

Apart from this group, other lesser-known groups have claimed responsibility for criminal actions in defense of animals. These include the Animal Rights Militia; the Justice Department,[1] a UK-based extremist group; Bakers for Animal Liberation; Guerilla Advertising Contingent; Kangaroo Wilderness Defense; the Lawn Liberation Front; and Pirates for Animal Liberation. The Animal Rights Militia, the Justice Department, and SHAC have been especially active and violent in both the United States and Great Britain in recent years.

1. The Justice Department is an extreme animal rights group based in the United Kingdom. See: Anti-Defamation League. 2010. "Justice Department Claims Responsibility for Threats Against UCLA Animal Researcher." December 3.

What criminal activity are these groups engaged in?

Researchers have classified the criminal activities of these groups into four groups:

- *Type I* commit minor crimes, involving little property damage, which may include such acts as civil disobedience, hanging banners, spray painting slogans, and smashing windows.
- *Type II* commit significant acts of property damage, including setting fire to research laboratories and using firebombs or incendiary devices.
- *Type III* engage in threatening behavior directed against people, including bomb hoaxes, e-mail threats, harassing phone calls, splashing people with red paint, pelting people with tofu pies, leaving dead animals on dinner plates, etc.
- *Type IV* make physical attacks against persons, including beatings and bombings.

Who and what is at risk?

The locations most at risk include federal research facilities, universities, factory farming operations, furriers, and fast-food restaurants. The groups use stolen footage from labs to create publicity materials and films. Research scientists, corporate officials, and their families are at heightened risk of being threatened or assaulted.

The groups use three forms of attack: (a) primary targeting, which can involve visits to the homes of those directly involved in using animals and delivering threats or violence; (b) secondary targeting that involves attacks on companies doing business with animal-related institutions, such as banks; and (c) tertiary targeting that involves harassing the customers or workers of these companies because they are doing business with animal-related institutions.

In the 1990s, Operation Bite Back and Operation Bite Back III, multistage campaigns led by the ALF, included the release of more than 10,000 mink from the Arritola Mink Farm in Mt. Angel, Oregon—the largest number of animals released to that time. These and other actions by the ALF led to legislation, including the federal Animal Enterprise Protection Act (1992), which criminalized causing more than $10,000 in damages at commercial and academic institutions that use animals.

Examples of action taken against extremists

The National Association for Biomedical Research (NABR) developed a coalition for research groups and pushed for the passage of the Animal Enterprise Terrorism Act in 2006. The Act is designed to protect enterprises and researchers who are engaged in animal-related research from the forceful, violent, and threatening acts of animal rights extremists. The Act protects not only primary, but also secondary parties, such as suppliers, from harassment, intimidation, threat, and violence.

California has been a prime target for animal activist attacks in the United States and has passed laws to address the problem. In 2008, for example, former Assemblyman Gene Mullin led an effort to pass the Researcher Protection Act, which made it a misdemeanor to publish personal information about researchers or their families, "with the intent that another person imminently uses the information to commit a crime involving violence or a threat of violence against the academic researcher or his or her immediate family member." The Act also outlaws entering the property of academic researchers to intimidate them and to cause them to stop their work.

Cedars-Sinai Medical Center in Los Angeles is one of many institutions that have adopted a variety of security measures. In addition to carefully screening employees before they are hired, these measures include changing the location of the research facility from the ground floor to a higher floor, instituting strict access controls (researchers can only enter the facility by using electronic key cards), and controlling the elevators by using security guards with key-cards for access.

The research community at large has undertaken public outreach to help people understand that animal research is necessary for medical progress and is heavily regulated by the government.

What promotes animal rights extremism?

- The existence of medical, university, or pharmaceutical research facilities that conduct experiments on animals
- Absence of laws protecting researchers and research institutions
- "Factory farming" operations
- Financial support given to these extremist groups by animal lovers

What can you do?

Collect intelligence on the most active groups and members within these groups through their websites and other sources. Determine if any of these groups are active in your jurisdiction or nearby.

Monitor their websites to identify any material used to threaten or frighten their intended victims.

Identify the methods and technology used by these groups to attack their victims.

Determine which type of criminal activity (refer to the four types discussed above) each group is likely to be engaged in (or has historically engaged in) and devise prevention strategies accordingly.

What can your agency do if extremists pose a threat?

Raise awareness about these groups through community meetings and publicity. Inform the public about the methods and technology used by these groups to attack their targets.

Encourage institutions or people most at risk to report any threat, harassment, or intimidation they may experience from animal rights extremist groups.

Inform these potential targets of security measures and responses that they can develop to protect themselves from current or future attacks, intimidation, or harassment.

Advocate legislative changes to control the criminal activities of these groups.

Control or limit any demonstrations that may result in criminal activity by these groups. Coordinate response strategies with other criminal justice agencies or agencies in nearby jurisdictions.

Support any efforts of the local research community to raise awareness about the importance of medical research.

Urge animal lovers not to give money to these extremist groups by informing them about the harms suffered by victims who are attacked.

READ MORE:

Don Liddick. 2006. *Eco-Terrorism: Radical Environmental and Animal Liberation Movements*. Westport, Connecticut: Praeger.

Home Office. 2004. *Animal Welfare-Human Rights: Protecting People from Animal Rights Extremists.* London: Communications Directorate.

36 INTERNET PEDOPHILE RINGS

PEDOPHILIA IS CLASSIFIED AS A MENTAL DISORDER AND IS DEFINED BY AN INTENSE DESIRE TO ENGAGE IN SEXUAL ACTIVITY with prepubescent children. However, many pedophiles claim that there is nothing abnormal about sexual activity between adults and children. These days, many pedophile rings operate and spread through the Internet. These include Candyman, Shangri-La, Girls 12–16, and Innocent Images, with a combined membership of many thousands.

Pedophile rings engage in a variety of activities, including:

- **The production and distribution of child pornography**, which is used not only for sexual stimulation and gratification, but also to assist in the seduction of a child, to lower the child's inhibitions, and to show what the offender wants the child to do. This is known as "grooming." Some pedophiles keep pictures of their sexual activity with children. These can be used to either pressure the child to remain silent about the activity, to exchange with other collectors, or to establish bona fides when making contact with other group members.
- **Distribution of information** about past or present child victims, access routes to vulnerable children, possible victim locations—such as special schools and hostels—methods and tips on grooming, and information on other pedophiles engaged in organized sexual abuse of children. Many different ways exist of distributing these materials, including e-groups, newsgroups, chat rooms, bulletin board systems, e-mail, websites, and peer-to-peer networks. Predators also use Internet social networking sites, such as MySpace, Twitter, and Facebook, to locate minors, and they can also use the Internet to carry out "live" chats with potential victims and to have "virtual sex" with the children.
- **Support groups** to promote such goals as "sexual liberation for all persons." The most prominent of the U.S. support groups is the North American Man/Boy Love Association (NAMBLA), but others include the Childhood Sensuality Circle, Pedophiliacs Anonymous, and Pedophile Information Exchange. They prepare materials and newsletters advocating legalization of sexual relations between adults and children. They serve to justify pedophilia in the members' minds and reinforce the belief that society, not the pedophile, is misguided.
- **Financial profit.** In many cases, the websites sell child pornography and can realize substantial profits for the operators. People involved in selling child pornography can be either pedophiles themselves, or people who are not sexually attracted to children but rather are motivated solely by financial gain.

What facilitates Internet child pornography rings?

- Lack of legal regulation of the Internet
- Cross-jurisdictional differences in laws and regulations regarding child pornography on the Internet
- Lack of law enforcement knowledge about the Internet
- The extensive possibilities the Internet provides to hide the users' identities
- The international operations of many of the pedophile rings
- The sophistication and availability of technology (e.g., mobile phones with cameras) that enhances the pedophiles' activities on and off the Internet
- The volume of Internet daily activity that makes it impossible to track every site and every person visiting these sites
- The affordability and ease of creating and operating new websites (operators can easily shut down a website that the police are investigating and open a new one)

- Pedophile rings that are knowledgeable about security measures, which can be employed to avoid detection. (Internet sting operations may have succeeded only in catching inexperienced operators)
- The historic reluctance of Internet Service Providers (ISPs) to monitor and censor content
- The reluctance of many victims (and their families) to report abuse
- A widespread perception that child abuse is committed by strangers, not by friends or relations
- The reluctance of parents to monitor their children's computer use
- The existence of pedophile support groups that encourage/justify such activities

Examples of actions taken against Internet child pornography rings

Police sting operations have identified and removed online pedophile rings. For example, Operation PIN, which established a "honeypot" website claiming to offer child pornography, involved the police from Australia, Canada, the U.K., and the United States. As the browsers clicked through screens warning of the explicit nature of the content, they came to a screen that announced that their attempt to obtain online child pornography had been traced and would be reported to local police.

In the United States, ISPs are legally required to report known illegal activity on their sites, but they are not required to search actively for such sites. Police may apply for a court order to seize ISP accounts. Microsoft has announced the development of the Child Exploitation Tracking System that links information, such as credit card purchases, Internet chat room messages, and conviction histories.

Some non-profit organizations seek to raise public awareness about Internet child pornography and will act as political lobby groups. These groups include Wired Safety and Safeguarding Our Children-United Mothers.

The National Center for Missing and Exploited Children operates a CyberTipline that allows parents and children to report child pornography and other incidents of sexual exploitation of children.

What can you do?

Cooperate with your department specialists in Internet crime. They know how to access encrypted sites and e-mails, which may be necessary for gathering intelligence about these groups.

Monitor the activities of child pornography groups, newsgroups, websites, and chat rooms. Postings on these sites for other pedophiles can be used to gather intelligence about online and off-line activities. For example, some sites list member's e-mail addresses to encourage private communication. This information can be used, instead, to gather intelligence and launch an investigation.

What can your agency do?

Authorize officers to enter pedophile newsgroups, chat rooms, or P2P networks posing as pedophiles and request child pornography images from others in the group. They can also enter child or teen groups posing as children and engage pedophiles who may send pornography or suggest a meeting.

In 1996, the San Jose (California) P.D. investigated a complaint against a man who had sexually molested and photographed a 10-year-old girl at a children's party given by his adult daughter in her home. The images were later transmitted via the Internet to members of what turned out to be the Orchid Club. The investigation into that club extended to a number of countries, including the U.K. Examination of the offender's computer uncovered links to the Wonderland Club, another covert pedophile group that used password protection and encryption to hide their activities. The case led to a worldwide investigation of members of both clubs, as well as to the discovery of a third club, the Roundtable.

Source: Associated Press. 1998. "Disgrace follows child porn bust." November 7.

Establish a well-publicized e-mail "hot line," which can be used to report any indications of distribution of child pornography.

Set up a "honey trap site" that purports to contain child pornography, which can be used to capture the IP address or credit card details of visitors trying to download images.

Involve the local community, which can help in raising awareness about the problem, as well as coming forward with information that may assist in arresting and prosecuting perpetrators.

Cooperate with local non-profit organizations in raising awareness about these groups through visits to local schools and youth centers.

READ MORE:

Richard Wortley and Stephen Smallbone. 2006. *Child Pornography on the Internet.* Problem-Oriented Guides for Police. Problem-Specific Guides Series, No. 41. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

Tony Krone. 2005. *International Police Operations against Online Child Pornography*. Trends and Issues in Crime and Criminal Justice, No. 296. Australian Institute of Criminology.

37 GRAFFITI CREWS

HARDLY ANY AMERICAN CITY IS ENTIRELY FREE OF GRAFFITI, MOST OF WHICH IS GANG-RELATED, HATE-INSPIRED, or simply vandalism. Much less common is "art graffiti," where the motive is to create a startling or even beautiful decoration on a publicly visible surface, such as the side of the building. Since this is done without the owner's consent, the graffiti shows the artist's daring and contempt for the law.

Art graffiti is often committed by organized groups or "crews." Most members are males aged 8–19, most are poor, and they come from a variety of ethnic backgrounds.

Crews choose highly visible sites for their graffiti, such as subway routes, rooftops, freeway walls, billboards, and bridges. They prefer sites that involve some element of risk and that will be seen by other crews. They sometimes choose locations, "walls of fame," near other writers' tags to achieve a symbolic co-presence with them. They might write compliments near well-executed pieces or cross out ("dis") or paint over ("go over") poor works.

To increase their status, graffiti crews may "go citywide" or might "tag the heavens" by writing on tall buildings. They often work at night, which gives them time to cover a greater area. They prefer the cold winter months, because the nights are longer, fewer police and others are about, and overcoats allow spray-cans to be easily concealed.

Graffiti crews sometimes engage in shoplifting, handling stolen goods, marijuana use, and drinking in public. They rarely belong to street gangs, but may be recruited by gangs to develop a tag for gang clothing, to mark the gang's territory, or to paint "Rest in Peace" murals for those who have died on the streets. In return, the taggers gain protection from the gang and are sometimes rewarded with drugs.

A tag is the writer's name or alias, or the name of the crew to which he belongs. Each writer tries to develop a distinctive tag that allows him to "get up" or be recognized by other graffiti artists.

Crews create more complex forms, called "throw-ups" and "pieces" or "murals." Throw-ups are generally multicolored and use large "bubble" or sausage-shaped letters. They may include personal symbols or tiny self-portraits. Pieces or murals are large-scale, multi-colored features that may include human figures, animals, and urban structures.

How are crews organized?

Crews range in size from as few as three to as many as several dozen individuals. They are formed for companionship and for undertaking pieces in difficult to reach locations or that entail risky and time consuming work. While crews have no formal hierarchy, members will take responsibility for certain tasks, depending on their standing in the group. Some work mopping up, filling in the colors, and serving as lookouts, while others write the pieces.

In addition to tagging or "piecing" together, crews may hold regular "art sessions" to work on collective designs, share the "piecebooks" in which they draw their designs, and hone their talents to create future large pieces.

Crews might make contact with other crews by going to "writers' corners," which are locations where they can meet established writers, exchange ideas, and, sometimes go out and hit together. Generally these writers' corners move around as a response to police crackdowns and increased surveillance.

Why become a graffiti artist?

- "Getting up" satisfies a need for recognition and respect. Belonging to a graffiti crew also provides a medium through which artists 'communicate' with each other
- A desire to "escape real life" through creating a new name and establishing a new identity—thus becoming a different person
- The illegal nature of the act provides excitement and re-affirms masculinity

In an article originally published in *Security Journal,* George Kelling of "Broken Windows" fame, documented the successful program to rid the New York City subway of the notorious graffiti that blanketed the trains in the 1970s and early 1980s. After years of failed initiatives, the subway management adopted a fresh approach: once a car had been cleaned of graffiti it would be taken out of service and cleaned again as soon as it attracted any fresh graffiti. This removed the incentive for graffiti writers to "get up" and eventually led to the elimination of the problem.

What facilitates art graffiti?

- The proliferation of graffiti websites that provide advice and information
- Widespread availability of spray paint and other graffiti aids, including those found on the Internet
- Difficulties of apprehending and successfully prosecuting graffiti artists
- Widespread public ambivalence about the seriousness of the problem, often promoted by social commentators who may praise the activity

Examples of what has been done to address the problem

- Police and citizen surveillance teams have staked out popular graffiti-writing areas using two-way radios, home video cameras, and night vision goggles.
- Freeway signs and bridges have been secured with razor wire, and buildings protected with graffiti-resistant coatings.
- Graffiti hotlines have been established and undercover transit and police officers have been deployed in the guise of high-school students and journalists.
- High school "bounty hunters" and others have been given monetary rewards for turning in writers.
- So-called "coercive" crime prevention has been used, involving curfews from late night until sunrise (on those under the age of 18), high levels of surveillance of public areas, and extensive rules of entry and behavior in such places as shopping centers and malls.
- Writer's parents have been arrested on charges of contributing to the delinquency of minors and have been billed for thousands of dollars in damages.
- Access to spray paint and other graffiti-writing materials has been curtailed by making it a misdemeanor to sell them (the availability of these materials on the Internet could limit the value of this approach).
- Rapid cleanup has been used to deny crews the reward of having their work seen by others, thus removing the incentive for putting up graffiti (see the text boxes in this step).
- The community has been enlisted in campaigns to combat graffiti by education, community watches, beautification programs, and "paint-outs."

How can you help your agency?

A wide repertoire of measures can be deployed against graffiti crews and you can best assist your department by identifying those most appropriate for your jurisdiction. Specifically, you could:

1. Map hot spots of art graffiti, distinguish them from other graffiti hot spots, and try to predict when these locations are most likely to be hit.
2. Identify chronic offenders or crews by close study of writers' corners and "walls of fame."
3. Try to identify older, more experienced writers, who often recruit novice writers.

The NYPD's Vandal Squad concentrated on removing the most prominent graffiti artists. For big busts they spent time researching and developing a profile of the writer's identity. Since active writers were extremely secretive about their identities, the Squad often made very public arrests of older writers, therefore discouraging the younger ones.

4. Monitor websites, such as graffiti.org, that promote graffiti writing. These websites provide a wealth of information not only on individual and crew activities, but also their associates and networks. See if they include specific information about your jurisdiction.

READ MORE:

Jeff Ferrell. 1993. *Crimes of Style: Urban Graffiti and the Politics of Criminality*. Boston: Northeastern University Press.

M. Sloan-Howitt, and George Kelling. 1992. "Subway graffiti in New York City: 'Getting Up' vs. 'Meanin It and Cleanin It.'" In *Situational Crime Prevention: Successful Case Studies,* ed. R.V. Clarke. Albany, New York: Harrow and Heston. (Reprinted from *Security Journal*.)

38 OUTLAW MOTORCYCLE GANGS

THE HELLS ANGELS ARE THE BEST KNOWN OF ALL OUTLAW MOTORCYCLE GANGS (OMG). These are criminal organizations that are mostly involved in the distribution of illegal drugs, though they also commit other crimes, including extortion, intimidation, kidnapping, money laundering, robbery, motorcycle theft, and homicide.

The gangs are strictly hierarchical and vary in size from a single chapter to hundreds of chapters worldwide. The "Big Four" American-based OMGs are the Hells Angels, the Outlaws, the Bandidos, and the Pagans (see Table 16 on page 106). Local-level OMGs usually comprise fewer than 50 members.

Most national-level OMGs maintain criminal networks of regional and local motorcycle clubs, commonly referred to as "support," "puppet," or "duck" clubs, whose members undertake crime in support of the larger OMGs, and who are a source of new members.

The 1% gangs

In July 1947, a fight between two motorcycle gangs led to arrests and considerable publicity. One of the gangs was the "P.O.B.O.B." (Pissed Off Bastards Of Berdoo), which one year later took the name "Hells Angels." Commenting on the incident, the president of the American Motorcycle Association declared that motorcycle riders are law-abiding citizens with only 1 percent causing trouble. This marked the birth of OMGs, some of whose members now wear a diamond-shaped patch with "1%" on their "cuts."

Approximately 20,000 OMG members reside in the United States. They are white males who ride "American Iron," i.e., Harleys and Harley facsimiles with engines of at least 750cc. The early requirement of having an American-made motorcycle still exists today. Riding any other motorcycle is grounds for expulsion from the group.

OMG members are identified by their "colors" or patches, which are sewn on denim jackets or black leather vests and referred to as "cuts." The top rocker of the three-piece patch identifies the gang. The center shield is the gang's logo, some of which are legally trade-marked or copyrighted. The bottom rocker identifies the area or territory which that chapter or gang claims to control.

Patches and tattoos denote members' status. For example, the Hells Angels' Filthy Few patch indicates that the wearer has committed a murder for the organization. Its Dequiallo patch indicates that the wearer has committed an act of violence toward a person in authority or violently resisted arrest. The Big Four OMGs used to not attack police officers because they believed that the resulting heightened enforcement would cost far more than was gained. Since the mid-1980s, however, attacks on police have increased.

Most OMG chapters have clubhouses that are used for business and social gatherings. These have meeting rooms, bars, gym equipment, and garage areas. They have extensive security, including video-cameras, telephone scramblers, and 24-hour watches.

What facilitates OMG activities?

- Failure by police to identify and remove more violent members of the gang
- Failure to disrupt the gang by identifying and removing its leadership
- Failure to identify and dismantle "support," "puppet," or "duck" clubs
- Lack of criminal intelligence information sharing among jurisdictions
- Absence of bylaws prohibiting fortified clubhouses
- High demand for illegal drugs

Did you know?

- OMGs often confiscate property from expelled members and may brutally remove gang tattoos.
- Bikers who deal with the police or rival gangs, or are drug addicts, face expulsion or death.
- Hells Angels have a saying: "Three can keep a secret if two are dead."
- Bikers hang rival colors or police items upside down to signal disrespect.
- Outlaw bikers are bringing more discrimination and harassment suits against police.
- The Internet is the preferred means of communication for some OMGs.

Examples of what has been done regionally and nationally to deal with OMGs

A variety of national and international initiatives have been launched to deal with OMGs, such as the National Association of Chiefs of Police's (NACP) National Strategy to Combat Outlaw Motorcycle Gangs, and Interpol's Project Rockers that monitors OMGs throughout the world and shares information with member states about OMG memberships, *modus operandi*, and criminal activities. The project posts "red notices" that seek arrest of OMG members with outstanding warrants, and "green notices" that provide information on those who operate internationally.

Project Focus—run by the Criminal Intelligence Service of Canada—provides Canadian authorities with current information on OMGs to help them devise effective biker enforcement policies. The project maintains information on active gangs, location of clubhouses, and photo albums of gang colors in North America. It also collates information on known members including plates, telephone numbers, tattoos, physical descriptions, nicknames, and addresses.

Table 16. "Big Four" American-based outlaw motorcycle gangs

HELLS ANGELS • 2,000-2,500 members in the United States and 26 other countries • Engages in drug trafficking and a variety of other crimes such as extortion, homicide, money laundering, and motorcycle theft • Most concentrated population in California; operates internationally
BANDIDOS • 2,000-2,500 members in the United States and 13 other countries • Mostly involved in drug trafficking • Active in the Pacific, Southeastern, Southwestern, and West Central U.S. regions
OUTLAWS • 1,700 members in the United States and 12 other countries • Similar involvement in drug dealing and crimes as the Hells Angels • The dominant OMG in the Great Lakes region
PAGANS • 900 members in the United States, none outside the United States • Cooperates with traditional organized crime groups • Operates mostly in the Northeastern United States

What can you do?

Assist your agency's on-going investigations of OMGs by constructing a social network analysis of gang members (see Step 19), using data from surveillance and informants and, if available, from wiretaps. This will assist you in describing the hierarchy of command and therefore where your agency should focus its efforts to arrest the leadership.

What can your agency do?

Establish task forces. Many police agencies have established task forces that gather intelligence about local OMGs. For example, task force members might stake out OMG clubhouses and systematically record those entering. The task forces include a network of correctional, parole, and probation officers that give police added leverage for interviewing potential informants and witnesses.

Use undercover operations and informants. Undercover agents have been used to infiltrate OMGs. This can be dangerous and the agent might have to make significant compromises because the initiation process usually involves activities that are illegal or conflict with ethical policies of police departments. An alternative is to make use of informants, but this can also result in serious threats to their safety.

Use technology. Computer-assisted dispatch (CAD) hazards files can alert responding officers to OMG members' homes, work places, and locations visited, so that the officers can write offense or incident reports.

Be sure to share information. Placing gang members into the National Crime Information Center files will help notify investigators when police contact is made for traffic violations or when tracking gang members' activities and movements.

Seek the passage of bylaws prohibiting fortified buildings. Canadian municipalities have done this to prevent fortified buildings from being used as bunkers for OMGs. The bylaws regulate security features, such as metal doors, bullet-proof windows, surveillance towers, and security technology.

READ MORE:

National Drug Intelligence Center. 2009. *National Gang Threat Assessment, 2009*. Tallahassee, FL: National Gang Intelligence Center.

39 STREET GANGS

LOW-INCOME NEIGHBORHOODS, MARKED BY UNEMPLOYMENT AND VIOLENCE, ARE THE MAIN BREEDING GROUNDS FOR street gangs. These gangs are no longer confined to large cities, but are now found in suburban and rural areas. Many are engaged in drug dealing, however they could also be involved in other criminal activities, including robbery, auto theft, drive-by-shootings, and homicide. Many gang members join to make money from crime, but they also see the gang as a brotherhood or a support system, which they join to seek protection and respect.

According to the National Drug Intelligence Center, there are an estimated 900,000 street gang members across the country. States with the largest gang populations are California, Illinois, Texas, Florida, and Ohio. About 90 percent of gang members are African American or Hispanic (with a few Asian gangs) and about half are under the age of 18.

Street gangs are classified into three main groups according to size and operational reach:

1. National gangs comprise several thousand members that operate both nationally and internationally, especially in Mexico and Central America. Some of these include: Almighty Latin Kings, the Crips, the Bloods, 18th Street, Asian Boyz, and Vice Lord Nation.
2. Regional gangs are composed of several hundred to several thousand members. These include Florencia 13, Fresno Bulldogs, Latin Disciples, Tango Blast, and United Blood Nation.
3. Local gangs, also referred to as neighborhood gangs, vary greatly in size from a handful of individuals to a hundred or more members.

How are they organized?

Most gangs are loosely knit coalitions of small, autonomous cliques. Leadership of these gangs is usually decentralized and nonhierarchical. It can change rapidly and may vary by the type of gang activity; e.g., drug sales leaders may differ from "gangbanging" leaders.

The more organized gangs may have clearly defined leaders and leadership roles. These roles may include "making sure all laws and policies are being followed," "giving orders," "being the thinkers," and "making the overall decisions for the group."

In 1990, Los Angeles instituted "Operation Cul-de-Sac" in Newton, an inner-city neighborhood plagued by drug and gang activity. Barriers were installed to impede drive-by shootings and drive-up drug purchases. Foot and bicycle patrols were stepped up to suppress these crimes and to improve police-community relations. The barriers prevented cars from entering the street, or required those that entered to leave the same way. This increased the risks for shooters, because their targets would have their own guns ready when the car returned. In the two years after the barriers were installed, only one homicide was recorded, whereas in the year before seven homicides were committed in the area. Homicides were not displaced elsewhere.

Source: Ronald V. Clarke. 2005. *Closing Streets and Alleys to Reduce Crime: Should You Go Down This Road?* Problem-Oriented Guides for Police, Response Guide No.2. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services. Accessible at www.cops.usdoj.gov.

Many organized gangs hold regular meetings to collect dues and discuss any problems, as well as to enhance group cohesion, to communicate responsibilities, and disseminate information.

Gang member affiliations can be identified through "colors" (clothing and emblems), tattoos, hand signs (used within the gang), and graffiti (gang symbols on clothing, school books, backpacks, and walls).

Learn about Internet databases, such as GangNet and Cal/Gang, that allow law enforcement agencies to identify individuals involved in gangs—their names, street names, addresses, known associates, gang hand signals, vehicles, and tattoos. Cal/Gang can be accessed by law enforcement officers in California, while GangNet is used in many states and in Canada. The Orange County (California) Gang Incident Trafficking System combines traditional crime mapping and gang crime reporting. Local analysts used the system to discover that adult gang members were far more likely to be involved in violence than juvenile gang members, a crucial fact that was used to redirect the agency's gang intervention programs.

Gang members can be classified as hardcore, associate, or wannabe members. These designations are based on their criminal performance, street-smarts, incarceration experience, or abuse endured for the group. Membership is sometimes defined by age, such as "youngsters," "old gangsters," "young homies," and "old homies."

Examples of action taken against gangs

Two federal statutes are used to prosecute street gangs: the Racketeer Influenced and Corrupt Organizations (RICO) Act, and the continuing criminal enterprise (CCE) statutes of the Comprehensive Drug Abuse Prevention and Control Act of 1970. These "conspiracy" statutes allow prosecutors to present evidence of multiple criminal acts committed by various members of the gang.

Some cities, including Los Angeles, San Antonio, and Chicago, have adopted gang injunctions as a way of addressing local gang problems. These restraining orders are issued against specific gang members by the city's Attorney's Office and approved by a judge. The orders prohibit the gang members from engaging in certain activities that may range from selling drugs or possessing a weapon, to congregating in a group, being out at night, and possessing a cell phone.

The National Gang Center provides descriptions of successful anti-gang programs, and offers links to tools and databases that assist police to address the gang problems within their jurisdictions. The Center collates daily newspaper reports on national gang activity, and maintains a database of professionals working with gangs.

The Boston Gun Project is the most successful program to date in addressing gang violence (See Step 26).

What can you do?

Although your jurisdiction might have no homegrown gangs, gangs are mobile and you might have to deal with those that come from nearby cities. You can gather intelligence about their colors, signs, activities, and rivalries either directly, or from the police agencies who are dealing directly with these gangs. You should seek information to answer questions such as:

- How prevalent is the problem and how many gangs are in operation? Are they national, regional, or local gangs?
- Which of them pose a threat and what criminal activities are they engaged in?
- How many gang members can be identified? What is their demographic profile, i.e., racial/ethnic composition, age group, immigration status?
- Who are the gang leaders (if any) and what information is available about them? What information should be gathered about them?

Identify hotspots where these gangs are more likely to operate and determine whether their operations also reach larger areas. Determine whether any geographic shifts in their operations occur, and decide how this can be dealt with.

Prioritize gangs by the level of violence of their members. Then focus on the most violent groups first.

With sufficient intelligence in hand, advise your department about response strategies that would work best. These may range from completely eliminating the gang problem to dealing with the problem more effectively.

What can your agency do?

Raise awareness about the gang problem through schools and community organizations and develop partnerships with the community to gain help in addressing the problem. These partnerships should include faith-based groups, social service agencies, and other law enforcement agencies. Most programs that have shown success engaged in collaboration with a wide range of actors and have used a combination of prevention, intervention, and suppression strategies.

READ MORE:

Scott Decker. 2008. *Strategies to Address Gang Crime*. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

40 AUTO-ACCIDENT FRAUD RINGS

CRIMINAL RINGS ARE FREQUENTLY INVOLVED IN AUTO-ACCIDENT INSURANCE SCAMS, of which there are two main kinds: (1) staged accidents for which insurance claims are made; and (2) false injury and physical damage claims, so-called "build ups," resulting from actual accidents. These cases sometimes include "jump-ins," people who were not present at the accident but who file claims.

The groups involved may use the funds from insurance frauds for other criminal activities, such as drug trafficking. Indeed, the rings include many former drug traffickers.

The rings often hit insurers with many small claims to stay under the company's anti-fraud radar. When insurers begin to investigate such claims, they may find they are dealing with large rings with a wide reach.

According to the FBI, auto-accident frauds cost the insurance industry about $20 billion a year. Densely populated states, such as New York, New Jersey, California, Florida, and Massachusetts are among the hardest-hit. New York City is especially vulnerable.

Who is involved and how are they organized?

Auto-accident fraud rings recruit "accident victims" in two main ways:

- They use **"runners"** to recruit phony victims, often new immigrants, who are paid for participating in fake auto accidents.
- They use **"steerers"** to recruit accident victims from news reports, by visiting hospital emergency rooms and by approaching people who visit the police to collect copies of accident reports. They show these people how to profit from the accident and take them, or refer them, to clinics associated with the rings or directly operated by them.

  These clinics pad the bills with expensive and unnecessary treatments and then collect payment from the insurance company.

In response to legislation that classified insurance frauds as felonies, the rings have shifted tactics from actual to paper accidents. This is done by using information from legitimate or falsified police reports to steer patients to medical clinics.

Two common scams

Scheme 1. Load a car with people, pull in front of another car and slam on the brakes. If the expected collision ensues, the innocent party is almost always liable. Young women and the elderly are frequently targeted, the former because they are more prone to admitting fault and the latter because they are prone to becoming flustered. These scams, called "swoop and squat," sometimes target buses, where the passengers, who work with the ring, immediately report injuries and file insurance claims. Bus drivers sometimes work directly with the ring.

Scheme 2. Load two cars with people, crash the cars, call the police and say that everybody was hurt. The insurance companies are then billed for unnecessary medical procedures. Again, these schemes may also include buses.

Instead of paying people to borrow their insurance and their cars, the rings may use false identities to purchase cars and insurance, and, therefore, to file false insurance claims.

Factors contributing to auto-accident insurance fraud

- Ordinary citizens who are willing to participate in the schemes, because they believe that: (1) they are entitled to compensation for money they have paid in policy premiums; (2) the frauds only hurt insurance companies who deserve to be "hit"

- Lack of insurance staff trained to detect fraudulent claims
- Lack of public awareness programs to educate potential victims
- Lack of state insurance fraud bureaus that can undertake cross-jurisdictional investigations

What has been done nationally to address the problem?

In 1976, Florida passed the False and Fraudulent Insurance Claims Act (FFICA), which made insurance fraud a specific offense. Florida also created the Division of Insurance Fraud to investigate frauds falling under the definitions of the FFICA. Since then, many other states have established similar insurance fraud bureaus.

The National Insurance Crime Bureau (NICB) was formed in 1992 by over 1,000 member insurance companies to help deal with insurance fraud. The NICB serves as a conduit between the insurance industry and federal, state, and local law enforcement agencies. It holds multiple databases, currently with more than 350 million records of suspicious claims, which insurance companies can access to check claims.

A successful prosecution

In November 2000, the Federal District Court in Brooklyn broke up a 53-member auto insurance fraud ring that cheated insurance companies out of more than $1 million by staging 27 crashes in New York City. Two employees of Medical Arts Rehabilitation clinic led the ring. They paid people $500 to stage an accident. These people recruited new drivers and passengers to crash their own cars, who were treated at the clinic for injuries that were never sustained. The clinic then billed insurance companies for up to $20,000 for medical services, while the passengers filed bodily injury claims for between $3,000 and $22,000. Many of the recruits were "unsophisticated and often recent arrivals to the United States."

Source: Alan Feuer. 2000. Car Crashes Were Staged For Fraud, U.S. Charges. *New York Times,* November 17.

Most insurance companies subscribe to the American Insurance Services Group Index, which provides data pertaining to bodily injury and workers' compensation. Many have established hotlines with interactive conversation that allows for the gathering of detailed information about possible insurance fraud claims. Many have also established Special Investigative Units (SIU) specifically to investigate possible fraudulent claims.

Randolph (Massachusetts) P.D. partnered with other state and county law enforcement entities to form the Community Insurance Fraud Initiative (CIFI), a task force to address the city's auto insurance fraud problem. The CIFI offered a $5,000 reward for information leading to the arrest and conviction of perpetrators of the fraud. Two hundred and sixty-three individuals were arrested, which, together with arrests made by other task forces operating in six nearby cities, resulted in a reduction of $100 million in fake auto accident claims in those cities in 2004.

What can you do?

Gather information on the time and location of auto-accidents, as well as the number of people involved in each accident to determine if possible rings are involved. Staged auto-accidents happen during busy times on busy streets, and generally involve many passengers.

Determine if there is a high concentration of auto accidents in neighborhoods or areas with high concentrations of immigrant populations. Gather information about the people involved in the accidents, including their age, gender, and ethnicity, which may help determine whether staged accidents are taking place.

Learn how to use the different databases provided by NICB designed to fight insurance fraud. The wealth of knowledge provided by this organization can prove valuable in your department's investigative efforts.

What can your agency do?

Coordinate fraud probes with the insurance companies as well as other law enforcement agencies—such as the Attorney General's office, district attorneys, or U.S. attorneys—as the problem may require a multi-jurisdictional approach.

Deploy undercover officers posing as accident victims to probe unscrupulous medical clinics that pad claims. Determine if these clinics work with an auto-insurance fraud ring and try to infiltrate their operations.

Execute wiretaps to gather information from medical clinics, lawyers, and employees of the insurance company suspected of involvement in the ring.

Work closely with community organizations and immigrant groups to educate them about the dangers and risks involved in taking part in staged auto accidents.

READ MORE:

Tony Baldock. 1997. *Insurance Fraud*. Trends and Issues in Crime and Criminal Justice, No. 66. Australian Institute of Criminology.

41 ORGANIZED SHOPLIFTERS

ORGANIZED SHOPLIFTERS STEAL LARGE AMOUNTS OF MERCHANDISE FOR RESALE. They may operate across state lines, and may target the same chain in different places. Their arrival in your town might be signaled by a spike in reports of goods being shoplifted in large quantities.

The groups are frequently composed of immigrants (legal or not) from the Middle East, South America, or Asia. This may be because they can sell the goods they steal to fellow immigrants who run small businesses. The groups sometimes also take part in drug trafficking, car theft, and burglary.

The FBI reports that organized retail theft costs businesses $12–$35 billion annually in stolen goods, lost sales, and replacement costs. It is believed that the profits from organized shoplifting are sometimes used to fund foreign terrorists; according to the CRISP report (in the Read more section), "money laundering has been proven in many, if not all, organized retail crime rings operated by Middle Easterners."

How are they organized?

Each group consists of several members with distinct roles: "boosters" steal the goods; "handlers" sell the goods to fences; and others take care of transport and logistics.

Boosters act alone or in groups. They steal large quantities at one time, usually of the same items. They carry tools to remove security tags, they use foil-lined bags to defeat electronic tags, and they may use cell phones to communicate with other group members while shoplifting. They may change bar codes so merchandise registers at a much lower price on checkout ("ticket switching"). They may use stolen credit cards and use the receipts to return stolen goods to the store for cash. In some cases, they may simply wheel carts full of merchandise out the doors to a waiting getaway van.

The stolen property may be held in rented storage units before being taken to the group's home base. The property is often sold to *street-level fences*, who might own a bodega, pawnshop, or gas station. Some fences operate from home, selling items door-to-door, in flea markets and local taverns, or even on the Internet. They might sell-on the goods to *mid-level fences*, who clean and repackage them to look like new and then sell them to *wholesale diverters*, who might mix them with legitimate goods for sale to retailers.

What facilitates the work of organized shoplifters?

- Their unexpected arrival in towns and cities and equally quick departure
- Their links with immigrant communities, which facilitate disposal of goods
- Complacent retailers who have not been victimized by organized shoplifters
- Low priority accorded by police, prosecutors, and judges to shoplifting and fencing operations
- Poor security in many stores that puts them at risk (see below)

Which stores are at risk?

1. Those that sell goods that are CRAVED (concealable, removable, available, valuable, enjoyable, and disposable). Designer clothing, over-the-counter medicine, electronics, DVDs, health and beauty supplies, razor blades and infant formulas are considered to be among the "hot products" targeted by organized shoplifters in supermarkets.
2. Large stores that make it easier for organized groups to hide among ordinary shoppers
3. Stores located close to highways that provide easy escape routes
4. Stores with many part-time associates who have less commitment, lack theft awareness, and have limited training

5. Stores with the security weaknesses that aid ordinary shoplifters (see *Shoplifting, 2nd Edition,* Problem-Oriented Policing Guide No 11). Such weaknesses include:
    a. Lax return policies that allow thieves to return stolen items to the store for credit or cash
    b. Unmonitored exits, blind corners/spots, high displays that conceal thieves from view, and open displays of high-risk items
    c. No security staff, poor stocktaking, and lacking security equipment such as electronic article surveillance and video-cameras
6. Stores that do not report shoplifting to the police

What is being done regionally and nationally?

Walmart, Target®, Lowe's®, Limited Brands, and other large retailers seek to identify organized shoplifting rings by investing in software that tracks regional patterns of theft.

Many states have passed laws that address organized retail crime and, in 2009, Congress passed the Combating Organized Retail Crime Act and the E-fencing Enforcement Act.

The Law Enforcement Retail Partnership database (LERPnet) was created for merchants to share information on organized shoplifting with local, state, and federal law enforcement, as well as with other retailers.

What can you do?

Regularly scan for stores with high shoplifting rates (see Table 17 on page 116) and try to determine the reasons. Notify your supervisors about the need to alert the stores to their problematic status and the need to take preventive actions. Keep in mind that reported shoplifting may be significantly lower than actual shoplifting due to differences in store security policies and staffing.

Alert other analysts and police officers to signs of organized shoplifting.

What can your agency do?

Work with local merchants to encourage reporting of shoplifting and early sharing of information about the arrival of an organized crime shoplifting group. Alert nearby jurisdictions to the possible arrival of these groups in their locations.

Educate retailers about theft prevention and the importance of reporting shoplifting incidents. Measures focused on organized shoplifting include: displays that prevent the removal of multiple packages at one time; cabinets that beep if open too long; and stamping the store's name on over-the-counter medicines or infant formula cans to reduce their re-sale value.

Reduce the opportunities to dispose of stolen goods by regularly monitoring pawnshops, flea markets, and used-goods stores. Visit local bodegas, taverns, and other small businesses, especially those owned by recent immigrants, to ask about suspicious attempts to sell them goods.

READ MORE:

Ronald Clarke and Gohar Petrossian. 2012. *Shoplifting* 2nd Edition. Problem-Oriented Guides for Police. Problem-Specific Guides Series, No. 11. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

Walter Palmer and Chris Richardson. 2009. *Organized Retail Crime: Assessing the Risk and Developing Effective Strategies.* ASIS International Foundation CRISP Report.

Table 17. Reported shoplifting by store in Danvers, Massachusetts

Scan regularly for stores with high rates of shoplifting. Crime analyst Christopher Bruce did this for the Danvers (Massachusetts) Police and produced this table. The store with the most shoplifting incidents was one of the largest in the town. But when size was taken into account by calculating the number of thefts per 1,000 square feet (see the final column of the table), the riskiest store turned out to be the one that had been ranked 3rd on the list before correcting for size; it was a tiny boutique store with staggeringly high shoplifting.

Visit the riskiest stores and try to understand why their rates of shoplifting are so high and what they might do to reduce the risks.

REPORTED SHOPLIFTING BY STORE IN DANVERS, MASSACHUSETTS, NOVEMBER 2008 TO OCTOBER 2010

Store	Thefts	Percent of All Thefts	Cumulative % Thefts	Cumulative % Stores	Thefts Per 1,000 Sq. Ft.
1	210	33%	33%	2%	2.06
2	152	24%	56%	3%	1.83
3	36	6%	62%	5%	144.00
4	29	5%	67%	6%	0.36
5	24	4%	70%	8%	0.32
6	23	4%	74%	10%	0.28
7	21	3%	77%	11%	0.26
8	15	2%	80%	13%	0.18
9	9	1%	81%	14%	0.11
10	9	1%	82%	16%	0.11
11	9	1%	84%	17%	0.14
12	6	1%	85%	19%	20.00
13	6	1%	86%	21%	0.10
14	5	1%	86%	22%	0.17
15	5	1%	87%	24%	0.07
16	5	1%	88%	25%	0.13
17	5	1%	89%	27%	3.13
46 Stores with <5 Thefts	72	11%	100%	100%	

42 ORGANIZED CAR THIEVES

TEMPORARY THEFT OF CARS, OFTEN COMMITTED BY JUVENILE JOYRIDERS OR, TO A LESSER EXTENT, FOR USE OF THE car in committing another crime, accounts for the bulk of car thefts. Permanent thefts, where the car is never recovered, are often committed by organized criminals, who are employing increasingly sophisticated tactics to outsmart today's anti-theft devices. These thefts account for the bulk of the costs of car theft. In 2011, 47.7 percent of the value of the vehicles stolen was never recovered according to UCR reports, causing losses of about $1.8 billion nationwide.

Several forms of permanent theft exist, including:

- "Rebirthing," which is giving the car a new identity for resale
- "Chopping" the car and selling its parts
- Exporting the car, which is accomplished by shipping it overseas from one of the nation's many sea ports or driving it over the border to Mexico

You should try to determine if a car theft ring is operating in your area, and whether the cars are stolen for export. Theft for export is particularly likely if you are close to the Mexico border or near a major port. This step describes two techniques that will assist you in this task. It does not describe the facilitating conditions for organized car theft, or the *modus operandi* involved, since these are used for illustrative purposes in Step 10, "Modify the conditions that facilitate organized crimes," and Step 11, "Study the *modus operandi* step-by-step."

Compare your auto theft rates with those of other jurisdictions

Officers in Chula Vista (California) P.D. suspected that being close to the Mexican border exacerbated the city's auto theft problem. The department's crime analysts tested this idea by calculating the theft rates for Chula Vista and neighboring cities. They found that Chula Vista's auto theft rates, and those of other cities closest to the border, were two to six times higher than ones further north in San Diego County (see Figure 17). Many vehicles were stolen from parking lots and driven across the border before owners had even discovered the thefts. The analysts also found that pick-up trucks—highly prized in Mexico—were at greatest risk, and that the recovery rates of these trucks stolen in Chula Vista were lower than in cities further from the border.

Organized car theft on the U.S./Mexico border

Resendiz has described a division of labor among those involved in the export of stolen vehicles from the United States to Mexico:

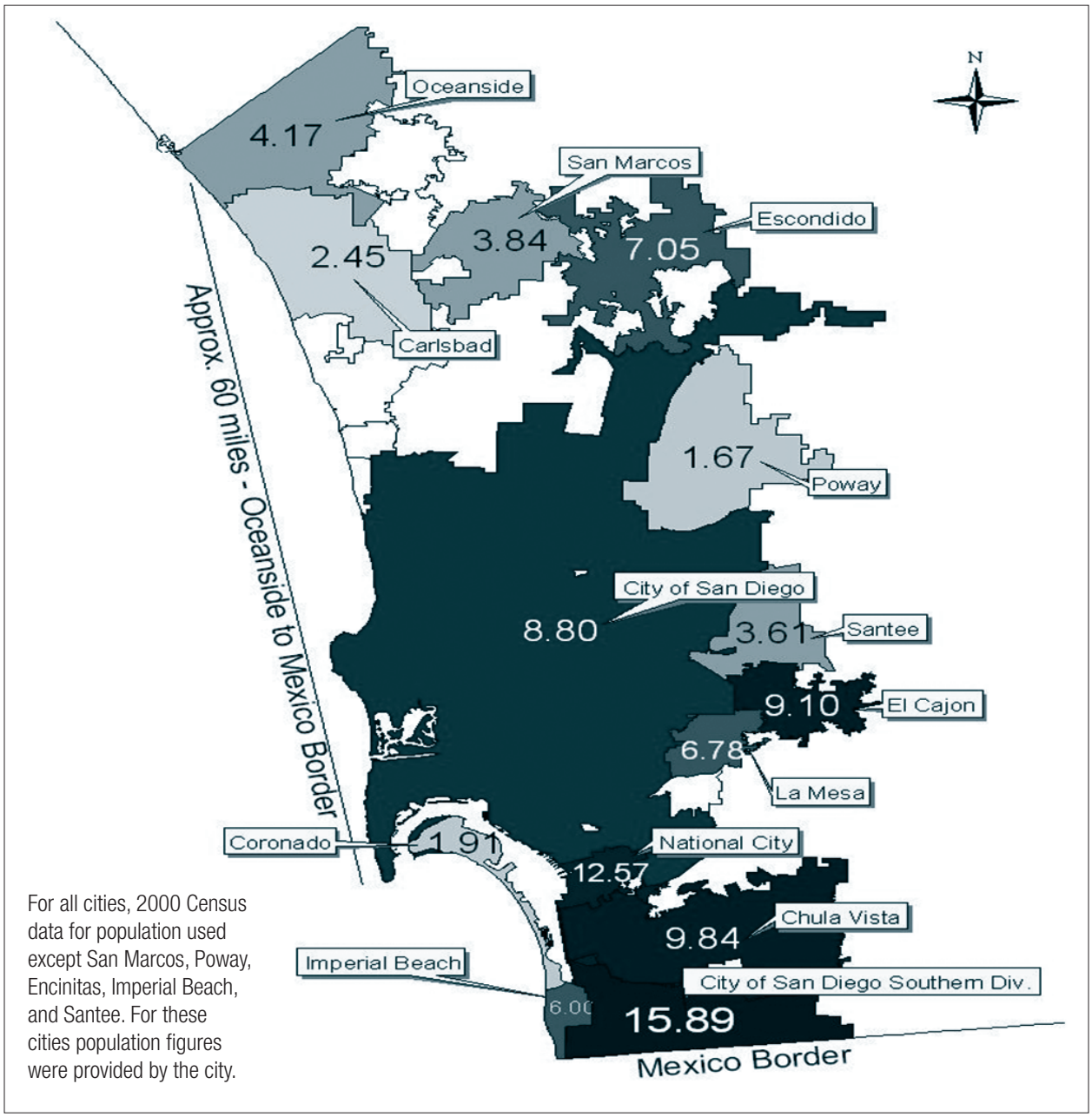
Chauffeurs provided vehicles to cruise around mall parking lots and residential areas to "shop" for possible target vehicles.

Specialists used different tools to steal different model vehicles. They used flat head screwdrivers and vise grips to open Chevrolets, master keys for Chryslers, dent-pullers, screwdrivers, and vise grips for Fords. They usually took between fifteen seconds to one and a half minutes to break into any car.

Mounters were responsible for driving the vehicle to the buyers in Mexico. Once the vehicle was crossed, it was dropped off at a designated hideout, and from there, to customers and buyers.

Source: Rosalva Resendiz. 1998. International Auto Theft: An Exploratory Research of Organization and Organized Crime on the U.S./Mexico Border. *Criminal Organizations* 12:25–30.

Figure 17. Vehicle theft rates per 1,000 residents in San Diego County, 2001



Source: Plouffe and Sampson 2004.

Calculate location quotients to identify a possible theft for export problem

The fact that many vehicles are stolen in your area may not mean that organized car thieves are operating; it could simply reflect a generally high rate of crime in your area. To test this you can calculate a Crime Location Quotient (CLQ). A CLQ compares the total number of a particular crime across a set of geographical units (for example, neighborhoods, cities, or counties), taking into account the distribution of other crimes in those units (see Figure 18 for an example of the calculations). It is the ratio of target crimes to all crimes in a jurisdiction (e.g., county) divided by the ratio of the target crimes to all crimes in a larger area (e.g., state).

Figure 18. CLQ calculation to estimate the prevalence of theft for export in U.S. counties

Researchers have recently used the CLQ calculation to estimate the prevalence of theft for export in U.S. counties.

They used the following formula:

CLQ= (a/b)/(X/Y)

a= total number of motor vehicle thefts within the county

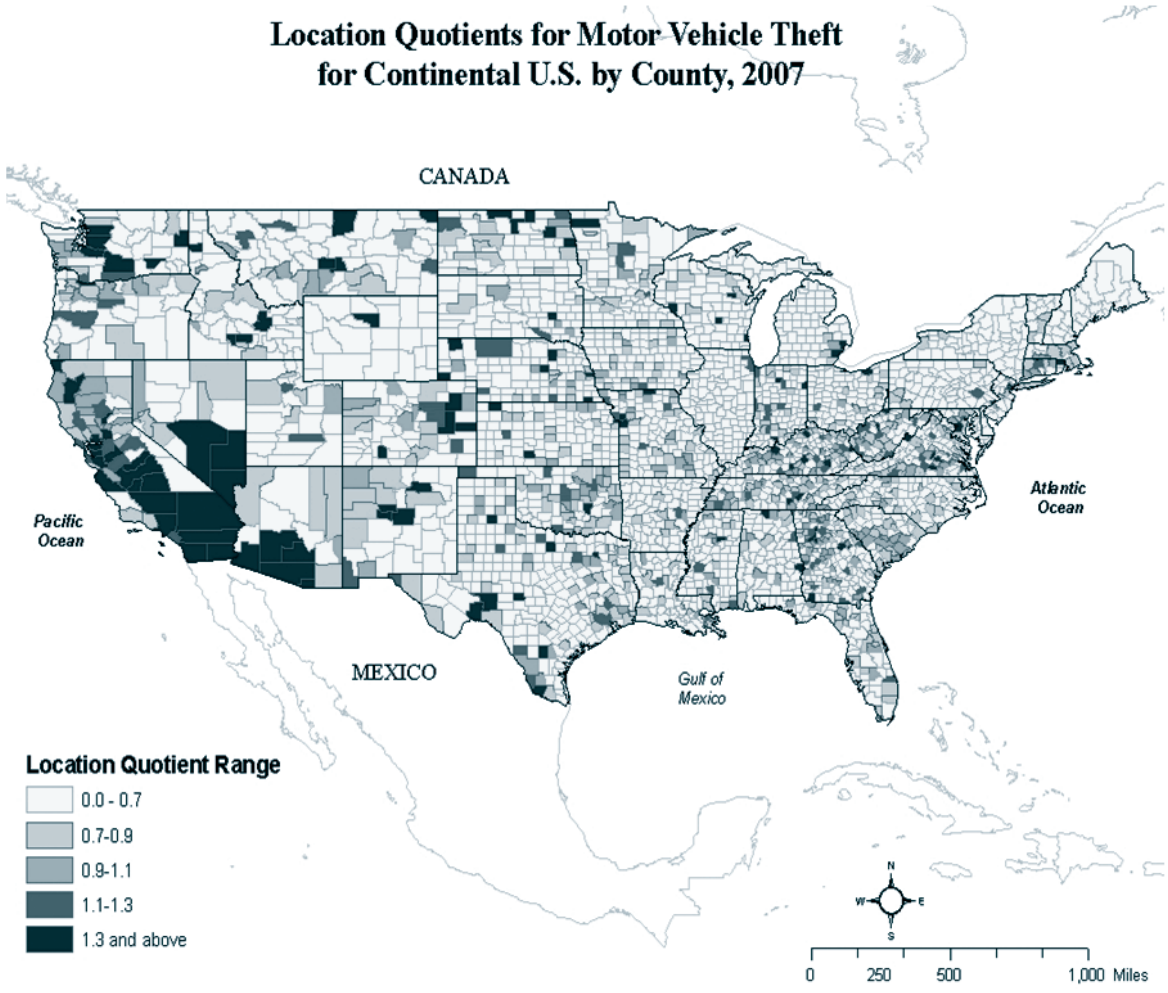
b= total number of all index crimes within the county

X= total number of motor vehicle thefts within the state where the county is located

Y= total number of all index crimes within that state

A CLQ value of 1.00 indicates an area has a typical representation of that crime compared to all other crimes. CLQ s over 1.00 indicate overrepresentation of a particular crime, while CLQ values under 1.00 signify underrepresentation.

The map shows that theft for export is prevalent near heavily-trafficked borders and ports in the United States.



What has been done to prevent theft for export?

Anything that makes it harder to steal a car will slow down the work of organized car theft rings, especially of the less sophisticated operators. Over the years, a wide variety of measures have been introduced to increase the risks or difficulty of car theft, including improvements to vehicle security, parking facilities, and vehicle documentation procedures. (In recent years, very promising reductions in theft have been reported for vehicles fitted with electronic immobilizers at manufacture—which is now a requirement for all new vehicles in the European Union, Canada, and Australia, but not yet in the United States.) In addition, some other measures specifically intended to reduce theft for export have been introduced, such as:

- The United States has developed a model bilateral agreement for the repatriation of stolen vehicles and has signed agreements with numerous countries in Latin America. U.S. agents have provided training to customs officials in these countries in ways to identify stolen cars.
- The National Insurance Crime Bureau has assisted these efforts by stationing officials in Mexico and other South American countries to assist the process of repatriation.
- U.S. Customs is field testing portable, hand-held computer scanners that will give inspectors in the field instant access to VIN information, as well as identify vehicles previously presented for export.
- X-ray machines that can detect vehicles concealed in containers are increasingly being deployed at major U.S. sea ports.
- Many local programs encourage citizens to participate in vehicle theft prevention. For example, a program implemented by the McAllen (Texas) P.D., "Citizens Against Auto Theft," involved placing colored decals on windows of automobiles. This alerted law enforcement officials that the car is not to be driven during certain hours of the day or driven into Mexico.

What can your agency do?

Should your analyses suggest that a theft for export ring is operating in your jurisdiction, your agency could implement a program such as that developed by McAllen P.D. Publicizing the problem can be another option. By analyzing your vehicle theft records you can determine which makes and models are at most risk, and the public information campaigns can be geared toward encouraging owners of these vehicles to better secure their cars.

READ MORE:

Nancy Plouffe and Rana Sampson. 2004. "Auto Theft and Theft from Autos in Parking Lots in Chula Vista, CA." In *Understanding and Preventing Car Theft*, ed., Michael G. Maxfield and Ronald V. Clarke. Vol. 17 of *Crime Prevention Studies*. Monsey, New York: Criminal Justice Press.

Gohar Petrossian and Ronald V. Clarke. 2012. *Export of Stolen Vehicles Across Land Borders.* Problem-Oriented Guides for Police. Problem-Specific Guides Series, No. 63. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

43 CLANDESTINE METHAMPHETAMINE LABS

METHAMPHETAMINE IS SUPPLIED BY TWO MAIN TYPES OF NETWORKS: (1) large, highly organized groups involved in trafficking illicit drugs, and (2) smaller, less organized groups of individuals typically involved in methamphetamine use.

The laboratories that produce methamphetamine have changed over time. There are now three main types of clandestine operations in the United States, which vary in organization, size, and production capacity: (1) super labs, (2) mom-and-pop labs, and (3) shake-and-bake or one pot labs. Shake-and-bake labs are the newest and most common type of production method. The shake-and-bake method can produce methamphetamine in about 30 minutes in a plastic bottle.

Clandestine laboratories today are primarily ephedrine and pseudoephedrine based. Most local laboratories in the United States are run by small networks of methamphetamine users and low-level dealers. Group members may coordinate efforts to acquire necessary supplies and chemicals. Restricted precursor chemicals may be obtained by "smurfing," whereby numerous individuals visit multiple retail outlets to make pseudoephedrine purchases. Group members also recruit others to purchase pseudoephedrine. Smurfing activities are increasing and evolving to include the illicit acquisition of bulk quantities of pseudoephedrine.

Clandestine laboratories are hazardous, toxic, and volatile. They are located in a variety of settings including homes, motel rooms, or vehicles. Smaller laboratories are portable and more difficult to detect. While laboratories were traditionally located in specific regions and in rural communities, they are now being found in cities across the United States. According to the DEA, 118,940 clandestine laboratories have been seized in the United States since 2004. Given that law enforcement detects a small percentage of labs, the true number is unknown.

Who is involved and how are they organized?

The groups involved in producing methamphetamine in clandestine laboratories continue to change as the problem evolves. Groups adapt to control efforts and may alter the way they communicate, acquire chemicals and supplies, and produce methamphetamine.

A successful prosecution

A federal prosecution in U.S. District court resulted in the conviction of 13 persons for conspiracy to manufacture methamphetamine. The defendants were charged with collecting chemicals needed to produce methamphetamine from multiple states for production purposes. The group was involved with producing methamphetamine in multiple locations including the home of a 60-year-old defendant. Sentences ranged from 3 years to 20 years.

Source: Todd South. 2012. 13-Person Meth Case Ends with Sentencing. *Chattanooga Times Free Press*, June 23.

Groups may be small (2–4 people) and loosely organized, or larger with more organization. They may be headed by independent operators or in conjunction with criminal gangs. Members may be recruited for specific roles related to manufacturing, including:

- Gathering supplies
- Purchasing precursor chemicals
- Recruiting others to purchase precursors
- Assisting with production
- Distributing methamphetamine

Cash or drugs may be exchanged for assistance. While local production is dominated by small and transient groups, larger, more organized groups have recently become involved in production in California.

Meth supply: at every step, offenders adapt, markets shift, and supply continues

The U.S. methamphetamine supply serves as an example of the challenges of responding to complex and evolving crime problems. Despite decades of attempts to control the supply of methamphetamine, clandestine production and trafficking continues and methamphetamine is widely available. Local manufacturers have continually adapted to control efforts by discovering alternative methods of production. Reductions in local supply are regularly offset by increases in production and trafficking from Mexico. There is need to develop a better understanding of the processes that underlie offender adaptation and offending evolution at local, national, and international levels.

Factors contributing to clandestine manufacturing

- Continuing demand for methamphetamine
- Profitability
- Increased use of smurfing to acquire bulk quantities of pseudoephedrine
- Retail outlets that sell pseudoephedrine products without questioning suspicious purchases
- Continuous adaptations in manufacturing production processes

What has been done nationally to address the problem?

In 2005, the U.S. Government passed the U.S.A. Patriot Improvement and Reauthorization Act. This legislation restricted retail access to pseudoephedrine, placed limitations on the purchase quantities, enhanced penalties for offenders, and increased regulations for distributors. Individual states have enacted various laws aimed at restricting access to precursors, criminalizing manufacturing-related activities, and increasing punishments. In 2006, Oregon became the first state in the United States to require a prescription for pseudoephedrine.

What can you do?

Conduct an in-depth analysis of the methamphetamine problem. Assess each dimension of the broader problem (i.e., use, trafficking, and manufacturing).

Data on drug treatment admissions are available from Substance Abuse and Mental Health Services Administration on the Treatment Episode Data Set (TEDS) website. Data on arrests, convictions, and sentences of criminal offenders can be obtained from criminal justice agencies.

Determine whether methamphetamine is being manufactured locally, imported, or both. Identify how much of the methamphetamine on the streets is being produced locally versus being trafficked in from out of state or out of the country.

If local production is occurring, gather information on the following:

- Type(s) of production processes being utilized
- Type(s) of laboratories producing methamphetamine
- The main ingredients being used
- Where offenders are obtaining ingredients and supplies
- How are offenders are obtaining precursor chemicals both legally and illicitly

Create a record of clandestine lab seizures and analyze this data to identify trends in production at the local level.

Review logs of local pseudoephedrine sales for suspicious patterns of purchases and to determine if certain retail outlets are selling disproportionately high rates of pseudoephedrine.

Look for information everywhere. You may need to talk to law enforcement officers, review police reports, and discuss the issue with community members who may have special knowledge about the problem. This could include pharmacists, persons who work in farming communities where anhydrous ammonia is

available, and personnel employed at stores where other chemicals and supplies needed to manufacture methamphetamine are sold. Understanding which communities have high rates of methamphetamine consumption and how many individuals with previous involvement in manufacturing or related activities reside in the area will be helpful.

What can your agency do?

Gather intelligence on clandestine manufacturing from confidential informants and by sharing information with other law enforcement agencies in the area. Intelligence sharing is essential for obtaining information on suspicious patterns of activity that may cross jurisdictional boundaries.

Coordinate investigations with other law enforcement agencies.

Conduct undercover surveillance operations in retail outlets that sell pseudoephedrine in communities known to have high rates of methamphetamine use or that sell disproportionately high rates of pseudoephedrine products.

READ MORE:

Rashi Shukla, Jordan Crump, and Emelia Chrisco. 2012. An Evolving Problem: Methamphetamine Production and Trafficking in the United States. *International Journal of Drug Policy* 23:426–435.

Michael Scott and Kelly Dedel. 2006. *Clandestine Methamphetamine Labs*, 2nd Edition. Problem-Oriented Guides for Police. Problem-Specific Guides Series, No 16. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

44 CRUISING

ON WEEKEND EVENINGS, CITY CENTER PUBS IN BRITAIN ARE CROWDED BY YOUNG MEN AND WOMEN who are there to see and to be seen. In Mediterranean countries, especially on warm evenings, the same demographic groups fill the cafes and stroll on the piazza. In North America, late on fine evenings in spring and summer, young people, sometimes in the hundreds or even thousands, "cruise" the local strip in their automobiles, driving slowly, bumper-to-bumper.

Cruising is a means for young men to show off their cars, to compare them with other people's cars, to find racing competitors, to socialize, and to impress young women. In many communities across the country cruising is considered a pastime and a rite of passage, encouraged and glorified by movies like *American Graffiti* and *The Hollywood Knights*. According to a 2002 survey conducted by Teenage Research Unlimited, 60 percent of teenagers spent at least four hours a week cruising in a car. Another survey of young cruisers between the ages of 19 to 21 revealed that 80 percent of the time their parents knew and approved of their cruising in the downtown area. It seems that parents preferred the downtown area because of the supervision of patrol officers.

On the other hand, cruising can bring many problems in its wake. It snarls traffic, it can prevent access by emergency vehicles, and it can bring commerce to a halt. It may also bring problems of litter, urinating in public, underage drinking, vandalism, and worse. It is these consequences of cruising that the police need to address, not the otherwise harmless behavior of ordinary young men and women looking for social interaction.

Cruising is generally confined to downtown areas, though in coastal communities it is common along beaches. Cruisers drive a wide range of cars that include classic cars (whose drivers tend to be older and cruise to show off their expensively restored vehicles); pickup trucks (on huge wheels and jacked up suspensions); mini-trucks, muscle cars, low riders (whose chassis ride just inches off the ground); imported customized European cars; and Harley-Davidson motorcycles.

Factors contributing to cruising

- Automobile ownership and accessibility to teenagers
- The need to be socially accepted
- The desire to show off vehicles
- Many cruisers are too young to go to bars or other places where they can socialize with friends and the opposite sex
- An unsupervised environment where youth can express themselves

What has been done nationally to address the problem?

The Salt Lake City Council in Utah passed an anti-cruising ordinance prohibiting cars from driving repeatedly (defined as driving three or more times in the same direction) past a "mobile traffic-control point" between 11:00 PM and 4:00 AM in an area identified by police as being congested.

Police in Lakewood, Colorado, employed a strategy of "modified diversion" by closing off known cruising locations during 8:00 PM and 2:00 AM, the time period when cruising was most likely to occur, while minimizing its impact on legitimate traffic and businesses in these areas. The closing was announced through a news media campaign, which began a week in advance of the operation. This effort resulted in complete elimination of the cruising problem in Lakewood.

When the enforcement strategies and the use of barriers failed to solve the cruising problem in Arlington, Texas, the police formed a "cruising committee" by forging partnerships with representatives of the city council, local business owners, and the parks, recreation, and transport

Santa Ana Cruising Abatement Project

The Santa Ana Police Department in California was faced with a serious cruising problem. On Sunday evenings, approximately 1,000 cruisers drove along a major thoroughfare to gather and socialize. The cruising night resembled a large street party, where loud music and alcohol consumption were common, creating problems for nearby residents. Merchants complained that traffic gridlock kept regular customers from their businesses, and many businesses closed early to avoid subjecting their customers to intimidation from the cruisers. The police department responded to the problem by focusing on two weaknesses of the cruisers: (a) they lacked knowledge of anti-cruising laws, and (b) many of the cruisers drove vehicles belonging to their parents or others. The police set up a control point, where information about each vehicle was quickly made available through specially-designed computer software. At the same time, officers distributed an anti-cruising warning to each vehicle moving through the check point. The contact with the drivers was intended to reduce anonymity. Follow-up letters were then mailed to the registered owners of the vehicles advising them that the car had been identified as cruising, an illegal activity in Santa Ana. The letter was intended to warn cruisers who drove their own vehicles, and to inform parents whose cars were being used by their children. The letter warned that anyone who returned to the area to cruise would be subject to arrest. The check points, as well as roadblocks leading to these points were eliminated after several weeks. The project proved to be successful in reducing cruising and related problems in the area.

departments, which leased a downtown parking lot on Friday and Saturday nights and opened it to the cruisers. It was staffed by police, equipped with portable restrooms and cleaned up the next morning. The approach proved highly effective, as it not only solved the cruising problem, but also helped reduce other related problems. Up to 1,000 cars continued to cruise there during an evening, but local people had no longer to endure litter, vandalism, noise, and other public order problems.

What can you do?

If cruising is a problem in your jurisdiction, you can gather information about the characteristics of the cruisers and determine if they are engaged in problematic behaviors that stem from cruising.

Map the locations as well as the days of the week and time of the day when cruising is most likely to occur. Gather as much information as possible about these temporal and geographic patterns. Think about possible interventions you could advise based on successful actions in other jurisdictions. Help your department find an alternative location for cruising that would lead to fewer problems but which would still be used by the young people.

What can your agency do?

Find out more about cruising by surveying local residents and businesses. Engage them in efforts to address the problem.

Once the cruising areas and times are identified, your department may increase enforcement in these areas during these designated times. Leaving aside arrests or citations for cruising, the presence of the police may reduce other related problems in the area.

Find an alternative cruising area that appeals to the cruisers and does not conflict with the area businesses or the residents. This area can be controlled by the officers to ensure security.

READ MORE:

Boise Police Department Planning Unit. 1990. *Downtown 'Cruising' In Major U.S. Cities and One City's Response to the Problem*. Boise, Idaho: Police Department.

Ron W. Glensor and Kenneth J. Peak. 2005. *Cruising.* Problem-Oriented Guides for Police. Problem-Specific Guides Series, No. 29. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

45 ILLEGAL STREET RACING

SOME STREET RACERS ARE WELL-OFF STUDENTS, MOTOR SPORT ENTHUSIASTS, AND EVEN MIDDLE-AGED BUSINESSMEN, but the three main groups are:

1. Young working-class males aged 16–25, some of whom attend trade schools or technical colleges, but many may have struggled in school and engaged in other delinquency. Most members of this group quite soon grow out of street racing.
2. Older white males (aged 25–40) who race older American-made "muscle" cars, such as Corvettes, Camaros, and Mustangs.
3. A wide age range of Asian and Hispanic males who generally drive later-model Japanese cars, such as Hondas, Acuras, Mitsubishis, and Nissans. This group currently dominates the street racing scene.

Races test a driver's skill and the capabilities of the vehicles involved. They often take place at night in largely deserted streets or industrial areas. Street racing is not illegal in some jurisdictions, but it tends to be associated with illegal activities, including auto theft, impaired driving, illegal vehicle modification, illicit gambling, gang related activity, trespassing, vandalism, and littering. Fatal crashes linked to street racing have been found to involve both alcohol and excessive speed and often occur on urban surface streets.

How are they organized?

Street races are often publicized by word of mouth and may be attended by dozens of racers and hundreds of spectators. During the race, lookouts keep watch for police using cell phones, police scanners, and walkie-talkies. Some groups may use police tape and false signs to block traffic for the duration of the race, or use rolling road-blocks to stage a race on a large highway.

In some cases, illegal racers may operate websites to post announcements about race locations and about expected police activity. Some websites provide information about the previous night's races, including ratings of police presence and crowd size. They may carry a link to the local police agency so the curious can see if a warrant has been issued for their arrest.

Forms of street racing

- **Drag racing** involves a contest between two vehicles that compete to cross a set finish line. In some jurisdictions drag racing is classified as a Class B misdemeanor. According to the National Highway Traffic Safety Administration, about 135 people die each year in street drag racing accidents.
- **Hat Racing**, also called "cannonball run" or "kamikaze," involves point-to-point races where drivers put money into a hat for the winner. These races are often long distance, sometimes from city to city.
- **Touge** or **Centipede** races, popularized in Japan, occur on mountain passes or around normal traffic, one car at a time, or chase-style with a convoy of vehicles.
- **Burnouts** involve spinning rear tires at high revolutions to produce smoke trails.
- **Donuts** involve accelerating a vehicle with full steering-wheel lock.
- **Rolling Road Blockages** or **Blockades** comprise vehicles traveling slowly in convoy on major highways to prevent other vehicles from passing, so that vehicles ahead can engage in racing.
- **Drifting** involves accelerating around a corner to cause the rear of the vehicle to slide out and the tires to slip on the roadway.

Factors contributing to illegal street racing

- Availability of vehicles to young drivers
- Lack of legitimate venues for racing and the existence of suitable abandoned or unsupervised locations
- The need for thrills and excitement, as well as the expression of masculinity
- Street racers' need for social status
- Existence of street racing movies and video clips on the Internet that can be imitated
- Lack of ordinances prohibiting street racing
- The support of spectators

Examples of what has been done to address the problem

Kent (Washington) Police Department partnered with other law enforcement agencies, private property owners, local businesses, and the insurance industry to develop an enforcement plan known as CRASH (Curb Racing and Achieve Safer Highways). Police conducted surveillance of racing locations to identify races in progress and, once identified, uniformed officers closed off exits from the locations to prevent participants from dispersing. Drivers operating vehicles in violation of the traffic code were cited or arrested. Vehicles operated by drivers whose licenses had been suspended or revoked were impounded.

Some jurisdictions have installed speed bumps, concrete barricades, and freeway billboards to control or inform racers. To discourage spectators, parking can be prohibited on public properties and roadways during prime racing hours in the race area.

Australia and New Zealand have addressed street racing through legislation directed at such activities as dangerous or careless driving, causing unnecessary noise and smoke as a result of "burnouts," and causing deliberate loss of traction doing "donuts." Drivers who take part in these behaviors can have their operator's license suspended and face the immediate impounding of their vehicles for periods of 48 hours to three months. Subsequent offenses may result in forfeiture of vehicles.

San Diego has acted to curb its street racing problem

- By passing a "spectator ordinance" making it an offense to attend an illegal street-racing event, and a "forfeiture ordinance" permitting the police to seize vehicles used in races.
- By establishing "DragNet," a special unit to deal with the races. Officers infiltrate the illegal street-racing group to videotape races and use driver and license plate information to arrest the offenders.
- By designating the Qualcomm Stadium as a location for races, held on Friday nights.

Annual street races are permitted in cities in Canada (Toronto and Montreal) and Australia (Sydney, Adelaide, and Melbourne). This allows racers to experience the fun, camaraderie, and excitement they seek within a safer racing environment. Police can either work with existing national programs (Beat the Heat, Racers Against Street Racing, the National Hot Rod Association) that encourage safe, on-track racing, or implement their own local program.

What can you do?

Determine whether you have an illegal street racing problem in your jurisdiction. If so, study the characteristics of the racers, the kinds of activities they are involved in, and who their supporters are.

Inform yourself about street racing through websites, such as Streetracing.com, RaceLegal.com and NHRA.com. These websites provide racing and club news, articles, calendars, chat rooms, auctions, and message boards for many cities and states. The NHRA website focuses on encouraging legal racing, and attempts to educate users about related laws and statistics, such as number of illegal racers who were recently killed, injured, cited, arrested, or who had vehicles seized or licenses revoked.

Through the chat rooms provided by these websites, you might be able to warn your department about upcoming races in your jurisdiction. Using network analysis you might be able to build up a picture of the major players involved in the groups. You can also infiltrate and monitor social networking sites to remain informed about upcoming street racing events.

What can your agency do?

Inform parents about the dangers of street racing so they can discourage their teenagers from participating. Ask parents to inform police about possible future street races that they hear about from their teenagers.

Place roadblocks leading to locations where street racing is most likely to occur. These locations should be supervised during prime hours for street racing.

Study solutions adopted elsewhere—in particular whether legal venues for street racing can be created, which can be more easily monitored and controlled.

READ MORE:

Ron Glensor and Kenneth Peak. 2004. *Street Racing. Problem-Oriented Guides for Police*. Problem-Specific Guides Series, No. 28.Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

46 SPRING BREAKS

THE ROOTS OF THE "SPRING BREAK" TRADITION CAN BE TRACED BACK TO THE FIRST COLLEGE SWIM FORUM, held in Fort Lauderdale in 1938. Since then, "spring break" has become a rite of passage among young college students across North America. It gained prominence through such films as *Where the Boys Are* (1960) and *Spring Break* (1983) and has been further popularized through MTV's "Spring Break" and the video series "Girls Gone Wild." Also, an industry of promoters of spring break trips advertise on college campuses.

Approximately half a million students each year vacation at popular spring break destinations. These include South Padre Island, Texas; Palm Springs, California; Fort Lauderdale, Daytona Beach, Pensecola, and Panama City Beach, Florida; and Lake Havasu, Arizona. Recent years have also seen increased numbers of students taking spring breaks in foreign destinations that include Cancun, Matzalan, and Acapulco, Mexico; as well as the Bahamas and Jamaica. Younger students may go to Mexico because of the lower legal drinking age of 18.

Students on spring break often engage in heavy alcohol consumption/binge drinking and some recreational drug use. One study at Panama City Beach found that an average male student had 18 drinks during the previous day, while an average female consumed 10 drinks. Binge drinking is higher among fraternity or sorority members, and among those who lead a party-centered lifestyle.

Students vacationing in groups are more likely to engage in pronounced substance abuse and in promiscuous sexual activity, which places them at a high risk of contracting sexually transmitted diseases. They might also engage in brawling, trespassing on waterfront properties, tearing down fences, and public urination.

Contributing factors

- A wish to get away from college and "winter blues"
- Opportunities afforded for easy socializing and new romantic involvements
- The anonymity afforded by spring breaks (at least in the minds of the students)
- The feeling of being a different person on holiday and, therefore, open to experiment with casual sex, drugs, and excessive drinking
- Commercial trip organizers encourage and facilitate visiting spring break destinations
- Commercial enterprises at resort destinations cater to spring break revelers

Examples of measures to curtail irresponsible behavior during spring breaks

Beachfront resorts in Destin, Florida, cooperated with local police by imposing a late night curfew on their private beaches during spring break. Several hotels floodlit their beaches to prevent trespassing, drinking, and other related behavior. In addition, police patrolled several miles of beach, concentrating where large crowds of teenagers might gather, stopping and making underage drinkers pour their beer onto the sand.

Police cameras were installed to monitor beaches and popular restaurants and bars in Sunset Beach, California. The police also increased uniformed and plainclothes patrols, set up DUI checkpoints, and enforced parking and traffic violations.

Residents of Pacific Beach, California, prevented a planned "pub crawl" by using a law prohibiting alcohol sales to intoxicated patrons. The organizers of the event pulled out after they received notice from the district's council member and the Department of Alcoholic Beverage Control, threatening to close down participating bars for 15 days should anyone be served alcohol who was already intoxicated.

Louisiana State University (LSU) held a "Smart & Safe Spring Break Festival" for students before spring break to provide them with abstinence information and information on health and safety issues. The university's police department deployed its motorcycle unit and K-9 bomb-sniffing dogs, performed intoxication demonstrations, and offered sign-ups for LSU's emergency text messaging and other services.

Inducements offered by bars to students at spring break

"all-you-can-drink" (generally a purchase of a meal is followed by unlimited beer and other alcoholic beverages)

"twofers" (offering two or more drinks for the price of one)

"coin nights" (involves flipping a coin, where the winner gets a free drink)

"ladies nights" (female customers are offered special discounts)

"bladder bursts" (promise of an enjoyable night—generally involving alcohol—where you don't want to miss anything by going to the bathroom)

"bar crawls" or **"bar hopping"** (going from one bar to another)

Operation Blitz' Em and Operation Spring Break in the Gold Coast, Australia, targeted speeding and drunk drivers during spring break. Random breath testing, unmarked cars, and speed cameras were deployed at hot spots and during high-risk times. Extra officers from the state traffic taskforce assisted local police.

What can you do?

Gather intelligence about the locations most likely to be visited by the students. Determine if these are mainly outdoors or indoors, and think of specific measures to address the issue based on the location type.

Identify bars with lenient underage drinking practices that might attract underage students during spring break.

Survey bars, restaurants, and motels that offer inducements to students at spring break and inform the owners and managers about possible dangers associated with these practices.

While students might bring their own drugs with them, there might be local supply sources that you need to identify and alert your police department about.

What can your agency do?

Control alcohol distribution by enforcing local ordinances against restaurant and bar owners, as well as alcohol vendors. Limit the number of liquor outlets during the spring break period. Working with vendors and bar owners to identify fake IDs can also help control underage drinking.

Establish police presence/visibility at and around locations identified as hot spots and monitor student behavior to ensure compliance with the law. The presence of uniformed police officers can help bring the situation under control by monitoring drinking, public nudity, drug use, and other related behaviors.

Partner with the local media to encourage and influence responsible student behavior while on spring break. Encourage the media to practice more socially responsible marketing efforts to promote healthier and safer spring break activities.

Local initiatives can involve offering financial rewards to individual "bounties" who report bars that serve intoxicated patrons, as well as underage students.

Provide free false-identification training for restaurant and bar employees to help reduce illegal sales to underage students.

Laws promoting responsible bar policies in certain states require servers, managers, and owners of restaurants and bars to attend a state-approved course every five years that includes information about alcohol's effect on the body, drunk-driving laws, effective server intervention techniques, and related topics. Similar programs can be implemented by your police department.

Warn potential offenders by posting signs specifying the ordinances (such as "nudity is prohibited in a public area") and that failure to follow these may lead to arrest.

Roads near the locations where spring breakers gather can be monitored by the police to discourage students from driving under the influence. Meanwhile, free shuttle services can be offered by the hotels to encourage safe travel. Consider closing certain streets.

Encourage universities to enforce disciplinary measures against students found to have engaged in binge drinking or drug use.

47 POLITICAL DEMONSTRATIONS

SINCE THE DEMONSTRATIONS AT THE 1999 MEETINGS OF THE WORLD TRADE ORGANIZATION IN SEATTLE, American police have increasingly been confronted with the problem of dealing with political protesters. There are four main kinds of political demonstrations:

1. **Marches**—proceeding from one location to another, such as the May 1, 2006, marches across the United States protesting the proposed immigration laws.
2. **Rallies**—gathering at a location to hear speakers or musicians, such as the November 3, 2007, student rally in Washington, D.C., to address issues on climate change and global warming.
3. **Picketing**—targeting a specific facility or building, such as the September 15, 2002, pickets at the Ukrainian Embassy in Washington, D.C., by the members of the Forum of Ukrainian Students of America, to honor Ukrainian journalists, and civil and political activists who had died after Ukrainian independence.
4. **Sit-ins/sit-downs**—nonviolent occupation of a building or public place and refusal to leave until demands have been met or an agreement reached. Sit-ins were widespread in the 1960s by African American college students across the United States campaigning to end racial segregation. A recent example is Occupy Wall Street in 2011.

Political demonstrations are generally peaceful, but violence and vandalism may occur, sometimes deliberately provoked by organizations such as the "Black Bloc", which exploit demonstrations to further their own political ends. Violent demonstrations are a particular problem for local police, as the inability to handle them properly may have serious implications for police-community relations.

The Black Bloc

- The Black Block is an international anarchist organization (also known as the Revolutionary Anti-Capitalist Bloc) started in Germany in 1987, which soon spread to the United States and Canada. Its unofficial center in America is Eugene, Oregon.
- It is best known for its violent demonstrations in Seattle in 1999 against the World Trade Organization. Other demonstrations include the 2001 demonstration at the Summit of the Americas in Quebec City, Canada; and the demonstrations in July 2001 in Genoa, Italy, at the General Assembly Summit. In recent years the Black Bloc has targeted such large American corporations as Banana Republic, Gap, Levi's, McDonald's, Old Navy, and Starbucks.
- Black Bloc protesters arrive at demonstrations dressed in three layers. The outermost layer is regular clothes worn at the beginning of the demonstration before the Black Bloc tactics are activated. The middle layer is all black clothing (and a black mask worn when the members are given the signal to engage in confrontation). The last layer involves regular clothes to escape from police.
- The Black Bloc often deploys in tight formations (in black) when confronting the police, or intimidating other groups.

Public-Order Policing

Aversion to disruption is used when police want to prevent demonstrations from interfering with the normal functioning of the city, for example, by denying the right to march on city streets and confining marches to sidewalks or to restricted areas and times of the day.

Controlling access involves the use of concrete or metal barriers to separate the protesters from the public and to control access through limited entry points.

Divide and conquer allows the police to have access to almost all parts of the demonstration by subdividing the crowds into smaller groups by the use of interlocking metal "french barriers." This makes it difficult for demonstrators to circulate freely, while allowing effective control of the crowds.

Shock and awe involves deploying a very large number of police officers to deter outbreaks of violence or other unlawful behavior. Police might employ less-than-lethal weapons to deal with protestors and commonly arrest leaders who promote violence or are themselves engaged in violence.

Zero tolerance involves the rigorous enforcement of legal statutes during demonstrations. Failure to comply with the provisions of a permit may be met by police in full riot gear shutting down sound systems and mass arrests of protesters at the expiration time of a permit to demonstrate.

Non-confrontational crowd management involves supporting the legitimate aims of demonstrators while avoiding confrontation that may alienate the crowd as a whole. Unruly or violent crowd members are carefully identified and removed by the police.

Dialogue policing is an extension of non-confrontational crowd management (Step 25). It aids communication between demonstrators and police commanders through specially-trained police officers in the crowd. This encourages self-policing among demonstrators, facilitates legitimate expression of freedom of speech and assembly, and prevents miscommunication between the police and demonstrators.

Source: Madensen and Knutsson 2010.

In most cases, your department will be called on to deal with smaller demonstrations that involve picketing or sit-ins. Sit-ins are common in administrative or congressional offices. For example, constituents may stage a sit-in in the office of their representative to protest his or her voting record. Sit-ins are especially common outside abortion and Planned Parenthood clinics.

Picketing is more common among employees who are dissatisfied with wages, long hours, working conditions, and related issues. Picketing will also sometimes be undertaken to block access to government buildings and corporations. Pickets are generally non-violent, but the police department's inability to handle the protests properly may lead to violent confrontations.

What can you do?

Stay informed about current political issues that may possibly become reasons for political demonstrations. Gather information on groups in your jurisdiction who are most likely to act on these issues. Study the backgrounds of these groups and determine their overall demonstration "style."

Political protesters use the Internet to voice their concerns, recruit new members, and to announce the locations and times where protests are to be held. Therefore, you can monitor the websites operated by these groups to gain understanding about their networks and activities. Some of these websites include:

- Infoshop www.infoshop.org
- Spunk Press www.spunk.org
- Anarchy Archives www.anarchyarchives.org
- Liberty for the People http://flag.blackened.net/liberty/liberty.html
- Noam Chomsky Archive www.zmag.org/chomsky/index.cfm
- Independent Media Center www.indymedia.org

Identify possible locations/targets, such as government buildings, corporate headquarters, financial institutions, and other symbolic buildings. Decide what strategies can be implemented and how these should differ from site to site and from group to group.

Gather information about strategies used by other police departments to handle similar situations. Determine if these strategies suit your police department's operational goals and whether any of the strategies would undermine community relations.

What can your agency do?

Police departments throughout the country have used a variety of approaches to control political demonstrators and other crowds (see *Public-Order Policing* on page 132). Which of these your department adopts in any particular situation may depend partly on its philosophy, but also on the groups they are dealing with.

Aggressive police intervention strategies may lead to violence in otherwise peaceful demonstrations, therefore, cooperative intervention is vital in controlling demonstrators. Keep in mind also, that advance changes to the setting can reduce damage. These include: blocking off streets and particular buildings; removing items such as building rubble that can be used as weapons; and temporary removal of street furniture such as trash cans that can be burned.

Lastly, your department can use electronic surveillance technologies to provide real-time information on demonstrations and quickly send in more police should the crowd turn violent.

READ MORE:

Tamara Madensen and Johannes Knutsson, eds. 2010. *Preventing Crowd Violence.* Vol. 26 of *Crime Prevention Studies*. Boulder, Colorado: Lynne Rienner Publishers, Inc.

48 STUDENT PARTY RIOTS

PARTIES ARE ALMOST SYNONYMOUS WITH STUDENT LIFE, BUT IF UNREGULATED, THEY CAN RESULT IN BEHAVIORS requiring police intervention. These behaviors include underage drinking, binge drinking, drunk driving, sexual misconduct, fighting, sexual assaults, drugs, violence, noise, litter, and vandalism.

Studies of blood alcohol concentration levels have found that students at fraternity parties get significantly more intoxicated than those at other parties. In one large study of 140 colleges, 44 percent of the students surveyed reported binge drinking and 19 percent were frequent binge drinkers—those who binged three or more times in two weeks.

Common features of student parties

- The students present are mostly young adults—some may be under 21
- Alcohol is generally consumed in large amounts and drugs may also be used
- The parties begin late at night and may continue into the early morning
- Males are most often responsible for fighting or destructive behavior
- The parties may result in noise complaints from local residents
- Drunk driving is common
- Students may engage in unplanned or unprotected sexual activity
- Other young adults not associated with the college may also gather at the parties
- Students may get into trouble with campus or local police

The "life cycle" of student parties

Madensen and Eck report that the larger parties have a "life cycle" of five stages, around which police should organize their responses (see Table 18 on page 135).

Examples of what has been done to address the problem

Michigan State University used campaigns designed to challenge the attitudes and expectations of students regarding "celebration drinking." The campaigns made use of student and local newspapers and incorporated the distribution of flyers in campuses, student residences, and at Greek Life fairs.

The Robert Wood Johnson Foundation funded "A Matter of Degree" (AMOD) to reduce high-risk drinking among college students, which resulted in significant changes in drinking behaviors and decreases in related drunk driving, wild party complaints, and charges of maintaining a disorderly house.

Some police departments offer the "Adopt-the-Cop" program. This makes a police officer available at student gatherings to serve as a mentor and advisor to ensure compliance with city and college requirements for student parties.

In Minnesota, the Winona City Council passed an ordinance to control and track keg distribution. Anyone purchasing two or more half-barrels of beer in a residentially zoned area was required to obtain council approval, and liquor retailers were required to keep detailed records of barrels sold.

Rutgers University enforces good behavior at Greek parties through its Board of Control, which comprises fraternity and sorority students who check on parties in progress to ensure there is no vandalism, sexual misconduct, fighting, or other misbehavior. Local police train these students in how to handle violent situations, write up violations of school policy, and call the police in case of violence. Parties are limited to Friday and Saturday nights and require registration with the Fraternity Affairs Office and the local police department. The Board of Control checks out the party

Table 18. Five stages of large parties

STAGE	SUGGESTED RESPONSES
1. Initial Planning. Deciding to host a party, when and where; deciding whom to invite and how to invite them. Students are invited through flyers posted months in advance, word of mouth, or simple cues indicating that there will be a student party/gathering somewhere soon.	Create a multi-agency task force with other community stakeholders, most importantly with the college concerned. Require a permit for a party of more than a few friends. Assign police officers as advisors to hosts of gatherings.
2. Preassembly preparation. Obtaining alcohol and food by hosts or guests before the party.	Ask students to participate in "student patrols" by establishing "peer security" groups within the gathering. Monitor advertisements for gatherings.
3. Assembling process. Heading for the party. Students may drive, take a taxi or bus, or simply walk to the location.	Facilitate orderly gathering by providing transportation to the event. Establish a positive police presence, intended to reduce anonymity for police and students and enhance communication. Establish gathering perimeters in order to gain control of disturbances.
4. Assembled gathering. Having congregated, students talk, drink, and possibly engage in other behaviors associated with student parties.	Use alternative deployment methods, such as horses and bike patrols. Videotape the party to reduce anonymity. Develop a standard operating procedure in case of a disturbance.
5. Dispersal process. The party is over and students return to their dorms or apartments. Drunk driving may be a problem if students have reached the party in their own vehicles.	Provide transportation from the event to dorms or other centralized locations. Ask people to leave when the party is over.

Source: Madensen and Eck 2006.

three times a night, between the hours of 10:00 PM and 2:00 AM, where a checklist is completed about control measures such as checking IDs, using stamps or bracelets to identify guests, and keeping the noise down.

What can you do?

Study local college policies on controlling student parties and make contact with university administration should you need to find out more about these policies and how they are enforced.

Work closely with campus police or security to gather information on upcoming parties by monitoring student newspapers and student postings at college campuses.

Work with local student organizations to gather information about times of the day and days of the week parties are most likely to be held, how long they last, types of drinks consumed, how alcohol is obtained, whether drinking games are played, and any associated problematic behaviors.

Make contact with local college fraternities and sororities to find out more about the policies currently used to monitor and control Greek parties.

What can your agency do?

Discuss the alcohol policies effective on campus with local college administrators and suggest possible improvements should you find the college has problems effectively controlling student parties. Organize regular meetings/presentations on college campuses to discuss the dangers associated with irresponsible behavior at student parties.

Encourage colleges to give warnings and impose disciplinary actions against students who are engaged in disorderly conduct, violence, or other behaviors associated with student parties.

Form a partnership with student organizations and campus police/security to promote a safe party environment and responsible behavior at student parties. At the beginning of each academic year, discuss alcohol laws, off campus behavior, and other safety issues related to student parties with fraternity and sorority presidents.

Make clear to local bars, restaurants, and liquor outlets that sales to underage students will not be tolerated. Promote responsible beverage services, strengthen enforcement of drunk driving laws, and, where necessary, seek changes in local zoning ordinances to reduce the density of alcohol sales outlets.

Work with local rental property owners to require them to provide safe and secure apartments to students living off campus. Encourage them to call police in the event of problematic parties being held in their apartments.

READ MORE:

Tamara Madensen and John Eck. 2006. *Student Party Riots*. Problem-Oriented Guides for Police. Problem-Specific Guide Series, No. 39. Washington, D.C.: U.S. Department of Justice, Office of Community Oriented Policing Services.

About the Authors

John E. Eck

John Eck is a criminal justice professor at the University of Cincinnati, where he teaches police effectiveness, research methods, and crime prevention. His research has focused on the development of problem-oriented policing, police effectiveness, crime patterns, and crime prevention. Dr. Eck was a member of the National Academy of Science's Committee to Review Research on Police Policy and Practices. With Ronald Clarke, he authored *Crime Analysis for Problem-Solvers: In 60 Small Steps*. He is also the author of many publications on problem-oriented policing, crime mapping, and crime prevention, some written for the Center for Problem-Oriented Policing. Dr. Eck received his bachelor's and master's degrees from the University of Michigan, and his doctorate from the University of Maryland's Department of Criminology.

Ronald V. Clarke

Ronald Clarke is university professor at Rutgers University and associate director of the Center for Problem-Oriented Policing. He was previously head of the British government's criminological research department, where he had a significant role in the development of situational crime prevention and the British Crime Survey. Dr. Clarke is the founding editor of *Crime Prevention Studies*, and his publications include *Designing out Crime* (HMSO 1980), *The Reasoning Criminal* (Springer-Verlag 1986), *Situational Crime Prevention: Successful Case Studies* (Harrow and Heston 1997), *Superhighway Robbery: Preventing E-commerce Crime* (Willan Publishing 2003), *Outsmarting the Terrorists* (Praeger 2006), and with John Eck, *Become a Problem Solving Crime Analyst* (U.S. Department of Justice 2005). He was formerly chair of the selection committee for the annual Herman Goldstein Award for Excellence in Problem-Oriented Policing.

Gohar Petrossian

Gohar Petrossian is an assistant professor at John Jay College of Criminal Justice. She is the author of *Export of Stolen Vehicles across Land Borders* (Problem-Specific Guide No. 63, with Ronald V. Clarke), co-author of *Shoplifting (2nd Edition)* (Problem-Specific Guide No. 11, with Ronald V. Clarke), and scholarly articles published in *Journal of Experimental Criminology* and *Security Journal*. She holds a doctorate in criminal justice from the School of Criminal Justice, Rutgers University-Newark, and a master's in criminal law and procedure from John Jay College of Criminal Justice.

KNOWING HOW INTELLIGENCE ANALYSIS CAN HELP SOLVE PROBLEMS and how problem solving can improve the effectiveness of intelligence analysis will aid any police practitioner interested in reducing crime or disorder. *Intelligence Analysis for Problem Solvers* fuses aspects of intelligence analysis with Problem-Oriented Policing. It is focused on the analysis of intelligence and has been written for three groups in local policing agencies: (1) intelligence officers and analysts, (2) crime analysts who may be called upon to use intelligence information and, (3) police managers who supervise crime and intelligence analysts.

COPS
Community Oriented Policing Services
U.S. Department of Justice

U.S. Department of Justice
Office of Community Oriented Policing Services
145 N Street NE
Washington, DC 20530

To obtain details on COPS Office programs,
call the COPS Office Response Center at 800-421-6770.

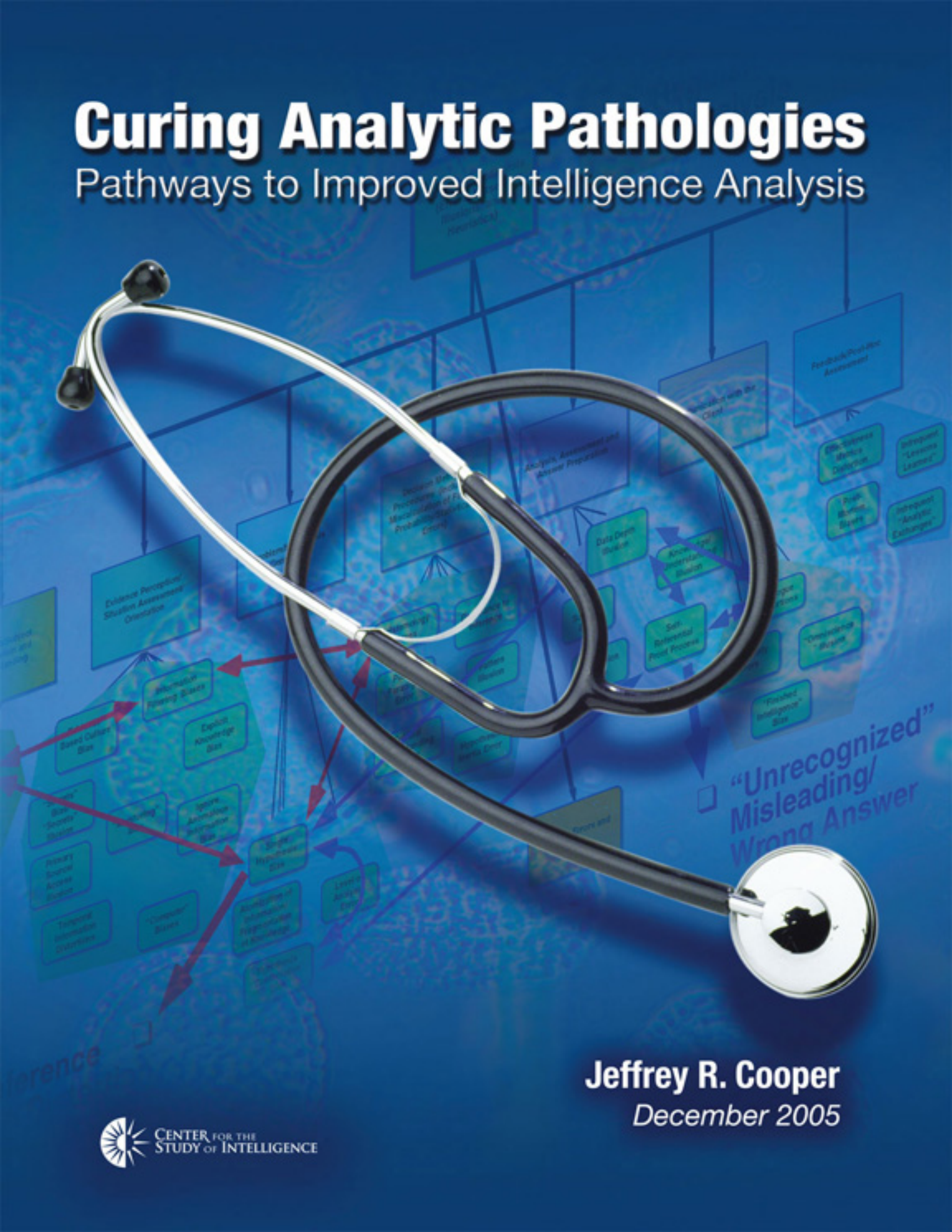
Visit COPS Online at **www.cops.usdoj.gov**.

ISBN: 978-1-935676-55-3
September 2013
e031313555

This Page Is Intentionally Left Blank

Curing Analytic Pathologies

Pathways to Improved Intelligence Analysis



Jeffrey R. Cooper

December 2005

Center for the Study of Intelligence

All statements of fact, opinion, or analysis expressed in this study are those of the author. They do not necessarily reflect official positions or views of the Central Intelligence Agency or any other US Government entity, past or present. Nothing in the contents should be construed as asserting or implying US Government endorsement of the study's factual statements and interpretations.

Curing Analytic Pathologies

The Center for the Study of Intelligence (CSI) was founded in 1974 in response to Director of Central Intelligence James Schlesinger's desire to create within CIA an organization that could "think through the functions of intelligence and bring the best intellects available to bear on intelligence problems." The Center, comprising professional historians and experienced practitioners, attempts to document lessons learned from past activities, explore the needs and expectations of intelligence consumers, and stimulate serious debate on current and future intelligence challenges.

In carrying out its mission, CSI publishes *Studies in Intelligence*, as well as books and monographs addressing historical, operational, doctrinal, and theoretical aspects of the intelligence profession. It also administers the CIA Museum and maintains the Agency's Historical Intelligence Collection.

Other works recently published by CSI include:

Analytic Culture in the U.S. Intelligence Community, by Dr. Rob Johnston (2005)
Directors of Central Intelligence as Leaders of the U.S. Intelligence Community, 1946–2005 (2005)
U.S. Intelligence Community Reform Studies Since 1947, by Michael Warner and J. Kenneth McDonald (April 2005)
Intelligence and Policy: The Evolving Relationship (June 2004)
Intelligence for a New Era in American Foreign Policy (January 2004)

Comments and questions may be addressed to:

Center for the Study of Intelligence
Central Intelligence Agency
Washington, DC 20505

Copies of CSI-published works are available to non-US government requesters from:
Government Printing Office (GPO)
Superindent of Documents
PO Box 391954
Pittsburgh, PA 15250-7954
Phone: (202) 512-1800
E-mail: orders@gpo.gov

Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis

JEFFREY R. COOPER

December 2005

Acknowledgments

The journey that produced this study owes much to many people. Some of them can be named, others cannot; but all of them have my deepest appreciation and deserve to be acknowledged for their support in this effort. And to my wife Lisa, who can be named—special thanks for putting up with me throughout.

I began to appreciate the depth of the Intelligence Community's analytic problems during a series of research and analysis efforts for various of its components starting in the mid-1990s, and I would like to thank the sponsors of those many efforts even though they cannot be named. Frank Jenkins, General Manager of Science Applications International Corporation (SAIC) Strategies Group, deserves special praise for allowing Fritz Ermarth and me to follow our instincts and start to investigate these issues before the failures became so very public. Particular thanks are owed to Henry Abarbanel for a discussion of the contrasts between the practice of science and that of intelligence analysis, a conversation that prompted me to focus on the deep cultural and process factors that affect analytic efforts rather than on the superficial symptoms and manifestations of the failures.

I owe a debt to Mike May, Dean Wilkening, and Scott Sagan of Stanford University's Center for International Security and Cooperation (CISAC) for inviting me to give a seminar on intelligence issues that forced me to organize and sharpen my concerns into the original briefing on "Analytic Pathologies," and I am truly grateful to both Aris Pappas and Stan Feder for reviewing that lengthy presentation slide by slide. Paul Johnson, Director of the Center for the Study of Intelligence, has my appreciation for an invitation to CSI's 2003 conference on "Intelligence for a New Era in American Foreign Policy"; as do the many intelligence professionals at that conference who helped by bringing their concerns into the open. I want to thank the members of the Marriott Group on the Revolution in Intelligence Affairs, as well as David Kay, Mike Swetnam, Gordon Oehler, and Dennis McBride of the Potomac Institute for providing forums for discussion and for helping me think through these issues with their insider perspectives. Thanks are also owed to several former senior intelligence officials who then pushed me to go beyond diagnosis and address the harder questions of fixing the problems.

I want to thank the Commissioners and my fellow staff members of the President's Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (the Silberman-Robb Commission) for the lengthy opportunity to delve into these issues, examine them in great depth, and analyze them within a truly professional search for understanding. I am also grateful to both the former and the current Program Managers, Lucy Nowell and Rita Bush, of Advanced Research and Development Activity's (ARDA's) Novel Intelligence from Massive Data (NIMD) Program, as well as my team partners on that effort—Stuart Card, Peter Pirolli, and Mark Stefik from the Palo Alto Research Center (PARC) and John Bodnar from SAIC—for discussions and research that led to significant insights on current practices of analysis. I must again thank Paul Johnson and CSI for providing the opportunity to publish this study and reach a far broader audience; without that spur, I would not have completed it. And to the CSI editors, Mike Schneider and Andres Vaart, my appreciation for their great help in getting me through this entire process and in substantially improving this monograph.

Beyond those I have already mentioned, I am also truly obligated to a large number of busy people who took the time and made the serious effort to read and review the earlier briefing and draft study, as well as to share their perspectives and thoughts. Their comments and suggestions were crucial to producing what I hope is a coherent structure and argument: Art Kleiner, Dan Cohen, Jeffrey Pfeffer, Charles Sabel, Dick Kerr, Stephen Marrin, Bill Nolte, Harry Rowen, Mike Mears, Bruce Berkowitz, Mike Warner, Deborah Barger, Joe Hayes, Bill Studeman, Russ Swenson, Ed Waltz, Frank Hughes, Carol Dumaine, David Moore, Rob Johnston, Mark Lowenthal, Kevin O'Connell, Carmen Medina, Jim Bruce, Joe Keogh, Greg Giles, Winsor Whiton, Bob Cronin, Gilman Louie, and John Seely Brown. In addition, many thanks are due Emily Levasseur, my former research assistant, for her invaluable contribution in helping me to conduct the research, find important sources and citations, review thousands of pages of source materials, organize and edit, and revise numerous drafts—all in good humor.

Finally, I give my sincerest apologies if I have forgotten anyone who contributed time and effort to this project. For any errors of omission or commission, I have only myself to hold responsible.

Foreword

Dear reader, my task in this foreword is to shackle your attention to the challenge of getting through Jeffrey Cooper's monograph that follows.

Your attention is deserved because the subject—what we label with deceptive simplicity "intelligence analysis"—is so important and so interesting. The scope of this monograph, like that of the analytic profession, is broad and deep, from support to military operations to divining the inherently unknowable future of mysterious phenomena, like the political prospects of important countries. Jeff Cooper's study, as befits the work of one who has long been an acute observer of the Intelligence Community and its work, is packed with critiques, observations, and judgments. It would be even more satisfying if the study could be further illuminated by clinical case studies of failures and successes. In principle, this lack could be remedied if the hurdle of classification could be cleared. In practice, it cannot currently be fixed because an adequate body of clinical, diagnostic case studies of both successes and failures and lessons learned, particularly from the most relevant, post-Cold War intelligence experience, simply does not now exist. Not surprisingly, Mr. Cooper, along with many other critics and reformers, such as the Silberman-Robb Commission (of which he was a staff member), recommends the institutionalization of a lessons-learned process in our national intelligence establishment. This is but one of a rich menu of admonitions to be found in this study.

Mr. Cooper has provided a good, thematic summary of the main points of his monograph. I shall not attempt to summarize them further in this foreword. But some overview comments are in order.

This study is fundamentally about what I would call the intellectual professionalization of intelligence analysis. It is about standards and practices and habits of mind. It is about inductive (evidence-based) analytical reasoning balanced against deductive (hypothesis-based and evidence tested) reasoning. It extols the value of truly scientific modes of thinking, including respect for the role of imagination and intuition, while warning against the pitfalls of "scientism," a false pretense to scientific standards or a scientific pose without a scientific performance. It talks about peer review and challenging assumptions and the need to build these therapeutic virtues into the analytical process.

Mr. Cooper makes reference to the standards and practices of other professions with a high order of cerebral content, such as law and medicine. Other recognized authors, such as Stephen Marrin and Rob Johnston, have written persuasively on this theme. I am struck by how frequently Mr. Cooper—and others—refers to the example of medicine, especially internal medicine, which has much to offer our discipline. But I am not surprised. When I was very young in this business, I was fretting about its difficulties in the company of my uncle, an old and seasoned physician. He walked to his vast library and pulled out for me a volume, *Clinical Judgment*, by Alvan Feinstein, a work now often cited by intelligence reformers. I later asked my mother, my uncle's younger sister, what made Uncle Walt such a great doctor. Her answer: He always asks his patients at the beginning, "how do you feel?" and he never makes it home for dinner on time. The model of internal medicine is a great one for critical emulation by intelligence analysis: science, training, internship, expertise, experience, and then seasoned judgment, intuition, unstinting diligence, and valued second opinions.

Most of what Mr. Cooper writes about concerns the intellectual internals of good intelligence analysis, i.e., standards, methods, the tool box of techniques, and the vital element of attitude toward understanding and knowledge building. With somewhat less emphasis but to good effect, he also addresses what might be called the environmental internals of the same: training, mentoring, incentives, management, and leadership. It is in this dimension that we must overcome the plague recognized by all informed critics, the tyranny of current intelligence, and restore the value of and resources for deep analysis.

This leads to a consideration of the “externals” of good intelligence analysis. To wit:

The full scope of analysis: This has to be appreciated for things to come out right. Analysis is not just what a hard-pressed analyst does at his desk. It is the whole process of cerebration about the mission and its product. This applies to not only the best answer to a current intelligence question on the table, but to establishing priorities, guiding collection, and, especially, to judging whether the best effort on the question of the day is good enough to support the weight of the situation and the policy decisions that have to be made.

Money and people: There is no gainsaying that a lot of our failings after the Cold War are the fault of resource and personnel cuts while old and new and more equally competing priorities were proliferating. We've got to fortify the bench strength of intelligence analysis. The president has called for that. Without improved practices, however, new resources will be wasted. We press for improved practices; but they need more resources to be implemented effectively.

External knowledge environments: Half a century ago, when the United States came to appreciate that it faced an enigmatic and dangerous challenge from the Soviet Union, it invested seriously in the building of knowledge environments on that subject, in the government, in think tanks, in academia, and in other venues. These external sources of expertise, corrective judgment, and early warning proved vital in keeping us on track with respect to the Soviet problem. We have yet to get serious about building such knowledge environments for the challenges of proliferation and, especially, concerning the great struggle within the world of Islam, from which the main threat of terrorism emerges. Related to this, Mr. Cooper's study properly places great importance on our improving exploitation of open sources.

Information security regimes: We are talking here about a complicated domain from classification to recruitment and clearance systems. What we have is hostile to the task of developing a comprehensive, communitywide knowledge base and operational efficacy in the age of information and globalization. We need to be more open on a lot of things, especially where the original reason for secrecy perishes quickly and the value of openness is great (as during the Cold War in regard to Soviet strategic forces), and to tighten up on secrecy where it is vital, for example, in protecting true and valuable cover.

One final—and perhaps most important—point: Mr. Cooper's study of intelligence analysis is shot through with a judgment that is shared by almost every serious professional I've heard from in recent years. And it applies to collection and other aspects of national intelligence as well. We cannot just rely on the new Director of National Intelligence (DNI) superstructure to put things right with our national intelligence effort. The problems and pathologies that inhibit

our performance and the opportunities for radically improving that performance are to be found down in the bowels and plumbing of this largely dutiful ship we call the Intelligence Community, and that is where we must studiously, and with determination, concentrate our efforts and our money.

—Fritz Ermarth[1]

[1] Fritz Ermarth is a former chairman of the National Intelligence Council; he is now a security policy consultant.

Contents

Introduction 1

Summary 3

Chapter One:
Making Sense of the US Intelligence Community 9

Chapter Two:
Assessing Critical Analytical Shortfalls 23

Chapter Three:
An Inventory of Analytic Pathologies 29

Chapter Four:
A Program for Transforming Analysis 41

Appendix:
The Analytic Pathologies Methodology 59

Bibliography 63

The Author 69

Introduction

As a result of a number of analytic projects for different intelligence agencies, a major focus of my work during the past several years has involved examining the practice of analysis within the US Intelligence Community.[1] This study was prompted by a growing conviction—shared by others, to be sure—that improving the analytic products delivered by Intelligence Community components had to begin with a critical and thorough appraisal of the way those products are created. A conversation with a physicist friend in 2002 had triggered thoughts on several basic differences between the practice of science and intelligence analysis. Shortly thereafter, an invitation to give a seminar on intelligence analysis at Stanford University led me to prepare a briefing entitled "Intelligence and Warning: Analytic Pathologies," which focused on a diagnosis of the problems highlighted by recent intelligence failures.[2] As Donald Stokes noted in his seminal book on science and technological innovation, *Pasteur's Quadrant*, "Pathologies have proved to be both a continuing source of insight into the system's normal functioning and a motive for extending basic knowledge."[3]

The Analytic Pathologies framework yields four insights that are crucial both to accurate diagnosis and to developing effective remedies. First, the framework enables analysts to identify individual analytic impediments and determine their sources. Second, it prompts analysts to detect the systemic pathologies that result from closely-coupled networks and to find the linkages among the individual impediments. Third, it demonstrates that each of these networks, and thus each systemic pathology, usually spans multiple levels within the hierarchy of the Intelligence Community. Fourth, the framework highlights the need to treat both the systemic pathologies and the individual impediments by focusing effective remedial measures on the right target and at the appropriate level.

In response to presentations to community audiences, a number of senior intelligence officials subsequently recommended that I use the diagnostic framework of the briefing to develop corrective measures for the dysfunctional analysis practices identified there. I circulated the resulting draft for comment and was delighted to receive many useful suggestions, most of which have been incorporated in this version.

---

[1] Although this paper will use the common terminology of "Intelligence Community" (IC), it is worth noting that the agencies of which it is composed seldom exhibit the social cohesion or sense of purpose that a real community should. A more appropriate term might be "intelligence enterprise," which is defined in Webster's Third International edition as "a unit of economic or business organization or activity."

[2] The briefing was first presented in early November 2003 to a seminar at Stanford University's Center for International Security and Cooperation (CISAC) and was revised for a Potomac Institute seminar on the "Revolution in Intelligence Affairs" on 17 May 2004. It will be cited hereafter as "Analytic Pathologies Briefing."

[3] Donald E. Stokes, *Pasteur's Quadrant: Basic Science and Technological Innovation.*

Several knowledgeable readers of the draft also raised the issue of the intended audience, strongly suggesting that this should be the senior decisionmakers, in both the Executive Branch and Congress, who could take action to implement the ideas it presented. They also pointedly recommended that the study be substantially condensed, as it was too long and "too rich" for that readership. That audience is, after all, composed of very busy people.

From the beginning, however, I have intended this study to serve as a vehicle for an in-depth discussion of what I believe to be the real sources of the analytic pathologies identified in the briefing—the ingrained habits and practices of the Intelligence Community's analytic corps—and not the organizational structures and directive authorities that are the focus of most legislative and executive branch reformers. Thus, my intended audience has been the cadre of professional intelligence officers who are the makers and keepers of the analytic culture. Without their agreement on causes and corrective measures, I believe real transformation of intelligence analysis will not occur.

Moreover, during the writing of this study, I was fortunate enough to serve on the selection panel for the inaugural Galileo Awards.[4] One of the winning papers focused on a similar issue—the appropriate audience for intelligence—and this reinforced my original inclination.[5] I have decided, therefore, not to condense this study in an effort to fit the time constraints of very high-level readers. I hope, instead, that the summary that follows this introduction proves sufficiently interesting to tempt them to tackle the remainder of the study, where the logic chains that I believe are necessary to convince intelligence professionals of the correctness of the diagnosis and the appropriateness of the suggested remedies are laid out in detail.

[4] The Galileo Awards were an initiative of DCI George Tenet, who, in June 2004, invited members of the Intelligence Community to submit unclassified papers dealing with all aspects of the future of US intelligence. DCI Porter Goss presented the first awards in February 2005.

[5] David Rozak, et al., "Redefining the First Customer: Transforming Intelligence Through Peer-Reviewed Publications."

Summary

Observations

A wide range of problems has contributed to the unease currently pervading the Intelligence Community;[1] a significant number of the most serious result from shortcomings in intelligence analysis rather than from defects in collection, organization, or management.[2] The obvious and very public failures exemplified by the surprise attacks of 11 September 2001 and by the flawed National Intelligence Estimate (NIE) of 2002 on Iraqi weapons of mass destruction (WMD) have resulted in a series of investigations and reports that have attempted to identify the causes of those failures and to recommend corrective actions.[3] These recommendations have usually emphasized the need for significant modifications in the organizational structure of the Intelligence Community and for substantial enhancements of centralized authorities in order to better control and coordinate the priorities and funding of community entities. The Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004, which created the office of Director of National Intelligence (DNI), was based on such foundations.[4]

The logic of this study differs from most of those recommendations with respect to both causes and corrective measures. The key observations in the original "Analytic Pathologies" briefing point in a fundamentally different direction for the root causes of the failures and for fixing the manifest problems. Most importantly, these observations lead to the conclusion that the serious shortcomings—with particular focus on analytic failures—stem from dysfunctional behaviors and practices *within* the individual agencies and are not likely to be remedied either by structural changes in the organization of the community as a whole or by increased authorities for centralized community managers. Those key observations, which follow, provide the conceptual foundation for this study.

1. There has been a series of serious strategic intelligence failures. Intelligence support to military operations (SMO) has been reasonably successful in meeting the challenges on the tactical battlefield of locating, identifying, and targeting adversary units for main force engagements. Similar progress in supporting counterterrorism operations has been claimed.[5] At the same time, however, other military and national users have been far less well served by the Intelligence Community across a range of functions. There have been significant shortfalls in support to post-conflict security and stabilization operations and

---

[1] See *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States* (cited as the *9/11 Commission Report*) and *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq* by the US Senate Select Committee on Intelligence, 7 July 2004 (hereinafter cited as *SSCI Report*).

[2] See Henry A. Kissinger, "Better Intelligence Reform," *Washington Post,* 16 August 2004: 17.

[3] For a review of the various commissions that have tackled intelligence reform, see Michael Warner and J. Kenneth McDonald, *US Intelligence Community Reform Studies Since 1947.* A detailed look at the work of one such recent commission is Loch K. Johnson, "The Aspin-Brown Intelligence Inquiry: Behind the Closed Doors of a Blue Ribbon Commission," *Studies in Intelligence* 48, no. 3 (2004): 1–20. Still, there is no guarantee that good intelligence will necessarily help decisionmakers reach good judgments or make good decisions, but poor intelligence can clearly corrupt good decision processes and amplify ill-advised tendencies in flawed processes.

[4] Intelligence Reform and Terrorism Prevention Act, PL 108–458, 2004 (hereinafter cited as IRTPA).

[5] See Testimony by Cofer Black, Coordinator for Counterterrorism, US Department of State, before the House International Relations Committee, 19 August 2004.

reconstruction efforts in Iraq. Analytic support has also come up short both in accurately capturing adversary thinking and intentions and in providing intelligence that identifies and characterizes developing strategic challenges, such as WMD.[6]

Moreover, within the past decade and a half, a series of intelligence failures at the strategic level, including serious failures in operational and strategic warning, have highlighted real weaknesses at this level and undercut the confidence of principal national users in the community's capabilities against important intelligence targets. These failures include Iraqi WMD developments (1991 onward), the global black-market in WMD, strategic terrorism (beginning with the attack on the World Trade Center in 1993), the North Korean nuclear program (1994), the emergence of globally-networked Islamic fundamentalism (1996 onward), the Indian and Pakistani nuclear programs (1998),[7] the 9/11 attacks (2001), and Iran's WMD programs (2002). Similar failures, as well as an apparent inability to provide accurate assessments and estimates on other important issues, such as the nuclear forces and strategies of China and Russia, affect national users at the highest levels and outweigh any increases in effectiveness at the tactical level.

Indeed, as a bottom-line assessment, this study contends that the Intelligence Community has been least successful in serving the key users and meeting the primary purposes for which the central intelligence coordinating apparatus was created under the National Security Act of 1947.[8] These principal officials are the president and his cadre of senior national security policymakers, not the departmental and battlefield users. As a senior intelligence official recently reminded us, those objectives were two-fold: not only to provide "strategic warning" in order to prevent another surprise such as Pearl Harbor, but also to help head off long-term challenges through a better understanding of the emerging strategic environment.[9]

***2. These failures each have particular causes, but the numerous individual problems are* interrelated.** These failures did not have a single locus—they occurred in technical collection, human source reporting, and analysis, among other critical functions—but neither do they reflect a series of discrete, idiosyncratic problems. Instead, they resulted from deep-seated, closely-linked, interrelated "systemic pathologies" that have prevented the Intelligence Community from providing effective analytic support to national users, especially effective anticipatory intelligence and warning.[10] The Intelligence Community's complicated

[6] It appears, for example, that the intelligence needed to support the security and stabilization operations in Iraq with effective "cultural awareness" during the post-conflict "Phase IV" has been far less than adequate. See comments by senior military officers at a conference in Charlottesville, Virginia, sponsored by CIA's Center for the Study of Intelligence (CSI). *Intelligence for a New Era in American Foreign Policy,* (hereinafter cited as *Charlottesville Conference Report*), 3–5.

[7] Perhaps the more serious error in the case of the Indian-Pakistani nuclear tests was not the failure to predict the timing of the catalytic Indian test (which was really more a failure by policymakers); arguably, it was the failure to estimate correctly the scale and status of the Pakistani weapons program, including its links to the global WMD black market.

[8] Michael Warner, "Transformation and Intelligence Liaison," *SAIS Review of International Affairs* (hereinafter *SAIS Review*) 24, no. 1 (Winter-Spring 2004): 77–89.

[9] See Deborah Barger, "It is Time to Transform, Not Reform, U.S. Intelligence," *SAIS Review* 24, no. 1 (Winter-Spring 2004): 26–27.

[10] The systemic pathologies are discussed in detail in Chapter Three.

organizational structure and the accreted practices of its analysts have combined to create what Charles Perrow calls “error-inducing systems” that cannot even recognize, much less correct their own errors.[11]

3. The Intelligence Community still relies on the same* collection paradigm *created for “denied areas.” Remote technical collection and targeted human access were appropriate means of penetrating denied areas and obtaining critical intelligence against a bureaucratized, centralized, and rigid superpower adversary that exhibited strongly patterned behavior. The problem presented by many of the new threats, whether from transnational terrorist groups or from non-traditional nation-state adversaries, however, is not that of accessing denied areas but of penetrating “denied minds”—and not just those of a few recognized leaders, but of groups, social networks, and entire cultures. Unfortunately, information for intelligence is still treated within the old “hierarchy of privilege” that emphasized “secrets” and was more appropriate for a bureaucratized superpower adversary who threatened us with large military forces and advanced weapons systems.[12] Without refocusing its energies, the Intelligence Community will continue to do better against things than against people.

4. Analytic* methods *also have not been updated from those used to fight the Cold War. There were intelligence failures during the Cold War, but the United States and its allies managed to stay on top of the challenge presented by our principal adversary. A relatively stable threat (and consistent single target) allowed the Intelligence Community to foster in-depth expertise by exploiting a very dense information environment, much of which the opponent himself created. That “Industrial Age” intelligence production model—organized for efficiency in high-volume operations and fed by large-scale, focused, multiple-source collection efforts conducted mostly with episodic “snapshot” remote systems that were very good at big fixed targets—built a solid foundation of evidence. This knowledge base allowed analysts to cross-check and corroborate individual pieces of evidence, make judgments consistent with the highest professional standards, and appreciate and communicate any uncertainties (both in evidence and inference) to users. In particular, this dense information fabric allowed analysts to place sensitive intelligence gathered from human sources or by technical means within a stable context that enabled confirmation or disconfirmation of individual reports. As national security challenges evolved during the years following the collapse of the Soviet Union, however, continued reliance on the Cold War intelligence paradigm permitted serious analytic shortfalls to develop.

5. The Intelligence Community presently lacks many of the scientific community's self-correcting features. Among the most significant of these features are the creative tension between “evidence-based” experimentalists and hypothesis-based theoreticians, a strong tradition of “investigator-initiated” research, real “horizontal” peer review, and “proof” by independent replication.[13] Moreover, neither the community as a whole nor its individual

[11] Charles Perrow, as cited in Robert Jervis, “What’s Wrong with the Intelligence Process?” *International Journal of Intelligence and Counterintelligence* 1, no. 1 (1986): 41. See also Charles Perrow, *Normal Accidents: Living with High-Risk Technologies.*

[12] Fulton Armstrong, “Ways to Make Analysis Relevant But Not Prescriptive,“ *Studies in Intelligence* 46, no. 3 (2002): 20.

analysts usually possess the ingrained habits of systematic self-examination, including conducting "after action reviews" as part of a continual lessons-learned process, necessary to appreciate the changes required to fix existing problems or to address new challenges.[14]

6. Intelligence analysis remains a "craft culture," operating within a guild structure and relying on an apprenticeship model that it cannot sustain.[15] Like a guild, each intelligence discipline recruits its own members, trains them in its particular craft, and inculcates in them its rituals and arcana. These guilds cooperate, but they remain distinct entities. Such a culture builds pragmatically on practices that were successful in the past, but it lacks the strong formal epistemology of a true discipline and remains reliant on the transmission, often implicit, of expertise and domain knowledge from experts to novices. Unfortunately, the US Intelligence Community has too few experts—either analytic "masters" or journeymen—left in the ranks of working analysts to properly instruct and mentor the new apprentices in either practice or values.

Conclusions

The Intelligence Community is not normally self-reflective and usually avoids deep self-examination, but recognition and acceptance of the seriousness of its problems by all levels of the community is a necessary prerequisite for true change, including significant modifications to current organizational cultures and ethos. Agreement on the basic diagnosis must, therefore, precede detailed propositions about effective remedies. I suggest that the following six premises, first articulated in the "Analytic Pathologies" briefing, summarize the most important conclusions to be drawn from the preceding discussion of the current enfeebled state of the Intelligence Community.

***1. The dysfunctional practices and processes that have evolved within the culture of intelligence analysis go well beyond the classic impediments highlighted by Richards Heuer in* The Psychology of Intelligence Analysis.**[16] A more effective analytic paradigm must be built that incorporates the best analytic methods from modern cognitive science and employs useful and easily usable supporting tools to overcome these impediments and prevent them from combining into systemic pathologies.

---

[13] "Evidenced-based" analysis is essentially inductive; "hypothesis-based" is deductive; they should be seen as complementary approaches, not competitors for ownership of the analytic process.

[14] For an exception, see John Bodnar, *Warning Analysis for the Information Age: Rethinking the Intelligence Process*. In fact, both the Joint Military Intelligence College (JMIC) and the Center for the Study of Intelligence have programs to create a discipline of intelligence by bringing together intelligence theory and practice. Regrettably, the results of these efforts have not yet penetrated the mainline analytic units.

[15] In fact, the analytic community self-consciously characterizes its practices and procedures as "tradecraft."

[16] Richards J. Heuer Jr., *The Psychology of Intelligence Analysis*. Building on the work on cognitive impediments to human judgment and decisionmaking of Daniel Kahneman, Amos Tversky, and others, in addition to his own long experience as a senior intelligence analyst, Heuer highlighted many psychological hindrances to making accurate judgments by individuals and small-groups.

2. More corrosively, the individual impediments form interrelated, tightly-linked, amplifying networks that result in extremely dysfunctional analytic pathologies and pervasive failure. A thorough reconceptualization of the overall analysis process itself is needed. The new approach would incorporate a better connected, more interactive, and more collaborative series of networks of intelligence producers and users. In addition, it must be designed to detect and correct errors within routine procedures, instead of leaving them to be found by post-dissemination review.

3. The new problems and circumstances call for fundamentally different approaches in both collection and analysis, as well as in the processing and dissemination practices and procedures that support them. It is clear that serious problems in the existing organizational structure of the Intelligence Community are reflected in poor prioritization, direction, and coordination of critical collection and analysis activities. However, many problems that are more fundamental and deep-seated exist inside the organizational "boxes" and within the component elements of the intelligence agencies themselves. Fixing these—dysfunctional processes, ineffective methods, and ingrained cultures—is not solely a matter of increased authorities, tighter budgetary control, or better management. A strategic vision that addresses the systemic pathologies, leadership that understands how key functions ought to be improved, and a sustained long-term commitment to rebuilding professional expertise and ethos will be essential.

4. Accurate diagnosis of the root causes of problems "inside the boxes" is required; otherwise remedies will be merely "band-aids." For example, the analytic problems occur at and among four organizational levels: 1) individual analysts; 2) analytic units, including their processes, practices, and cultures; 3) the individual intelligence agencies; and 4) the overall national security apparatus, which includes the entire Intelligence Community in addition to the executive bodies responsible for making policy. Solving problems at all four of these interlocking levels requires an integrated attack that includes solutions addressed to the right level and tailored for each problem element.

5. The Intelligence Community must bring more perspectives to bear on its work and create more effective "proof" and validation methods in constructing its knowledge. It should, in particular, adopt proven practices from science, law, and medicine, including more open communication and self-reflection.

6. Whatever the details of structures or authorities, the new Director of National Intelligence (DNI) leadership must assure that the corrective measures are implemented within each agency and across the community. Moreover, all this should be done in the knowledge that change will be continual and that there will be no static resting place where the "right" solutions have been found; organizational structures and processes must be designed to evolve with and adapt to that realization.[17]

Recommendations

Curing the flaws in intelligence analysis will require a sustained emphasis on rebuilding analytic capabilities, refocusing on human cognitive strengths enhanced by innovative support tools, and restoring professional standards and ethos among the analysts

themselves. Most of the recent reform recommendations notwithstanding, more guidelines and tighter management oversight are no substitute for analytic expertise, deep understanding, and self-imposed professional discipline—all achieved not only by formal education and training, but also through assimilation from following experienced mentors. Moreover, neither curiosity nor expertise on the part of the individual analysts can be restored by directives from the top; they must come from an appropriate recruiting profile, effective training, continual mentoring at all levels, time to learn and practice the craft of analysis—both individually and collaboratively—and constraining the "tyranny of the taskings" that prevents analysts from exercising curiosity and pondering more than the obvious answer.[18]

To ensure that the Intelligence Community can provide more effective capabilities to meet the increasingly complex challenges of 21st-century security issues, this study recommends rebuilding the overall paradigm of intelligence analysis from its foundations. The essential components of this effort are:

1. ***A revamped analytic process;***

2. ***An entirely revised process for recruiting, educating, training, and ensuring the professional development of analysts (including the essential aspect of mentoring);***

3. ***Effective mechanisms for interactions between intelligence analysts and users;***

4. ***A proper process for "proof," validation, and review of analytic products and services;***

5. ***An institutionalized lessons-learned process;***

6. ***Meaningful processes for collaboration within the Intelligence Community.***

Furthermore, although implementing each of these processes separately would produce significant improvements in the quality of analysis, a more effective approach would be to mount a broad-gauged, systematic, and integrated effort to deal with the entire analysis process.

[17] A medical analogy might make this argument clearer. Although a low-cholesterol diet, proper exercise, routine physicals, a low dose of aspirin, and moderate intake of alcohol may be useful over the long-term for preventing heart disease, patients in acute cardiac distress require more forceful intervention to save them. The measures listed above would have been useful before the attack, and they may be appropriate after recovery, but they are not effective during an acute crisis or in the immediate aftermath, when patients must be kept under observation to be certain they are "taking their medicine."

[18] Professor Jeffrey Pfeffer of the Graduate School of Business at Stanford University is one of several commentators who have emphasized the importance of "slack" to enable collaboration and collective efforts—including discussion, review and comment, professional development, and service to the "community of practice," as well as pursuing the scent of curiosity.

Chapter One: Making Sense of the US Intelligence Community

The Intelligence Community is an exemplar, even if not a healthy one, of a truly complex adaptive system.

A Complex Adaptive System

With its fifteen diverse agencies and its wide range of functional responsibilities, the Intelligence Community presents a very complicated set of organizational arrangements. Thinking of it in terms of traditional organizational analysis or systems engineering methods in an effort to explain its working does not suffice because it far more resembles a living ecology with a complex web of many interacting entities, dynamic relationships, non-linear feedback loops (often only partially recognized), and specific functional niches that reflect momentarily successful adaptations to the environment.[1] These complex interrelationships among its components create dynamic adaptations to changing conditions and pressures and make the Intelligence Community especially difficult to understand.[2] In fact, it is an exemplar, even if not a healthy one, of a truly complex adaptive system.

During the Cold War, proportionately more resources supporting a larger cadre of experienced analysts devoted to a simpler and relatively static priority target, as well as a broad array of established sources, disguised many of the Intelligence Community's dysfunctional aspects and growing internal problems. The community's loosely federated structure and complicated, if not Byzantine, processes had previously appeared tolerable, even if not fully successful, because making changes appeared to present a greater risk.[3] In the face of a drastically changed security environment, however, it is exactly the combination of complexity and opaqueness that has masked the increasingly dysfunctional misalignment of "dinosaur" analytic processes and methodologies from earlier recognition by both analysts and consumers of intelligence, much less by outsiders.[4]

Even for insiders, the workings of the Intelligence Community are difficult to understand because, as a rule, its members are not deeply self-reflective about its practices and processes. For outsiders, however, these difficulties are magnified by the community's compartmentation, security restrictions, and intrinsic opaqueness. That is why applying traditional organizational analysis that concentrates on structure is doomed to failure; understanding these complex adaptive systems requires more synthesis than traditional "reductionist" analysis.[5] In this case, moreover, it is a complex adaptive system that, insulated by security barriers, has managed to ignore and—probably because of its centralized direction, however imperfect—suppress important external signs of change and to amplify self-protective internal signals, which often reflect strongly ingrained cultural preferences.

The results of the Intelligence Community's failure to recognize the increasing dysfunction were both paradoxical and unfortunate. They were paradoxical because—although it has been accused of not adapting to dramatically changed conditions—the commu-

[1] A feedback loop, in systems analysis, is a relationship in which information about the response of the system to stimuli is used to modify the input signal (see "Feedback," *Principia Cybernetica Web*). A non-linear loop is one that creates non-proportional responses to stimuli.

[2] See Peter M. Senge, *The Fifth Discipline: The Art & Practice of the Learning Organization*. Senge is the founder of the Organizational Learning Laboratory at MIT.

[3] The pressures of the Manichean confrontation with the Soviet Union tempered enthusiasm for drastic and disruptive changes. These might have improved effectiveness, but they would also have provoked bureaucratic and congressional battles over power and jurisdiction.

[4] After all, the dinosaurs were superbly adapted to their environment; even if they perceived the signals of change, they became extinct because they could not adapt to unfamiliar environmental conditions.

[5] An appreciation of the distinction between a complicated system and one that is complex and adaptive is important for accurate diagnosis and effective solutions. A hallmark of complex adaptive systems is that they produce "emergent behavior," which cannot be prediced by analysis of their component elements or structure.

nity adapted all too well. And they were unfortunate because the pressures to which it did adapt flowed from misperceptions inside and outside the Intelligence Community engendered by the collapse of the Soviet Union: that there would be no significant challenges to American interests; that the end of the Cold War reduced the need for a "national security state"; that there should be a substantial "peace dividend," a large part of which would be paid by the Intelligence Community. The community's adaptive processes did accommodate these changes internally—especially the need to "survive" the huge budget cuts and to become relevant to the articulated needs of the paying customers.

It is important not only to locate the level at which obvious symptoms occur, but also the level at which problems can be solved.

However, these internal pressures outweighed the huge new challenges emerging in the external security environment. Responding to these would demand new expertise and a new knowledge base, along with appropriate methods, tools, and perspectives—all of which required more resources, focused leadership, and strong commitment, which was not there. As a result, the community fostered a series of processes that were increasingly maladapted to needs emerging in the new geostrategic environment. By responding to the wrong signals, it created Perrow's "error-inducing systems."[6]

Relating Structure and Process

Unfortunately, most Intelligence Community reform proposals concentrate on changes in structure and in directive and managerial authorities. Analytic problems, however, actually take place not just at the level of the community as a whole, but at four distinct levels, as well as in the complex interrelationships, both vertical and horizontal, among them.[7] Thus, it is important not only to locate the level at which the obvious symptoms appear, but also the level at which the problem can be solved. In this way, the root causes of failure can be identified and appropriate and effective corrective measures taken.

The National Security Community. The relevant entities include the National Security Council (NSC), the Office of the Director of National Intelligence (ODNI), and the national policymaking and operational elements in the Department of State and the Department of Defense.[8] Among the failures at this level can be misdirected priorities and misallocation of resources; poor communication and coordination; and inconsistent apportionment of authority, responsibility, and capability among the main entities. Such failures flow downward and can easily percolate throughout the subordinate organizations.

For the Intelligence Community, a particular problem at this level may involve its relationships with top-level users, especially managing their expectations. On the one hand, for example, the Intelligence Community often demonstrates an inability or unwillingness to say "no" to consumer requests, which leads to additional priority taskings without concomitant resources or relief from other ongoing activities. Similarly, the Intelligence Community often conveys an illusion of omniscience that fails to make clear its state of knowledge on an issue, the underly-

[6] See Perrow, *Normal Accidents.*
[7] The briefing on "Analytic Pathologies" graphically illustrates the multi-level interplay of these problems. See Appendix A for a summary.
[8] At this level, for the Intelligence Community, it is the ODNI and the Intelligence Community elements that are responsible for critical functions—collection, analysis, special activities, and community management—that interact directly with senior principals. With a DNI and an ODNI organization in place, these relationships are likely to become even more complicated.

ing quality of the intelligence, or the degree of uncertainty—all of which can leave the Intelligence Community seemingly responsible for decisions taken on the basis of "bad intelligence."

The Intelligence Community. This level currently includes the fifteen component intelligence agencies. Failures at this level can include misdirected priorities and budgetary allocations within the Intelligence Community; lack of effective procedures and oversight of them among component agencies; poor communication and coordination among agencies; a lack of enforceable quality-control processes; toleration of substandard performance by individual agencies; poor communitywide technical standards and infrastructure that hinder information sharing; and poor management and oversight of security procedures that impede effective performance. Errors at this level also encompass failures by groups or individuals to make critical decisions, to exercise appropriate authority, or to take responsibility for gross errors that should be worthy of sanction or dismissal.[9]

The Individual Analytic Units and Organizations. It is essential to appreciate the importance of particular analytic environments within specific sub-organizations—an office within the CIA's Directorate of Intelligence, for example. It is these entities, rather than the organization as a whole, that create the work processes and practices that form the immediate cultural matrix for an analyst's behavior.[10] Failures at this level can include dysfunctional organizational processes, practices, and cultures that inhibit effective analysis by individuals and sub-units; management attitudes and directives that stress parochial agency objectives; toleration of poor performance; excessive compartmentation and special security procedures that erect barriers to effective execution; poor prioritization and assignment of workflow; inability to create and protect "slack" and conceptual space for intellectual discovery; ineffective recruitment and training; maintaining stand-alone information and analysis infrastructures, including ineffective support for individual analysts; poor direction and management of the analytic process; and, simply, ineffective management of the analytic cadre. This is probably the most important level for creating consistently high-quality analysis because of its impact on the analytic environment, on the selection of methods and processes, and on the work life of individual analysts. Errors at this level are perhaps the most pernicious, however, and they have been widespread and persistent.

Individual Analysts. Failures at this level can include poor performance due to lack of ability, lack of domain knowledge, lack of process expertise, poor social network contacts, or ineffective training; pressures to favor product over knowledge; lack of time; being too busy and too focused to maintain peripheral vision and curiosity, even on high priority work; failure to cooperate and collaborate with others; lack of suitable tools and support; misguided incentives and rewards; and an organizational culture and work practices that tolerate second-rate analysis.

To illustrate the impact of this multi-level hierarchy and underscore the importance of correctly identifying the locations of causative factors in analytic errors, for example, consider the case of an analyst who fails to interpret correctly the evidence pertinent to

[9] See Statement by Admiral David Jeremiah (USN, ret.), Press Conference, CIA Headquarters, 2 Jun 1998, for a suggestion that failures by senior managers to make key decisions had been an important factor in the CIA's failure to warn of an impending Indian nuclear test. (The subject was the "Jeremiah Report" on the 1998 Indian nuclear test.)
[10] See Karl E. Weick, *Sensemaking in Organizations*.

a task and draws a wrong conclusion. At first glance, the obvious approach should be to focus corrective actions on the analyst: what caused the failure, and what are the appropriate remedies? Simple incompetence, a rush to complete the assignment, a lack of domain knowledge needed to recognize critical linkages, or a failure to employ appropriate methods could all be causative factors. At this level, the obvious remedies to these problems are better screening, training, and mentoring.

It could be, however, that the problem lies with the analytic unit, its work processes, and its management: the tasking was high priority, and this analyst, whose expertise is on another subject, was the only one available; appropriate tools and methods were not provided; training in relevant domain knowledge or on effective new tools had been postponed due to production pressures; or, given the production cycle, the analyst lacked sufficient time to search for all the relevant evidence. The problem could reside even farther up the hierarchy, among the agencies of the Intelligence Community: key data from another agency was not made available, due to compartmentation restrictions or because incompatible information infrastructures prevented the analyst from easily searching another agency's holdings. Finally, the failure could actually reside at the topmost level, with community management: this account was given such low priority that no collection resources had been assigned to gather information or to provide consistent analytic coverage or, because of the thinness of the evidence base, the inability to answer the question was not made clear to the requester at the start.

However, it is exactly here that the "5 Whys Approach" of the Quality Movement proves its value.[11] Applying this approach, which features a progressively deeper, recursive search, forces the investigator to trace a causative factor to its source.[12] Assume that, in this example, it is a lack of domain knowledge.

Why was an analyst not fully knowledgeable in the domain working that account?

She was covering for the lead analyst, who is away on temporary duty (TDY).

Why did the analytic manager assign that analyst to the task?

She was the only one available.

Why was the analyst not fully knowledgeable on her backup account?

She is an apprentice analyst with only a short time on the account and inadequate mentoring. Her training had been postponed due to scheduling. She didn't have time to be curious and follow the information scent. She could not access the lead analyst's "shoebox."[13]

Why couldn't she access the shoebox of the lead analyst?

[11] The Quality Movement took root in the United States during the 1990s, when US auto manufacturers were challenged by the emergence of higher quality Japanese automobiles made by automakers who had adopted the principles of two US engineers, W. Edwards Deming and Joseph Juran. The principles provide a systematic set of processes and metrics for improving the quality of manufacturing processes.

[12] A recursive search is one in which successive searches build on the results of earlier searches to refine the answers returned. (See National Institute of Standards and Technology, *Dictionary of Algorithms and Data Structures*.)

[13] Although seldom used today, many analysts once referred to the personal files where they stored such items as the results of research as "shoeboxes." It is used here to emphasize the particularity of the methods employed by analysts.

It is his personal collection of tentative hypotheses and uncorrelated data kept as a personal Word file and is not in an accessible database. The shoebox is actually a pile of paper put in temporary storage when the lead analyst went on TDY.

Why is the lead analyst unwilling to share his shoebox?

Why is there no accessible collaborative system for sharing shoeboxes?

The questions would continue through as many rounds as the questioner needed to satisfy himself that he had found the root cause.

Although the previously cited reports on intelligence failures usually point to organizational stove-piping and technical shortcomings as the most important contributors to failures in collaboration, the sources of such failure are actually more widespread and complex—and more frequently reflect shortcomings in work practices and processes, organizational culture, and social networks.[14] In addition, the proposed solutions that focus on structures and authorities disregard the critical interrelationship between structure and processes and ignore as well the importance of organizational culture on institutional effectiveness. As Stephen Marrin, among others, has noted:

Structure and process must work together in a complementary fashion, and structural changes alone without corresponding changes to existing processes would simplify the workings of the Intelligence Community in some ways, but cause greater complexity in others.[15]

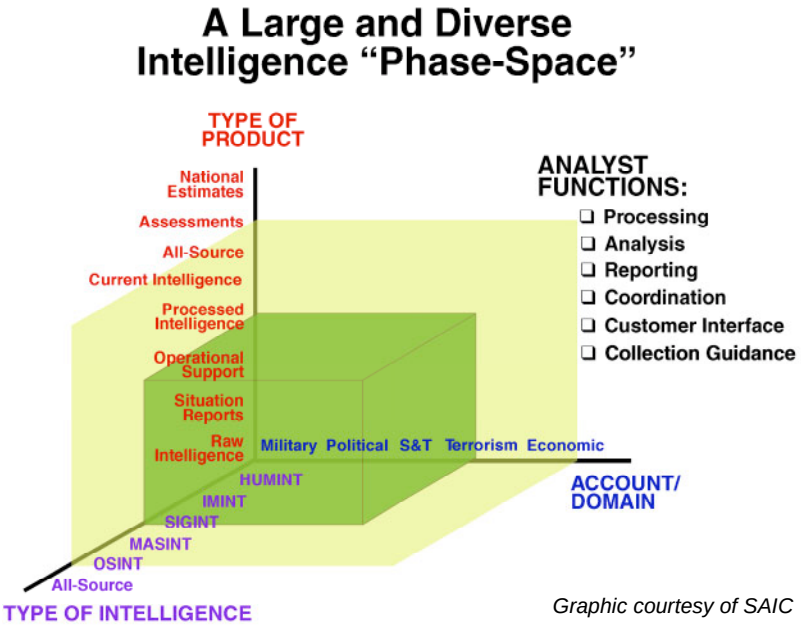
The significant structural reforms legislated in 2004 will also entail substantial short-term transition costs to effectiveness as new organizational arrangements are implemented, processes are developed, and outmoded roles and systems are replaced. The really difficult task will be to redesign the processes, so that they are consistent and complementary to the structural changes that are being made.

Incorrect diagnoses of the causes of analytic failures probably arise from not recognizing the variety and complexity of the roles, missions, and tasks that confront analysts.

The Analysis Phase-Space

At a basic level, incorrect diagnoses of the causes of analytic failures probably arise from not recognizing the variety and complexity of the roles, missions, and tasks that confront analysts. This diversity results in a complex phase-space, illustrated below, that contains a significant number of discrete analytic regions. These certainly cannot be treated as though their perspectives and needs were homogeneous or even similar. The tasks required of a signals intelligence analyst attempting to locate a terrorist's cell-phone call are fundamentally different from those of an all-source analyst drafting an NIE on Chinese strategic nuclear doctrine. Therefore, because intelligence collection and analysis are not based either on a suite of all-purpose tools or on fungible human expertise that can be instantly swiveled to focus effectively on a different set of problems, this phase-space also implies the need for a similar diversity of analytic processes, methods, knowledge bases, and expertise.

[14] Technical systems and infrastructures enabling collaboration are important, but they are only a small part of the solution to fostering effective collaboration. For more on this topic, see discussion beginning on page 57.
[15] Stephen Marrin, in a review of William E. Odom, "Fixing Intelligence: For a More Secure America," *Political Science Quarterly*, 119, no. 2 (Summer 2004): 363.



Graphic courtesy of SAIC

A phase-space is a conceptual tool used by physicists to represent the abstract set of all potential dynamic values of a system that can be produced by every combination of system variables possible in each dimension. The relatively simple, 3-valued phase-space for analysis shown above includes dimensions for different domains and accounts, types of products and services, and sources of intelligence.

Differentiating Intelligence Roles

Moreover, given this diverse phase-space, conflating three distinct roles played by all-source intelligence adds to the underlying confusion over intelligence missions and functions, the priorities among them, their requirements, and the capabilities needed to make each effective. The traditional assumption that there were only two sets of intelligence consumers, each with distinct mission needs, often led to contraposing support to military operations, which was assumed to be tactical in focus, and national user support, which was assumed to demand deep analysis. In reality, meeting the disparate needs of the users intelligence must serve requires recognizing three distinct roles for all-source intelligence.[16] Two of them, Support to Military Operations (SMO) and Support to Policy Operations (SPO), focus primarily on issues needing immediate information capabilities to assist decisionmaking on current operations. Although SMO and SPO issues are of interest to both national and departmental users, the third role, Warning and Estimative Intelligence (WEI), largely emphasizes issues that are almost exclusively the province of national users and usually take place over longer time horizons.[17]

In all cases, however, although it still uses the term "support," the Intelligence Community must move beyond the notion that it is segregated from the rest of the national security community and that it merely provides apolitical information to decisionmakers. Intelligence has now become an integral element of both the policy and military operational processes; and the success or failure of its judgments can have the most significant consequences in both domains.[18] Increasingly-integrated military operations, in which intelligence directly drives operations, and command centers in which intelligence personnel are fully integrated, are tangible evidence of such changes. As a result, it is important that intelligence appreciate not only the central-

[16] It is important to recognize that these regions have fuzzy boundaries, overlap to some degree, and are not totally distinct.

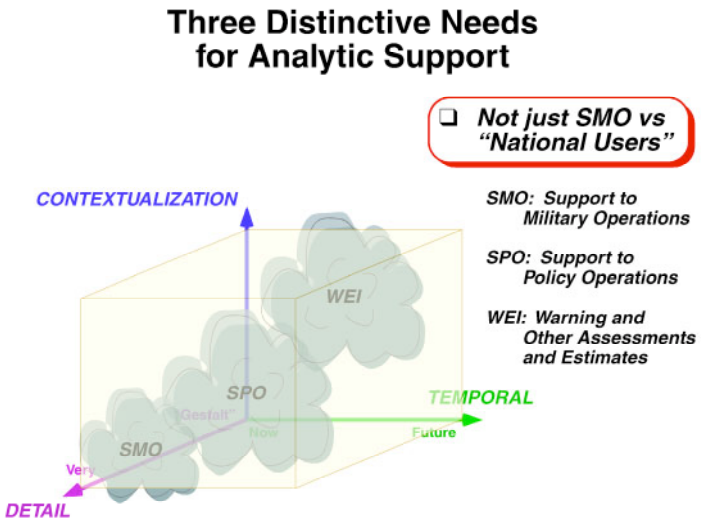
[17] The intelligence role that often leads to confusion over appropriate categorization is warning, and especially the tactical warning component. Because warning is intimately connected to a decision on a responsive action, it is sometime mistakenly considered to be a decision-support activity; in reality, it is more appropriately seen as a part of the informative function that assists policymakers in thinking about issues before they occur, helping to create coherent, contextualized reference frames. Moreover, because tactical warning is *tactical*, it is often forgotten that it is of principal concern to high-level strategic users because it almost always involves activities that could have the most serious political and strategic consequences. Thus, these three roles cover two distinct functions: SMO and SPO emphasize situational awareness and immediate decision support, while WEI focuses on anticipation of future circumstances.

ity of its role, but also the increased obligations and responsibilities that such a role brings.[19]

Support to Military Operations (SMO): This traditional intelligence role has usually focused on assisting current military operations. Much of this information concerns current numbers, locations, and activities of hostile units, and other information addresses significant elements of the physical environment in which military forces are operating.[20] Other military users need quite specific current data on subtle technical characteristics of adversarial equipment and forces to serve, for example, as targeting signatures or to support electronic warfare (EW) activities. Regardless of type, intelligence supporting operating forces demands extraordinary accuracy, precision, and timeliness to ensure that it is immediately "actionable" under conditions that are highly stressful and potentially lethal.[21]

Increasingly, however, military operators have other operational intelligence needs, such as support for information operations and for security and stabilization in Iraq. To prosecute these missions successfully, the military now also needs far more cultural awareness and timely accurate information on adversary thinking, motivations, and intentions.

Support to Policy Operations (SPO): Making explicit that this is a distinct role emphasizes the importance of intelligence to daily policymaking across the entire spectrum of national security concerns; it is the



Graphic courtesy of SAIC

"national user" cognate of SMO. SPO provides policymakers and senior officials (importantly including senior civilian defense officials, combatant commanders, and other military officers) with indispensable situational awareness, including important background information, to assist them in executing and overseeing ongoing policy activities and in planning and framing policy initiatives. As it is as intensely focused on providing actionable information, it is as heavily oriented as SMO to current intelligence and reporting. However, SPO differs from SMO somewhat in content and priorities in that it has always included a greater proportion of less quantifiable, softer information, such as political and economic

[18] I am grateful to Dr. Russell Swenson of the Joint Military Intelligence College for persuading me to sharpen this point. See Russell G. Swenson, with Susana C. Lemozy, "Politicization and Persuasion: Balancing Evolution and Devolution in Strategic Intelligence," unpublished manuscript. When the CIA was created, expectations about intelligence capabilities and its role were significantly different than they are today. At the policy level as well, there is now an expectation that intelligence will be available to guide policy creation and inform course changes if necessary.
[19] A valuable guide to appropriate comportment in these circumstances is Herbert Goldhamer's *The Adviser.*
[20] The US Army, which has extensive doctrine on operations, calls this intelligence preparation of the battlefield (IPB). This includes specific information on mission, enemy, time, terrain, and troops available (METT-T).
[21] A critical example is the need for technical details, so that enemy weapons, such as improvised explosive devices (IEDs), can be countered.

trends in major countries and groups and assessments of foreign leaders and their intentions.

Warning and Estimative Intelligence (WEI): Mary McCarthy, a former National Intelligence Officer (NIO) for Warning, commented on the recommendations of a DCI-chartered study conducted in 1992:

> *According to that ten-member panel of highly respected intelligence and policy veterans, providing policymakers with persuasive and timely intelligence warning is the most important service the Intelligence Community can perform for the security of the United States.*[22]

A warning process . . . allows decisionmakers to think through responses they might be obliged to make in haste.

McCarthy defines warning as "a process of communicating judgments about threats to US security or policy interests to decisionmakers."[23] Thus, warning provides vital support to "national users" in their principal *strategic* missions—understanding the complex geostrategic environment, fostering vision of objectives, assessing alternatives and determining strategy, and protecting against consequential surprise; most importantly, when done properly, warning is forward looking and anticipatory.[24]

Warning is sometimes thought to be merely alerting decisionmakers to immediately threatening activities, but, in reality, it is a far more complex function and actually addresses two very different kinds of problems. One type of warning is concerned with monitoring activities previously recognized as potentially dangerous, such as a hostile missile launch, and cueing appropriate responses. The second type is a discovery function that assists decisionmakers in identifying those situations and activities whose consequences could have significant (and usually adverse) effects—and which may not necessarily be obvious. When performed effectively, a warning process provides decisionmakers with an anticipatory sensitization that allows them to think through, in a disciplined way, the responses they might someday be obliged to make in haste. Assessments and estimates, on the other hand, also are usually forward looking, but they are designed to be informative rather than part of a process closely tied to triggering contingent responses.

Further complicating the matter is that both types of warning also operate over three different horizons. *Strategic* warning has always been understood as looking out toward the distant future; it is intended to recognize that a possible threat may be looming—even if it is not imminent—and to provide time to take appropriate preparatory actions, including policies and actions that might prevent the threat from eventuating.[25] *Operational* warning also looks out in order to identify the characteristics of the threat (the likely and particular methods of attack), so that offsetting contingency plans and actions can be prepared. From this detailed understanding of enemy intentions, capabilities, and concepts, operational warning also serves to identify indicators that an

[22] Mary McCarthy, "The National Warning System: Striving for an Elusive Goal," *Defense Intelligence Journal* 3 (1994): 5. Warning is considered the classic "strategic intelligence" role and was the principal reason for the creation of the CIA.
[23] Ibid.
[24] There have always been terminological problems associated with the word "strategic." During the Cold War, users of the word often conflated level of analysis (global and synoptic), time horizon (forward-looking), and magnitude of the stakes (very large), with instrumentality (nuclear) and distance (intercontinental).
[25] To some degree, these terms have always been confusing because they described two very different types of problems. Strategic, operational, and tactical warning related to surprise nuclear attack were very patterned, but focused on two distinct problems: surprise attack executed by known forces and surprises that were truly unanticipated.

attack is in preparation. Finally, *tactical* warning is the immediate alerting function that a specific (with respect to time, place, or character) hostile activity has begun or is about to begin.

An important but often overlooked element of warning over all three horizons is the key role played by negative evidence, which can help confirm that potentially threatening activities are **not** occurring and prevent costly and potentially consequential responses from being taken or scarce resources from being squandered.[26] During the confrontation between the United States and the Soviet Union, and, in particular, during periods of high tension between them, one of the most important functions of warning was to inform the leaders that, "Today is not the day."

Both the warning and estimative functions are designed to focus more on informing decisionmaking with context and long-term implications than with supporting ongoing activities. The preparation of assessments and estimates, as well as development of warning indicators, has more to do with analysis and judgment than with reporting; it demands deep expertise as well as an ability to place knowledge of the subject in broad context. These important functions serve the entire national security community.[27]

Although warning is often misconstrued as a current intelligence problem, even tactical warning of specific targets, times, and means must build on this deeper foundation of pre-emptive analysis of threats and responses if it is to be effective. During the Cold War, recognizing that we were engaged in a long-term competition, we were prepared to adjust our intelligence priorities so that analysts could provide assessments of future capabilities and indications of intentions, even though the day-to-day threats were most grave. As was the case in facing the Soviet Union, there may well be tensions today in choosing between serving SMO and SPO, on the one hand, and assuring adequate resources for WEI, on the other hand, as continued access to information needed for an understanding of enemy intentions and capabilities could be sacrificed by meeting the needs for immediately actionable intelligence.

Although warning and estimative intelligence may be seen as the core missions of strategic intelligence, they are also less tied to the details of ongoing operations in which the formal relationships between policymakers and intelligence provide a unique advantage and leverage for intelligence insights. Today's decisionmakers have many more sources of information than did their predecessors when the Intelligence Community was created; in turn, the Intelligence Community holds far less of a monopoly over information about foreign events and technology developments. Moreover, as one senior intelligence official noted, policymakers see themselves and their staffs as substantively knowledgeable on issues of interest as the Intelligence Community and capable of serving as their own intelligence analysts.[28] As a result, users increasingly

Today's decisionmakers have many more sources of information than did their predecessors. . . ; in turn, the Intelligence Community holds far less of a monopoly over information about foreign events and technology developments.

[26] Perhaps the scarcest resource is a senior decisionmaker's attention, which can easily be wasted.
[27] As an indication of the long time horizon involved in this function, both civilian and military defense officials need to look well into the future to develop strategy, plan forces, support research and development, and acquire systems.
[28] See Charles E. Allen, "Intelligence: Cult, Craft, or Business?" in "Comments of the Associate Director of Central Intelligence for Collection" at a Public Seminar on Intelligence at Harvard University, spring 2000. See http://pirp.harvard.edu/pdf-blurb.asp?id+518: 15. Henry Kissinger may be the most obvious example of this tendency, but it has continued since the Nixon administration and has come to include a far greater proportion of policy officials, especially as the sources of information on foreign developments have expanded dramatically and become available in near real-time. See Henry A. Kissinger, "America's Assignment," *Newsweek*, November 8, 2004: 38–43.

see themselves as participants in a process of judgments.[29] An experienced national-level user wrote recently,

> *Today, the analyst no longer sets the pace of the information flow. The sources of information now available to the policy-level consumer…are far, far greater than a quarter century ago. It is almost a given that today's policy-level consumer of intelligence is well informed in his or her area of interest and not dependent on an intelligence analyst for a continuing stream of routine, updating information.*[30]

Implications of Differentiating Roles

Careful differentiation among the three intelligence roles discloses dimensions that are both analytically important and more meaningful for contemplating intelligence reform than the usually misleading bimodal distinctions between national vs. military users or tactical vs. strategic objectives. What truly distinguishes these intelligence roles is their *perspective and emphasis*—a significant distinction that has been lost in recent arguments over intelligence reform.

To begin with a particularly important point, a tactical or a strategic focus does not necessarily distinguish military from civilian users.[31] Moreover, the less quantifiable and, therefore, *softer* information and analysis on individuals, decisionmaking, and social dynamics that used to be produced primarily for national users is now increasingly demanded to support military operations at the tactical level. Such information is inherently more judgmental and inferential—and, therefore, less precise—than analysis of physical or technical characteristics in orders-of-battle (OOBs) and tables of organization and equipment (TOEs). It is less amenable to counting or to the gathering of external physical signatures by technical collection systems; it is more dependent on language skills, deep expertise on the region and cultures, and knowledge of the personalities.[32] It is also harder to validate or prove than estimates of technical factors. Such capabilities go beyond "reporting" that used to be the core of current intelligence.

However, both SMO and SPO are, by nature, mission- or task-oriented and tightly focused on the problem at hand; and this narrowed focus has significant time and perceptual implications for analysts and the intelligence sources supporting them.[33] Given the stress, time pressures, and immediate—as opposed to potential—stakes attendant on current operations, human decisionmakers try to concentrate only on the immediate situation and the information relevant to it, while actively screening out other inputs. This is the intelligence analogue of human "foveal vision," which offers the highest visual resolution but also a very narrow field-of-view.[34]

[29] As one senior intelligence official remarked in a private meeting, "We are all in the business of making judgments; but too many in the Intelligence Community continue to believe that they are instead providing crystalline analyses."
[30] Clift, "Intelligence in the Internet Era," *Studies in Intelligence* 47, no. 3 (2003).
[31] This distinction might have been clearer before civilian leaders began taking detailed interest in overseeing tactical operations—as began during the Vietnam War with presidential interest in the selection of bombing targets. With respect to the Soviet Union during the Cold War, national and military users had clear areas of primary interest; national users were focused on intelligence illuminating key political, economic, technological, and social factors affecting national power and intentions, while military users were more focused on the likely force capabilities and doctrines of potential adversaries. After the Cold War, improving technical capabilities and the emergence of the "strategic corporal" combined to increase the interest of civilian policymakers in overseeing tactical operations.
[32] Several senior military participants at the Charlottesville conference highlighted these demands. See *Charlottesville Conference Report*, 2–5.
[33] There is a very large body of literature on the physical and psycho-perceptual effects on human judgment and decisionmaking under stress that is relevant to these distinctions.

In contrast, warning and estimative intelligence are the analogues of human "peripheral vision," in which there is low resolution but a wide field-of-view. Peripheral vision is very sensitive to cues of dynamic change, which trigger anticipatory responses. Although warning is concerned with activating the response cycle, and estimative intelligence is intended to create a frame of reference for the decisionmaker, both are intended, through preconditioning and anticipatory consideration, to enable a more appropriately and contextually sensitized response on the part of users.[35]

Another important implication of the differing emphasis on decisions with a long-term view and those requiring prompt action—the classic distinction between strategic and tactical—concerns the nature of the advantage to be gained from the information, and, therefore, how it is exploited. In recent years, the tasks of intelligence, and its successes and failures, have focused on providing immediately actionable (in this sense, tactical) intelligence to users—information that can provide a rapid or near-instantaneous advantage, whether for interdicting hostile military forces, preventing terrorist incidents, or supporting diplomatic initiatives. Emphasizing current intelligence for actionable exploitation may have created an unintended mind-set that undervalues the immense importance of knowing and understanding the adversary's intentions throughout the course of the confrontation, even at the cost of foregoing exploitation of these sources for temporary advantage on the battlefield or in the diplomatic conference room.[36] This stress on current intelligence also influences the priorities among the types and attributes of information we collect, the nature of the collection and processing systems, the analytical methods we use, the stresses we place on analysts, and the metrics by which we assess the performance of intelligence.[37]

There is yet another important distinction between these roles. By looking out to the future, WEI is basically a surprise-preventing function intended to heighten a policymaker's ability to visualize the consequences of anticipated and unanticipated events and to prepare for them mentally; it is not designed to be "evidence-based truth-telling" that will stand up in court. In addition, as we better appreciate the implications of emergence and the emergent behaviors of complex adaptive systems, we need to place greater emphasis on anticipation while recognizing that precise prediction or forecasting is even harder than previously understood. Appreciating the differences in perspective created by these roles is very important because failing to make clear distinctions between them may aggravate a major problem before the Intelligence Community: the disconnect between the emphasis on current reporting or providing situational awareness, which must be evidence-based, and

[34] The fovea, a small pit at the back of the retina, forms the point of sharpest vision. The intensely narrow concentration of foveal vision is recognized as being a major contributor to "change blindness."
[35] One type of warning function amenable to focused monitoring involves potential surprise from a recognized adversary undertaking a feared but pre-identified activity (such as a Warsaw Pact invasion across the Inner-German border). This other warning function serves to guard against truly unexpected or unforeseen events. In both cases, they are designed to encourage thinking about, and contingency planning for, "surprises" before they occur.
[36] The widely repeated—but apocryphal—story that perhaps best exemplifies this understanding of "strategic intelligence" is that of Churchill's allowing Coventry to be bombed in order to safeguard the long-term informational advantages gained from Allied code-breaking achievements against the Axis. The immeasurable importance of such intelligence in the successful Allied efforts to interdict Rommel's supply lines during the North African campaign and in winning the crucial Battle of the Atlantic testify to these other equities with possibly higher priority.
[37] Barger, 26. Although her specific comment refers to the impact of precision (timeliness and resolution, for example) on the quality and quantity of intelligence, her larger point is that functional needs stemming from roles and missions drive what the Intelligence Community provides its users and how it does so.

When one tries to assess the adequacy of Intelligence Community performance … or prescribe changes … the appropriate answers will almost certainly differ greatly from one role to the other.

the policymaker's need for anticipatory judgments, which, by nature, trade the confidence derived from hard evidence for an intuitive, or *gestalt,* understanding of the whole derived from inference.[38] It is unlikely that analysts will have firm evidence to offer the policymaker to support alternative interpretations of the future, and they will need to rely on inference and informed speculation that is persuasive to decisionmakers.[39] In particular, as one experienced intelligence analyst noted,

> *"Getting inside the other guy's head" can only be conjectural because, in most cases, even the "other guy" doesn't know exactly why he's doing what he's doing.*[40]

Even if there are predictive judgments to be made in both SMO and SPO,[41] they tend to have short time horizons and reasonably short inferential chains; as the predictive time-constants are short, observation of adversary actions can serve to validate or disprove these judgments and thereby improve confidence in them and the analyst's judgment.

Those providing SPO, in particular, must continually walk a fine line between serving the policymakers' needs for relevant, focused, direct support and maintaining objectivity in providing the evidence and analysis. Staying close to the evidence assists the analyst in walking this line. At the same time, the author of this monograph noted a clear consensus among senior intelligence officers at a recent non-attribution conference that analysts can best serve policymakers by offering them thoughtful and thought-provoking views that challenge their assumptions. It must be recognized, however, that helping to alter policymakers' assumptions is intruding directly into the policymaking process and, thereby, crossing the boundary that Sherman Kent tried to establish. As the policymakers demand judgments on actions and consequences farther in the future (moving the intelligence role from SPO to WEI), not only will the intrinsic uncertainties increase, but also the potential for tensions between policymaker and analyst over the objectivity (and validity) of the judgments and the conflicts among differing judgments.[42]

Another of these distinctions affects intelligence requirements and planning. Unlike SMO and SPO, where the users can clearly identify their areas of interest, priority issues, and information needs, the Intelligence Community must look beyond its users' perceptual horizons if it is to perform warning and estimative functions effectively. Almost by definition, with anticipatory intelligence, policymakers will be unable to tell the community where to look. Unfortunately, although the Intelligence Community must recognize that attempting to divine requirements for warning and other anticipatory intelligence from the users is not likely to be fruitful, it also must appreciate that it alone will bear the blame for failing to warn against the inevitable surprises arising from outside the fields-of-view of users. This demands, in turn, that the Intelligence Community have some discretion and flexibility to allocate resources in areas not currently considered to be priority targets: listening

[38] *Gestalt*, a German word meaning "form" or "shape" is used in psychology to connote holistic understanding of the entirety of a phenomenon. This follows Kendall's approach of "creating pictures," as noted by Jack Davis in "The Kent-Kendall Debate of 1949," *Studies in Intelligence* 35, no. 2 (1991).
[39] This is a comment to the author by a senior intelligence officer who has served in both roles.
[40] Private communication to the author from John Bodnar, 3 November 2004.
[41] The military, in particular, is increasingly emphasizing "predictive battlespace intelligence" as a central component of "information superiority." It is usually, however, a different kind of prediction than that required to support SPO.
[42] As the founder of Air Force and Joint Staff Studies and Analyses, Lt. Gen. Glenn Kent (USAF, ret.), paraphrasing Shakespeare, once warned analysts, "Neither a prostitute nor a proselytizer be."

too closely to the customers, and looking only where directed, guarantees future strategic warning failures.

It is absolutely essential that the Intelligence Community and those who depend on it understand the principal distinctions between these two functions. In their conclusions about the nature of the Intelligence Community's problems, the extraordinary differences between the report of the 9/11 Commission and that of the SSCI on Iraqi WMD reveal the dangers of conflating the two distinct functions or ignoring the differences between the three roles. When one tries to assess the adequacy of Intelligence Community performance across these domains, identify shortfalls, or prescribe changes—whether in business practices, tools, or organizational arrangements—the appropriate answers will almost certainly differ greatly from one role to the other.

Chapter Two: Assessing Critical Analytical Shortfalls

Many of today's principal analytic problems arise from continued reliance on analytic tools, methodologies, and processes that were appropriate to … the Cold War.

As astute members of the Intelligence Community have observed, intelligence capabilities (and the organizations that provide them) are not general purpose tools but, rather, specialized and "finely honed" instruments that evolve and adapt to the specific challenges and requirements placed upon them.[1] Many of today's principal analytic problems arise from continued reliance on analytic tools, methodologies, and processes that were appropriate to the static and hierarchical nature of the Soviet threat during the Cold War and were, in that environment, largely successful. We possessed several decided advantages that enabled us to overcome some of the limitations on our capabilities: a careful and cautious "Main Enemy" that was also a far simpler and slower target than those we face today; more time; many and more experienced analysts; and varied and well-established sources of information, including the adversary's own vast outpouring of seemingly trivial but very useful data.

Given these advantages, the Intelligence Community was able to:

- Concentrate, focus, and build a deep foundation of cumulative evidence;
- Foster longstanding and deep expertise in its analytic cadre by exploiting a very dense information environment;
- Rely on multiple-source collection, which generally allowed us to cross-check information and make judgments consistent with the highest professional standards;
- Largely neglect intelligence collection and analysis on "soft" cultural, societal, and people issues (other than the most prominent elites), because the plans and intent of the adversary were in the hands of a small Politburo and because we "knew" that knowledge of the plans and intent of subordinate elements or nations—for example, Poland—was rarely necessary;[2] and
- Employ an intelligence model that could rely on collecting "secrets" in voluminous quantities and required a mass production approach for producing reports.[3]

That was also a period of relative information scarcity on worldwide events, and the Intelligence Community had a substantial comparative advantage over other information providers through access to intelligence obtained by clandestine collection.

The United States had many Cold War successes, of course, but there were always significant shortcomings in American intelligence capabilities. These shortcomings resulted in surprises that had important and unanticipated consequences for US policy. Among these were the Egyptian/Syrian attacks on Israel opening the 1973 Yom Kippur War, the 1974 Indian nuclear test, the fall of the Shah and the accompanying ascendance of a fundamentalist Islamic regime in Iran in 1979, the unexpectedly rapid collapse of the Warsaw Pact in 1989, and the dissolution of the Soviet Union in 1991.

The traditional intelligence methods were even less successful against some important targets that have carried over into the

[1] See Aris A. Pappas and James M. Simon Jr., "The Intelligence Community: 2001–2015," *Studies in Intelligence* 46, no. 1: 39–47; Bruce Berkowitz, "Intelligence for the Homeland," *SAIS Review* 24, no. 1 (Winter-Spring 2004): 3.
[2] To appreciate the costs of this view, see the brief account on page 41 of Professor Murray Feshbach's use of Soviet and Russian health statistics to derive an important conclusion.
[3] The bureaucratized nature of the Soviet Union and the state of telecommunications throughout the Cold War allowed the United States to exploit its technological prowess and employ effective remote collection capabilities in addition to the traditional method of using human sources.

post-Cold War era—such as Iran, China, North Korea, nuclear proliferation, and the global WMD black-market. In these cases (exemplified by the 1998 Indian and Pakistani nuclear tests), we have had serious shortcomings in understanding because, in the face of the numerous, continuing, and competing demands for higher priority current intelligence, we were unwilling or unable to make the long-term commitments to build the deep knowledge base the task required.

Today, the United States may need to take action more frequently on the basis of ambiguous intelligence, against harder to recognize threats, from less risk-averse enemies—especially the shifting groups of radical Islamic fundamentalists who foment terrorist activities and may wield capabilities that could devastate cities, societies, or economies. These new Islamic adversaries also pose, as did the Soviet Union, a long-term ideological challenge whose character and "operational code" we do not currently understand. Unlike the Soviet Union, however, which was a hierarchical, bureaucratic state whose organizational character we did understand, the new targets are more dynamic and complex. These new groups morph frequently and metastasize like cancers, emerging with new personalities and network linkages and threatening new targets.[4]

As a result, today's Intelligence Community must contend with:

- Little foundational knowledge on major adversaries and cultures;
- Fragmentary evidence and sparse intelligence flows, which often cannot be substantiated or contextualized—even against the highest priority current targets;
- Thin domain ("account") expertise, due to multiple and shifting priorities and frequent shuffling of relatively inexperienced analysts;[5] and
- An analysis model that remains heavily dependent on "secrets," even when the key intelligence questions may involve mostly "mysteries" and "obscurities."[6]

Aggravating these existing shortcomings, a cascade of significant and complex developments that will pose substantial new challenges is already evident, making the adequacy of the community's current capabilities even more problematic.[7] These changes involve more dynamic geostrategic conditions, more numerous areas and issues of concern, smaller and more agile adversaries, more focus on their intentions and plans and less on large physical objects and weapons systems, a more open information environment, and more widespread understanding of American intelligence methods and capabilities by our adversaries. Additionally, the sense of vulnerability to terrorist attack on US territory left by 9/11 has created huge new demands on the Intelligence Community to provide information for homeland security.[8] The immensity of these challenges complicates the task of developing appropriate cures for the real causes of inherited shortcomings and of heading off new analytic shortcomings.

[4] Marc Sageman, "Understanding Terror Networks," FPRI E-Note, 1 November 2004.
[5] In addition, inexperienced analysts may lack the ability to tap sources of deep expertise available through connections to long-standing professional networks.
[6] Fritz Ermarth originally developed this typology. For the details, see page 40.
[7] Barger, 28.
[8] At the same time, the breaching of old distinctions between foreign and domestic intelligence activities has increased public concern over potential threats to privacy.

The lengthy reports of the 9/11 Commission and the SSCI report on Iraqi WMD laid out in great detail their views on why these two failures occurred. Although they occurred in very different substantive domains, at very different levels of analysis, in different parts of the intelligence organizations, and exhibited significantly different failure modes and causative reasons, both reports tended to locate the causes in problems related to information sharing and coordination, instances of insufficient collection and poor data, and "errors" of analytic judgment by individuals and groups.[9]

The Intelligence Community now finds itself under intense scrutiny and faced with the need to transform in fundamental ways in order to meet the entire range of national security intelligence challenges only partially recognized in the legislatively mandated reforms. Addressing these challenges requires fundamentally new approaches in both collection and analysis as well as in the processing and dissemination methods that support them. As Barger aptly notes: what is needed is revolution, not reform.[10]

Misunderstanding Analytic Processes

The litany of failures should have been a tip-off to the deep-seated nature of the analytic problems. Such a series of "idiosyncratic" errors by individuals and small groups within an organization are, however, more likely to be symptoms than root causes, as Perrow convincingly demonstrated in case studies of Three Mile Island and Chernobyl.[11] A pattern of repeated errors is often a signal of seriously dysfunctional methods—fundamental and systematic failures of procedures and processes throughout an organization.[12] From this perspective, the proximate causes of the failures identified in both the report of the 9/11 Commission and the SSCI report on Iraqi WMD hardly appear to be convincing root causes of these recent intelligence failures.

A more accurate diagnosis of the sources of our intelligence shortcomings requires a deeper and more thoughtful analysis of why organizations make mistakes—causes that go beyond obvious superficial conditions created by flawed organizational structures and insufficient directive authorities. As Charles Sabel noted, "There he [Herbert Simon in *Administrative Behavior*] showed that modern organizations were efficient precisely because they systematically turned habits—the disposition to react to particular situations in a characteristic, but open-ended way—into rigid routines."[13] Not unexpectedly, these routines "work" for the specific conditions they were developed to address. They rarely perform well for off-design conditions, however, and, often, the better they work for the design conditions, the more narrow the set of conditions for which they are appropriate. Paradoxically, the better they work, and, therefore, the more efficient the organization at its routine tasks, the greater the danger that the organization will fail to be sensitive to its environment and changes occurring there. As with the dinosaurs, scores of major American corporations have fallen victim to this pat-

Major American corporations have fallen victim to a pattern of "overadaptation" and "change blindness." The Intelligence Community runs the same risk.

[9] Indeed, the IRTPA was largely driven by the recommendations of the 9/11 Commission, which focused mostly on one, albeit important, aspect of intelligence needs, that of counterterrorism. But, as noted above, the IRTPA reforms mandate changes that affect all functions of the Intelligence Community.
[10] Barger, 28.
[11] Perrow, *Normal Accidents.*
[12] For examples of the consistent nature of such errors, see the following: the "Jeremiah Report"; Interview with Richard Kerr, MSNBC, 14 July, 2003 (concerning the "Kerr Report" on the Iraqi WMD NIE). An unclassified portion of that report is in *Studies in Intelligence* 49, no. 3 (2005) (hereinafter cited as Kerr, et al.).
[13] Charles F. Sabel, "Theory of a Real Time Revolution."

tern of "over adaptation" and "change blindness."[14] The Intelligence Community runs the same risk.

The Problem of the Wrong Puzzle

Frequent public references to "failing to connect the dots" are especially problematic for an accurate understanding of intelligence errors and failures. This view of the analytic shortfalls is particularly perverse, because it masks the true nature of the analyst's challenges. The flawed "connect the dots" analogy flows from the image of the children's game book in which lines are to be drawn between a set of numbered dots in order to make a recognizable picture. That analogy assumes, however, that—as in the children's book—the dots exist, that it will be obvious which dots connect to which others and in what order.[15] The problem is that this simple analogy overlooks a well-known phenomenon in psychology that is often illustrated by the "Rubin Vase Illusion": that evidence really does not "speak for itself"; rather, that information is "perceived and interpreted."[16] Humans are extremely good at finding patterns, even when there is none—hence the classic intelligence aphorism, "You rarely find what you're not looking for and usually do find what you are looking for."[17]

Talk of a "science of analysis" is a conceit . . . . The reality is otherwise.

If we are to use a puzzle analogy, perhaps a more appropriate model might be that of a guest at a resort hotel who, on a rainy afternoon, wanders into the game room and finds a box holding a large number of jigsaw puzzle pieces. As the cover of the box is missing, there is no picture to guide him in reconstructing the puzzle, nor is there any assurance that all the pieces are there. Indeed, when he discovers that there are several other empty puzzle boxes on a shelf, it is not even clear that all the pieces in the box belong to the same puzzle. Reconstructing the puzzle in this example is a far different and more difficult challenge than linking numbered dots, where the outline of the image is reasonably apparent.[18]

Both the dots analogy and the model of evidence-based analysis (discussed in the following section) understate significantly the need for imagination and curiosity on the part of the analyst.

The Myth of "Scientific Methodology"

Many well-informed outside commentators and intelligence professionals continue to talk about the "science of analysis," and only some of them are truly aware of the shaky foundations of this belief or of its real implications.[19] But this talk of a "science of analysis" is a conceit, partly engendered by Sherman Kent's dominating view of intelligence analysis as a counterpart of the scientific method.[20] The reality is otherwise; analysis falls far short of being a "scientific method" in the common, but usually misunderstood, sense. Moreover, this view of science itself is "scientism," which fails to recognize the important role of less "ratio-

[14] See Carol Loomis, "Dinosaurs?" *Fortune*, 3 May 1993: 36*ff.* An accompanying sidebar recounted how a senior Sears executive pointed behind himself to the tens of volumes of corporate practices and rules that governed the corporate response to any conceivable problem. The emergence of mid-market national discount chains wasn't covered; and, therefore, "…wasn't a problem they had to address."
[15] This relatively simple problem is known formally in mathematics as a "directed graph."
[16] Edgar Rubin, 1915. Heuer discusses such perceptual problems using different examples in Chapter 2 of *The Psychology of Intelligence Analysis*.
[17] This remark is often attributed to Amrom Katz, a pioneer in aerial and overhead reconnaissance.
[18] Heuer, Chapter 6.
[19] See, for example, Frank Hughes and David Schum, *Evidence Marshalling and Argument Construction*.
[20] Sherman Kent, *Strategic Intelligence.* See also Jack Davis, "The Kent-Kendall Debate."

nal" and less "scientific" elements, such as imagination and intuition.[21] As Mark and Barbara Stefik, knowledgeable and respected participants in the discipline of science, have written about science and innovation in a recent book.

> *The word "theory" usually connotes a formal way of thinking logically or mathematically. In this formal sense, theory takes its place in a knowledge-generating process called the scientific method. The scientific method includes hypothesis formation, experiment planning, execution, and data analysis. In this scheme, theory is used to make predictions. Theory is created by a process that includes hypothesis formation and testing.*
>
> *Unfortunately, this notion of theory and the working methods of science and invention leaves out imagination. This makes it both boring and misleading….[22]*

Citing a well-known commentary by a Nobel laureate, the Stefiks add:

> *In [Peter] Medawar's view, the standard scientific paper promotes an error of understanding how science is done because it confuses proving with discovering.[23] The layout of a scientific paper makes it appear that the doing of science is the careful laying out of facts. Once the facts are in, the conclusions follow. This makes it seem like science is all about deduction. Unfortunately, this formal structure leaves out the creative part of discovery and invention. The structure of a scientific paper is only about proof, promoting the systematic marshalling of evidence. In this abbreviated story, once a scientist has by some means figured it out, the paper lays out the conclusions logically.[24]*

A more realistic and useful appraisal of the process of intelligence analysis comes from Charles Allen, a long-time senior intelligence official: "I want to speak mainly about the art and craft of intelligence…. We could have talked about the science of intelligence, but, by and large, as far as I'm concerned, the science of intelligence is yet to be invented. I don't see it. It's not really there."[25] This is not to suggest that rigor, accuracy, clarity, and precision are not required in intelligence analysis; given the stakes, they are obviously essential. But demanding a false precision from an analysis process that is itself incorrectly modeled on a common misunderstanding of the methods of science is not likely to improve the quality of analysis. Indeed, an important issue for both managers and users of analysis to consider is the likelihood that there may be little concordance between precision in the details of the answer and the accuracy of the overall (*gestalt)* judgment. A process and methodology too focused on provable evidence may get the details right at the cost of ignoring important inferential judgments that need to be conveyed in order to provide a true sense of the uncertainties of both evidence and judgment.[26]

A process and methodology too focused on provable evidence may get the details right at the cost of ignoring important inferential judgments.

[21] The term "scientism" is used to connote the frequent confusion between the appearance of a formal scientific methodology and the actual conduct of science, which may be intuitive, but is nonetheless subject to rigorous proof.
[22] Mark Stefik and Barbara Stefik, *Breakthrough: Stories and Strategies of Radical Innovation*, 110.
[23] The Stefiks are referring to Peter Medawar's article, "Is the Scientific Paper Fraudulent? Yes; It Misrepresents Scientific Thought," published in the *Saturday Review* 47, 1 August 1964: 42–43.
[24] Stefik and Stefik, 110–11.
[25] Allen.
[26] For more on this subject, see the section on "Evidence-based Scientism" in Chapter Three.

The Flaws of a "Tradecraft" Culture

Intelligence analysis remains largely a craft culture that is conducted within a self-protective guild system and taught by means of a broken apprenticeship process. There are other fields, such as science, medicine, and warfare, in which knowledge is also understood to be tentative and not subject to formal "proof," as is possible in mathematics. Within such professions, the cumulative practices, habits, and mindsets of an evolved culture are especially important for the creation of knowledge and the transmission of expertise. As with intelligence, these other communities are ones in which much of the knowledge needed for effective performance relates to the often-arcane processes of the craft (tradecraft, as the Intelligence Community terms it). This knowledge is tacit and difficult to elicit from the experts, and it is usually best communicated by personal example and practice.[27] However, the culture of intelligence lacks many of the formalized processes, such as "peer review," and the cumulative knowledge structures that the academic, military, and medical communities have created to address similar challenges in building a solid foundation of understanding that can be passed to successor practitioners. Perhaps for these reasons, intelligence analysis is not yet a true profession. Within this culture, therefore, effective mentorship is especially important for transmitting expertise and, perhaps more significantly, for imparting professional standards and values to apprentices.

[27] The professions of medicine and law refer to themselves as "practices," which reflects their roots in the guild system. More importantly, perhaps, this usage conveys that the essential elements of a profession (ethos, ethics, and skills) are human values best transmitted by people.

Chapter Three: An Inventory of Analytic Pathologies

Although many of the reform proposals responding to the recent intelligence failures took diametrically opposed positions with respect to the role of the DCI, the creation of the DNI, and the functions of the CIA within a "transformed" Intelligence Community, they were mostly quite similar in that they focused both on wiring diagrams and formal authorities as the mechanisms for reform and on creating a "czar" to execute those authorities through centralized management.[1] As is often the case, reform legislation took a structural route to address problems that flow from dysfunctional processes, inbred cultural practices and habits, and failures of human leadership.

Although the legislative changes have restructured the community, other than emphasizing "competitive analysis" and more HUMINT, the IRTPA contains little significant language about reforming the internal functional processes of intelligence—collection and analysis. The legislation failed to take into account several key distinctions that any intelligence reform proposals must recognize: differences in issue domains; tactical vs. strategic consequences; narrowly focused vs. synoptic collection and analysis; reporting vs. deep analysis; immediate vs. long-term decision horizons; foveal vs. peripheral perception; action vs. exploitation; and defined, tasked requirements vs. speculative information gathering.

Some recommendations, in fact, could aggravate the already dysfunctional conditions, further damaging analytic capabilities. The IRTPA directed the establishment of centers for priority issues, as recommended by the 9/11 Report, but these are likely to place even more emphasis on current intelligence, whether or not this was intended. Integrated centers combining operators and analysts do foster better sharing and collaboration among them, but they invariably place the emphasis for analysts on operational support. Moreover, creating static structures and rigid processes designed to deal with fixed areas or issues is not a particularly sound response to events and conditions that are very fluid and fuzzy. These can be better handled by operating within a process that allows flexibility and discretion. Finally, with an already severe shortage of effective managers and experienced intelligence officers (including analysts, operators, and collectors), establishing more centers with mandated institutional positions and priorities can only further dilute an already over-stressed cadre of intelligence professionals.

. . . establishing more centers with mandated institutional positions and priorities can only further dilute an already over-stressed cadre of intelligence professionals.

An Inventory of Analytic Pathologies

Curing analytic shortcomings cannot be done by making minor modifications to the existing processes or even by wholesale replacement or upgrading of the analytic cadre.[2] Although it may be tempting to focus on better educating and training the analysts—the better for them to be able to "connect the dots"—altering the analytic model and the processes on which that model relies is almost certainly a more appropriate response to the profound problems besetting intelligence analysis. Without fixing the fundamental shortcomings in analytical processes, the system will always depend on the ability of individuals to work around the impediments, which adds additional stress to an already burdensome set of tasks.

[1] See, for example, a bill proposed by Rep. Jane Harman, the "Intelligence Transformation Act of 2004" (HR4104): "The goal…should be to enhance the DNI's ability to coordinate and integrate operations, focus the community on priorities, share information better…and so on, but not detract from the support that cabinet secretaries need and expect from their intelligence organization, and not dilute competitive analysis."

[2] One excuse for the very heavy cuts in mid- and senior-level analytic cadres in the early 1990s was that it was necessary to weed out those whose expertise was presumed to be passè and, therefore, no longer needed.

At the same time, it should be acknowledged that there are limitations on the depth and quality of the expertise available within the community. The past decade has shown that the Intelligence Community is likely to find itself behind academic and commercial sectors in many frontier areas simply because, for the most part, that is where these frontiers are first explored. Furthermore, given the unpredictable nature of emerging challenges and the often short response time they allow, the community is unlikely to have on hand sufficient regional, cultural, linguistic, technical, or specialist expertise to meet high priority threats to our national interests. Therefore, unless community management decides to forgo having all needed expertise within the community—to open its boundaries, remove the barriers, and create mechanisms to draw on external expertise and knowledge—these impediments to exploiting outside expertise will frustrate its ability to meet emerging mission challenges.

Interestingly, even if the old analytic methods and processes developed during the Cold War were themselves capable of addressing the emerging security challenges of post-Soviet adversaries, a review of postmortems of intelligence failures prior to 9/11 and the Iraqi WMD fiasco showed that these processes and procedures were routinely violated, frequently leading to failures.[3] In addition to shortcomings in the basic analytic paradigm and processes, according to the study, the system lacked enforceable self-correcting features and functioning compliance mechanisms. This suggests that there has been a more fundamental failure in leadership and in the basic institutional and management mechanisms for assuring effective performance of oversight, assessment, accountability, and responsibility. That these failures persisted for so long should be of concern to members of the analytic community, their leadership and management, and the oversight bodies as well. It is a warning sign that better oversight and enforceable compliance procedures are needed, because the analytic community itself may no longer possess the internal self-discipline or professional standards to do so.[4] This also clearly implies that greater attention to professional ethos and standards must be an integral part of efforts to transform analysis.

Indeed, well before 9/11, several articles written by experienced community officials pinpointed fundamental shortcomings within the community's analytical capabilities and highlighted dysfunctional processes as the causes.[5] Thus, the longstanding failure modes within the existing intelligence analysis paradigm must be identified and corrected, along with the management and oversight procedures, if the community is to meet new needs.[6]

Two elements of the current paradigm are especially worthy of attention. ***First is the inefficiency of the "account" structure.*** The account system, by its very nature, creates institutional and individual "ownership" of important intelligence domains. The ben-

[3] See Jack Davis, "Improving CIA Analytic Performance: Strategic Warning," and "Improving CIA Analytic Performance: DI Analytic Priorities."
[4] Several retired, formerly very senior, CIA officials have made this point about erosion of professional élan—ethos, ethics, and standards—that help keep the analyst from, as General Kent put it, succumbing to the temptations of prostitution or proselytizing (see footnote 43 on page 22). One attribute of a profession, especially a "learned profession," is that members can work without supervision. This is also one of the characteristics that define journeymen in a craft system.
[5] Carmen Medina, "What To Do When Traditional Models Fail," *Studies in Intelligence* 46, no. 3 and Russ Travers, "The Coming Intelligence Failure," *Studies in Intelligence* 40, no. 2.
[6] See Berkowitz, 3. That each organization develops tradecraft and evolves practices that may not transfer easily if challenged by new functions complicates the community's ability to shift its focus and assets to meet new challenges.

efit is that it provides a basis for accountability; the disadvantage is that ownership inhibits sharing, cooperation, and collaboration. It has also encouraged "stovepiping" by collection discipline and the control of information by collectors through originator-control (ORCON) restrictions. A fundamental redesign of analysis should start by dismantling both the notion of information ownership and the paradigm of "accounts," while maintaining accountability for performance; information must become the common property of the community, and someone with authority must oversee sharing and configuration management.[7] Such changes are likely to involve altering the existing institutional mechanisms in order to forge interagency virtual "clusters" to perform the analytic functions while creating "mission managers" with the authority to assure that important subjects and user needs are properly serviced.

The second element is the Intelligence Community's strong cultural orientation towards an "evidence-based scientism." Although this approach may be appropriate for the current intelligence functions that rely heavily on gisting and reporting and dominate both SPO and SMO, it clearly limits the ability of analysts to address the anticipatory intelligence needs of decisionmakers, which usually demand more reliance on judgments and inference chains and less on specific evidence. In return for more focus on the WEI role, decisionmakers who rely upon anticipatory intelligence must realize its inherent properties and limitations and be prepared to accept greater uncertainty in assessments and estimates in order to obtain better *gestalt* understanding.[8]

We need to understand that "warning" is largely built on modeling (either explicit or implicit) and synthesis, which are deductive processes, and not on analysis, which is an inductive process. In all cases, analysis processes should also access more non-traditional sources and incorporate a wider range of information to construct corroborative fabrics that can confirm or disconfirm critical information and hypotheses. The rigor and strength of these methods must rely less on narrow tests of the quality of the evidence or adherence to formalisms than on analysts being sufficiently "mindful" to recognize the pitfalls they may encounter in blind application of approved methodologies.[9] In addition, there is a huge research literature on decisionmaking under uncertainty that could be exploited to introduce innovative techniques for analysis and decision support. What all this comes down to, however, is not to disregard the need for rigor of method and quality of evidence, but, rather, to suggest that a construct of analysis too narrowly tied to a misunderstood "scientific method" needs to be augmented and leavened with intuition, curiosity, and a thirst for discovery—all essential elements of good science.[10]

Beyond these two fundamental changes, eight other problematic features of the current intelligence environment need to be addressed.

A fundamental redesign of analysis should start by dismantling both the notion of information ownership and the paradigm of "accounts."

[7] Creation of an "information commons" must be done in full awareness of the problems associated with the conundrum of commons, the conflict for resources between individual interests and the common good. Garrett Hardin, "The Tragedy of the Commons," *Science* 162 (1968): 1243–8.
[8] It is like the saying, "better to be approximately correct than precisely wrong." Josh Kerbel, "Thinking Straight: Cognitive Bias in the US Debate About China," *Studies in Intelligence* 48, no. 3 (2004).
[9] In this regard, several commentators, among them Sabel, Fishbein, and Treverton, have recognized the potential applicability of practices drawn from "High Reliability Organizations" (HROs). Both this issue and "mindfulness" will be addressed in greater depth in Chapter Four.
[10] This thought owes much to comments by Stephen Marrin in a private communication on 1 November 2004.

3. The Tyranny of Current Intelligence

Over the past decade, the Intelligence Community's efforts to be responsive to its customers' demands for current intelligence have dominated collection and analysis. As a senior analyst noted, "The Intelligence Community really [is] focused on current intelligence, on policy support. It does very little research. It has very little understanding below the level of the policymaker and, in my view, on many issues. I think that, in some ways, these two groups are reinforcing each other's worst habits."[11] The disappearance of the long-term Soviet threat and the chaos of the post-bipolar geostrategic environment shifted policymaker interests to a series of *crises du jour*. Policymakers demanded that intelligence for their current problems receive priority as the US and Allied interventions in Somalia, Haiti, Bosnia, Kosovo, and elsewhere proceeded. At the same time, the Pentagon's increasing demands for support in ongoing military operations, including such prolonged activities as *Northern* and *Southern Watch* in Iraq, placed tremendous demands on the intelligence system for a continuing stream of timely support products.[12]

Prior to the 1991 Gulf war, no commanders of regional or functional military forces—other than those for strategic forces—could expect to receive direct and timely support from national assets, especially to support tactical operations.[13] That war, and the glimpse it provided of the power of modern information systems to overcome shortcomings in C4ISR (command, control, communications, computers, intelligence, surveillance, and reconnaissance) fueled an intense push to obtain "information superiority." This, in turn, created nearly insatiable appetites among military commanders for real-time intelligence support and gave birth to the concept of "net-centric warfare" (NCW).[14] Many of the new C4ISR systems (including national systems), and much of the effort and funds expended by the Intelligence Community since the Gulf War, have focused on providing direct, real-time support to forces engaged in combat by closing the "sensor-to-shooter" loop and to meeting the information needs of the senior-level commanders directing those operations. When there are American forces deployed in active military operations, as there have been on a near-continual basis since the end of the Cold War, the highest priority is now accorded to providing intelligence to support them.

4. Overemphasis on Production

At the same time as demands to support military operations generated huge requirements across the Intelligence Community, standing collection and analysis requirements to fill databases and to produce routine scheduled products set priorities for a substantial part of the intelligence "phase-space." The entire intelligence system is dominated by the demands of processing

[11] *Intelligence and Policy: The Evolving Relationship*, Center for the Study of Intelligence, June 2004, 7.
[12] These are not new problems. Defense Secretary Donald Rumsfeld, as chairman of the Commission on Ballistic Missile Threats, highlighted the failure of executive and legislative leadership to establish appropriate priorities while besieging the community with ad hoc taskings. See Side Letter to the Rumsfeld Report, 18 March 1999, 2.
[13] Those needs and the impediments on access to national systems underwrote the very large military programs known as TIARA (Tactical Intelligence and Related Activities). National systems are also known as National Technical Means, the term used to refer to them in arms control agreements.
[14] In *Network Centric Warfare: Developing and Leveraging Information Superiority*, David S. Alberts, John J. Garstka, and Frederick P. Stein define NCW as "an information superiority-enabled concept of operations that generates increased combat power by networking sensors, decisionmakers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace."

huge amounts of information gathered by collection systems whose architecture was largely designed during the Cold War to address a very different problem. This huge inflow created a production-oriented model and an "efficiency paradigm" better suited to the "Industrial Age" than to the Information Age of the Twenty-first century.[15] The volume of collected intelligence is so vast that, even with automated assistance, human analysts can effectively review and evaluate only a small part of the flow.

The existing paradigm for intelligence analysis and dissemination still relies largely on published paper reports as the mechanism for delivering products to users. Furthermore, without effective metrics to assess the value of intelligence to decisionmakers as well as the impact of analysis on the quality of their decisions, it is simple measures of data collected, traffic processed, and reports produced that have influenced critical decisions on priorities and resource allocation within the Intelligence Community. Meeting the new challenges will require a greater emphasis on adaptability and agility, as well as processes that are better able to respond to non-routine requests and high-priority challenges. The price to be paid for this, however, may be a reduction in efficiency as measured by the usual output-oriented metrics of mass-produced products normally used in cost-benefit calculations of routinized processes. Such calculations underweight the ability to meet unexpected situations and the "slack" that is usually essential in an adaptable organization.

5. Over-Reliance on Previous Judgments

The problem of "finished intelligence" stems from the conceit that any intelligence product is more than a snap-shot of knowledge believed to be true at that time and that "finished intelligence" is, by virtue of the formal coordination and review processes, "truer" than the pieces of raw intelligence from which it was built. The roots of this conceit date back to the period when the Intelligence Community was seen to possess domain expertise found neither in its user communities nor outside government, and its assessments could be considered authoritative. During that period, the Sherman Kent posture of standing apart from policy users could be considered an appropriate style. Fully coordinated "finished intelligence" products, such as NIEs, do convey authoritativeness as the *current, agreed judgment* of the Intelligence Community. These products also carry a sense that they and their conclusions can stand the test of time. These latter assumptions, however, are not necessarily warranted. As most "finished" intelligence products involve substantial interpretation, analysis, synthesis, and judgment, and they are more likely to have lengthy inference chains that compound uncertainty issues in more fragmentary reporting.

The validity of the earlier judgments expressed in finished products is especially important because of the common practice of "layering," that is, using previous, formally coordinated products as the starting point for new assessments and estimates.[16] Although this practice helps to assure the consistency of an analytic line, building on established judgments or on prior positions of an analyst, branch, group, office, or agency is also a reason to be wary. As a former senior intelligence official noted,

[15] Sabel, 52ff.
[16] See Conclusion 4, *SSCI Report*, 22–23.

> *Judgments which any analytical actor has the greatest incentive to defend must be subjected to the most critical scrutiny.*[17]

The danger arises because, unlike academic practice, there is no sustained or sanctioned process of after-the-fact ("ex post facto" or "ex post") review. Finished products are rarely subjected to a considered re-examination, nor do they receive explicit testing by other parties trying to replicate their findings—unless there is an obvious major intelligence failure. Moreover, errors that are recognized subsequent to publication are often not corrected, by means either of timely notification to readers or of corrections fully incorporated throughout the knowledge base.[18] Other knowledge intensive enterprises, such as law, medicine, and science, also depend on cumulative foundational knowledge; but they do far better at maintaining the accuracy and currency of these critical intellectual resources than does the Intelligence Community.

The community too often treats probing questions as attempts to "shape" (that is, "politicize") analyses rather than genuine inquiries into the quality of evidence and the strength of inferences.

Even a cursory reading of the report on Iraqi WMD highlights the mutually reinforcing dangers of the "finished intelligence" conceit and of "layering." Too often, the presumed authoritativeness of a formal product leads users to accept its judgments as established and its underlying evidence as validated. These products then become the baseline for updated assessments, and, as a result, the cumulative impact of errors is amplified and becomes pervasive.[19] In fact, the conceit is even more damaging to the effectiveness of the Intelligence Community in an era when policymakers are increasingly likely to be their own "senior analysts" and may not believe that "finished intelligence" represents the final word on a topic. Today, these officials bring other information and their own expertise to the task of arriving at a comprehensive judgment, and intelligence material is only one input into that process.[20] Yet the community too often treats probing questions as attempts to "shape" (that is, "politicize") analyses rather than genuine inquiries into the quality of evidence and the strength of inference chains.

6. The Neglect of Research

This emphasis on current intelligence, with its consequent time pressures and the methods needed to meet production demands, has produced a range of distorting effects that are not fully recognized.[21] First, it has severely undercut the ability of analysts to do in-depth research by requiring that most analytic effort be devoted to short-term taskings. Second, by denying most analysts the opportunity to work on deep products under the tutelage of a senior mentor, this emphasis has damaged a key element of the indispensable apprenticeship process, a *sine qua non* for effectively training and developing professionally competent intelligence practitioners. Third, in order to meet daily requirements, the production aspects of the current intelligence cycle have been accorded undue priority.[22] Fourth, the emphasis on current intelligence helped to create an incentives and rewards system for the analysts biased towards short-term reporting rather than deep analysis. And, fifth, without explicit management support, the time pressures on, and implicit incentives for, analysts to focus on current

[17] Private communication from Fritz Ermarth, 23 January 2005.
[18] See the "Curveball Report," cited in the *SSCI Report*, 482 and 492.
[19] See, for example, the *SSCI Report*, 32–33 and 484.
[20] Jack Davis, "Paul Wolfowitz on Intelligence-Policy Relations," *Studies in Intelligence* 39, no. 5 (1996).
[21] See Chapter Four for a more complete discussion
[22] This is also a problem for newspapers, and it explains why newspapers, with their daily production cycle, are different from magazines, which can afford to pay more attention to sustained investigative journalism.

production have made the pursuit of curiosity difficult. In contrast, within the scientific community, "investigator-initiated" research is a primary contributor to discovery and innovation, as well as a powerful factor in validating the research of others. The Intelligence Community has need of just such a procedure.

Over the past decade, the Intelligence Community has made several attempts to redirect attention to long-term research and products that reflect such efforts, but, without a sustained base of interested customers in the senior policy community, these have not succeeded.[23] Analysts have seen the emphasis on the President's Daily Brief (PDB) and similar serial products as a clear indication of where interest (and therefore success) is to be found.[24] Although some suggest that current intelligence can provide the basis for deep understanding, it seems obvious that attempting to achieve this by compiling current reporting is not a satisfactory method for producing integrated, synoptic analyses that are set in full context. A better route to meeting the competing demands of producing both current intelligence and deep analytical products would be to exploit the expertise and domain understanding of the experienced analysts doing in-depth research to identify, select, extract, and put into context the important tidbits from the reporting stream—and to use those as a basis for more in-depth and sustained exchanges with users of intelligence.

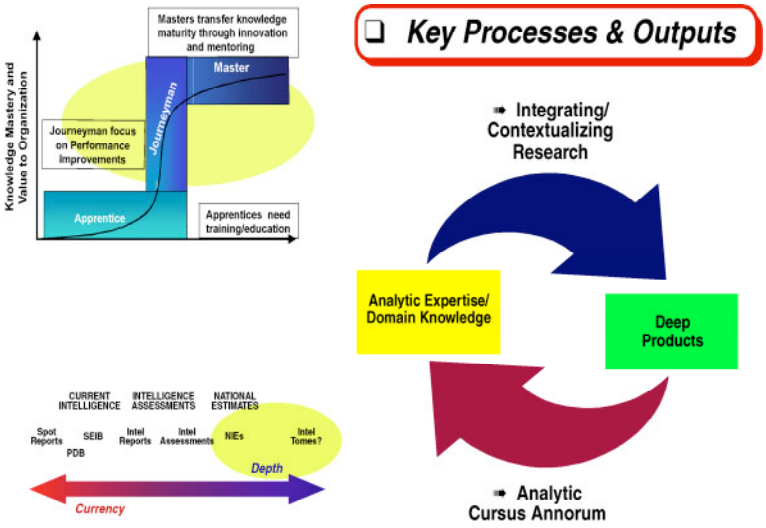
7. The Neglect of Anticipatory Intelligence

The "information revolution" has unsettled intelligence officials by providing policymakers with alternative sources for both coverage of developments and in-depth research and understanding on issues of interest to them, as well as allowing them to become their own intelligence analysts, if they so choose. These trends have left Intelligence Community managers struggling to emulate the success of television as the provider of real-time news and has prompted the worrisome notion that customers might now see intelligence as less relevant. But the community must go beyond the current interest areas of its customers if it is to perform its primary national function of preventing surprise. In the new and very dynamic geostrategic environment, perhaps the most important element of warning is the anticipatory function against the unexpected—*discovering* new activities that might prove inimical to US national interests and obtaining information about them. Leads to issues of this kind are not likely to come from customer requests; as noted, in science, "investigator-initiated" research is a particularly important driver for discovery and innovation.

Waiting on the policy community to furnish requirements for anticipatory intelligence all but assures that there will be serious warning failures.

Correcting this problem demands that the leadership of the Intelligence Community be prepared to spend real resources on issues that are not immediately "customer-relevant," even when confronted by what seem to be limitless demands to focus on high-priority subjects. Waiting on the policy community to furnish requirements for anticipatory intelligence all but assures that there will be serious warning failures—and the commu-

[23] See Douglas MacEachin, "The Tradecraft of Analysis: Challenge and Change in the CIA," *Studies in Intelligence* 46, no. 3 (2002): 23–28. It is also interesting to note that the NIE on Iraqi WMD was requested by the Senate Select Committee on Intelligence and the Senate Armed Services Committee, not by executive branch policymakers.
[24] See Rob Johnston*, Analytic Culture in the U.S. Intelligence Community.* Indeed, in response to these concerns, the Commission on the Intelligence Capabilities of the U.S. Regarding Weapons of Mass Destruction strongly urged that the PDB not become the centerpiece of the DNI's analytic focus.



Graphic courtesy of SAIC

nity will shoulder the blame for the policymakers "surprise." Faced with its concerns about diminishing relevance, the anticipatory role is one the Intelligence Community should grasp. At the same time, the dichotomy between current situational awareness based on a stream of detailed reporting and anticipatory or predictive intelligence is more apparent against a new enemy who relies on "stilettos and stealth" than it was against the Soviet Union, which amassed large stocks of advanced weapons whose visible and patterned development path took well over a decade and then allowed us to collect hard evidence on them by exercising those capabilities extensively. For a community which frequently restates the mantra that it is "an evidence-based" culture, this divergence of reduced collection capabilities against lower signature targets and the increasing demands for anticipatory judgments resting on long inference chains will create an uncomfortable problem in producing these assessments.

8. The Loss of "Keystone Species" and "Intellectual Middleware"

The relatively recent ecological concept of "Keystone Species" denotes organisms that play a central role within an environment, either as a resource or as a control mechanism. Within the Intelligence Community, the most important of these "keystone species" is perhaps the "journeymen" analysts.[25] These experienced analysts (say, those with seven or more years of analytic experience) are the functional equivalent of doctoral students, post-doctoral fellows, and assistant professors in academia and of the house staff (interns and residents) in medical education, both of which are also guild/craft systems. Journeymen perform the bulk of the work of producing products, making incremental improvements in process, teaching the apprentices, and disseminating knowledge and skills as they move to new communities. The journeymen carry institutional memory, transmit knowledge to junior analysts, and inculcate in them such vital professional values as intellectual curiosity, humility, and an ethos of continual learning. In addition, they form the core of a high-trust social network built on longstanding prior contacts that is essential to the diffusion of knowledge within the Intelligence Community and the national security community as a whole.

Recognizing the journeymen's role as a "keystone species" helps to explain the severe disruptions caused by the disproportionate drawdown in their numbers triggered by the budget cutbacks of the early 1990s. To a con-

[25] "Journeyman" is not used in a pejorative sense, but, rather, in the traditional guild meaning of the term. In CIA parlance, these are now called "fully qualified" analysts. Military homologues are Navy chief petty officers ("chiefs") and Marine gunnery sergeants ("gunnies").

siderable extent, this cadre, with its deep professional expertise, was sacrificed because of the disinterest of the policy community; nonetheless, the senior management of the Intelligence Community allowed it to happen. Moreover, increasing pressures for "broadening" rotational assignments and "up-or-out" promotion policies make it more difficult to retain the remaining cadre of deeply skilled experts as working analysts.

The loss of journeymen also underscores the crucial importance for the analytical profession of soft cultural factors and people-related processes, such as mentoring. Inadvertently, as mentors disappeared, the important socialization and professionalization processes that are essential to train, guide, and acculturate the current flood of apprentice analysts went with them. A further difficulty is that, absent either emphasis on, or demand for, research products, the departure of experienced analysts and the focus on current intelligence and reporting makes it difficult to train and mature newcomers in creating such deep products.

As a consequence, the community also lost the "intellectual middleware"[26] that was a central element of its knowledge base and what one former senior intelligence officer terms its "ecology of expertise."[27] Intellectual middleware is the profound complementary understanding of both domain and process that is gained from long experience. Along with the knowledge base built-up over years, middleware is a necessary link between current intelligence and deep understanding of a domain; it provides the essential capabilities necessary for either considered in-depth judgments or meaningful quick-response products. As a conference participant with extensive analytic experience noted, "Dick Kerr did a study…of all the analysis that was written on Iraq [by the CIA]…. He said…it was very good, there was a lot of detail, there was a lot of information, but he came away from all that analysis having no real sense of what Iraq, the country, was all about."[28] Of course, working on research projects contributes to the production of middleware, which, in turn, serves as a resource for all other products and advice; this is something that working on a succession of current and limited studies can never do.

The Intelligence Community once had a fairly standard method for introducing analysts to the process of research, which was to have them draft a new edition of a lengthy product known as a National Intelligence Survey (NIS). Working on a project such as this created in-depth analytic expertise and domain knowledge on a country or area. Above all, the knowledge gained by producing an NIS would enable an analyst to provide policymakers with the essential context for current intelligence, to render informed judgments, and to produce timely answers to important questions. Unfortunately, the importance of the NIS process was not recognized within the community, and the practice was abandoned.

9. Failure to Develop Analytic Tools and Methods for Validation

Most of the tools available to support analysis provide help for specific analytic techniques or intelligence disciplines, such as

[26] This term from the computer science community denotes software that performs intermediary functions (such as translation and data exchange) between heterogeneous systems, enabling them to function in an integrated, interoperable manner. The connotation of middleware is "glue" that enables not just interoperability but, in this context, also cross-fertilization.

[27] This concept of an "ecology of expertise," articulated by Fritz Ermarth, is a powerful tool for thinking about the Intelligence Community's role.

[28] See *Charlottesville Conference Report*, 6 and Kerr, et al.

imagery intelligence (IMINT) and signals intelligence (SIGINT), rather than for all-source analysis. Even so, there are formal methodologies taught and employed within the community for all-source analysis, especially for assessing and marshalling evidence, and there are structured methods that support hypothesis assessment.[29] Consistent with its "craft" culture, the Intelligence Community has used practical experience rather than formal validation methods to assess utility and select these tools. Rob Johnston has observed, however, that there is a large number of tools and methods available to the analytic community, but few are consistently employed—and none has been tested or validated to assure its effectiveness and utility.[30] As one seasoned analyst commented, "… imagine a nuclear powered Navy in which all the Reactor Plant Operating Manuals are written by the current ship's engineer and whenever he got relieved they were all shredded and the new engineer had to write his own."[31] Of course, as has often been noted by students of intelligence, that an agency or community opinion is wrong does not automatically mean that the process followed in reaching that opinion was flawed.[32] Again, quoting Charles Allen,

> *We're not very good at evaluating the quality of intelligence analysis independent of the outcome. We're outcome oriented, rather than process oriented.*
>
> *Conversely, when the policy succeeds and a desirable outcome occurs, we feel satisfied with the conduct of intelligence and generally look no further. The cumulative effect of this process is that it undermines the very essence of intelligence analysis.*[33]

Within the diverse domain of intelligence analysis, one would expect that analytic methods and tools would vary significantly, not only depending on the sources of intelligence available and the subject matter, but also on the epistemology of the question at hand—whether the problem is, to use Fritz Ermarth's typology, a secret, a mystery, or an obscurity. "Secret" means the information exists but must be acquired—usually by clandestine collection methods—and interpreted. A "mystery" is a question for which a set of possible outcomes may be known but whose particular outcome can be known only after the fact. An "obscurity" involves questions that are often unrecognized and not seen to be relevant until they are posed explicitly—which requires curiosity, a quality often in short supply. Data to illuminate obscurities are also often available—even if found in non-traditional sources that require imagination to identify, if procedures to filter signal from noise can be developed, and if appropriate inference chains can be constructed from the evidence. For example, Murray Feschbach drew accurate inferences about the internal strength of the Soviet system from totally "out-of-domain," low-level, openly-available statistical data on morbidity and mortality published by the Soviets themselves.[34]

The Intelligence Community, however, as a function of its history and culture, has constructed a "hierarchy of privilege" for information that still gives the most weight to

[29] See, for example, Hughes and Schum, "Evidence Marshalling and Argument Construction."
[30] Johnston, 72.
[31] Private communication from John Bodnar.
[32] Put another way, "There are too many targets and too many ways of attacking them for even the best intelligence agencies to discover all threats in time to prevent them from happening." Kerr, et al.
[33] Allen, 3.
[34] See, *inter alia*, *Russia's Health and Democratic Crises* and *Russia's Demographic and Health Meltdown*. Feschbach is currently a senior scholar at the Woodrow Wilson Center and Research Professor Emeritus at Georgetown University.

secret intelligence. Similarly, many users of intelligence information accord greater credence to reports with higher levels of classification. And, of course, the Intelligence Community often perceives its comparative advantage with decisionmakers in secret information that only it can access and supply. At the same time, unfortunately, the more evidence and judgments are restricted in dissemination by compartmentation and distribution limitations, the more likely it is that questionable judgments will pass unchallenged. This is an especially serious problem for HUMINT, which, by its nature, provides only a very narrow perspective on events for which direct confirmation may not be available. Yet timely, authoritative, and credible HUMINT is sometimes—however rarely—the only way to obtain information that can determine strategic direction.

10. The Hindrances of the Security Mindset

The current security mindset is an additional impediment to cooperation among and within intelligence agencies, between intelligence agencies and policy agencies at all levels of government, and between community analysts and outside expertise resident in both non-government and foreign sources. This mindset is extremely risk averse with respect to potential information loss, and it fosters procedures that make it difficult to pull together and share files of relevant information, to bring fresh perspectives to bear, and to exploit the synergies of expert collaboration. This current security paradigm views problem domains as discrete and separable and insists that protection of information (and, therefore, sources and methods) is more important than effective exploitation and cross-fertilization. Two problem areas, in particular, are the traditional barrier between the intelligence and law enforcement functions and between foreign and domestic intelligence. Under the pressure of countering the terrorist threat, however, these distinctions are eroding.

The Intelligence Community often perceives its comparative advantage with decisionmakers in secret information that only it can access and supply.

Chapter Four: A Program for Transforming Analysis

The following sections lay out some fundamental guidelines, or pathways, for transforming analysis, provide a set of principles upon which to base a restructured analysis paradigm, and suggest six specific areas for attention.[1] To be effective, however, necessary changes need to be implemented within the system, not just identified. Even a cursory look at the fate of previous Intelligence Community reform efforts does not lead to expectations of great success in such an endeavor. For this reason, the path suggested here offers the opportunity to make some early course corrections that can be initiated without formal sanction and with minimal changes to existing structures and authorities.[2] It also offers the possibility of winning support from the professional intelligence cadre, who must be convinced that the measures recommended are both effective and sensible. If they are not convinced, institutional inertia, if not outright resistance, will impede change. For example, groups of analysts could take ownership of these areas proposed for action, thereby legitimating the transformation effort as an organic program instead of one imposed from above.[3]

Developing a New Concept for Analysis

Several recent assessments contend that the Intelligence Community's problems are manifestations of fundamental and systematic problems within each agency's internal processes, cultures, and organizational structures.[4] Moreover, these shortcomings do not result from a flawed community architecture or from insufficient directive authorities and budgetary control over the community as a whole—although they may be aggravated by them.

There are two fundamental challenges in rebuilding analysis, with a substantial degree of contradiction and inherent tension between them. The first is to avoid being confidently wrong (as in the NIE on Iraqi WMD) by staying closer to available evidence. The second is to provide judgments on complex and often unfamiliar adversaries and on their likely behavior based on fragmentary and frequently ambiguous information (as in the circumstances leading up to the 9/11 attack).[5] The community has still not made the shift to recognizing that the dominant intelligence problems are not penetrating "denied areas," but rather understanding "denied minds." This shift requires rethinking not only the types of information that analysts need, but also the nature of the information gathering necessary to provide that information. In terms of the latter, intelligence practitioners will need to accept that the appropriate mechanisms will not be limited to remote clandestine collection systems or case officers.

The community still has not recognized that the dominant intelligence problems are not penetrating "denied areas," but understanding "denied minds."

The larger issue of how to allow a classic hierarchical organization to meet the challenges of a more fluid environment and dynamic networked adversaries must be faced squarely, but it is also an effort well beyond the scope of this study. Recognizing that this factor is important, however, the discussion below does focus on directly addressing the sources of analytic failures, including several problems stemming from a hierarchical organization model that has been both badly applied and misapplied.

[1] A comprehensive discussion of remedial measures is beyond the scope of this paper.
[2] Several reviewers, all of whom are experts in management theory and organizational behavior, suggested this idea in parallel.
[3] See Michael Mears, "The Intelligence Community Genome: RIA Paper #3." It is an insightful look at the practical challenges of organizational transformation in the Intelligence Community.
[4] See Jeffrey Cooper, "Intelligence & Warning: Analytic Pathologies," and Johnston.
[5] See Kerr, et al. for a more extensive discussion by seasoned analysts on improvements needed in analysis.

The primary purpose of analytic effort is "sensemaking" and understanding, not producing reports. . . .

Principles for a New Paradigm

A new paradigm should start with a set of basic principles to guide the rebuilding process, restore professional standards to the conduct of analysis, and help redress the effects of evolved dysfunctional practices. These principles should be mutually agreed between the leadership of the Intelligence Community and the cadre of professional analysts as the basis for an "analytic compact" that will affect priorities and taskings as well as incentives and rewards for performance. Furthermore, even if users do not fully agree, they also should understand these principles to be the foundation that guides the analytic community in its work. In the long-term, it is clearly in the interest of policymakers to rebuild the community's expertise and knowledge so that intelligence can provide highly contextualized and meaningful judgments, whether on current or future issues.

These principles ought, above all, to convey that "analysis" needs to be construed broadly and not solely in a narrow, "reductionist" context that seeks to "know" by decomposing a phenomenon into its constituent parts and approaching it analytically only on the basis of induction from detailed evidence. Many complex phenomena may be better comprehended by approaches that are based more on synthesis—that is, understanding the larger picture—by focusing on the relationships among the parts and on the emergent behavior produced by such interactions. These principles—which, of course, are not meant to be exhaustive—will recognize, therefore, that:

Philosophy and Values

- Analysts must have a "duty of curiosity," and the analytic process must encourage and reward a deep and meaningful understanding of the phenomena under investigation;
- Analysts must be responsible for defining knowledge needs and, therefore, collection requirements; to do this effectively, they must understand collection capabilities and be sensitive to their limitations;
- Analysts must be active participants in developing integrated strategies for collection and analysis, seeking information instead of being merely passive recipients;
- The primary purpose of analytic effort is "sensemaking" and understanding, not producing reports; the objective of analysis is to provide information in a meaningful context, not individual factoids;
- The knowledge discovered and the expertise created when an analyst researches a problem is at least as important as "finished intelligence" products that may result;
- Learning is an activity that is valued highly by both analysts and the organization;
- Not all intelligence need be immediately "actionable;" informing decisionmakers and enhancing the quality of the decision process is a critical objective;
- Intuition and creative thinking, including positing hypotheses to be tested, are as important to analysis as evidence-based inductive approaches.

The Overall Approach

- There are different analytic problems, and there are diverse approaches and methods for resolving them; in many cases, appropriate and intuitively usable tools may enable their consistent use and enhance the effectiveness of these approaches;

- There should be no assumed "hierarchy of privilege" of sources or analytic methods; a wider range of methodologies needs to be employed routinely and consistently, not seen as exceptional "alternative" techniques;

- Analytic tools are intended to support, not supplant, rigorous and structured cogitation by human analysts;

- There should be better access to, and exploitation of, open-source information as an element of all-source analysis;

- Deductive hypothesis-based methods should be employed more often as a complement to traditional evidence-based inductive approaches;

- There should be more use of formal tests of diagnosticity of evidence, thereby improving the ability to confirm or deny hypotheses;

- Collaboration during the analytical process should be routine, not exceptional, and workloads should be balanced accordingly;

- Review and assessment—including peer review—must be an integral element of the analysis and should not be conducted only after-the-fact;

- There should be greater recognition of the propaedeutic and heuristic roles of writing—as tools of discovery and learning—for the analyst; writing is not just a method of transmitting information to the user;

- Contrarian methods and "Red Teams" should be a routine part of the analytic process;[6]

- As opposed to the incremental approach, in which new evidence is assessed piecemeal for its effect on the course of judgments made, more use should be made of a "stock-take" approach, in which the entire collection of evidence is reviewed holistically;[7]

- "Process watchers," charged with recognizing cognitive impediments and process failures, should become integral parts of analytic teams;[8]

- In addition to reviewing products at hand, analytic managers and senior Intelligence Community overseers should subject the knowledge base and domain expertise to continual appraisal in order to assess whether the scaffolding of evidence and the inferential reasoning is sufficiently strong to bear the weight of the judgments being made and the policy decisions that may rest upon them.[9]

[6] Composition of the teams, however, might better be rotational and *ad hoc*. See also Kerr, et al., 52: "Indeed, although certain gaps were acknowledged, no product or thread within the intelligence provided called into question the quality of basic assumptions…."
[7] The "stock-take" originated in the UK atomic weapons program; it differs fundamentally from the more usual practice, which holds that new information will appropriately correct earlier judgments. But this approach, based on Bayesian logic, depends on the earlier "priors," which may never be carefully reexamined.
[8] Professor Daniel Kahneman, who teaches at Princeton University, also suggested this approach in the slightly different military "command and control" (C2) context in an interview with me in October 2000. Johnston discusses this approach at length in his chapter on "Integrating Methodologists into Teams of Experts."
[9] Fritz Ermarth made this suggestion in a communication to me on 23 January 2005.

Analysts should expect users to "pull threads" and question judgments in open dialogue.

Interaction with Users

- There may not be a "right" answer, and there may be limits on "knowability";
- Users are owed an honest assessment of the quality of evidence, uncertainties in judgments, and the "knowability" of the answer; transparency in the logic chain and application of evidence is essential;
- Such assessments can be better conveyed through conversation and dialogue than through static "finished" products;
- Analysts should expect users to "pull threads" and question judgments in open dialogue.

Management and Oversight

- Management's first responsibility should be to remove impediments to analysts' ability to function effectively; the core management function is to ensure the process is being followed and is adapting as necessary to changing needs;
- Commitment by analysts rather than enforced compliance by managers must become the driving force in renewed analytical practices;
- Management must be knowledgeable about the practice of analysis and must provide appropriately focused incentives for those they supervise;
- Managers must encourage self-awareness, questioning of existing procedures, and striving for continuous improvement;
- The organization should create a "learning environment"—not only for domain knowledge, but also for process and methodological expertise;
- The organization must encourage not only "near-miss" analysis and error detection, but also the consistent reporting of anomalies and errors;
- There should be toleration of first errors, but no tolerance for repeating the same mistake; being wrong will happen, but failing to learn should be subject to sanction.

Cautions and Precautions

- Self-awareness of cognitive biases and institutional prejudices, as well as a more self-reflective manner, should be intrinsic elements of an analyst's mindset;
- There is no "revealed truth," and assertion by reference to evidence or previous "finished" intelligence products is not proof;
- "Truth" is not held solely by the Intelligence Community, either here or abroad;
- "Truth" is also not necessarily the first priority of users' questions, but answers by analysts should be;
- Ongoing re-examination and revalidation of previous judgments is very important; unless care is taken to validate and maintain the currency of the library of finished intelligence, "layering" poses significant dangers for the analytic process;

- Keeping an open mind—framing multiple hypotheses and looking at different potential interpretations of "the evidence"—is essential if locking in premature judgments is to be avoided;

- Regardless of the apparent rigor of the process, an analyst must approach analytic issues with "mindfulness" of the potential pitfalls in evidence and analytic methods that are being applied to a particular problem;[10]

- Tools and methodologies should be tested and evaluated for analytic effectiveness and usability before adoption, and analysts should have an important role in evaluating them;

- Because "mindfulness" only goes so far in detecting one's own biases and cognitive failings, a supervisory function that watches over the conduct of the process is important;[11]

- Differences in culture and governance mechanisms are real—not all human actions are determined by Western notions of rational thought or Enlightenment values—and they affect societal and individual preferences and decision metrics.

Additionally, if at all possible, the first audience for the knowledge gained should be the peer "community of practice" rather than the policy users.[12] Too much focus on "serving the first customer" may have served to shortchange the depth of analysis and the rigor that would be demanded by knowledgeable peers. Moreover, analysis must pay more attention to how the knowledge is conveyed to the users while, at the same time, recognizing that the message should rest on a "sound story." The analytic process must reinstill a sense that the discipline of writing serves to discover the story, not only to convey it, and appropriate incentives to encourage these behaviors must be instituted.

Getting Started: Six Fundamentals

If at all possible, the first audience for knowledge gained should be the peer "community of practice" rather than the policy users.

This set of principles provides the basis for a systematic campaign to enhance analytic effectiveness in the three interrelated areas of people, process, and technology. The process dimension defines the characteristics and qualities of the enhancements needed in the people and technology areas, and that is the focus of this study. The people dimension must address, in addition to recruitment and training, impediments to good work and work practices, retention, and professional development, as well as appropriate organizational and institutional incentives to overcome them. The technology dimension must be centered around enabling and facilitating both the people and process dimensions, not simply on updating the technical infrastructure to move more data faster.

The corrective measures proposed here address six processes that are indispensable to restoring the Intelligence Community's capability to perform effective intelligence analysis. These proposals emphasize:

[10] See Warren Fishbein and Gregory Treverton, *Rethinking "Alternatives Analysis" to Address Transnational Threats.*
[11] The standard approach to addressing bias and prejudice in judgment and decisionmaking has been through training to recognize one's own cognitive errors. During my research on cognitive impediments to C2 decisionmaking for the Defense Advanced Research Projects Agency (DARPA), Professor Daniel Kahneman pointed out that this approach has not succeeded, despite more than 25 years of trying. Kahneman was awarded the Nobel Prize in Economics for his work on imperfections in decisionmaking. (Personal interview, October 2000.)
[12] This issue was highlighted in Rozak, *et al*.

1. A reconceptualized set of processes and procedures (including tools, methods, and practices) for analysis;

2. An integrated process for recruiting, training, educating, and professionalizing analysts based on a traditional graduate education model emphasizing close mentoring;

3. A new, more interactive process for communication between users and intelligence analysts throughout the intelligence cycle;

4. A fundamentally revised process for establishing "proof," validating evidence and judgments, and reviewing those judgments;

5. A process for capturing the lessons of experience and advancing organizational learning; and

6. A process for continual collaboration and sharing.

A Revamped Analytic Process

Effective intelligence analysis requires the coupling of deep expertise with innovative approaches and intuition instead of the constraining formalism of "scientism." Although adopting methods of alternative analysis[13] and setting up red teams are a useful start, creating a more coherent structure and a demanding, self-reflective analytic process must also involve more than calls for lateral, out-of-the-box, or non-linear thinking on the part of individual analysts. Real change must alter the very modes of thought that dominate the expectations and practices of today's users, managers, and creators of all-source analysis. Both "sensemaking" and curiosity should be basic elements of this transformed paradigm.[14]

Models already exist for such a new paradigm, as a review of other domains in which failure of work processes can have large potential adverse consequences demonstrates. These domains fall into two distinct categories: 1) where the standardized procedures may not be sufficient to prevent routine but costly failures and 2) where routine procedures are clearly insufficient to face extraordinary conditions. In all of these models, however, the salient features are a high degree of self-awareness, emphasis on early error detection and correction, and the ethos of a "learning organization."

In the first category are organizations, such as those engaged in manufacturing and transaction processing, which specialize in maximizing the effectiveness of routine operations through continuous attention to improvements in the process. For these organizations, even small variances in outcome are a signal that routine procedures need to be adjusted, or significantly altered, in order to correct errors that cumulatively could become worrisome. These organizations have adopted the emphasis of the Quality Movement on consistent, continual self-examination and improvement; perhaps the best known of these is Toyota with its formalized *kaizen* (continuous improvement) system. Other organizations have implemented similar techniques; among these are the "5 Whys Approach," which focuses on recursive questioning to identify the root causes of failure rather than its superficial symptoms, and the Six Sigma Movement, which emphasizes consistency and reductions in process variance.[15]

[13] See Fishbein and Treverton, 2, for a succinct and useful discussion of "alternatives analysis."
[14] "Sensemaking" in this context means the ability to perceive, analyze, represent, visualize and make sense of one's environment and situation in a contextually appropriate manner. See both Fishbein and Treverton, 3, and Cooper, "*Sensemaking: Focusing on the Last Six Inches*."
[15] See the Six Sigma website, http://www.isixsigma.com/.

In the second category, such domains include the nuclear power industry, civil aviation, and aircraft carrier operations. These organizations recognize that routine operations can produce or face conditions that unexpectedly turn extraordinary, with serious, adverse consequences. The paradigm for organizations of this type is the High Reliability Organization (HRO) model.[16] Some commentators would also include hospitals, and especially their high-risk specialty units, as HROs because of the large consequences of error. Built-in practices—formal protocols, structured procedures, and self-awareness measures such as mortality and morbidity (M&M) conferences—are a sign that hospitals recognize the risks of errors.[17]

A common denominator of both categories of organizations is that they "…reliably forestall catastrophic outcomes through 'mindful' attention to ongoing operations."[18] As Fishbein and Treverton note, quoting Karl Weick and Kathleen Sutcliffe, "The unifying trait of HROs is that they exhibit the quality of 'mindfulness,' defined as:

> *…the combination of ongoing scrutiny of existing expectations, continuous refinement and differentiation of expectations based on new experiences, willingness and capability to invent new expectations that make sense of unprecedented events,…and identification of new dimensions of context that improve foresight and current functioning.*[19]

These organizations address the possibility of extraordinary events by building procedures that are designed to do more than maximize effectiveness and efficiency in the conduct of routine operations. The organization is focused on addressing *non-routine operations*, so that the unexpected "…doesn't surprise or disable them" and "…coping actions seldom make the situation worse."[20] These organizations see small errors in routine operations, in addition to their role as process signals, as indications that organizational compliance and managerial oversight are slipping—and that such slippage could presage worse failures.

Both categories of organization understand that successful day-to-day operations can give rise, in effect, to *mindlessness*, defined as inattention to the environment and to internal procedures. In these circumstances, people slip into routines, fail to notice changes in a larger context, see new phenomena in old categories, and use incoming information (even if it indicates significant variances) to confirm expectations. *Mindfulness*, on the other hand, emphasizes continuous updating and assessing alternate interpretations and implications of incoming information; even small signs of failure can suggest serious problems in organizational processes and compliance with them. In these organizations, according to Wieck and Sutcliffe, there is a "preoccupation with failure, both past and present"; and there is a concomitant stress on early error detection and cor-

Successful day-to-day operations can give rise to* mindlessness*, defined as inattention to the environment and to internal procedures.

Mindfulness*, on the other hand, emphasizes continuous updating and assessing of alternate interpretations and implications of incoming information.*

[16] A number of perceptive commentators have pointed to HRO as a useful model, although often for diverse reasons. See Sabel, Johnston, and Stephen Marrin in "Preventing Intelligence Failures by Learning from the Past," and Fishbein and Treverton.
[17] The continuing high rates of medical errors and the increasing appearance of "iatrogenic" (that is, physician-induced) diseases in hospitals suggest, however, that these organizations have a long way to go before they can be fully recognized as HROs.
[18] Karl E. Weick and Kathleen M. Sutcliffe, *Managing the Unexpected: Assuring High Performance in an Age of Uncertainty*, 23.
[19] Fishbein and Treverton, 4, quoting Weick and Sutcliffe, 25.
[20] Weick and Sutcliffe, 42.

rection at the lowest levels, as well as emphasis on error reporting upwards as part of the self-assessment "contract."[21]

Each category contains proven features that recommend themselves for inclusion in a new synthesis for a transformed intelligence analysis process.[22] ***From the High Reliability Organization,*** the feature is "mindfulness," which is composed of five processes (and sub-processes below them): anticipating and becoming aware of the unexpected; containing the unexpected; near-miss analysis; active management; and enhancing containment. The most important elements in creating an anticipatory capability are a reluctance to simplify interpretations, which increases blind spots by filtering and abstracting key details; recognizing the effect of categorization on expectations by continually reexamining categories and event coding; and reassessing the basic assumptions and keystones of one's analysis and analysis process. In addition, the stress on "near-miss analysis" is designed to recognize imperfections and errors before they cause consequential failures.

The process watcher function is intended to focus exclusively on identifying errors in the analytic process, not on alternative interpretations of the evidence or different logic chains.

> *Both [near-miss and line stoppages in a just-in-time system] trigger root-cause analysis meant to uncover not only the proximate cause of the incident, but to eliminate, through redesign of the organization if necessary, the background conditions which generated the immediate source of the danger.*[23]

From the Quality Movement, the synthesis model adopts the "5 Whys Approach," employing a recursive questioning process that emphasizes the importance of identifying root causes of errors. This involves looking beyond the obvious first answer to the "what went wrong" question to the serially deeper causes until the base source of error is found. ***From medicine***, there are two elements worth including. First is the practice of mortality and morbidity conferences, which focus on both near-miss and failure analysis. The second is the practice of "grand rounds" in which house staff, students, and attending physicians brief and review especially difficult cases. Both measures underscore the importance of open and collaborative communication in identifying and assessing hard problems, including both those that were resolved successfully and those that failed. Such open communication is essential to both investigatory and teaching roles. Finally, ***the introduction of a "process watcher,"*** as suggested by Kahneman, is intended to bring a clear and unbiased, outside expert's eye to analytic teams. The process watcher function, unlike that of a Red Team, is intended to focus exclusively on identifying errors in the analytic process, not on alternative interpretations of the evidence or different logic chains.

In light of the real challenges to conducting complex analysis effectively, it is important that the Intelligence Community identify and evaluate tools and methodologies that can help analysts make sense of complex phenomena rife with ambiguous or incomplete evidence—and then actually provide them. The revamped paradigm must also include processes that are more specifically directed toward strengthening the practice and content of analytic methods. This paradigm would very likely incorporate more widespread and routinized use of formalized techniques, such as Analysis of Com-

[21] Weick and Sutcliffe, quoted in Fishbein and Treverton.
[22] This study will develop a brief outline of such organizational characteristics, but a comprehensive treatment will require a separate paper.
[23] Sabel, 30.

peting Hypotheses (ACH), to explore multiple hypotheses and would employ appropriate supporting tools to facilitate their use.[24] There would also be more emphasis on the use of negative evidence and on its implications for key assumptions and inferences, especially when the orientation is toward current intelligence.[25] Finally, new collaborative mechanisms, such as "blogs" (web logs), "wikis" (wikipedia entries), and groupware could be employed to facilitate better communication and a more continuous dialogue among the parties within the community of interest.[26]

This new analytic paradigm is designed to lead analysts to reflect more intensively on the practice of their trade. It is also intended to develop more structured procedures and to instill in both individual analysts and analytic units the discipline to follow them. Such changes will need to be implemented carefully, so as not to interfere with individual creative processes and existing analytic practices that are effective, especially those that are unorthodox and not easy to assess with formalized metrics. It will be especially important to guard against the danger that too much introspection will cause analysts to avoid risk by dodging judgments.

Recruiting, Training, Educating, and Developing Professionals

In the wake of 9/11, the Intelligence Community has been able to take advantage of an upwelling of public support to tap a large pool of candidate analysts. These candidates are, on the surface, talented, diverse, and well educated; but they will require extensive training and professionalization in order to become effective and productive contributors to the analytic community. Furthermore, in current circumstances, when analysts should more frequently be addressing the challenge of "discovery" and open-ended, undefined problems than more readily defined monitoring tasks, they are confronted by time pressures that leave them with little latitude for reflection and wondering. Moreover, our educational system increasingly produces linear thinkers more comfortable "painting within the lines" and pointed more toward likely solutions than toward broader problem-solving capabilities.[27] It is unclear if these shortcomings can be corrected by better-targeted recruitment and more effective training, or if it must be addressed by redesigning fundamental processes and practices; it is likely that both tracks will be needed.

However the question of academic preparation is resolved, rebuilding the apprenticeship and mentoring system is crucial. It is essential, therefore, to reconstitute the "keystone species" represented by the journeyman analyst.[28] This cannot be done by bringing in a flood of young, inexperienced analysts; dousing them with a short period of classroom training (begrudged by their managers and mostly focused on the right tone and format for reports); and leaving them to learn good practices while sifting for nuggets of current intelligence.

There is no known mechanism that can turn the apprentices into "instant" journeymen; they cannot be transformed by lectures,

[24] An example is the ACH Tool developed by Palo Alto Research Center (PARC) for the Novel Intelligence from Massive Data (NIMD) Program under the Intelligence Community's Advanced Research and Development Activity (ARDA).
[25] Kerr, et al.
[26] See Calvin Andrus's Galileo Award winning paper, "Toward a Complex Adaptive Intelligence Community," in *Studies in Intelligence* 49, no. 3 (2005).
[27] As Daniel Goleman noted in his answer to the "2005 *Edge* Question," an annual survey by *The Edge*, an internet site favored by the technical community.
[28] Additional incentives to retain these experts appear worth considering.

As an Intelligence Analyst's Rite of Passage Might Look

As the Stefiks made admirably clear in their book about innovation:

> *Graduate school is a rite of passage for becoming researchers and inventors. Graduate schools create the next generation of researchers and inventors who are primed to step into positions in the world of science and innovation.*
>
> *The experience of graduate school draws on a much earlier tradition than undergraduate education, or even high school and grammar school. Education prior to graduate school is dominated by a program of lectures, exercises and exams. Such educational practices have a predetermined curriculum intended to serve classes of students essentially in lock step….*
>
> *In contrast, graduate school is based on the older tradition of mentoring and apprenticeship. Graduate education is about assisting students to take on a professional practice. The curriculum is more tailored. Students acquire the practice by working with multiple mentors, adjusting the emphasis to fit their career objectives. Students discover, sometimes by osmosis, elements of practice that would seldom be encountered in a classroom setting. Graduation requires demonstrated mastery at the level of a practitioner in the field.*[1]

[1] Stefik and Stefik, 85.

abstract study, or classroom exercises; nor can software tools enable them to substitute for more experienced analysts.[29] This challenging task demands a focused, directed effort at deep analysis within a subject area, most likely through a tutoring and apprenticeship model.[30] In addition, revised classroom instruction, based on a significantly strengthened curriculum emphasizing analytic methodologies and methods, could have an important role within a rebuilt program for professional development. The Intelligence Community should move away from "training courses" that take analysts off-line for weeks to months and reintegrate this type of training directly into the "practice" of intelligence analysis, as is done in clinical education for medicine and law. Moreover, it is absolutely essential to create a professional "duty of curiosity," which the training process would embed in the professional ethos and management would encourage, even in the face of time pressures to meet priority taskings. Further, a peripatetic career for senior analysts—"moving around to move up," often increasingly farther from the actual practice of analysis—is not a useful way to foster deep expertise or to create effective role models. Reestablishing a new cadre of effective professional intelligence analysts will require basic changes in their career patterns, potentially requiring that the military practice of tracking and protecting vital sub-specialties with their own career ladders be emulated.

These factors prompt the thrust to restructure the career path of intelligence analysts, perhaps along the lines of medical or science graduate education—especially doctoral and post-doctoral—that integrates classroom learning, research, and clinical practice. In neither case are education and training separated; each is seen as an integral element in producing a practicing member of the medical or scientific community. In this context, then, deeper analytical products are essential to building the process expertise and domain knowledge of the analyst and to rebuilding the domain knowledge base. Together, these capabilities enable a skilled analyst to contextualize current intelligence for the decisionmaker.

Such a restructured program should also seek to foster an open seminar atmosphere during the training process and impart to analysts the practice of critical collaborative discussion within a professional network

[29] Frank J. Hughes, *Preparing for the Future of Intelligence Analysis*.
[30] Hughes, 2–3

carried directly into the workplace. Moreover, in this process, in which socialization is seen as an important aspect of absorbing the ethics and ethos that should guide a professional, a close relationship with a mentor is crucial. The mentorship process also reinforces the HRO's emphasis on a "culture of learning," a habit of error reporting developed by encouraging openness, tolerance of even "stupid questions," and professional collaboration as a norm.

The drastic shortages in the cadre of experienced analysts prompt three final thoughts on this process. First, the Intelligence Community must bring back sufficient mentors (even if on contracts that permit double-dipping), so that it can truly support the apprenticeship model with highly personalized mentoring. This will not be an easy task; mentors will need to be chosen carefully and supervised properly, so that the right lessons from experience are passed on—not cynical views carried away from previous experience with a dysfunctional process. Second, the community also needs to give up the conceit that it can develop software and tools that will make the novices into journeymen or experts without their going through this lengthy process of apprenticeship. This is not to say, however, that appropriate tools either do not exist or cannnot be developed to help them do their jobs better and perhaps progress through the cycle more quickly. Third, and perhaps most important in the interim, the Intelligence Community should look for alternative ways to produce the intelligence insights that the journeymen used to provide while, at the same time, reestablishing the vital interrelated processes that created and fostered the development of "intellectual middleware." During this effort, managers must avoid the temptation to use these mentors to supplement the analytic cadre or to force the apprentices to rush their "analytical" fences.

About Apprenticeships

There is often a gap between what can be learned in formal lessons and what needs to be conveyed in total.…

When graduate students begin working with their mentors, they are embarking on a journey with an experienced guide. Apprenticeship amounts to going around the research cycle a few times, asking questions, and getting help at the trickier steps.[1]

[1] Stefik and Stefik, 86.

User-Community Interactions

The current processes for interaction between the Intelligence Community and its consumers, especially senior policymakers, do not work well at either end of the "Intelligence Cycle." The community does a less than satisfactory job of communicating its judgments to these customers.[31] At the same time, few users have any real education or understanding of the Intelligence Community's capabilities and limitations. To a large degree, both problems can be ascribed to too little sustained dialogue, interaction, engagement, or mutual understanding; both parties fail to understand that they are in a collective process of discovery, sensemaking, and judgment. These failings have not come about by accident, however, but by community preference. They flow from what have been deeply rooted beliefs—especially strong at CIA—that too close an association with policymakers and their political concerns runs the danger of contaminating "pristine" intelligence analyses with "policy judgments."[32] As noted ear-

[31] The term "Intelligence Cycle" is itself part of the problem. With its Industrial Age antecedents, it usually conveys the notion of a self-contained "batch" process rather than a continuous spiral of interactions.

lier, maintaining an appropriate degree of objectivity is a difficult problem; but a good solution is to be found neither by substituting users' judgments for those of intelligence professionals nor by the professionals ignoring users' real interests and needs.

Since the collapse of the Soviet Union, this mutual lack of understanding, combined with the lack of a sustained strategic policy that would provide consistent guidance and priorities, has forced the Intelligence Community to divine targets and priorities from immediate customer requirements rather than from a longer time horizon with a more strategic, synoptic, and open-minded field of view. Moreover, this tendency was reinforced throughout most of the 1990s by budget pressures that drove the community to focus on issues "relevant" to senior policymakers —and, therefore, defensible in budget hearings. Unfortunately, this approach guarantees myopia, and the Intelligence Community winds up bearing the blame for "failures" to see threats from outside the policymakers' fields-of-vision.

Analysts and their managers should be prepared to be forthright in admitting what they don't know and in identifying explicitly the uncertainties in judgments they provide.

The current "over-the-transom" process for taskings and questions often leaves the working analyst without a good understanding of the real issues at stake or the purposes to which customers will put the answers once delivered. Yet, both are important if uncertainties and sources are to be addressed in a context that the policymaker can appreciate. When the Intelligence Community provides its analyses and judgments, too much emphasis is given to the format in which the information is presented, and there is too little real dialogue with the users. The layout—too frequently formal, precisely-formatted, sterile "finished products"—often masks uncertainties and points of contention unless the reader is witting enough to "pull the threads," an effort that can lead to charges of politicization.

The community should move away from the notion that "finished intelligence" conveys certainty; highlighting and clarifying disagreements, especially over fundamental assumptions and judgments, would be of more value to high-level policymakers.[33] At the same time, the false expectations conveyed by the "conceit of finished intelligence" and the "illusion of omniscience" must be changed on both sides. Users must learn that there may not be a "right" answer; that the "more probable" case in the forecast set may not be the situation that will eventuate; and that, therefore, a range of thoughtful (and thought through) contingency responses may be necessary.

Equally, analysts and their managers should be prepared to be forthright in admitting what they don't know and in identifying explicitly the uncertainties in judgments they provide. This means providing greater transparency and traceability as they construct inference chains based on explicitly denoted qualified evidence, other information, assumptions, and hypotheses.[34] Analysts must themselves remember and remind policymakers of Heisenberg's rule: that we are not simply outside observers of a process who have no effect on the outcome; our perceptions and actions are integral elements in a multiplayer game with strongly coupled feedback loops and action-reaction cycles.[35] Finally, it must be recognized that the frequent lack of deep understanding of intelligence on the part of its primary policy users suggests that a serious education effort needs to be undertaken.

[32] See Davis, "Kent-Kendall Debate."
[33] See Kerr, et al. on "Integration with the Policy Community," 52.
[34] This has important and challenging implications for the estimative methods used by a community self-defined as "evidence-based."
[35] German mathematician Werner Heisenberg (1901-1976). I am indebted to John Bodnar for highlighting this issue.

Members of other communities—the strategic nuclear community may be the best example—deal with arcane subjects that must be communicated clearly to national decisionmakers who often lack experience or expertise in such matters. They have addressed this problem by developing formal procedures for educating their users and managing their expectations.

Unfortunately, if all the policymakers see is a continuous flow of "current information" while lacking deep knowledge of a topic or the time to synthesize and integrate what they do learn into a coherent picture, an Intelligence Community version of Gresham's law may well apply—factoids devoid of context will drive out thinking. This situation has implications not only for management of the technical systems that support and encourage collaboration and sharing, but also for the important social aspects of group behavior and the mechanisms for interaction between policy users and the analysts. It has significant implications both for the roles intelligence analysts will play and for the modalities through which they produce and communicate their analyses to users.

Communicating complex judgments and degrees of confidence in those judgments is best done through conversation among the parties, which demands different mechanisms than simple dissemination of "facts." If the mechanisms for interaction with the users of intelligence are designed only to support the provision of individual pieces of evidence rather than to engage both parties in an extended conversation in which ambiguity and subtlety can be communicated, it is unlikely that either party will be satisfied with these interactions. Indeed, it is worth asking whether the Intelligence Community has any unique contributions to make to anticipatory judgments compared with what policymakers can provide themselves, and, if so, what are they? Posing the question this way emphasizes that such anticipatory assessments are in the realm of judgment, an area that the community, in its quest for "rigor," has often tried to avoid. Now, given the variety of alternative information sources available to the policymaker, is even superb "current reporting" enough to make the community essential, especially to the policy users?

"Proof," Validation, and Review

The community needs to create processes that capture the best of the legal system's adversarial model and the scientific community's horizontal peer review.

Failures in the pre-war estimates concerning Iraq's WMD capabilities highlight deep-seated problems in the extremely "self-referential"—that is, customarily internal, collegial, and lacking rigor—process for reviewing and validating intelligence judgments. At the same time, there is absolutely no excuse for allowing easily correctable errors, such as "Key Judgments" that differ from the body of the text or references to earlier assessments that portray their judgments inaccurately, to be conveyed to consumers.[36] The existing process relies fundamentally on an analyst-level coordination process augmented by a hierarchical review process, most often by managers who possess less specific knowledge and are farther removed from the craft of analysis. The community needs to create new processes that capture the best of the legal system's adversarial model of open combat and the scientific community's truly horizontal peer review and independent replication, sprinkling in alternative analyses and red teams to do so on both process and substance.

Such processes, even if conducted totally inside the community, are bound to be distressing, as knowledgeable individuals subject an analyst's evidence, assumptions,

[36] See *SSCI Report*, 286 and 300.

hypotheses, and logic to increased scrutiny. These mechanisms, including workshops and roundtables, would be useful; but if they are composed solely of Intelligence Community members, or those who defer to them, then the problem of a self-referential "proof process" will continue. Therefore, painful as it might prove to be, the Intelligence Community must step outside its usual circle and exploit a wider range of expertise.

To understand "what works" and "what doesn't work," the Intelligence Community should establish an institutional "lessons-learned" process.

In addition to peer review, the scientific community has fostered a range of self-correcting features, such as tension between experimentalists and theoreticians. It also relies on a wider range of alternative proof models. Such additional mechanisms for validation should be examined for incorporation in the revamped intelligence analysis process. Furthermore, as in medicine, law, and science, mechanisms need to be developed and implemented to ensure that knowledge bases are updated and corrected as necessary and that users are notified of major errors in previous reports, so that the cumulative knowledge base is as accurate as possible.[37]

Finally, both the Intelligence Community and its users must have an accurate calibration of whether intelligence is "on top" of important issues and domains. The review process must go beyond assessments of individual products and personnel performance to create processes that assess the "state of knowledge" and the community's (and its users') awareness of that state. This type of self-diagnosis is badly needed, especially as it creates an environment for self-criticism combined with a license to look at the adequacy of information both on specific issues and across wide domain areas.

After-Action Reports and Lessons-Learned Processes

Unlike medicine or law, militaries do not usually have the luxury of a continuous stream of real opportunities to "practice" their craft or profession. To address these problems, the US military counts on intensive individual and unit training, institutionalized after-action reports and lessons-learned processes, and the exercise of complete operational organizations before units participate in actual operations. It also instantiates understanding of what works best as formal "doctrine" that can be studied and inculcated to provide a common frame of reference and instinctive procedural basis. One can find very similar systems created in both academia and medicine to educate and train their incoming members. In these other professions, there is little distinction or separation between education, research, and training; rather, there is a continuum of learning that depends heavily on the "hands-on" transmission of domain knowledge and process expertise.

In order to understand both "what works" and "what doesn't work," the Intelligence Community should establish an institutionalized lessons-learned process. This would include not only postmortems on major failures but also on successes and near misses.[38] The purpose of this process is not to assign blame, which is traditionally an inspector general function, nor is it to punish; rather, it should serve as an aid to individual and organizational learning. Both after action reports, developed originally at the US Army's National Training Center (NTC), and lessons-learned processes, used by the Army and the US Joint Forces Command (JFCOM), are effective methods and would be good starting points for creat-

[37] This problem is significantly aggravated by the lack of a coherent information infrastructure.
[38] This is very much like Klein's "premortems," cited in Fishbein and Treverton, 7. See also Gary Klein, *Intuition at Work: Why Developing Your Gut Instinct Will Make You Better at What You Do*, 88.

ing an Intelligence Community effort. A good complement to the lessons-learned process is the use of wargaming and scenario methods, developed on an accurate historical basis, to force the participants to examine the situation, the players, their interactions, and the outcomes in a thoughtful manner.

After action reports and lessons-learned processes can also furnish objective evidence of the utility of tools and methodologies and their suitability for addressing various kinds of problems. Without such a measured baseline of effective procedures, methods, and tools, it is difficult to create consistent processes to select and adopt appropriate analytic methodologies or to train and exercise personnel. In addition, a baseline makes credit assignment and personnel efficiency reviews more reliable. As another former analyst and thoughtful observer of the analytic process has written,

> *The identification of causes of past failure leads to kernels of wisdom in the form of process modifications that could make the intelligence product more useful. A more effective, more accurate intelligence capability may still be vulnerable to the cognitive and institutional pathologies that cause failure, but a self-conscious and rigorous program based on the lessons derived from the existing literature would strengthen the intelligence product.*[39]

Key Questions in Reviewing Lessons Learned

Veteran analyst Charles Allen provides a list of questions that a lessons-learned process can assist in answering:

- What set of hypotheses was being considered? Was the set comprehensive, or was there bias in the selection of hypotheses? What *a priori* probability was attached to each hypothesis? Again, was there bias?
- Was there a good understanding about the observables that were expected to differentiate between the hypotheses? Was intelligence collection requested on the basis of these differentially diagnostic observables?
- Were all the available data considered? How were the data weighted? What degree of credibility was accorded the sources?
- Was the possibility of deception considered and accounted for?
- Was the analytic process logically correct? Was the confidence in rendered judgments correctly estimated? If so, and if the confidence was low, was additional collection requested?
- Were the judgments presented in a timely and adequate manner?
- And, of course, was intelligence collection responsive and timely?[1]

[1] Allen, 3–4

Collaboration

Several of the recent investigations point to the important role in these intelligence failures of lapses in sharing information and coordinating efforts among the constituent elements of the Intelligence Community. Not surprisingly, the suggested remedies often involve establishing new directive authorities to mandate coordination and collaboration and build or improve the technical information infrastructures that could support collaborative activities. In fact, solutions do not start with either directive authorities or new IT systems, although an improved, technically sophisticated information infra-

[39] Stephen Marrin, "Preventing Intelligence Failures by Learning from the Past," *International Journal of Intelligence and Counterintelligence*, 2004. A recent conference on lessons learned, sponsored by the Center for the Study of Intelligence, discussed this question at some length and provides an excellent point-of-departure for implementation projects. See *Intelligence Lessons Learned Conference*.

structure would help. Rather, effective collaboration is fundamentally a matter of culture and values; what is needed is, first, to create appropriate incentive structures for sharing and, second, to forge expert social networks and effective "distributed trust" systems. These are problems of organizational culture that demand active leadership at all levels of management throughout the community.

Sharing of private information among experts is task for which technical solutions exist, but the community's technical, organizational, cultural, and incentive structures fail to support it.

Moreover, as mentioned previously, the success of the Intelligence Community depends on the promotion of an entire set of effective collaborations: among analysts; between analysts and collectors; between analysts and operations officers; between analysts and the intelligence users; and not least, between community analysts and information sources outside the intelligence or national security enterprise. For example, tasks such as target assessment and collection planning involve complex collaborative activity among analysts and collectors. Often there are subtle bits of information that appear significant only in the context of tidbits from other disciplines or aspects of tradecraft which may be little understood—or not at all—outside the ranks of its own practitioners. Each of these collaborations involves a distinct "community of interest" or "community of practice" and represents a different type of social construct; none is fundamentally dependent on building more elaborate technical infrastructures as its primary need. Fostering effective collaborations can serve an important bootstrapping function as well, because participants in the collaboration are likely to become effective champions of more collaboration.

Furthermore, true collaboration within the Intelligence Community should address more than simply sharing raw intelligence among different analytic components or taking part in the coordination process for finished products. The Intelligence Community understands how to do these tasks, even if they are not implemented effectively today. The real challenge and greatest leverage will come from sharing private information, initial hypotheses and tacit knowledge, among networks of experts in order to increase the opportunities for discovery of previously unrecognized significance. This is a task for which technical solutions are now known and feasible, but the community's technical, organizational, cultural, and incentive structures fail to support it. A true collaborative environment must build effective trust systems among community analysts and collectors, especially between the DI and the DO. Indeed, such trusted environments should extend beyond the Intelligence Community to policymakers and, eventually, to other sources of expertise outside of the community and even outside the United States.

Another important reason for fostering collaboration is that of reducing information costs. Such reductions can result not only from the powerful impacts of information technologies on organizational forms, but also from the role of "social networks" as a medium for sharing among trusted members. Such networks, especially those among journeymen analysts, substantially reduce the transaction costs of creating and transmitting knowledge; in particular, they are a low-cost information resource for the essential tacit knowledge, both domain and process, that is so difficult to elicit and instantiate in formal knowledge systems. Moreover, because of the wide-ranging social network that journeymen build over their years of service, these networks can both help to diffuse account-specific insights into other areas and infuse other perspectives into their domain, often cutting across formal community security compartmentation restrictions. As with many examples of military C2, it is these informal networks and processes that truly enable the system to function. The potential of using "groupware," such as Groove and

other collaboration platforms, in building and strengthening these social networks bears careful exploration and experimentation.[40]

Finally, the Intelligence Community's security mindset should also be addressed. The overall approach to security—mandated from the top by the newly created DNI if it is to have sufficient weight to become the new paradigm—must move away from the existing risk-averse model, which really seeks to avoid problems. Despite the likelihood of significant opportunity costs, the direction must be toward a risk management model like that increasingly being adopted for information security in other government agencies and the private sector. One approach would take responsibility for personnel and IT security out of the hands of dozens of individual agencies and make them the responsibility of a single community manager who would also have the power to adjudicate equities and make risk management decisions.[41] A single authority under the new DNI would issue security clearances and set security requirements for IT that would apply throughout the federal government (or at least the executive branch), among government contractors, and, ideally, to state and local government agencies, as required. This system would also eliminate the need to have clearances passed, making expedient collaboration easier. Uniform security standards for IT systems could make the electronic sharing of information and on-line collaboration among analysts substantially easier, thereby enabling the formation of collaborative "communities of interest" within a secure information environment.

[40] Groove is a software package that creates a virtual private network (VPN) within an information network that controls access to a shared collaborative space and provides a variety of tools to facilitate information sharing and collaboration. It is accepted by some components of the Intelligence Community as secure and trustworthy, but it is not widely employed at this time.

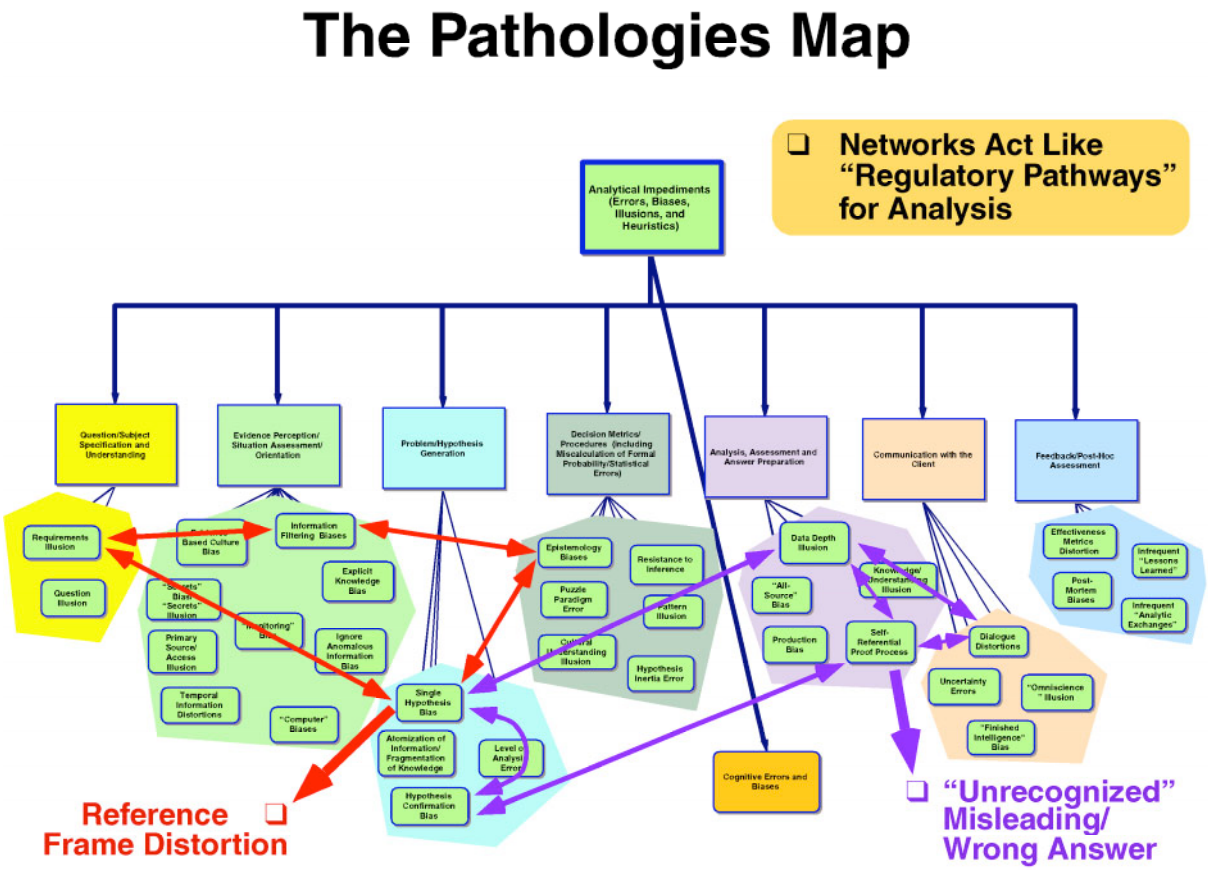
[41] The IRTPA, creating the Information Sharing Executive Program Manager, does mandate this, at least for counterterrorism information.

Appendix:
The Analytic Pathologies Methodology

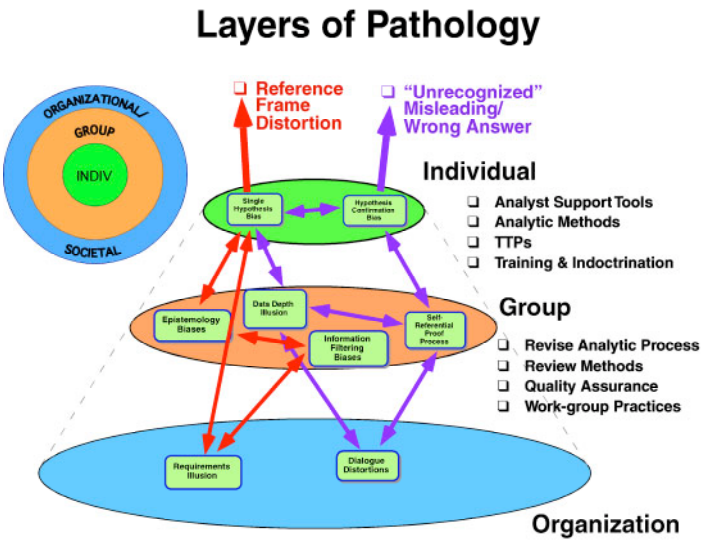
The “Analytic Pathologies” methodology expands the typical portrayal of the five-part intelligence cycle (planning and direction, collection, processing, analysis and production, and dissemination) to include seven elements in the analytic process:

- question specification and subject understanding
- evidence acquisition and situation perception/assessment
- problem/hypothesis specification
- decision metrics and procedures
- analysis, assessment, and answer preparation
- communication with the client
- feedback and post-hoc assessment.

More consistent with current research on judgment and decisionmaking, this expansion permits a closer look at the analytic process itself. This approach also makes it possible to capture explicitly the important calibration functions of interactions with cli-



Graphic courtesy of SAIC



Graphic courtesy of SAIC

ents in framing questions and in delivering answers, and it highlights the importance of explicit feedback for self-assessment. In this approach it is also possible to identify more completely the impediments to analysis and to specify the location and distorting effects of each step in the process.

Finally, the methodology explicitly lays out the key processes and functions (as well as impediments) at three organizational levels: individual analysts, work groups and agencies, and the Intelligence Community as a whole. This layout enables investigators to examine the causes of analytic problems and locate their organizational sources; these problems can occur not only where they directly interfere with the analytic process, but also in the functions which support agency and community analytical processes. With that information, appropriate corrective measures can be identified more easily.

Thus, although the Intelligence Community organizational level provides direction, priorities, and controls budgetary resources—which are important support mechanisms and enablers of output functions—it does not itself directly perform any intelligence functions, except analyses conducted by the National Intelligence Council (NIC), now a part of the office of the Director of National Intelligence.

The effectiveness of the Analytic Pathologies methodology as a diagnostic tool suggests its potential utility when used as a framework for developing corrective measures. The diagnostic effort highlights the importance of properly identifying the organizational level at which impediments impinge upon successful analytic practice, as well as the level at which corrective actions must be taken to restore important functions—and these are often not the same. For example, there are a substantial number of impediments to effective performance by individual analysts, but the appropriate corrective measures need to be instituted at the group or organizational level instead of the analytical level. Different corrective measures also have different time constants of effectiveness to be accommodated, both in planning and in measuring improvement; otherwise, phasing conflicts could easily induce resonant oscillation in processes and control mechanisms.

The explicit differentiation among these elements allowed by this methodology can enable individual and organizations at all levels to develop tools to recognize and use pathology self-assessments. It also allows the development of appropriate measures of effectiveness or indicators of performance targeted at relevant outputs rather than inputs. Thus, extending the Analytic Pathologies framework to use as the basis for developing corrective measures offers promise that it may be able to identify and, therefore, avoid perverse consequences that might result from altering structures and processes while attempting to make them more effective.

IC Functions and Outputs at Three Levels

Level	Key Functions	Outputs
Intelligence Community	• Direction and Leadership • Setting Priorities • Budgetary Control	• Policies • Oversight • Budgetary Allocation
Work Group/Agency	• Training and Acculturation • Work Practices and Habits (TTPs) • Rewards and Incentives • Review Processes • Organizational Knowledge Base	• Review • Production • Dissemination • Customer Interfaces • Work Processes • Technical Infrastructure • Organizational Culture
Individual	• Analytic Expertise • Domain Knowledge	• Answers • Hypotheses • Knowledge Products • Increased Knowledge • On-demand Expertise

Bibliography

Alberts, David S, John J. Garstka, Frederick P. Stein. *Network Centric Warfare: Developing and Leveraging Information Superiority.* Washington DC: C4ISR Cooperative Research Program, 1999.

Allen, Charles. “Comments of the Associate Director of Central Intelligence” for Collection at a Public Seminar on Intelligence at Harvard University, spring 2000. (<http://pirp.Harvard.edu/pdf-blurb.asp?id+518>.)

Andrus, Calvin, “Toward a Complex Adaptive Intelligence Community: The Wiki and the Blog.” *Studies in Intelligence* 49, no. 3 (2005).

Armstrong, Fulton. “Ways to Make Analysis Relevant but Not Prescriptive.” *Studies in Intelligence* 46, no. 3 (2002).

Barger, Deborah. “It Is Time to Transform, Not Reform, US Intelligence,” *SAIS Review of International Affairs* 24, no. 1 (Winter-Spring 2004).

Berkowitz, Bruce. “Intelligence for the Homeland.” *SAIS Review of International Affairs* 24, no. 1 (Winter-Spring 2004).

Bodnar, John. *Warning Analysis for the Information Age: Rethinking the Intelligence Process*. Washington, DC: Joint Military Intelligence College, July 2004.

Black, Cofer. “Testimony by Ambassador Cofer Black, Coordinator for Counterterrorism, Before the House International Relations Committee ‘9/11 Commission Report Recommendations,’” Washington, DC, 19 August 2004. http/wwwc.house.gov/international-relations/108/bla081904.htm.

Center for the Study of Intelligence*. Intelligence and Policy: The Evolving Relationship*. Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, June 2004.

Center for the Study of Intelligence. *Intelligence for a New Era in American Foreign Policy*. Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, January 2004.

Center for the Study of Intelligence. *Intelligence Lessons Learned Conference.* Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, May 2005.

Clift, A. Denis. “Intelligence in the Internet Era.” *Studies in Intelligence* 47, no.3 (2003).

Congress of the United States, Public Law 108-458 (17 December 2004), “Intelligence Reform and Terrorism Prevention Act (IRTPA).”

Cooper, Jeffrey R. “Intelligence and Warning: Analytic Pathologies” (Powerpoint Briefing). SAIC, McLean, VA. November 2003.

———. “Sensemaking: Focusing on the Last Six Inches.” Paper prepared for the American Institute of Aeronautics and Astronautics, Information and Command and Control Technical Committee, August 2002.

Cooper, Jeffrey R. and John Seely Brown. “Intelligence: We’ve Lost Our Edge.” *Washington Post*, 10 May 2005.

Davis, Jack. *Improving CIA Analytic Performance: DI Analytic Priorities.* Sherman Kent Center for Intelligence Analysis, Occasional Papers, v.1, no. 3. Washington, DC: Central Intelligence Agency, September 2002.

———*. Improving CIA Analytic Performance: Strategic Warning.* Sherman Kent Center for Intelligence Analysis, Occasional Papers, v.1, no.1. Washington, DC: Central Intelligence Agency, September 2002.

———. “Paul Wolfowitz on Intelligence-Policy Relations,” *Studies in Intelligence* 39, no. 1. (1995).

———*. Strategic Warning: If Surprise is Inevitable, What Role for Analysis?* Sherman Kent Center for Intelligence Analysis, Occasional Papers, v. 2, no.1. Washington, DC: Central Intelligence Agency, January 2003.

———. ”The Kent-Kendall Debate of 1949.” *Studies in Intelligence*. 35, no. 2 (1995).

Feschbach, Murray. *Russia’s Health and Demographic Crises: Policy Implications and Consequences.* Chemical and Biological Arms Control Institute (Health and National Security Series), April 2003.

———. “Russia’s Demographic and Health Meltdown.” Congress of the United States, Joint Economic Committee, *Russia’s Uncertain Economic Future,* 107th Congress, 1st Session. Washington, DC. Government Printing Office, December 2001.

Feinstein, Alvan R. *Clinical Judgment*. Baltimore, MD: Williams & Wilkins, 1967.

Fishbein, Warren, and Gregory Treverton. *Rethinking “Alternatives Analysis” to Address Transnational Threats.* Washington, DC: Central Intelligence Agency, The Sherman Kent Center for Intelligence Analysis, Occasional Papers, v. 3, no. 2, October 2004.

Goldhamer, Herbert. *The Adviser.* New York: Elsevier, 1978.

Goleman, Daniel, “Answer to 2005 Edge Question?” *The Edge.* http://edge.org/q2005/q05 print.html.

Hardin, Garrett. “The Tragedy of the Commons.” *Science* 162 (1968): 1243–48.

Hayden, Michael V. (Lt. Gen., USAF). Statement Before the Joint Inquiry of the Senate Select Committee on Intelligence and the House Permanent Select Committee on Intelligence, 17 October 2002.

Heuer, Richards J., Jr. *The Psychology of Intelligence Analysis.* Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 1999.

Hughes, Frank J., *Preparing for the Future of Intelligence Analysis.* Washington, DC: Joint Military Intelligence College, January 2003.

Hughes, Frank J. and David Schum. "Evidence Marshalling and Argument Construction." Washington, DC: Joint Military Intelligence College, Student Course Notes.

Jeremiah, David (Admiral, USN, ret.). Press Conference, CIA Headquarters, 2 June 1998.

———. *The Intelligence Community's Performance on the Indian Nuclear Tests* (1998).

Jervis, Robert. "What's Wrong with the Intelligence Process?" *International Journal of Intelligence and Counterintelligence* 1, no. 2 (Spring 1986).

Johnson, Loch. "The Aspin-Brown Intelligence Inquiry: Behind the Closed Doors of a Blue Ribbon Commission," *Studies in Intelligence* 48, no. 3 (2004).

Johnston, Rob. *Analytic Culture in the U.S. Intelligence Community: an Ethnographic Study.* Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 2005

Kahneman, Daniel. Maps of Bounded Rationality: A Perspective on Intuitive Judgment and Choice. (Nobel) Prize Lecture, 8 December 2002. Princeton University, Department of Psychology.

———. Interview with author, October 2000.

Kahneman, Daniel, Paul Slovic, Amos Tversky, eds. *Judgment Under Uncertainty: Heuristics and Biases.* New York: Cambridge University Press, 1982.

Kent, Sherman, *Strategic Intelligence for American World Policy.* Princeton, NJ: Princeton University Press, 1951, revised edition 1966.

Kerbel, Josh. "Thinking Straight: Cognitive Bias in the US Debate on China," *Studies in Intelligence* 48, no. 3 (2004).

Kerr, Richard, Thomas Wolfe, Rebecca Donegan, and Aris Pappas. "Issues for the US Intelligence Community," *Studies in Intelligence* 49, no. 3 (2005).

———. Interview, MSNBC, 14 July 2003

Kissinger, Henry A. "America's Assignment," *Newsweek*, 8 November 2004.

———. “Better Intelligence Reform,” *Washington Post*, 16 August 2004.

Klein, Gary. *Intuition at Work: Why Developing Your Gut Instinct Will Make You Better at What You Do.* New York: Doubleday, 2002.

Loomis, Carol. “Dinosaurs?” *Fortune*, 3 May 1993.

Marrin, Stephen. Review of William E. Odom, *Fixing Intelligence For a More Secure America, Political Science Quarterly* 119, no. 2 (Summer 2004).

———. “Preventing Intelligence Failures by Learning from the Past,” *International Journal of Intelligence and Counterintelligence,* 17, No. 4 (Oct–Dec 2004).

MacEachin, Douglas. *CIA Assessments of the Soviet Union: The Record Versus the Charges.* Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 1996.

McCarthy, Mary. “The National Warning System: Striving for an Elusive Goal,” *Defense Intelligence Journal* 3, no. 1 (Spring 1994).

Mears, Michael. “The Intelligence Community Genome: RIA Paper #3.” Unpublished manuscript, spring 2004.

Medawar, Peter. “Is the Scientific Paper Fraudulent? Yes; It Misrepresents Scientific Thought,” *The Saturday Review*, 47, 1 August 1964.

Medina, Carmen. “What To Do When Traditional Models Fail,” *Studies in Intelligence* 46, no. 3 (2002).

National Commission on Terrorist Attacks Upon the United States (The 9/11 Commission). *The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks Upon the United States.* Washington, DC: Government Printing Office, 2004.

National Institute of Standards and Technology (NIST). *Dictionary of Algorithms and Data Structures.* http://www.nist.gov/dads.

Odom, William E. *Fixing Intelligence: for a More Secure America.* New Haven: Yale University Press, 2003.

Pappas, Aris A. and James M. Simon, Jr. “The Intelligence Community: 2001–2015,” *Studies in Intelligence* 46, no.1 (2002).

Perrow, Charles. *Normal Accidents: Living with High-Risk Technologies*. New York: Basic Books, 1984.

Pfeffer, Jeffrey, with Charles A. O’Reilly. *Hidden Value: How Great Companies Achieve Extraordinary Results with Ordinary People.* Boston: Harvard Business School Press, 2000.

Pfeffer, Jeffrey, with G. R. Salancik. *The External Control of Organizations: A Resource Dependence Perspective.* New York: Harper and Row, 1978. (Republished by Stanford University Press, 2003.)

Principia Cybernetica Web. “Feedback.” http://pespmc1.vub.ac.be/FEEDBACK.html (accessed 31 Aug 2005).

Rozak, David, Alexander Lee, James B. Petro, and Lisa Lechler. “Redefining the First Customer: Transforming Intelligence Analysis through Peer-Reviewed Publications” in 2004 Galileo Papers. Washington, DC: Central Intelligence Agency, 2005.

Rumsfeld, Donald. “Sideletter to Report of the Commission to Assess the Ballistic Missile Threat to the United States,” 18 March 1991. http://www.house.gov/hasc/testimony/106thcongress/rumsfeldsideletter.htm.

S2845: An Act to Reform the Intelligence Community and the Intelligence and Intelligence-related Activities of the United States Government and for other purposes. (Short title: National Intelligence Reform Act of 2004.) 6 October 2004.

Sabel, Charles F. “Theory of a Real Time Revolution,” forthcoming in *Organizational Studies* (2005). Forthcoming in Charles Heckscher, Paul Adler, eds., *Collaborative Community*. Oxford, UK: Oxford University Press, 2005.

Sageman, Mark. “Understanding Terror Networks,” Foreign Policy Research Institute, E-Note, 1 November 2004. Available at http://www.fpri.org/enotes/20041101.middleeast.sageman.understandingterrornetworks.html.

Senate Select Committee on Intelligence of the 108th U.S. Congress. *Report on the US Intelligence Community’s Prewar Intelligence Assessments*. Washington, DC: July 2004: 14. Available at: <http://www.realcities.com/multimedia/nationalchannel/news/070904_senate_report.pdf>.

Senge, Peter M. *The Fifth Discipline: The Art & Practice of the Learning Organization*. New York: Doubleday/Currency, 1990.

Shirky, Clay. “A Group Is Its Own Worst Enemy” (June 2003). “Networks, Economics, and Culture Mailing List.” Available at http://www.shirky.com.

Simon, Herbert. *Administrative Behavior*. New York: The Free Press, 1997.

Six Sigma: <http://www.isixsigma.com/>

Stefik, Mark and Barbara Stefik. *Breakthrough: Stories and Strategies of Radical Innovation.* Cambridge, MA: MIT Press, 2004.

Stokes, Donald E. *Pasteur’s Quadrant: Basic Science and Technology Innovation*. Washington, DC: The Brookings Institution, 1997.

Swenson, Russell and Susana C. Lemozy. “Politicization and Persuasion: Balancing Evolution and Devolution in Strategic Intelligence,” unpublished manuscript (date?)

Travers, Russ. “The Coming Intelligence Failure,” *Studies in Intelligence* 40, no. 2 (1996).

Warner, Michael. “Transformation and Intelligence Liaison,” *SAIS Review of International Affairs* 24, no. 1 (Winter–Spring 2004).

Weick, Karl E. *Sensemaking in Organizations.* Thousand Oaks, CA: Sage Publications, 1995.

Weick, Karl E. and Kathleen M. Sutcliffe. *Managing the Unexpected: Assuring High Performance in an Age of Complexity.* San Francisco: Jossey-Bass, 2001.

The Author

Jeffrey R. Cooper is Vice President for Technology, Chief Scientist of Strategies, and Director of the Center for Information Strategy and Policy at Science Applications International Corporation. He has undergraduate and graduate degrees from The Johns Hopkins University, where he was later Professorial Lecturer in Arms Control and Defense Analysis at the School of Advanced International Studies.

Mr. Cooper's core interest has been the use of information to improve intelligence analysis, decisionmaking, command and control, and operational effectiveness. During the past several years, Mr. Cooper has focused on analyzing intelligence failure and evaluating methods to improve all-source analysis. He was a professional staff member of the Presidential Commission on Future Intelligence Capabilities (The Silberman-Robb Commission).

With a long-time focus on strategic analysis and military transformation, Mr. Cooper is a founding member of the Highlands Forum, a program sponsored by the Secretary of Defense to identify national security-related cutting-edge technology. He has also served on numerous Defense Science Board task forces and summer studies. He has held senior government positions in the White House and the Department of Energy.

"This study is fundamentally about what I would call the intellectual professionalization of intelligence analysis. It is about standards and practices and habits of mind. It is about inductive (evidence-based) analytical reasoning balanced against deductive (hypothesis-based and evidence-tested) reasoning. It extols the value of truly scientific modes of thinking, including respect for the role of imagination and intuition, while warning against the pitfalls of "scientism," a false pretense to scientific standards or a scientific pose without a scientific performance. It talks about peer review and challenging assumptions and the need to build these therapeutic virtues into the analytical process."

Fritz Ermarth
Chairman of the National Intelligence Council, 1988-93

This Page Is Intentionally Left Blank

Joint Military Intelligence College

November 1997
DVP-2600-1828-97

DEFENSE AND INTELLIGENCE ABBREVIATIONS AND ACRONYMS

The Joint Military Intelligence College supports and encourages research on intelligence issues that distills lessons and improves support to policy-level and operational consumers.

DEFENSE AND INTELLIGENCE ABBREVIATIONS AND ACRONYMS

JOINT MILITARY INTELLIGENCE COLLEGE
WASHINGTON, DC
NOVEMBER 1997

This document has been approved for unrestricted public release by the
Office of the Secretary of Defense (Public Affairs)

CONTENTS

Foreword..... V

Abbreviations and Acronyms..... 1

Codes for Geopolitical Areas..... 230

Geopolitical Areas by Codes..... 239

DEFENSE AND INTELLIGENCE ABBREVIATIONS AND ACRONYMS

Foreword

This comprehensive list of intelligence abbreviations and acronyms includes those used presently, as well as those in use for approximately the last ten years. Sources for this list include the last DIA Lexicon published in 1991, numerous glossaries from Unified Command and Combat Support Agency documents, and contributions, from the faculty of the Joint Military Intelligence College. The expansion of any item may vary somewhat from one organization to another, but this list will hopefully contribute to greater standardization.

This editor is indebted to kSgt Hannah Reddy (USA) and SSgt Angela Wimbush (USAF) of the College, who spent many hours in collating this list. Debbie Linesberry of the U.S. Special Operations Command collaborated by adding that command's most frequently used acronyms. 2LT Vincent Littrell (USAF) and SFC Mark McCurry (USA) helped ensure that the list contains as few errors as possible, and the editor extends his thanks for that dedicated assistance.

All users are invited to submit additions and corrections. To promote the usefulness of the list, older or superseded acronyms will be discarded only if their retention would create confusion. This list is also published under the JMIC home page on Intelink, where it will be updated regularly. Readers are urged to send new acronyms or abbreviations by mail to: Defense Intelligence Agency, Joint Military Intelligence College, MC Attn: Dr. R. Swenson, Bolling AFB, Washington, DC 20340-5100: by Ingternet to AFswerg@dia.osis.gov, or by Fax to (202) 231-2171.

Dr. Russell G. Swenson, Editor and Director, Office of Applied Research

ABBREVIATIONS AND ACRONYMS

A

A2	Air Force Intelligence Staff Officer (component level)
AA	(1) Attack Assessment; (2) Attrition Analysis; (3) Antiaircraft; (4) Avenue of Approach; (5) Automatic Associator
AAA	(1) Antiaircraft Artillery; (2) Air Avenue of Approach
AAAOB	Antiaircraft Artillery Order of Battle
AABNCP	Advanced Airborne National Command Post
AAC	Alaskan Air Command
AACB	Aeronautics and Astronautics Coordinating Board
AACE	Army Alternate Command and Control Element
AACOMS	Army Area Communications System
AACS	Attitude and Antenna Control Subsystem
AAD	Airborne Assault Division
AADC	(1) Army Air Defense Command; (2) Area Air Defense Commander
AADCCS	Area Air Defense Command and Control System
AADP	Area Air Defense Plan
AADS	Antiaircraft Defense System
AAE	Army Acquisition Executive
AAF	Army Airfield
AAFES	Army & Air Force Exchange Service
AAFIF	Automated Air Facilities Information File
AAG	Army Artillery Group
AAI	Air-to-Air Intercept
AAIFF	Air-to-Air Identification Friend or Foe
AAM	Air-to-Air Missile
AAO	Analysis of the Area of Operations
AAR	(1) Active Array Radar; (2) After Action Report
AAS	Analyst Automation Segment
AASLT	Air Assault
AATS	Automated Architecture Tool Suite
AAVS	Aerospace Audiovisual Service
AAW	Anti Air Warfare
AAWC	Anti Air Warfare Commander
AB	Air Base
AB2	Air Battle Command System (ABCS) Brigade and Below
ABC	Airborne Corps
ABCCC	Airborne Battlefield Command and Control Center
ABCOMM	Alternate/Backup Communications

ABCS	Army Battle Command System
ABIC	Army Battlefield Interface Concept
ABIT	(1) Airborne Imagery Transmission; (2) Airborne Information Transmission Program
ABM	(1) Antiballistic Missile; (2) Automatic Building Machines
ABMA	Army Ballistic Missile Agency
ABN/Abn	Airborne
ABNCP	(1) Airborne Command Post; (2) Airborne National Command Post
ABR	Available Bit Rate
ABW	Air Base Wing
AC	(1) Air Crew; (2) Active Component; (3) Air Conditioning; (4) Alternating Current
A/C	Aircraft
A2C2	Army Airspace Communications and Control
AC-130	AFSOF Spectre Gunship
AC2SMAN	Alaskan Command and Control System Military Automated Network
AC2MP	Army Command and Control Master Plan
ACA	(1) Alternate Command Authority; (2) Airspace Control Authority
ACAAM	Air Courses of Action Assessment Model
ACACS	Army Command and Area Communications System
ACAT	Acquisition Category
ACC	(1) Access Control Center; (2) Air Control Center; (3) Aviation Component Commander, (4) Air Component Commander, (5) Air Combat Command; (6) Army Component Command
ACCB	Army Configuration Control Board
ACCHAN	Allied Command Channel
ACCIS	Allied Command and Control Information System
ACCISS	(1) Automated Command and Control Intelligence Support System; (2) Alaskan C2 Intelligence Support System
ACCO	Army Central Control Office
ACCS	(1) Airborne Command and Control Squadron; (2) Airborne Command and Control System; (3) Advanced Communications Control System
ACDA	Arms Control and Disarmament Agency
ACDS	Advanced Combat Direction system
ACDUTRA	Active Duty Training
ACE	(1) Allied Command, Europe; (2) Advance Communications Element; (3) Aviation Combat Element; (4) Analysis Control Element; (5) Assistant Corps of Engineers; (6) Airborne Command Element
ACES	Automated Command and Control Evaluation System
ACEVAL	Air Combat Evaluation
ACF	Alternate Command Facility
ACFT	Aircraft
ACI	Airborne Controlled Intercept

ACINT	Acoustic Intelligence
ACIS	Arms Control Intelligence Staff
ACL	Access Control List
ACLANT	Allied Commander Atlantic
ACO	(1) Access Control Officer; (2) Airspace Control Officer
ACOC	(1) Area Communications Operations Center; (2) Air Combat Operations Center
ACOM	Atlantic Command
ACOS	Assistant Chief of Staff
ACOS/I	Assistant Chief of Staff for Intelligence (Navy)
ACOUSTINT	Acoustical Intelligence
ACP	(1) Alternate Command Post; (2) Assault CP; (3) Allied Communications Publications; (4) Airspace Control Plan
ACPERS	Army Civilian Personnel System
ACQ	Acquisition
ACR	(1) Armored Cavalry Regiment; (2) Automated Change Recognition
ACS	(1) Afloat Correlation System; (2) Aerial Common Sensor; (3) AUTODIN Switching Center; (4) Airborne COMINT System; (5) Assistant Chief of Staff
ACS/I	Assistant Chief of Staff for Intelligence
ACSA	Allied Communications Security Agency
ACSB	Amphibious Contingency Support Briefs
ACSC	Air Command and Staff College
ACSI	Assistant Chief of Staff Intelligence, HQ USAF
ACT	(1) Air Combat Tactics; (2) Advanced Concepts and Technology Program
ACTD	Advanced Concept Technology Demonstration
ACTEDS	Army Civilian Training, Education, & Development System
ACTS	(1) Advanced Communications Technology; (2) Advanced Communications Technology Satellite
ACUS	(1) Area Common User Systems; (2) Army Common User System
ACV	(1) Armored Command Vehicle; (2) Air Cushion Vehicle; (3) Armored Combat Vehicle
ACW	(1) Aircraft Control and Warning; (2) Anticarrier Warfare; (3) Air Control Wing
AD	(1) Air Defense; (2) Destroyer Tender; (3) Air Division; (4) Artillery Division; (5) Active Duty
A/D	Analog/Digital
ADA	Air Defense Artillery
ADACP	Alcohol & Drug Abuse Control Program
ADAPCP	Alcohol & Drug Abuse Prevention & Control Program
ADAPT	Automated Decisionmaking and Program Timeline
ADARS	Army Defense Acquisition Regulation Supplement
ADATS	Air Defense Antitank System
ADBT	Advanced Data Base Technology

ADC	(1) Aide-de-Camp; (2) Air Direction Center; (3) Assistant Division Commander; (4) Air Data Computer; (5) Air Defense Coordinator
ADCAP	Advanced Capability
ADCC	Air Defense Command Center
ADCCP	Advanced Data Communications Control Procedures
ADCOM	(1) Aerospace Defense Command (now SPACECOM); (2) Administrative Command
ADCON	Administrative Control
ADCSOPS	Assistant Deputy Chief of Staff for Operations and Plans
ADD	(1) Air Defense District; (2) Assistant Deputy Director (DIA)
ADDIS	Advanced Deployable Digital Imagery System
ADDISS	Advanced Deployable Digital Imagery Support System
ADDO	Associate Deputy Director of Operations
ADDO(MA)	Associate Deputy Director of Operations for Military Affairs (DIA)
ADDO(MS)	Associate Deputy Director of Operations for Military Support (NSA)
ADDS	Army Data Distribution System
ADDU	Additional Duty
ADE	(1) Audio Deception Emitter; (2) Aerial Delivery Equipment
ADEW	Airborne Directed Energy Weapons
ADF	Automatic Direction Finding
ADFH	Air Deployable Forward Headquarters
ADG	Deperming Ship
ADI	Air Defense Initiative
ADIC	Aerospace Defense Intelligence Center
ADIEC	Army Deployable Imagery Exploitation Capability
ADIO	Additional Duty Intelligence Officer
ADISS	Advanced Defense Intelligence Support System
ADIZ	Air Defense Identification Zone
ADL	(1) Ada Design Language; (2) Armistice Demarcation Line
ADLP	Advanced Datalink Protocol
ADM	(1) Atomic Demolition Munitions; (2) Advanced Development Model; (3) Acquisition Decision Memorandum
Admin	Administration/Administrative
ADN	ACE DGZ Number (NATO)
ADNET	Antidrug Network
ADOC	Air Defense Operations Center
ADP	(1) Automated Data Processing; (2) Airborne Data Processing
ADP-MIS	Automated Data Processing Management Information System

ADP-T	(1) Automated Data Processing and Associated Telecommunications; (2) Automated Data Processing and Associated Training
ADPCM	Adaptive Differential Pulse-Code Modulation
ADPE	Automated Data Processing Equipment
ADPS	(1) ASARS Deployable Processing Station; (2) Automated Data Processing System
ADPSSM	Automated Data Processing Systems Security Manual
ADPSSO	ADP Special Security Officer
ADPSSP	Automated Data Processing System Security Program
ADRG	Advanced Digitized Raster Graphics
ADRI	Arc Digital Raster Imagery
ADS	(1) Automated Data System; (2) Air Defense Sector; (3) Airlift Defensive System; (4) Acoustic SOF Detection System; (5) Advanced Distributed Simulation
ADSS	Aerospace Defense Systems Subcommittee
ADSTAR	Advanced Document Storage & Retrieval System
ADSW	Active Duty for Special Work
ADT	(1) Active Duty For Training; (2) Additional Duty Training
ADTLP	Army Doctrine and Training Literature Program
ADTOC	Air Defense Tactical Operations Center
ADTS	Adversary Threat Squadron
ADV	Advance(d)
ADVAL	Air Defense Evaluation Test
ADVON	Advanced Echelon
ADW	Air Defense Warning
ADX	Air Defense Exercise
ADZ	Air Defense Zone
AE	(1) Atomic Energy; (2) Assault Echelon; (3) Ammunition Ship; (4) Aerial Exploitation; Application Entity
AEAO	Airborne Emergency Action Officer
AEB	Aerial Exploitation Battalion
AEC	ASARS Exploitation Cell
AEDS	Atomic Energy Detection System
AEELS	(1) Automatic ELINT Emitter Location System; (2) Airborne ELINT Emitter Location System
AEICC	Area Emergency Information Coordination Center
AEM	Missile Tender
AEMS	Automated Edge Measurement System
AEN	Arbitrary ELINT Notation
AEOS	Advanced Electro-Optical Sensor
AEROFLOT	Former Soviet Union Civil Airline
AES	(1) Atomic Energy Site; (2) Airborne ELINT System
AESC	Aerospace Environmental Support Center
AETC	Air Education and Training Command
AETCAE	Army Europe Technical Control and Analysis Element
AEV	Armored Engineer Vehicle

AEW	Airborne Early Warning
AEW&C	Airborne Early Warning and Control
AF	(1) Air Force; (2) Armed Forces; (3) Stores Ship
AFAC	Airborne Forward Air Controller
AF ACSI	Air Force Chief of Staff Intelligence
AFAITC	Armed Forces Air Intelligence Training Center (Goodfellow AFB, TX).
AFAL	Air Force Armament Laboratory
AFAMPE	USAF Automated Message Processing Exchange
AFAMRL	Air Force Aerospace Medical Research Laboratory
AFAP	Artillery-Fired Atomic Projectile
AFARN	Air Force Air Request Net
AFAS	Advanced Field Artillery System
AFATDS	Advanced Field Artillery Tactical Data System
AFB	(1) Air Force Base; (2) Airframe Bulletin; (3) Antifriction Bearing
AFC	(1) Automatic Frequency Control; (2) All-source Fusion Center (Marine Corps)
AFC4A	USAF Command, Control, Communications and Computer Agency
AFCA	Air Force Collection Assets
AFCC	(1) Air Force Communications Command; (2) Air ForceComponent Command
AFCEA	Armed Forces Communications Electronics Association
AFCENT	Allied Forces Central Europe (NATO)
AFCS	(1) Automatic Flight Control System; (2) Army Facility Component System
AFCSC	Air Force Cryptologic Support Center
AFDB	Auxiliary Floating Drydock (large)
AFDD	Air Force Doctrine Document
AFDIGS	Air Force Digital Graphic Systems
AFDL	Auxiliary Floating Drydock (small)
AFDM	Auxiliary Floating Drydock (medium)
AFDT	AEELS Fixed Downlink Terminal
AFEOC	Air Force Emergency Operations Center
AFEWC	Air Force Electronic Warfare Center
AFFIS	Airfield Facilities Information System
AFFOR	Air Force (Component) Forces
AFGCCS	USAF Global Command and Control System
AFGL	Air Force Geophysics Laboratory
AFGWC	Air Force Global Weather Central
AFGWC/FNOC	Air Force Global Weather Center/Fleet Numerical Operations Center
AFGWS	Air Force Ground Weather Stations
AFIA	Air Force Intelligence Agency
AFIC	(1) Air Force Information Center; (2) Air Force Intelligence Command; (3) Air Force Intelligence Center

AFICE	Air Forces Iceland
AFICP	Air Force Intelligence Communications Plan
AFIES	Armed Forces Imagery Exploitation System
AFIISP	Air Force Intelligence Information Systems Plan
AFIO	Association of Former Intelligence Officers
AFIP	Air Force Intelligence Plan
AFIS	Air Force Intelligence Service/Study
AFISA	Air Force Intelligence Support Agency
AFIT	Air Force Institute of Technology
AFITC	Air Force Intelligence Training Center
AFIWC	Air Force Information Warfare Center
AFLAN	AFSOC Local/Wide Area Network
AFLANT	U.S. Air Forces, Atlantic
AFLC	Air Force Logistics Command
AFLE	Air Force Liaison Element
AFLO	Air Force Liaison Office
AFM	Air Force Manual
AFMD/GF	Air Forces of the Military District/Group of Forces
AFMC	Air Force Materiel Command
AFMIC	Armed Forces Medical Intelligence Center
AFMPC	Air Force Military Personnel Center
AFMSIS	Air Force Modeling and Simulation Information System
AFMSS	Air Force Mission Support System
AFNET	(1) Air Force Network; (2) Air Force Data Network
AFNORTH	Allied Forces Northern Europe (NATO)
AFNORTHWEST	(1) Allied Forces Northwest Europe (NATO); (2) Air Forces Northwest Region
AFOC	Air Force Operations Center
AFOE	Assault Follow-On Echelon
AFOSI	Air Force Office of Special Investigations
AFOSP	Air Force Office of Security Police
AFOSR	Air Force Office of Scientific Research
AFOTEC	Air Force Operational Test and Evaluation Center
AFR	(1) Air Force Reserve; (2) Air Force Regulation
AFRES	Air Force Reserve
AFS	(1) Air Force Station; (2) Combat Stores Ship
AFSAA	Air Force Studies and Analyses Agency
AFSAC	Air Force Special Activities Center
AFSAT	Air Force Satellite
AFSATCOM	Air Force Satellite Communications System
AFSC	(1) Air Force Systems Command; (2) Air Force Specialty Code; (3) Armed Forces Staff College
AFSCOORD	Assistant Fire Support Coordinator
AFSCF	Air Force Satellite Control Facility
AFSCN	Air Force Satellite Control Network

AFSIP	Air Force Satellite Intelligence Program
AFSOB	Air Force Special Operations Base
AFSOC	Air Force Special Operations Command
AFSOD	Air Force Special Operations Detachment
AFSOE	Air Force Special Operations Element
AFSOF	Air Force Special Operations Forces
AFSOS	Air Force Special Operations School
AFSOUTH	Allied Forces Southern Europe (NATO)
AFSOUTHCOM	Air Force Southern Command
AFSPACECOM	Air Force Space Command
AFSPC	Air Force Space Command
AFSPCIP	Air Force Space Command Intelligence Plan
AFSPOC	Air Force Space Operations Center
AFSSE	Air Force Space Surveillance Element
AFSST	Air Force Space Support Team
AFSTC	Air Force Space Technology Center
AFTAC	Air Force Technical Applications Center
AFTACIES	Air Force Tactical Imagery Exploitation System
AFTF	Air Force Task Force
AFTFWC	Air Force Tactical Fighter Weapons Center
AFV	Armored Fighting Vehicle
AF/VC	Air Force Vice Chief of Staff
AFWAL	Air Force Wright Aeronautical Laboratory
AFWARNS	Air Force Warning System
AFWCCS	Air Force Wing Command and Control System
AFWL	Air Force Weapons Laboratory
AG	(1) Adjutant General; (2) Miscellaneous Auxiliary Ship
AGARD	Advisory Group for Aerospace Research and Development (NATO)
AGB	Icebreaker
AGC	Automatic Gain Control
AGCCS	Army's Global Command and Control System
AGDS	Deep Submergence Support Ship
AGE	Experimental Auxiliary
AGEF	Frigate Research Ship
AGEH	Experimental Auxiliary (Hydrofoil)
AGER	Intelligence Research Ship
AGES	Advanced Ground Exploitation System
AGF	Miscellaneous Command Ship
AGHS	Patrol Combatant Support Ship
AGI	Intelligence Collection Ship
AGL	(1) Buoy Tender; (2) Above Ground Level
AGM	(1) Air-to-Ground Missile; (2) Missile Range Instrumentation Ship
AGMR	Major Communications Relay Ship

AGMS	Armored Ground Mobility System
AGOR	Oceanographic Research Ship
AGOS	(1) Ocean Surveillance Ship; (2) Air-Ground Operations School (NATO); (3) Air-Ground Operations System
AGP	Patrol Craft Tender
AGR	Army Guard Reserve
AGS	(1) Hydrographic Survey Ship; (2) FSU Automatic Grenade Launcher
AGT	Agent
AGZ	Actual Ground Zero
AH	(1) Hospital Ship; (2) Alternate Headquarters
AHFEWS	Army High Frequency Electronic Warfare System
AI	(1) Airborne Intercept; (2) Air Intelligence; (3) Artificial Intelligence; (4) Air Interdiction; (5) Airborne Interceptors; (6) Area of Interest; (7) All-Source Intelligence
A3I	Accelerated Architecture Acquisition Initiative
AIA	(1) Army Intelligence Agency; (2) ACE Intelligence Architecture; (3) ACE Interface Architecture; (4) Air Intelligence Agency
AIAA	American Institute of Aeronautics and Astronautics
AIA/IRD	Air Intelligence Agency/Intelligence Reserve Detachment
AIAWS	Automated Intelligence Analyst Workstation
AIB	Atlantic Intelligence Board
AIC	(1) Atlantic Intelligence Command; (2) Afloat Intelligence Center
AICBM	Anti-Intercontinental Ballistic Missile
AID	(1) U.S. Agency for International Development; (2) Aerospace Information Digest; (3) Army Information Digest; (4) Accident, Incident, Deficiencies; (5) Active Integral Defense
AIDES	(1) Analyst Intelligence Information Display and Exploitation System; (2) Automated Intelligence Display and Exploitation System
AIDS	(1) Acoustic Intelligence Data System; (2) Advanced Identification System; (3) Acquired Immune Deficiency Syndrome
AIF	(1) Automated Installations Intelligence File; (2) Army Industrial Fund; (3) Airfield Installation File; (4) Air Intelligence Flight; (5) Automated Installation File
AIFV	Armored Infantry Fighting Vehicle
AIG	(1) Address Indicator Group; (2) Air Intelligence Group
AIIC	Advanced Imagery Interpretation Course
AIIF	Automated Installation Intelligence File
AIIRS	Automated Intelligence Information Retrieval System
AIM	(1) Air Intercept Missile; (2) Active Inert Missile; (3) ADCOM Intelligence Memorandum
AIMD	Aircraft Intermediate Maintenance Department
AIMP	(1) Army Intelligence Management Plan; (2) Army Intelligence Master Plan; (3) Advanced Imagery Management Program; (4) Automated Information Management Program

AIMTB	Artificial Intelligence Module Testbed
AIN	Advanced Intelligence Network
AIO	Air Intelligence Officer
AIOEC	Association of Iron Ore Exporting Countries
AIP	(1) Architecture Implementation Plan; (2) Anti-Surface-Warfare Improvement Program
AIPR	Automated Information Processing Request
AIR	American Institute for Research
AIRA	Air Attache
AIRCENT	(1) Air Forces Central Region (NATO); (2) Allied Air Forces Central Europe
AIRCOM	Air Command
AIRCOMTERM	Airborne Communications Terminal
AIRES	Advanced Imagery Requirements and Exploitation System
AIRES II	Airborne Reconnaissance Electronic System II
AIREW	Airborne Infrared Early Warning
AIRK	Area Interswitch Rekeying Key
AIRLO	Air Liaison Officer
AIRREQRECON	Air Request Reconnaissance
AIR	(1) Replenishment Oiler; (2) American Institute of Research
AIRS	(1) Advanced Inertial Reference Sphere; (2) Automated Information Retrieval Systems
AIRTAPS	Aerial Imagery Reconnaissance Tracking and Plotting System
AIS	(1) Automated Indicator System; (2) Advanced Indications Structure; (3) Advanced Indications System; (4) Army Intelligence Survey; (5) Automated Information System; (6) Air Intelligence Squadron
AISA	Automated Intelligence Support Activity
AISS	Automated Information Systems Security
AIST	Air Intelligence Support Team
AITE	Advanced Indications Technology Experiment
AIU	Army Interrogation Unit
AIWO	Air Intelligence Warning Officer
AIWS	Advanced Interdiction Weapon System
AJ	Antijamming
AJCC	Alternate Joint Communications Center
AJFP	Adaptive Joint Force Package
AJNPE	Airborne Joint Nuclear Planning Element
A/JSIC	Alternate JSIC
AK	(1) Cargo Ship; (2) FSU Kalashnikov Family of Assault Rifles; (3) Automatic Remote Rekeying
AKA	Also Known As
AKDC	Automatic Key Distribution Center
AKD/RCU	Automatic Key Distribution/Rekeying Control Unit
AKL	Light Cargo Ship
AKM	(1) Apogee Kick Motor; (2) AK-47 Assault Rifle
AKMC	Automated Key Management Center

AKMS	Automated Key Management System
AKR	Vehicle Cargo Ship
AKTCAE	Army Korea Technical Control And Analysis Element
ALAIRCOM	Alaskan Air Command
ALARM	Alert, Locate and Report Missiles
ALASAT	Air-Launched Antisatellite
ALASCOM	Alaskan Communications Inc.
ALB	Air-Land Battle Doctrine (FM 100-5)
ALBM	Air-Launched Ballistic Missile
ALC	Accounting Legend Code
ALCATS	Automated Lines of Communication and Target System
ALCC	Airlift Control Center
ALCE	Airlift Control Element
ALCM	Air-Launched Cruise Missile
ALCOM	Alaskan Command
ALCOP	Alternate Command Post
ALCOR	ARPA Lincoln C-Band Observable Radar
ALCS	Airborne Launch Control System
ALD	Airlift Division
ALE	(1) AIRES Lifecycle Extension; (2) Automated Link Establishment
ALERT	Attack and Launch Early Report to Theater (AF)
ALES	AIRES Life Extension System
ALF	Auxiliary Landing Field
ALFA	Advanced Liaison Forward Area
ALL	Airborne Laser Laboratory
ALMS	Automated Logistics Management System
ALO	(1) Air Liaison Officer; (2) Authorized Level of Organization
ALOC(S)	Air Line(s) of Communication
ALPS	Accidental Launch Protection System
ALRAAM	Air-Launched Long-Range Air-to-Air Missile
ALRP-S	Army Long-Range Plan for Space
ALRPG	Army Long-Range Planning Guidance
ALS	(1) Active Laser Seeker; (2) Airborne Link Segment
ALSA	Air-Land-Sea Application (Center)
ALSS	Advanced Location Strike System
ALT	(1) Alternate; (2) Altitude
ALTAlR	ARPA Long-Range Tracking and Instrumentation Radar
ALTREV	Altitude Reservation
ALUSNA	American Legation U.S. Naval Attache
ALUSNLO	American Legation U.S. Naval Liaison Officer
ALWT	Advanced Lightweight Torpedo
ALWTIC	Annual Land Warfare Technical Intelligence Conference

AM	(1) Ante Meridian (Before Noon); (2) Amplitude Modulation; (3) Asset Manager; (4) Aerographers Mate
AMAB	Air Mobile Assault Brigade
AMASS	(1) Advanced Marine Airborne SIGINT System; (2) Advanced Marine Air Support System
AMBISS	Automated Map-Based Intelligence Support System
AMC	(1) Airspace Management and Control; (2) Army Materiel Command (Formerly DARCOM); (3) Air Mobility Command; (4) Air Mission Commander
AMCC	(1) Ashore Mobile Contingency Communications; (2) Ashore Mobile Command Center
AMC/IN	AMC Deputy Chief of Staff for Intelligence
AMCIT	American Citizen
AMCM	Airborne Mine Countermeasures
AMD	Activated Metal Decoy
AMDT	AEELS Mobile Downlink Terminal
AME	Airspace Management Element
AMEMB	American Embassy
AMETS	Artillery Meteorological System
AMF	Allied Command Europe Mobile Force (NATO)
AMH	Automated Message Handling
AMHA	Army Management Headquarters Activity
AMHS	Automated Message Handling System
AMIDS	Airborne Mine Detection System
AMIM	Army Modernization Information Memorandum
AMIP	Army Model Improvement Plan
AMIRS	Army Multispectral Imagery Requirements Study
AMIS	Advanced Microwave Imaging Sensor
AMM	Army Modernization Memorandum
Ammo	Ammunition
AMMS	(1) Allowance Material Management System; (2) Acquisition Milestone Management System
AMOPES	Army Mobilization and Operations Planning and Execution System
AMOPS	Army Mobilization Operations and Planning System
AMOS	Air Force Maui Optical System
AMP	(1) Amplification; (2) Army Modernization Plan; (3) Acquisition Master Plan
AMPDS	Automated Message Processing Dissemination System
AMPE	Automated Message Processing Exchange
AMPHI	Aerial Mission Photographic Indoctrination
AMPHIB	Amphibious
AMPL	Amplitude
AMPS	(1) Automated Mission Planning System; (2) Automated Message Processing System; (3) Aim Point System
AMRAAM	Advanced Medium-Range Air-to-Air Missile

AMRWS	Advanced Remote Miniaturized Weather Station
AMS	(1) Automated Message System; (2) Auto-Manual System; (3) Autonomous Message Switch; (4) Advanced Mapping Spectrometer
AMSAT	Amateur Radio Satellite
AMSC	Advanced Military Spaceflight Capability
AMS-H	Advanced Missile System Heavy
AMSSA	Assured Mission Support Space Architecture
AMST	Advanced Medium STOL Transport
AMT	ACTS Mobile Terminal
AMTF	Airmobile Task Force
AMTP	Army Mission Training Plan
AMU	Astronaut Maneuvering Unit
AMW	Amphibious Warfare
AN	(1) Net Tender; (2) Army/Navy
ANALIT	Analyst-to-Analyst Message Format
ANC	African National Congress
ANCC	(1) Ashore Navy Communications Capability; (2) Automated Network Control Center
ANDVT	Advanced Narrowband Digital Voice Terminal
ANEX	Analyst-to-Analyst Exchange Message Format
ANFO	Ammonium Nitrate Fuel Oil
ANG	Air National Guard
ANGB	Army National Guard Base
ANGLICO	Air and Naval Gunfire Liaison Company
ANL	Net-Laying Ship
ANLYS	Analysis
ANMCC	Alternate National Military Command Center
ANMIC	Alternate National Military Intelligence Center
ANR	(1) Alaskan NORAD Region; (2) Active Noise Reduction
ANRPC	Association of Natural Rubber-Producing Countries
ANSI	American National Standards Institute
ANVIS	Aviator's Night Vision Imaging System
AN/VRC	Army Navy Vehicle Radio Communications
ANZUS	Australia, New Zealand, United States
AO	(1) Action Officer; (2) Oiler; (3) Authenticator Organization; (4) Area of Operations; (5) Aerial Observer
AOA	(1) Amphibious Objective Area; (2) Angle of Attack; (3) Angle of Arrival; (4) Airborne Optical Adjunct
AOB	(1) Air Order of Battle; (2) Advanced Operational Base
AOBTS	Air Order of Battle Textual Summary
AOC	(1) Air Officer Commanding (U.K.); (2) Air Operations Center; (3) Army Operations Center
AOCC	Area Operations Control Center
AOCS	Aviation Officers Candidate School
AOE	Fast Combat Support Ship
AOFDA	U.S. AID Office for Foreign Disaster Assistance

AOG	Gasoline Tanker
AOI	(1) Area of Influence; (2) Area of Interest
AOIC	Assistant Officer in Charge
AOIR	(1) ACE Operational Intelligence Requirements; (2) Area of Intelligence Responsibility
AOL	Area of Limitation
AO&M/NM	Administration, Operations, and Maintenance/Network Management
AOO	Air Operations Order
AOP	(1) Area of Probability; (2) Air Operations Plan
AOR	Area of Responsibility
AOS	(1) Special Liquids Tanker; (2) Amphibious Objective Study; (3) Area of Separation
AOSG	Amphibious Operation Support Graphic
AOSS	Automated Office Support System
AOT	Transport Oiler
AOTF	Acoustic-Optic Tunable Filter
AP	(1) Armor-Piercing; (2) Air Police; (3) Transport Ship; (4) Associated Press; (5) Ammonium Perchlorate; (6) Antipersonnel; (7) Application Processor
AP-I	Armor Piercing Incendiary
APB	(1) Self-Propelled Barracks Ship; (2) All Points Bulletin; (3) Antipersonnel Bomb; (4) Acquisition Program Baseline
APC	(1) Armored Personnel Carrier; (2) Area of Positive Control; (3) Adaptive Predictive Coding
APCC	Alternate Processing and Correlation Center
APFSDS	Armor-Piercing, Fin-Stabilized, Discarding Sabot
APHIS	USDA Animal and Plant Health Inspection Service
APL	(1) Barracks Craft (non self-propelled); (2) Applied Physics Laboratory (Johns Hopkins University)
APM	Army Program Memorandum
APMS	(1) Automated Production Management System; (2) Advanced Precision Measurement System
APO	(1) Army Post Office; (2) Air Post Office
APOD	Aerial Port of Debarkation
APOE	Aerial Port of Embarkation
APORTS	Aerial Ports File (JOPES)
APP	Application
APPS	Applications
Appl	Application
Approx	Approximately
APPS	Analytical Photogrammetric Position System
APS	(1) ASARS-II Processing Segment; (2) Air Planning System
APT	(1) Automatic Picture Transmission; (2) Airport
APU	Auxiliary Power Unit
APVO	FSU Air Defense Aviation
APW	American Prisoner of War

AQF	Advanced QUICKFIX
AR	(1) Advanced Readiness; (2) Army Regulation; (3) Action Required; (4) Repair Ship; (5) Agent Report; (6) Army Reserve; (7) Army
ARABSAT	Arab Satellite (Communications Organization)
ARB	Battle Damage Repair Ship
ARC	(1) Cable Ship; (2) Acquisition Review Committee; (3) Armored Reconnaissance Carrier; (4) Air Reserve Component
ARCENT	U.S. Army Forces Central Command
ARCENT-K	USACENT forward element-Kuwait
ARCENT-SA	USACENT forward element-Saudi Arabia
ARCH	Architecture
ARCOM	Army Command
ARDC	Air Research and Development Command
AREC	Air Element Coordinator
ARCS	(1) Automated Reproduction and Collating System; (2) Acquisition Radar and Control System
ARD	Auxiliary Repair Drydock
ARDF	Airborne Radio Direction Finding
ARDM	Auxiliary Repair Drydock
AREPT	Agent Report
ARF	Airborne Relay Facility
ARFCOS	Armed Forces Courier Service
ARFOR	Army Force(s)
ARG	(1) Amphibious Readiness Group; (2) Internal Combustion Engine Repair Ship
ARIS	Advanced Range Instrumentation Ship
ARL	(1) Landing Craft Repair Ship; (2) Airborne Reconnaissance Low; (3) Army Research Lab; (4) Aerial Reconnaissance Liaison
ARL-I	Airborne Reconnaissance Low-Imagery
ARLANT	U.S. Army Forces, LANTCOM
ARLEA	Army Logistics Evaluation Agency
ARLO	Air Reconnaissance Liaison Officer
ARM	(1) Antiradiation Missile; (2) Atmospheric Radiation Measurement
ARMA	Army Attache
ARMISE	Army Reserve Military Intelligence Support Element
ARMLO	Army Liaison Officer
ARMS	Automated Resource Management System
ARNG	Army National Guard
ARO	(1) Area Records Officer; (2) Auxiliary Readout
ARP	Alert Response Plan
ARPA	Advanced Research Projects Agency
ARPAC	Army Pacific
ARPANET	Advanced Research Projects Agency Network
ARPS	Advanced Radar Processing System

ARPV	Advanced Remotely Piloted Vehicle
ARR	Radiological Repair Ship
ARRC	(1) ACE Rapid Reaction Corps; (2) Allied Rapid Reaction Corps
ARRN	Andean Ridge Radar Network
ARRS	Aerospace Rescue and Recovery Service
ARS	(1) Salvage and Rescue Ship; (2) Aerial Reconnaissance and Surveillance; (3) Airborne Receiver System; (4) Air Rescue Service
ARSA	(1) Annual Reevaluation of Safe Areas; (2) Airborne Reconnaissance and Surveillance Architecture
ARSGS	Airborne Reconnaissance SIGINT Ground Systems
ARSO	Assistant Regional Security Officer
ARSOA	Army Special Operations Aviation
ARSOC	Army Special Operations Command
ARSOF	Army Special Operations Forces
ARSOFE	Army Special Operations Forces, Europe
ARSOFSUPCOM	Army Special Operations Forces Support Command
ARSOTF	Army Special Operations Task Force
ARSP	Advanced Reconnaissance Support Program
ARSPACE	Army Space Command
ARSPACECOM	Army Space Command
ARSPOC	Army Space Operations Center
ARSST	Army Space Command Space Support Team
ARSTAF	Army Staff
ART	(1) Aerial Reconnaissance Team; (2) Amateur Radio Transceiver
ARTADS	Army Tactical Data System
ARTAS-K	Army Training and Support-Kuwait (former name for ARCENT-K)
ARTBASS	Army Training Battle Simulation Systems
ARTCC	Air Route Traffic and Control Center
ARTEP	(1) Army Readiness Training Evaluation Program; (2) Army Training and Evaluation Program
ARTISS	Advanced Requirements Tasking Information and Support System
ARTPP	Airborne Reconnaissance Technology Program Plan
ARTS	Automated Remote Tracking Station
ARTY	Artillery
ARV	(1) Armored Recovery Vehicle; (2) Armored Reconnaissance Vehicle; (3) Aircraft Repair Ship
ARW	Air Refueling Wing

AS	(1) Submarine Tender; (2) Air Surveillance; (3) Analysis Subsystem; (4) Air Station; (5) Anti Spoofing; (6) Advanced Sensors
ASA	Army Space Agency
ASA	(M&RA)Assistant Secretary of the Army (Manpower and Reserve Affairs)
ASAB	All-Source Analysis Branch
ASAC	All-Source Analysis Center
ASAP	(1) As Soon As Possible; (2) Advanced Sensor Applications Program
ASAR	Advanced Synthetic Aperture Radar
ASARC	Army Systems Acquisition Review Council
ASARS	Advanced Synthetic Aperture Radar System
ASART	(1) AEELS Support Analysis Reporting Terminal; (2) Analysis Support and Reporting Terminal
ASAS	All-Source Analysis System
ASAS-AS	All-Source Analysis System All-Source Workstation
ASAS-E	All-Source Analysis System-Extended
ASAS-SS	All-Source Analysis System Single-Source Workstation
ASAS-W	All-Source Analysis System WARRIOR
ASAT	(1) Antisatellite; (2) Antisatellite Treaty; (3) Advance Satellite Antenna Technology
ASB	(1) Air Surveillance Broadcast; (2) Army Science Board
ASC	(1) AUTODlN Switching Center; (2) Army Service Component; (3) Army Space Command; (4) Advanced Systems Course
ASCAMP	Advanced Single-Channel Manpack
ASCII	American Standard Code for Information Interchange
ASCC	(1) Air Standardization Coordinating Committee; (2) Alternate Space Control Center
ASCII	American National Standard Code for Information Interchange
ASCM	Antiship Cruise Missile
ASCON	Automatic Switched Communications Network
ASD	Assistant Secretary of Defense
ASD (C3I)	Assistant Secretary of Defense (Command, Control, Communications, and Intelligence)
ASD (C4I)	Assistant Secretary of Defense (Command, Control, Communications, Computers and Intelligence)
ASD (ISA)	Assistant Secretary of Defense for International Security Affairs
ASD (S&R)	Assistant Secretary of Defense for Strategy and Requirements
ASD (SO/LIC)	Assistant Secretary of Defense for Special Operations and Low Intensity Conflict
ASDC	Advanced Space Data Corporation
ASDEP	Army Space Exploitation Demonstration Programs
ASDIA	All-Source Document Index
ASDIAZ	All-Source Document Index Automated File-Compartmented
ASDIAZO	All-Source Document Index Automated File-ORCON
ASDIC	Armed Services Documents Intelligence Center

ASDS	(1) Automated SIGINT Dissemination System; (2) Advanced SEAL Delivery System
ASDV	Auxiliary SEAL Delivery Vehicle
ASE	(1) Aircraft Survivability Equipment; (2) Airborne Support Element
ASEAN	Association of Southeast Asian Nations
ASED	Army Space Exploitation Demonstration
ASEDP	Army Space Exploitation Demonstration Program
ASEMA	Army Special Electronic Mission Aircraft
ASF	All-Source Format
ASFC	All-Source Fusion Center
ASG	Area Support Group
ASGOBS	Army Standard Ground Order of Battle System
ASI	(1) Additional Skill Indicator; (2) U.S. Army Space Institute; (3) All-Source Intelligence
ASIC	All-Source Intelligence Center
ASICC	All-Source Intelligence Coordinating Center
ASIDS	Airborne Secondary Imagery Dissemination System
ASIP	All-Source Imagery Processor
ASIPS	Army Standard Intelligence Plotter System
ASIS	Army Space Initiatives Study
ASIT	Adaptable Surface Interface Terminal
ASM	(1) Air-to-Surface Missile; (2) Antiship Missile; (3) Attache Support Message
ASMD	Antiship Missile Defense
ASMT	Assessment
ASN (RDA)	Assistant Secretary of the Navy (Research, Development and Acquisition)
ASOC	Air Support Operations Center
ASOG	Air Support Operations Group
ASOS	Air Support Operations Squadron
ASP	Ammunition Supply Point
ASPAC	Asian and Pacific Council
ASPADOC	Alternate Space Defense Operations Command
ASPB	Assault Patrol Support Boat (Riverine Warfare Craft)
ASPIC	Armed Services Personnel Interrogation Center
ASPJ	Airborne/Advanced Self-Protection Jammer
ASPO	Army Space Program Office
ASPS	All-Source Production Section
ASR	(1) Submarine Rescue Ship; (2) Airport Surveillance Radar; (3) Adaptive Situation Recognizer
ASRP	(1) Airborne SIGINT Reconnaissance Program; (2) Airborne SIOP Reconnaissance Plan
ASRRS	Army Survivable, Recovery and Reconstitution System
ASSC	Alternate Space Surveillance Center
ASSET	All Source Satellite Evaluation Tool

ASSIST	(1) Army System for Standard Intelligence Support Terminals; (2) Automated Special Security Terminals; (3) Automated Special Security Information System; (4) Automated Information System Security Incident Support Team
ASSM	Antiship Surface Missile
ASSOTW	Airfields and Seaplane Stations of the World
ASSR	Autonomous Soviet Socialist Republic
ASST	(1) Antiship Surveillance and Tracking; (2) Assistant
ASSW	Antisurface Ship Warfare
ASTAG	Army Service and Technology Advisory Group
ASTEC	Advanced Satellite Technology and Extremely High Frequency Communications
ASTERIX	Automated Analyst Support Tools
ASTMP	Army Science and Technology Master Plan
ASTP	APOLLO-SOYUZ Test Program
ASU	(1) FSU Airborne Self-Propelled Antitank Gun; (2) Approved for Service Use
ASUW	Antisurface Warfare
ASU SWA	Administrative Support Unit Southwest Asia
ASUWC	Antisurface Warfare Commander
ASV	Armored Support Vehicle
ASW	(1) Antisubmarine Warfare; (2) Aircrew Survival Weapon
ASWC	Antisubmarine Warfare Commander
ASWCCS	Antisubmarine Warfare Command and Control System
ASWOC	Antisubmarine Warfare Operations Center
ASWTF	Antisubmarine Warfare Task Force
AT	(1) Antitank; (2) Air Transit; (3) Simple Antenna (Electronic Component); (4) Air Technician; (5) Awaiting Transportation; (6) Antiterrorism, (7) Annual Training
ATA	(1) Actual Time of Arrival; (2) Ocean Tug; (3) Air Transport Association; (4) Advanced Tactical Aircraft; (5) Air Traffic Agency
ATAC	ASAP Technical Advisory Committee
ATACC	Advanced Tactical Air Command Center
ATACMS	(U.S.) Army Tactical Missile System
ATACMS ER	Army Tactical Missile System Extended Range
ATACS	(1) Analyst-to-Analyst Communications Service; (2) Army Tactical Communications System
ATAF	Allied Tactical Air Force (NATO)
ATARS	Advanced Tactical Aerial Reconnaissance System
ATAS	(1) Air-To-Air Stinger; (2) Automatic Terrain Avoidance System
ATB	(1) Air Technical Battalion; (2) Advanced Technology Bomber
ATBM	Antitactical Ballistic Missile
ATC	(1) Air Traffic Control; (2) Air Training Command, USAF; (3) Air Target Chart; (4) Mini-Armored Troop Carrier (Riverine Warfare Craft)
ATCAE	Army Technical Control and Analysis Element

ATCC	Air Traffic Control Center
ATCCS	Army Tactical Command and Control System
ATCH	ASW Torpedo-Carrying Helicopter
ATCU	Airfield Traffic Control Unit
ATD	(1) Actual Time of Departure; (2) Advanced Technology Demonstration
ATDB	ACE Target Data Base
ATD/IFD	Advanced Technology Demonstration/Integrated Feasibility Demonstration
ATDL	Automated Tactical Data Link
ATDS	Airborne Tactical Data System
ATE	Automatic Test Equipment
ATETS	Atomic Heat and Powerplant
ATF	(1) Advanced Tactical Fighter; (2) Amphibious Task Force; (3) Fleet Ocean Tug; (4) Aviation Turbine Fuel; (5) After the Fact
ATFD	Automated Tactical Fusion Division
ATGIN	Atomic Ground Intercept
ATGL	Antitank Guided Launcher
ATGM	Antitank Guided Missile
ATH	Above The Horizon
ATI	Automated Tactical Intelligence
ATIC	Aircraft Technical Intelligence Conference
ATIMS	Advanced Technical Information Management System
ATL	ACE Threat List
ATLIS	Airborne Tracking Laser Identification System
atm	Atmosphere
ATM	(1) Antitank Missile; (2) Air Target Materials; (3) Air Target Mosaic; (4) Antitactical Missile; (5) Asynchronous Transfer Mode; (6) Air Tasking Message
A-TM	Alpha Team (Special Forces Operational Detachment)
ATMDE	Army Theater Missile Defense Element
ATMG	Arms Transfer Management Group
ATMOS	Atmospheric Trace Molecules Spectroscopy
ATMP	Air Target Materials Program
ATO	(1) Air Tasking Order; (2) Abort-To-Orbit
ATOC	Allied Tactical Operations Center (NATO)
AFTOCONF	Air Tasking Order Confirmation
ATOL	Assisted Takeoff & Landing
ATOS	Atlantic Theater Operational Intelligence System
ATP	(1) Allied Tactical Publication (NATO); (2) Advanced Technology Program; (3) Advanced Tracking Prototype; (4) Advanced Tactical Planner
ATP-FO	Automated Tracking Prototype Follow-On
ATP/RMBUX	Advance Tracking Prototype/Rocky Mountain Basic UNIX
ATR	Automatic Target Recognition
ATRS	Advanced Tactical Reconnaissance System

ATS	(1) Salvage and Rescue Ship; (2) Automated Tasking System; (3) Audit Trail Server; (4) Applications Technology Satellite
ATSS	Alaskan Transportable Satellite System
AT&T	American Telephone and Telegraph
ATT	Technical Assistance Training Team
ATTCS	Army Tactical Command and Control System
ATTD	Advanced Technology Transition Demonstration
ATTE	Assistant Theater Topographic Engineer
ATTG	Automated Tactical Target Graphic
ATTN/Attn	Attention (to the attention of)
ATTP	ACOM Tactics, Techniques, and Procedures
ATWC	Atmospheric Tactical Warning Connectivity
AU	Air University
AUD	Arbitrary Unit Designator
AUGTDA	Augmentation Table of Distribution and Allowances
AUM	Air-to-Underwater Missile
AUS	Army of the United States
AUSA	Association of the United States Army
AUSCANUKUS	Australia, Canada, United Kingdom, United States
AUSD	Assistant Deputy Under Secretary for Defense
AutoID	Automatic Identification
AUTODIN	Automatic Digital Network
AUTOSEC	Automation Security
AUTOSEVOCOM	Automatic Secure Voice Communications Network
AUTOVON	Automatic Voice Network
AUTUMN FORGE	NATO Exercise
AUXCP	Auxiliary Command Post
AV	(1) Armored Vehicle; (2) Audio-Visual; (3) Air Vehicle; (4) Auxiliary Vector
AVCS	Attitude and Velocity Control System
AVF	All-Volunteer Force
AVGAS	Aviation Gasoline
AVHRR	Advanced Very High Resolution Radiometer
AVIM	Aviation Intermediate Maintenance
AVLB	Armored Vehicle-Launched Bridge
AVMF	FSU Naval Aviation
AVMT	Aviation Maintenance Trainer
AVN	Aviation
AVP	Authorized Vendor Program
AVR	Aircraft Rescue Vehicle
AVSAT	Aviation Satellite System
AVSCOM	Aviation System Command
AVT	Auxiliary Aircraft Landing Training Ship
AVUM	Aviation Unit Maintenance

AW	(1) Air Warning; (2) Automatic Weapon(s); (3) Water Tanker; (4) All-Weather
AWACS	Airborne Warning and Control System
AWADS	Adverse Weather Aerial Delivery System
AWARS	All-Weather Reconnaissance System
AWC	(1) Air War College; (2) Army War College; (3) Air Warfare Center
AWDS	Automated Weather Distribution System
AWE	Advanced Warfighting Experiment
AWESS I	Automatic Weapon Effect Signature Simulator
AWGN	Additive White Gaussian Noise
AWIS	(1) Army WWMCCS Information System; (2) Aircraft Wireless Intercom System
AWN	Automated Weather Network
AWOP	(1) Absent Without Pay; (2) Automated Weaponeering Optimization Program
AWS	(1) Air Weather Service; (2) Advance Warning System; (3) Analyst Workstation
AWSS	Area Weapon Scoring System
AWT	Water Transport
AWWIMS	Automated Worldwide Warning Indicator Monitoring System
AWX	All-Weather
AXAF	Advanced X-ray Astrophysics Facility
AXP	Allied Exercise Publication
AXT	Training Ship
AZ	Azimuth

B

BA	(1) Budget Authority; (2) Budget Activity
BAA	Broad Agency Announcement
BAC	(1) Budget Activity Code; (2) Broad Area Coverage
BAD	Baseline Assessment Document
BADGE FINDER	Proper Name of System
BADGE KEEPER	Proper Name of System
BAE	Battlefield Area Evaluation
BAG	Battalion Artillery Group
BAI	(1) Battlefield Air Interdiction; (2) Backup Aircraft Inventory; (3) Battlefield Artificial Intelligence
BALTAP	Baltic Approaches (NATO Naval Command)
BAN	Base Area Network
BANDIT	Bragg Area Network for Digital Intelligence Transmission
BAO	Basic Attack Option
BAOR	British Army of the Rhine
BARB	Beacon-Aided Radar Bombing
BARCS	Battlefield Area Reconnaissance System
BAS	(1) Broad Area Search; (2) Battlefield Automated Systems; (3) Billet Access System
BASIC	Battle Area Surveillance & Integrated Communications
BASOPS	Base Operations
BASS	Battlefield Surveillance System
BAT-D	Battlefield Deception
BATF	Bureau of Alcohol, Tobacco, and Firearms
BATO	Balloon-Assisted Take-Off
BATS	Ballistic Aerial Target System
BAWB	Bomber Activity Weekly Brief
BB	Battleship
BBBG	Battleship Battle Group
BBLS	Barrels
BBO	Booster Burnout
BBS	Brigade/Battalion Simulation
B2C2	Brigade and Below Command and Control System
BCA	Broadcast Control Authority
BC2A	Bosnia Command and Control Augmentation
BCBL	Battle Command Battle Lab
BCC	Base Communications Center
BCDSS	Battle Command Decision Support System
BCE	Battlefield Coordination Element
BCI	Bit-Count Integrity
BCR	(1) Battlefield Communications Review; (2) Baseline Change Request
BCS	Broadcast Control Station

BCT	(1) Base Consolidated Telecommunications; (2) Betac Command Team
BCTP	Battle Command Training Program
BCV	Battle Command Vehicle
Bd	Baud
BDA	(1) Battle Damage Assessment; (2) Bomb Damage Assessment
BDA/PSA	Bomb Damage Assessment/Post Strike Assessment
BDE/Bde	Brigade
BDM	Budget Decision Memorandum
BDP	Battlefield Development Plan
BDS	(1) Base Development Survey; (2) Bulk Data Service
BDSP	Battle Dress System Project
BE	Basic Encyclopedia
BEMT	Basic Electronic Maintenance Trainer
BENELUX	Belgium, Netherlands, Luxembourg
BER	Bit Error Rate
BES	Budget Estimate Submission
BETA	Battlefield Exploitation and Target Acquisition
BEYOND DUTY	Proper Name of System
BF	Battle Force
BFA	Battlefield Function Area
BFACS	BFA Control System
BF(S)BL	Battle Focus (Support) Battle Lab
BFCS	Ballistic Framing Camera System
BFE	Blacker Front End
BFI	Battlefield Interdiction
BFM	Basic Flight Maneuvers
BFMA	Battlefield Functional Mission Area
BFOV	Broad Field of View
BG	(1) Battle Group; (2) Brigadier General
BGN	Board on Geographic Names
BGPHES	Battle Group Passive Horizon Extension System
BGW	Battlefield Guided Weapon
BGWU	Battle Group Workup
BH	Busy Hour
B-H	Bosnia-Hercegovina
BI	Background Investigation
BIACC	Basic Integrated Aircraft Command and Control
BIC	Battlefield Information Center
BICC	Battlefield Information Coordination Center
BICES	Battlefield Information Collection and Exploitation Systems (NATO)
BICM	Battlefield Intelligence Collection Model
BIDS	Battlefield Information Distribution System
BIF	Basic Imagery File

BIFF	Bistatic Identification Friend or Foe
BIIB	Basic Imagery Interpretation Brief
BIIR	Basic Imagery Interpretation Report
BIM	Ballistic Intercept Missile
BIOLDEF	Biological Defense
BIOLOPS	Biological Operations
BIOLWPN	Biological Weapons
BISS	Baseline Intelligence Summary Supplement
BIT	Binary Digit
BITE	Built-In Test Equipment
BITS	Base Information Transfer System
BIU	Bus Interface Unit
Bks	Barracks
BKS	Broadcast Keying Station
BL	Bomb Line
BLDG	Building
BLEST	Berm-Loaded Explosive Simulation Technique
BLEU	Belgium-Luxembourg Economic Union
BLIP	Background Limited IR Photography
BLOS	Beyond Line-of-Sight
BLSS	Base Level Self-Sufficiency Spares
BLT	Battalion Landing Team
BLUE FLAG	ACC command and control exercise
BM	(1) FSU Truck-Mounted Multiple Rocket Launcher; (2) Ballistic Missile
BMATT	Briefcase Multi-Mission Advanced Tactical Terminal
BM/C2	Battle Management/Command and Control
BM/C3	Battle Management/Command, Control, and Communications
BMC	Battle Management Cell
BMCT	Beginning of Morning Civil Twilight
BMD	(1) Ballistic Missile Defense; (2) FSU Airborne Combat Vehicle
BMDO	(1) Ballistic Missile Defense Organization; (2) Ballistic Missile Defense Office
BMDSCOM	U.S. Army Ballistic Missile Defense Systems Command
BMEWS	Ballistic Missile Early Warning System
BMG	Basic Mission Guidance
BMNT	Beginning of Morning Nautical Twilight
BMP	FSU Armored Infantry Combat Vehicle
BMSS	Ballistic Missile Systems Subcommittee
BN/Bn	Battalion
BND	Bundesrepublik Nachrichtendienst (German Intelligence Service)
BOA	Broad Ocean Area
BOCCA	Board for Coordination of Civil Aircraft (NATO)
BOIP	Basis of Issue Plan

BOMREP	Bombing Report
BOQ	Bachelor Officers' Quarters
BOS	(1) Battlefield Operating System; (2) Base Operating Support
BP	(1) Battle Position; (2) Bandpass
BPA	(1) Battlefield Psychological Activities; (2) Blanket Purchase Agreement
BPE	Beacon Precision Enlarger
BPF	Bandpass Filter
BPI	Bits Per Inch
BPPBS	Biennial Planning, Programming, and Budgeting System
BPR	Business Process Reengineering
BPS	(1) Basic Psychological Operations Study; (2) Bits Per Second; (3) Beachman Processing System
BPSK	Burst Pulse Shift Key
BR	Blade Rate
B/R	Bridge/Router
BR/Br	Branch
BRAC	Base Realignment and Closure (Commission)
BRDM	FSU Wheeled Amphibious Armored Reconnaissance Vehicle
BRET	Bistatic Reflected Energy Target
BRI	Basic Rate Interface
BRIXMIS	British Commanders-In-Chief Military Liaison Mission
BRL	Bomb Release Line
BRP	Bomb Release Point
BRS	(1) Beachman Reporting System; (2) Backup and Recovery System (3) Beach Reconnaissance System
BRU	Bomb Release Unit
BS	Broadcast Service
BSA	Brigade Support Area
BSD	(1) Battlefield Surveillance Device; (2) Battlefield Surveillance Display
BSS	Broadcast Satellite Service
BSSC	Battle Staff Support Center
BSSG	Brigade Service Support Group
BST	(1) Battle Staff Team; (2) Betac Support Team
BSTS	(1) Boost Surveillance and Tracking System; (2) Boost Phase Surveillance and Tracking System
BT	Basic Training
BTA	Best Technical Approach
BTF	Battalion Task Force
BTG	Basic Target Graphic
BTI	Balanced Technology Initiative
BTR	FSU Armored Personnel Carrier
BTRY	(1) Battery; (2) Field Artillery
BTU	British Thermal Unit
BTW	By The Way

BUD/S	Basic Underwater Demolition/Sea-Air-Land (SEAL)
BUIC	Back-Up Intercept Control
BUNT	British Underground Nuclear Test
BUR	Bottom Up Review
BVITS	Baseline Video Imagery Transmission System
BVR	Beyond Visual Range
BW	(1) Biological Warfare; (2) Bandwidth; (3) Beamwidth; (4) Bomb Wing
B&W	Black and White
BWC	Biological Weapons Convention
BWP	Basic Working Paper
BZ	Buffer Zone

C

C	(1) Crisis; (2) Confidential; (3) Coniferous
C1	Combined Staff Personnel Officer
C2	(1) Command and Control; (2) Combined or Coalition Forces Intelligence Staff
C2S2LAN	Command and Control Support System LAN
C2W	Command & Control Warfare
C3	Command, Control, and Communications
C3OB	C3 Order of Battle
C3S	Command, Control, and Communications Systems
C4	Command, Control, Communications, and Computers
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
C4S	Command, Control, Communications, and Computer System
C5	Combined Staff Strategic Planning and Policy Officer
C6	Combined Staff Command, Control and Communications Systems Officer
CA	(1) Cryptanalysis; (2) Heavy Cruiser; (3) Civil Affairs; (4) Combat Assessment; (5) Controlling Authority; (6) COMSEC Account; (7) Command Authority; (8) Counterair
CAA	(1) Concepts Analysis Agency (U.S. Army); (2) Combined Arms Army (FSU); (3) Command Arrangement Agreement
CAB	(1) Current Analysis Branch; (2) Civil Affairs Brigade; (3) Civil Affairs Battalion
CAC	(1) Combined Arms Center; (2) Collection Advisory Center; (3) Control and Analysis Center; (4) Crisis Action Center; (5) Civil Affairs Command; (6) Civil Applications Committee; (7) U.S. Army Combined Arms Command
CACDA	Combined Arms Combat Development Activity
CACM	Central American Common Market
CACTIS	Community/Computer Automated Counterterrorism Intelligence System
CAD	(1) Computer-Assisted Design; (2) Conceptual Architecture Document
CADES	COMIREX Advanced Exploitation System
CADIZ	(1) Canadian Air Defense Identification Zone; (2) Coastal Air Defense Identification Zone
CADOB	Consolidated Air Defense Order of Battle
CADS	Containerized Ammunition Distribution System
CADST	Civil Affairs Direct Support Team
CAE	Computer Aided Engineering
CAF	(1) Crisis Augmentation Facility; (2) Combat Air Forces
CAFMS	Computer-Assisted Force Management System
CAG	(1) Carrier Air Group; (2) Collective Address Group; (3) Commander, Air Group
CAI	Computer-Aided Instruction
CAIF	Command Automated Intelligence File

CAIMS	Conventional Ammunition Information Management System
CAJIT	Central America Joint Intelligence Team
CaLANdar	Da Vinci E-Mail Application
CALS	Computer-Aided Acquisition and Logistics Support
CALT	Civil Affairs Liaison Team
CAM	(1) Computer-Assisted Modeling; (2) Computer Aided Manufacturing
CAMO	Computer-Aided Manual Operation
CAMPS	(1) Computer-Aided Management Planning System; (2) Computer-Aided Mission Planning System; (3) Compartmented All-Source Analysis System Message Processing System
CAMS	(1) COMIREX Automated Management System; (2) Communications Area Master Station
CANDOB	Consolidated Aerospace Defense Order of Battle
CANR	Canadian NORAD Region
CAN	Coastal Air Navigation Supplement
CANT	Chinese Atmospheric Nuclear Test
CANUK	US Canada, United Kingdom, United States
CANUS	Canadian - United States
CANUS LANDOP	Canada-United States Land Operations Plan
CAO	(1) Crisis Action Organization; (2) Chief Administrative Officer; (3) Central Action Office
CAO(SOP)	Coordination of Atomic Operations (Standard Operating Procedure)
CAOC	Combined Air Operations Center
CAOCC	Combined Air Operations Coordination Center
CAP	(1) Combat Air Patrol; (2) Civil Air Patrol; (3) Countermeasures Advisory Panel; (4) Crisis Action Planning; (5) Crisis Action Procedures; (6) Capabilities
CAPSULE JACK	Proper Name of System
CAR	(1) Canadian Airborne Regiment; (2) Chief, Army Reserve
CARC	Corrective Action Review Committee
CARDA	(1) Continental Airborne Reconnaissance for Damage Assessment; (2) CONUS Airborne Reconnaissance for Damage Assessment
CARE	Cooperative for American Relief Everywhere, Inc.
CARG	Crisis Action Review Group
CARGRU	Carrier Group
CARIBJIC	Caribbean Joint Intelligence Center
CARIBROC	Caribbean Regional Operations Center
CARICOM	Caribbean Common Market
CARIFTA	Caribbean Free Trade Association
CARL	Category Assignment Responsibility List
CARP	Computed Air Release Point
CARS	(1) Contingency Airborne Reconnaissance System; (2) Common Automated Recovery System

CARVE	Criticality, Accessibility, Recuperability, Vulnerability, and Effect
CARVER	Criticality, Accessibility, Recuperability, Vulnerability, Effects and Recognizability
CAS	(1) Close Air Support; (2) Calibrated Air Speed; (3) Collision Avoidance System; (4) Crisis Action System; (5) Crisis Action Staff; (6) Combined Arms and Services Staff School
CASC	Crisis Action Support Cell
CASE	Computer-Assisted Software Engineering
CASIC	Combined All-Source Intelligence Center
CASLAN	Command Automated Software Local Area Network
CASS	(1) Collection Analysis Support Subsystem; (2) Command Activated Sonobuoy System
CAST	(1) Catalogue of Approved Scientific and Technical Intelligence Tasks; (2) Canadian Air/Sea Transport Group; (3) Computer-Assisted Self Training; (4) Computer Assisted Satellite Track
CAT	(1) Conventional Arms Transfer; (2) Crisis Action Team; (3) Combined Arms Team; (4) Crisis Augmentation Team; (5) Category
CAT-1	RECategory-1 Receive Equipment
CATF	(1) Commander, Amphibious Task Force; (2) Civil Affairs Task Force
CATIS	(1) Computer-Aided Tactical Information System; (2) Computer-Aided Tactical Intelligence System
CATIS/IESS	Computer-Aided Tactical Information System/Imagery Exploitation Support System
CATS	(1) Combined Arms Training Systems; (2) Combat Airlift Tactics' School
CATSS	Cartographic Applications for Tactical and Strategic Systems
CAV	Cavalry
CAVU	Ceiling And Visibility Unlimited
CAWS	Commercial Analyst Work Station
CB	Chemical, Biological
C-band	3.9 to 6.2 GHz Communications Band
CBD	Commerce Business Daily
CBF	Common Budget Framework
CBI	(1) Complete Background Investigation; (2) Computer Based Instruction
CBI/T	Computer-Based Instruction/Training
CBJB	Congressional Budget Justification Book
CBM	Confidence Building Measure(s)
CBO	Congressional Budget Office
CBR	(1) Chemical, Biological, and Radiological; (2) Case Based Reasoning; (3) Constant Bit Rate
CBRN	Caribbean Basin Radar Network
CBRS	Concept Based Requirements System
CBS	Combat Battle Simulation
CBT	(1) Computer-Based Training; (2) Combating Terrorism

CBTDEV	Combat Developer
CBTI	Combat Intelligence
CBU	Cluster Bomb Unit
CBW	Chemical and Biological Warfare
CBZ	Confidence Building Zone
CC	(1) Command Center; (2) Command Ship; (3) Cloud Cover; (4) Collection Center; (5) Computer Compatible; (6) Communications Controller; (7) Commander
C-C3	Counter Command, Control, and Communications
CCA	Communications Control Authority
CCB	Configuration Control Board
CCC	(1) CARDA Control Center; (2) Consolidated Command Center; (3) Command and Control Center
CCD	(1) Conference of the Committee on Disarmament; (2) Charged Coupled Device; (3) Camouflage, Concealment, and Deception
CCE	Contingency Communications Element
CCEB	Combined Communications Electronic Board
CCEP	Commercial COMSEC Endorsement Program
CCF	Collection Coordination Facility
CCF-SS	Collection Coordination Facility-Support System
CCG	(1) Combat Control Group; (2) Crisis Coordination Group; (3) Combat Communications Group
CCG-NB	Communications Control Ground-Narrowband
CCGD	Commander, Coast Guard District
CCGP	Combat Communications Group
CCHC	Headquarters Commandant
CCI	Controlled Cryptographic Item
CCIC	Concentrated Counterdrugs Intelligence Collection
CCIP	Command Center Improvement Program
CCIR	International Radio Consultative Committee (French Acronym)
CCIRID	Charge-Coupled Infrared Imaging Device
CCIRM	Collection Coordination and Intelligence Requirements Management
CCIS	(1) Command, Control, and Intelligence Support; (2) Common Channel Intelligence Signaling
CCISCMO	Community Counterintelligence and Security Countermeasures Office
CCISS	Command & Control Intelligence Support Squadron
CCITT	Consultative Committee for International Telephone and Telegraph
CCJ1	USCENTCOM Manpower, Personnel, and Administration Directorate
CCJ2	USCENTCOM Intelligence Directorate
CCJ3	USCENTCOM Operations Directorate
CCJ4/J7	USCENTCOM Logistics and Security Assistance Directorate
CCJ5	USCENTCOM Plans and Policy Directorate

CCJ6	USCENTCOM Command, Control, Communications, and Computer Systems Directorate
CCJA	USCENTCOM Staff Judge Advocate
CCM	(1) Cross-Country Movement; (2) Counter-Countermeasure
C3CM	Command, Control, and Communications Countermeasures
CCMF	Consolidated Collection Management Facility
CCN	Crisis Communications Network (CIA)
CCO	(1) Communication Collection Outstation; (2) COMINT Collection Outstation; (3) Circuit Control Officer; (4) Chief, Combat Operations
CCO/SCO	Central Control Office/Sub-Control Office
CCP	(1) Consolidated Cryptologic Program; (2) Communications Checkpoint; (3) Contingency Communications Package
CCPC	Critical Collection Problems Committee
CCPDS	Command Center Processing and Display System
CCPDS-R	Command Center Processing and Display System Replacement
CCS	(1) Collection Capabilities Statement (HUMINT); (2) COMINT Collection Subsystem (3) Combat Control Squadron; (4) Communications Control Set; (5) Command and Control Systems; (6) Constellation Control Station
CCS2	Command and Control Subordinate System
CCSA	USCENTCOM Scientific and Technical Advisor
CCSC	Cryptologic Combat Support Console
CCT	(1) Combat Control Team; (2) Combat Coordination Team
CCTC	Command and Control Technical Center
CCTF	(1) Contingency Communications Test Facility; (2) Combined Coalition Task Force
CCTP	Continuously Computed Target Point
CCTS	Combat Crew Training Squadron
CCTT	Close Combat Tactical Trainer
CCTV	Closed Circuit Television
CCTW	Combat Control Training Wing
CCWT	Command Center Watch Team
CD	(1) Controlled Dissemination; (2) Certificate of Destruction; (3) Civil Defense; (4) Coastal Defense; (5) Calendar Day; (6) Committee on Disarmament; (7) Collateral Damage; (8) Compact Disc; (9) Command Ship; (10) Counter Drug; (11) Command Director; (12) Combat Developments; (13) Community/Service-Developed
C&D	Cover and Deception
CDA	Congressionally Directed Action
CDC	(1) Career Development Course; (2) Combat Direction Center; (3) Combat Development Center
CD-ROM	Compact Disk-Read-Only Memory
CDAS	Central Data and Applications Support
C-Day	Day in Which Movement From Origin Begins
CDB	Central Data Base
CDCS	Communications Distribution Control Segment

CDE	(1) Conference on Disarmament in Europe; (2) Compound Damage Expectancy; (3) Center of Distance Education
CDEC	Captured Document Exploitation Center
CDF	Central Document File
CDI	Compact Disc Interactive
CDIP	(1) Consolidated Defense Intelligence Program; (2) Council of Defense Intelligence Producers
CDIS	(1) Communications Data Interface System; (2) Counterdrug Intelligence System
CDIST	Canadian Department of Industry, Science, and Technology
CDL	Common (high bandwidth) Data Link
CDLF	Consolidated Domestic Launch Forecast
CDM	Common Digital Map
CDMA	Code Division Multiple Access
CDP	(1) Central Data Processor; (2) Company Distributing Point
CDPS	Coherent Data Processing System
CDR	(1) Critical Design Review; (2) Commander
CDRL	Contract Data Requirements List
CDRUSAJFKSWC	Commander, United States Army John F. Kennedy Special Warfare Center
CDRUSELEMNORAD	Commander, U.S. Element NORAD
CDRWESTCOM	Commander, U.S. Army Western Command
CDS	(1) Chief of Defence Staff (Canadian); (2) Combat Delivery System; (3) Cryptographic Device Services; (4) Combat Direction System
CDSE	Cryptologic Direct Support Element
CDSORG	Civil Direction of Shipping Organization
CDST	C3CM Data Support Team
CDT	(1) Central Daylight Time; (2) Communications Data Terminal
CDTS	Computer-Directed Training System
CDU	Control Display Unit
CDV	Compressed Digital Video
CE	(1) Circular Error; (2) Cost Effectiveness; (3) Civil Engineer; (4) Communications-Electronics; (5) Corps of Engineers (U.S. Army); (6) Current Exploitation; (7) Counterespionage; (8) Command Element; (9) Collection Emphasis
C&E	Collection and Exploitation
C-E	Communications Electronics
CEAO	West African Economic Community
CEC	(1) Cooperative Engagement Capability; (2) Consolidated Expenditure Center
CECOM	Communications and Electronics Command
CED	(1) Collection, Exploitation, and Dissemination; (2) Captured Enemy Document
CEE	Captured Enemy Equipment
CEI	Communications Electronic Instructions

CEL	Celestial
CELT	Current Emitter Location Testbed
CEM	Concepts Evaluation Model
CEMA	Council for Mutual Economic Assistance
CENTAF	(1) Central Region Air Forces (NATO); (2) U.S. Air Force Component, USCENTCOM
CENTAG	Central Army Group (NATO)
CENTAM	Central America
CENTCOM	U.S. Central Command
CENTJIC	Joint Intelligence Center USCENTCOM
CENTLANT	Central Sub-Area of Eastern Atlantic Area
CENTO	Central Treaty Organization
CEO	(1) Communications Electronic Officer (USMC); (2) Chief Executive Officer
CEOI	Communications Electronics Operations Instructions
CEP	(1) Circular Error Probable; (2) Construction Electrician (Power); (3) Common Electronic Parts; (4) Civil Emergency Planning; (5) Committee for Energy Policy of OECD; (6) Capital Equipment Plan; (7) Concept Evaluation Program
CEPG	Combined Exercise Planning Group
CEPIR	Current Exploitation Photographic Interpretation Report
CEPR	Compromising Emanation Performance Requirement
CER	(1) Cryptographic Equipment Room; (2) Communication Equipment Room
CERP	(1) Combined Economic Reporting Program; (2) Capital Equipment Replacement Program
CERT	Computer Security Emergency Response Team
CES	Concept Exploration Studies
CESM	Cryptologic Electronic Warfare Support Measures
CEST	Contingency Exploitation Support Team
CETA	Chinese-English Translation Assistance
CEWI	Combat Electronic Warfare Intelligence
CF	Canadian Forces
C6F	Commander, U.S. Sixth Fleet
C7F	Commander, U.S. Seventh Fleet
CFA	(1) Combined Field Army (Korea); (2) Covering Force Area; (3) Combined Force Air Component Commander
CFB	Canadian Forces Base
CFC	(1) Combined Field Command (Korea); (2) Combined Forces Command (ROK/US); (3) Combined Federal Campaign
CCFC	Commander in Chief, ROK-U.S. Combined Forces Command
CFD	Common Fill Device
CFE	(1) Conventional Forces Europe; (2) Communications Front-End
CFER	CFE Replacement
CFE-U	Communications Front-End-Upgrade
CFI&I	Center for Integration and Interoperability
CFIS	Combined Forces Command Information System, (CFC)

CFL	(1) Coordinated Fire Line; (2) Cease-Fire Line
CFMS	Combat Fuels Management System
CFP	(1) Contingency Force Pool; (2) Concept Formulation Process
CFR	Commander Force Reconnaissance
CFSO	Counterintelligence Force Protection Source Operations
CFSR	Contract Funds Status Report
CFV	Cavalry Fighting Vehicle
cg	Center of Gravity
CG	(1) Guided-Missile Cruiser; (2) Consolidated Guidance; (3) Commanding General; (4) Coast Guard; (4) Chairman's Guidance
CGEUSA	Commanding General, 8th US Army
CGF	Central Group of Forces (FSU Forces in Czechoslovakia)
CGFMFLANT	Commanding General, Fleet Marine Forces Atlantic
CGM	Computer Graphics Metafile
CGN	Guided Missile Cruiser Nuclear Powered
CGS	(1) Coast & Geodetic Survey; (2) Common Ground Station; (3) CONUS Ground Station
CGSC	Command and General Staff College (U.S. Army)
CGUSARPAC	Commanding General U.S. Army Pacific
cGy/hr	CentiGray hour
CH	(1) Aviation Cruiser; (2) Channel; (3) Communication Helmet
CHAALS	Communications High Accuracy Airborne Location System
CHAALS-X	CHAALS Exploitation
CHABNCP	Chief, Airborne Command Post
CHAMPUS	Civilian Health And Medical Program of the Uniformed Services
CHARS	Characters
CHB	Cargo Handling Battalion
CHBDL	Communications High Bandwidth Data Link
CHCMSA	Chief, Cruise Missile Support Activity
CHCSS	(1) Chief, Central Security Service; (2) Chief, Cryptologic Support Service
CHG	Guided-Missile Aviation Cruiser
CHGN	Nuclear-Powered Guided-Missile Aviation Cruiser
CHIP	Communications Handbook for Intelligence Planners
CHJUSMAGK	Chief, Joint U.S. Military Assistance Group, Korea
CHJUSMAGPHIL	Chief, Joint U.S. Military Assistance Group, Philippines
CHJUSMAGTHAI	Chief, Joint U.S. Military Assistance Group, Thailand
CHMAAGDOMREP	Chief, Military Assistance and Advisory Group, Dominican Republic
CHMDO JAPAN	Chief, Military Defense Office, Japan
CHN	Nuclear-Powered Aviation Cruiser
CHODC INDIA	Chief, Office of Defense Cooperation, India
CHOP	(1) Change of Operational Command; (2) Change of Operational Control
C-HUMINT	Counter Human Resources Intelligence

CHUSMLO	Chief, U.S. Military Liaison Office
CI	(1) Counterintelligence; (2) Counterinsurgency; (3) Current Intelligence
C2I	Command, Control, & Intelligence
C3I	Command, Control, Communications, and Intelligence
C4I	Command, Control, Communications, Computers, & Intelligence
C4I2	Command, Control, Communications, Computers, Intelligence and Information
CIA	Central Intelligence Agency
CIAC	Computer Incident Assessment Capability
CIAD	(1) Combat Intelligence Applications Division; (2) Command Intelligence Architecture Document
CIAP	(1) CIA Program; (2) Command Intelligence Architecture/Planning Program
CIARDSCIA	Retirement and Disability System
CIAS	Counterintelligence Analysis Section
CIB	Combat Infantryman's Badge
CIC	(1) Combat Information Center; (2) Combat Intelligence Center; (3) Combined Intelligence Center
C3IC	Coalition Coordination and Communications Integration Center
CICAC	Counterintelligence Control and Analysis Center
CICC	Consolidated Intelligence Communications Center
CIC Server	Combined Intelligence Center Server
CICWS	Combined Intelligence Center Workstation
CID	(1) Criminal Investigation Division; (2) Combat Intelligence Division
CIDBS	Combined Intelligence Center Integrated Database Server
CIDC	Combined Interview and Debriefing Center
CIE	Communication Intercept and Exploitation
CIEF	Consolidated Imagery Exploitation Facility
CIF	(1) Corps Interrogation Facility; (2) Consolidated Intelligence Facility
CIFAX	Enciphered Facsimile
C4IFTW	C4I For The Warrior
CIG	(1) Computer Image Generation; (2) Combined Intelligence Group
CIGSS	Common Imagery Ground Surface System
CIHS	Classified Information Handling System
CIK	Crypto-Ignition Key
CIIC	Current Intelligence and Indications Center
CIID	Command Intelligence Implementation Document
CILMS	Covert Infrared Lighting and Marking System
CILO	Counterintelligence Liaison Office(r)
CILOP	Conversion in Lieu of Procurement
CIM	Corporate Information Management
CIMAS	CENTCOM Iranian Military Activities Summary
CIMEX	Civil Military Exercise (NATO)

C-IMINT	Counter Imagery Intelligence
CIMOC	Civil Military Operations Center
CIMP	COMSEC Interoperability Master Plan
CIN	Cargo Increment Number
CINC	(1) Commander in Chief; (2) Commander of a Combatant Command
CINCACOM	Commander in Chief, U.S. Atlantic Command
CINCAFLANT	Commander in Chief, United States Air Forces, Atlantic
CINCAL	Commander in Chief, Alaska
CINCARLANT	Commander in Chief, United States Army Forces, Atlantic
CINCCENT	Commander in Chief, Allied Forces Central Europe (NATO)
CINCCFC	Commander in Chief, Combined Forces Command, Korea
CINCEASTLANT	Commander in Chief, Eastern Atlantic (NATO)
CINCENT	Commander in Chief, Allied Forces, Central Europe
CINCEUR	Commander in Chief, U.S. Forces Europe
CINCFOR	Commander in Chief, Forces Command
CINCFORSCOM	Commander in Chief, U.S. Army Forces
CINCHAN	Commander in Chief, Channel (NATO)
CINCIBERLANT	Commander in Chief, Iberian Atlantic Area
CINCLANT	Commander in Chief, Atlantic Command
CINCLANTFLT	Commander in Chief, Atlantic Fleet
CINCLANTFLTDETSO	Commander in Chief, Atlantic Fleet Detachment SOUTHCOM
CINCMAC	Commander in Chief, Military Airlift Command (archaic)
CINCNORAD	Commander in Chief, North American Air Defense Command
CINCNORTH	Commander in Chief, Allied Forces Northern Europe (NATO)
CINCONAD	Commander in Chief, Continental Air Defense Command
CINCPAC	Commander in Chief, Pacific Command
CINCPACAF	Commander in Chief, Pacific Air Force
CINCPACFLT	Commander in Chief, Pacific Fleet
CINCPACREP	Commander in Chief, Pacific Representative
CINCSAC	Commander in Chief, Strategic Air Command
CINCSOC	Commander in Chief, Special Operations Command
CINCSO	Commander in Chief, Southern Command
CINCSOUTH	Commander in Chief, Allied Forces Southern Europe (NATO)
CINCSPACE	Commander in Chief, U.S. Space Command
CINCSPECOMME	Commander in Chief, Specified Command, Middle East
CINCTAC	Commander in Chief, Tactical Air Command
CINCTRANS	Commander in Chief, Unified Transportation Command
CINCTRANSCOM	Commander in Chief, U.S. Transportation Command
CINCUKAIR	Commander in Chief, United Kingdom Air Defense Region (NATO)
CINCUNC	Commander in Chief, United Nations Command
CINCUSACOM	Commander in Chief, U.S. Atlantic Command
CINCUSAFE	Commander in Chief, U.S. Air Forces, Europe
CINCUSAREUR	Commander in Chief, United States Army, Europe

CINCUSARPAC	Commander in Chief, United States Army, Pacific
CINCUSNAVEUR	Commander in Chief, U.S. Naval Forces, Europe
CINCWESTLANT	Commander in Chief, Western Atlantic (NATO)
CINF	Community Imagery Needs Forecast
CINSGCY	Counterinsurgency
CIO	(1) Central Imagery Office; (2) Chief Information Officer
CIOC	(1) Combined Intelligence Operations Center (Korea); (2) Combat Intelligence Operations Center
CIOP	(1) Controlled Intelligence Operational Proposal; (2) CIO Program
CIP	(1) Consolidated Intelligence Program; (2) Country Information Package; (3) Critical Intelligence Parameter; (4) Combined Interoperability Program; (5) Crypto-Ignition Plug; (6) Correlation and Integration Processor
CIPE	(US) CENTCOM Imagery Production Element
CIPEC	Intergovernmental Council of Copper Exporting Countries
CIPHONY	Enciphered Telephone
CIPL	ClNC's Integrated Priority List
CIPMS	Career Intelligence Professional Management System
CIPR	(1) Consolidated Intelligence Production Requirement; (2) Counterintelligence Production Registry
CIPS	Counterintelligence Periodic Summary
C2IPS	C2 Information Processing System
CIR	(1) Central Intelligence Report; (2) Continuing Intelligence Requirement
CIRC	Central Information Reference and Control
CIRCOL	Central Information Reference and Control On-Line System
CIRIS	Consolidated Intelligence Resources Information System
CIRK	Common Interswitch Rekeying Key
CIRL	Current Intelligence Requirements List
CIRT	Computer Security Incident Response Team
CIRVlS	Communications Instructions for Reporting Vital Intelligence Sightings
CIS	(1) Country Intelligence Study; (2) Communications Intercept System; (3) Compensated Imaging System; (4) Canadian Intelligence Service; (5) Chief, Intelligence and Security (Canadian); (6) Combat Instruction Set; (7) Combat Information System; (8) Commonwealth of Independent States; (9) Combat Intelligence System
CISA	C4I Integration Support Activity
CISC	Counterintelligence Support Cell
C3ISC	C3I Systems Committee
CI/SCM	Counterintelligence and Security Countermeasures
CISD	Command Intelligence Strategy Document
CISE	(1) (US) CENTCOM Intelligence Support Element; (2) Corps Intelligence Support Element
CISO	(1) Counterintelligence Support Officer; (2) Counterintelligence Staff Officer
CISPOTREP	CI Spot Report

CISR	Communications Intelligence Security Regulation
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
CIT	Counterintelligence Team
CITA	Combat Intelligence and Targeting on Arrival
CITS	CENTCOM Imagery Transmission System
CIV	Civilian
CIVC	Carrier Intelligence Center
CIVIC	Civilian Vulnerability Indicator Code
CISION	Enciphered Television
CIW	(1) Consolidated Intelligence Watch; (2) CMOC Intelligence Watch
CIWC	CIW Commander
CIWG	Cooperative Interaction Working Group
CIWS	Close-In Weapon System
C&J	Collection and Jamming
CJB	Congressional Justification Book
CJCS	Chairman, Joint Chiefs of Staff
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CJIATF-E	Commander, Joint Interagency Task Force-East
CJIATF-W	Commander, Joint Interagency Task Force-West
CJIT	Combined Joint Interrogation Team
CJTF	Commander, Joint Task Force
CJTF-AK	Commander, Joint Task Force-Alaska
CJTF-FA	Commander, Joint Task Force-Full Accounting
CK	Compartment Key
CKG	Cooperative Key Generation
CL	Light Cruiser
C-LAMP	Community Laser Measurement Program
CLASS	Close Air Support System
Class	Classification/Classified
C&LB	Coasts and Landing Beaches
CLF	Commander, Landing Force
CLMD	COMSEC Local Management Device
CLNC	Clearance
CLO	(1) Counterdrug Liaison Officer; (2) Chief Logistics Officer
CLOCE	Contingency Lines of Communication, Europe
CLS	(1) Contractor Logistics Support; (2) Clandestine Lighting System
CLSC	COMSEC Logistics Support Center
CLSP	Composite Launch Sequence Plan
CL/TECH	Clear Language Technical Report
cm	Centimeter
CM	(1) Memorandum by the Chairman, Joint Chiefs of Staff; (2) Collection Management; (3) Countermeasure(s); (4) Cruise Missile; (5) Collection Manager; (6) Collection Management Division; (7) Countermine; (8) Countermine Activities

CMA	(1) Countermission Analysis; (2) Collection Management Authority; (3) Community Management Account
CMAA	(1) Command Master at Arms; (2) Chief Master at Arms
CMAFB	Cheyenne Mountain Air Force Base
CMAFS	Cheyenne Mountain Air Force Station
CMAH	CINC Mobile Alternate Headquarters
CMAS	Cheyenne Mountain Air Station
C-MASINT	Counter-Measures and Signature Intelligence
CMB	Collection Management Branch
CMC	(1) Cheyenne Mountain Complex; (2) Commandant, U.S Marine Corps; (3) Command Master Chief
C/MC	Command Master Chief
CMCA	Cruise Missile Carrier Aircraft
CMCC	(1) Commander in Chief, Mobile Command Center; (2) Component Mobile Command Center
CMCDS	Community Multilateral Counterterrorism Database System
CMCI	Computed Mission Coverage Index
CMCM	Commandant, U.S. Marine Corp Memorandum
CMCS	(1) COMSEC Material Control System; (2) COMINT Mission Control System
CMD	(1) Collection Management Division; (2) Command
CMDC	Command Cell
CMDR	Commander
CM&D	Collection Management and Dissemination
CME	Communications Monitoring Equipment
CMEA	Council for Mutual Economic Assistance
CMEC	Captured Material Exploitation Center
CMF	Combat Mission Folder
CMFC	Combined Marine Forces Command
CMIC	Combined Military Interrogation Center
CMISE	Corps Military Intelligence Support Element
CML	Chemical
CMO	(1) Collection Management Office; (2) Civil Military Operations; (3) Central MASINT Office
CMOC	(1) Cheyenne Mountain Operations Center; (2) Civil Military Operations Center; (3) Central MASINT Operations Cell
CMOS	Complementary Metal-Oxide Semiconductor
CMOTF	Civil Military Operations Task Force
CMP	(1) Combat Mission Planning; (2) Configuration Management Plan
CMPF	Confidential Military Purpose Funds
CMPS	Compartmented Mode Processing System
CMR	Crisis Management Room
CMRS	Collection Management Requirements System
CMS	(1) Combat Mission Section; (2) Command and Management System; (3) Community Management Staff; (4) Collection Management System; (5) Common Mapping Standard

CMS/RMG	Community Management Staff, Resource Management Group
CMSA	Cruise Missile Support Activity
CMSI	Civilian Multi-Spectral Imagery
CMSS	Collection Management Support System
CMST	(1) Collection Management Support Terminal; (2) Collection Management System Tools
CMT	(1) Crisis Management Team; (2) Critical Mobile Target
CMTC	Combat Maneuver Training Center
CMTC-IS	CMTC-Instrumentation System
CMTS	(1) Critical Mobile Target Server; (2) Compliance Monitoring Tracking System
CMW/CMWS	Compartmented Mode Workstation
CN	Counternarcotics
CNA	(1) Center for Naval Analysis; (2) Coordinates Not Available; (3) Critical Node Analysis
CNAC	(1) Customs National Air Command, Oklahoma City; (2) Customs National Aviation Center
CNAD	Conference on NATO Armament Directors
CNAVSPACECOM	Commander, Navy Space Command
CNC	(1) Counternarcotics Center; (2) Computerized Numerical Control
CNCS	Cryptonet Control Station
CN-CMS	Counternarcotics Command and Management System
CNES	Centre National d'Etudes Spatiales (French National Space Agency)
CNET	(1) Chief of Naval Education and Training; (2) Centre National d'Etudes Des Telecommunications
C3NET	Command, Control, and Communications Networks
CNFJ	Commander, U.S. Naval Forces Japan
CNFK	Commander, U.S. Naval Forces Korea
CNFM	Commander, U.S. Naval Forces Marianas
CNI	(1) Communicating NATO Intentions; (2) Communications, Navigation, or Identification
CNIC	Combined Naval Intelligence Center
CNIN	Composite Network, Front-End Internal Network
CNIPS	Counternarcotics Information Processing System
CNK	Cryptonet Key
CNMI	Commonwealth of the Northern Mariana Islands
CNN	Cable News Network
CNO	Chief of Naval Operations
C/No	Ratio of carrier to noise in a 1Hz bandwidth
CNOC	(1) Counternarcotics Operations Center; (2) Combined Naval Operations Center
CNOM	Chief of Naval Operations Memorandum
CNOR	Command Not Operationally Ready
CNR	(1) Chief of Naval Research; (2) Combat Net Radio
CNRIU	Combat Net Radio Interface Unit
CNS	Commercial Network Survivability

CNSWTG	Commander, Naval Special Warfare Task Group
CNTL	Command Nuclear Target List
CNVFD	Color Night Vision Fusion Device
CNWDI	Critical Nuclear Weapons Design Information
CO	(1) Commanding Officer; (2) Company
CO3	Combined Staff Public and Governmental Affairs Officer
CO6	Combined Staff Judge Advocate
CO7	Combined Staff Command Surgeon
COA	Course of Action
COB	(1) Close of Business; (2) Collated Operating Base; (3) Chief of Base; (4) Command Operating Budget
COBE	Cosmic Background Explorer
COBOL	Common Business Oriented Language
COC	Combat Operations Center
COCOM	(1) Coordinating Committee; (2) Combatant Command
COD	Carrier On-board Delivery
CODIS	Continuity of Defense Intelligence Systems
COE	Common Operating Environment
COEA	Cost and Operational Effectiveness Analysis
COFIR	Compendium of Future Intelligence Requirements
COFs	Central Operating Facilities
CofS	Chief of Staff
COG	(1) Combined Operations Group; (2) Continuity of Government; (3) Center of Gravity
COI	Communities of Interest
COIC	Combat Operations Intelligence Center (USAFE)
COIN	Counterinsurgency
COINS	(1) Consolidated On-Line Intelligence System; (2) Community On-Line Intelligence Network Systems
COINS-II	Community On-Line Intelligence System-II
COIR	Commander's Operational Intelligence Requirements
COIS	Combat Operations Intelligence System
COLISEUM	Community On-Line Intelligence System for End Users and Managers
COLL	Collection
COLLECT	Collection
COLOP	Collection Opportunity (messages)
COLT	Combat Observation and Laser Team
COM	(1) Computer Output to Microform; (2) Chief of Mission (U.S. Embassy); (3) Collection Operations Management; (4) Commander
COMA	Court of Military Appeals
COMACC	Commander, Air Combat Command
COMAAFCE	Commander, Allied Air Forces Central Europe
COMAFFOR	Commander, Air Force Forces
COMAFOSI	Commander, Air Force Office of Special Investigations

COMAFSOC	Commander, U.S. Air Force Special Operations Command
COMAFSPACE	Commander, Air Force Space Command
COMALCOM	Commander, Alaskan Command
COMAMC	Commander, Air Mobility Command
COMARSPACECOM	Commander, Army Space Command
COMASPC	Commander, Air Force Space Command
COMAINT	Command Maintenance
COMAIR-BALTAP	Commander, Allied Air Forces, Baltic Approaches
COMAIRSOUTH	Commander, Allied Air Forces, Southern Europe
COMALCOM	Commander, Alaskan Command
COMALF	Commander of Airlift Forces
COMANR	Commander, Alaskan NORAD Region
COMANTDEF-COM	Commander, Antilles Defense Command
COMARFOR	Commander, Army Forces
COMARSOC	Commander, U.S. Army Special Operations Command
COMARSOF	Commander, U.S. Army Special Operations Forces
COMATF	Commander, Amphibious Task Force
COMBALTAP	Commander, Allied Forces, Baltic Approaches
COMBAT DF	Combat Direction Finding
COMBENE-CHAN	Commander, Benelux Sub-Area Channel
COMBISCLANT	Commander, Bay of Biscay Submarine Area
COMCANLANT	Commander, Canadian Atlantic Submarine Area
COMCARGRU	Commander Carrier Group
COMCENTAG	Commander, Central Army Group, Central Europe
COMCENTLANT	Commander, Central Submarine Area
COMCM	Communication Countermeasures & Deception
COMCO	Canadian SSO
COMCRUDESGRU	Commander Cruiser Destroyer Group
COMDT COGARD	Commandant, U.S. Coast Guard
COMECON	Council for Mutual Economic Assistance
COMEDCENT	Commander, Central Mediterranean Area
COMEDEAST	Commander, Eastern Mediterranean Area
COMEDNOREAST	Commander, Northeast Mediterranean Area
COMEDOC	Commander, Western Mediterranean Area
COMEDS	CONUS Meteorological Data System
COMEDSOUEAST	Commander, Southeast Mediterranean Area
COMEX	(1) Committee on Exchanges; (2) Communications Exercise
COMFAIRKEF	Commander, Fleet Air Keflavik
COMFIVEATAF	Commander, Fifth Allied Tactical Air Force, Southern Europe
COMFLDCOMDASA	Commander, Field Command, Defense Atomic Support Agency
COMFOURATAF	Commander, Fourth Allied Tactical Air Force Central Europe
COMGIB	Naval Commander, Gibraltar
COMGIBMED	Commander, Gibraltar Mediterranean Command
COMGTMODEFCOM	Commander, Guantanamo Defense Command
COMICEDEFOR	Commander, Iceland Defense Force

COMIDEASTFOR	Commander, Middle East Force (USN)
COMINEWARCOM	Commander, Mine Warfare Command
COMINT	Communications Intelligence
COMINTADTSK	COMINT Advisory Tasking Message
COMIREX	Committee on Imagery Requirements and Exploitation
COMIS	Collection Management Information System
COMJAM	Communications Jamming
COMJSOC	Commander, Joint Special Operations Command
COMJSOTF	Commander, Joint Special Operations Task Force
COMJTF	Commander, Joint Task Force
COMJUWATF	Commander, Joint Unconventional Warfare Task Force
COML	Commercial
COMLANDFOR	Commander, Land Forces
COMLANDJUT	Commander, Allied Land Forces, Schleswig-Holstein & Jutland
COMLANDNORWAY	Commander, Allied Land Forces, Norway
COMLANDSOUTH	Commander, Allied Land Forces, Southern Europe
COMLANDZEALAND	Commander, Allied Land Forces, New Zealand
COMLANTAREA	Commander, Coast Guard Atlantic Area
COMLOGNET	Combat Logistics Network
COMM	(1) Communication; (2) Commercial
COMM(S)	Communication(s)
COMMAIRCHAN	Commander, Allied Maritime Air Force, Channel
COMMAIRNORLANT	Maritime Air Commander, Northern Submarine Area
COMMARBASPAC	Commander, Marine Corps Base, Pacific
COMMARDEZSECAK	Commander, U.S. Maritime Defense Zone Sector, Alaska
COMMARFOR	Commander, Marine Forces
COMMARFORJAPAN	Commander, Marine Forces, Japan
COMMARFORK	Commander, Marine Forces, Korea
COMMARFORPAC	Commander Marine Corps Forces, Pacific
COMMARFORSOUTH	Commander, Marine Corps Forces, South
COMMCEN	Communications Center
COMMDET	Communications Detachment
COMMO	Communications
COMMS CTR	Communications Center
COMMZ	Communications Zone
COMNAVAIR	Commander, Naval Air Forces
COMNAVAIRLANT	Commander, Naval Air Forces, Atlantic
COMNAVAIRPAC	Commander, Naval Air Forces, Pacific
COMNAVBALTAP	Commander, Allied Naval Forces, Baltic Approaches
COMNAVFOR	Commander, Naval Forces
COMNAVFORK	Commander, Naval Forces, Korea
COMNAVINTCOM	Commander, Naval Intelligence Command
COMNAVLOG	Commander, Naval Logistics
COMNAVMARIANAS	Commander, Naval Forces, Marianas
COMNAVNON	Commander, Allied Naval Forces, North Norway

COMNAVSCAP	Commander, Allied Naval Forces, Scandinavian Approaches
COMNAVSEASYSCOM	Commander, Naval Sea Systems Command
COMNAVSECGRU	Commander, Naval Security Group
COMNAVSOF	Commander, Naval Special Operations Forces
COMNAVSPACECOM	Commander, Naval Space Command
COMNAVSPECWARCOM	Commander, Naval Special Warfare Command
COMNAVSURF	Commander, Naval Surface Forces
COMNAVSURFLANT	Commander, Naval Surface Force, U.S. Atlantic Fleet
COMNAVSURFPAC	Commander, Naval Surface Force, Pacific
COMNORECHAN	Commander, Northern Submarine Area, Channel
COMNORLANT	Commander, Northern Submarine Area
COMNORTHAG	Commander, Northern Army Group, Central Europe
COMNSWU	Commander, Naval Special Warfare Unit
COMOCEANLANT	Commander, Ocean Atlantic
COMOCEANSYSLANT	Commander, Oceanographic Systems Atlantic
COMOCEANSYSPAC	Commander, Oceanographic Systems Pacific Company
COMOPS	Communications Operations Summary
COMP	Compatible
COMPACAF	Commander, Pacific Air Forces
COMPASS	Computerized Movement Planning and Status System
COMPATWINGSLANT	Commander, Patrol Wings Atlantic
COMPHIBGRU	Commander, Amphibious Group
COMPLYMCHAN	Commander, Plymouth Submarine Area, Channel
COMPUINT	Computer Intelligence
COMPUSEC	Computer Security
COMPW	Composite Wing
COMPWING	Composite Wing
COMS	Collection Operations Management System (HUMINT)
COMSAT	Communications Satellite
COMSC	Commander, Military Sealift Command
COMSEC	Communications Security
COMSECONDFLT	Commander, U.S. Second Fleet
COMSEVENTHFLT	Commander, U.S. Seventh Fleet
COMSIXATAF	Commander, Sixth Allied Tactical Air Force, Southeastern Europe
COMSIXTHFLT	Commander, U.S. Sixth Fleet
COMSOC	Commander, Special Operations Command
COMSOC-K	Commander, Special Operations Command, Korea
COMSOCEUR	Commander, Special Operations Command, Europe
COMSOCLANT	Commander, Special Operations Command, Atlantic
COMSOCPAC	Commander, Special Operations Command, Pacific
COMSOCSOUTH	Commander, Special Operations Command, Southern Command
COMSOTFE	Commander, Support Operations Task Force, Europe
COMSPOT	Communications Spot Report
COMSTAT	Communication Status Report

COMSTRATCOMWING ONE	Commander, Strategic Communications Wing One
COMSTRICKFLANT	Commander, Striking Fleet Atlantic (Afloat)
COMSTRIKFLTLANT	Commander, Striking Fleet, Atlantic
COMSTRIKFORSOUTH	Commander, Striking Force, South
COMSTS	Commander, Military Sea Transportation Service
COMSUBACLANT	Commander, Submarine Forces, Allied Command, Atlantic
COMSUBEASTLANT	Commander, Submarine Force, Eastern Atlantic
COMSUBGRU	Commander, Submarine Group
COMSUBGRU 8/CTF MED	Commander Submarine Group (Mediterranean)/Commander Task Force Mediterranean
COMSUBLANT	Commander, Submarine Force, U.S. Atlantic Fleet
COMSUBMED	Commander, Submarines, Mediterranean
COMSUBPAC	Commander, Submarine Forces, Pacific
COMSUBWESTLANT	Commander, Submarine Force, Western Atlantic Area
COMSUPNAVFOR	Commander, Supporting Naval Forces
COMTAFNORNOR	Commander, Allied Tactical Air Force, North Norway
COMTAFSONOR	Commander, Allied Tactical Air Force, South Norway
COMTASKFORNON	Commander, Allied Task Force, North Norway
COMTECHREP	Complementary Technical Report
COMTHIRDFLT	Commander, Third Fleet
COMTRAPAC	Commander, Training Command, Pacific
COMTWOATAF	Commander, Second Allied Tactical Air Force, Central Europe
COMUKADR	Commander, UK NATO Air Defense Region
COMUSAFAK	Commander, U.S. Air Forces, Alaska
COMUSAFFOR	Commander, United States Air Force Forces
COMUSAFJ	Commander, U.S. Air Forces, Japan
COMUSAFK	Commander, U.S. Air Forces, Korea
COMUSAFTF	Commander, United States Air Force Task Force
COMUSARAK	Commander, U.S. Army Forces, Alaska
COMUSARCENT	Commander, U.S. Army Forces Central Command
COMUSARFOR	Commander, United States Army Forces
COMUSARSO	Commander, United States Army Forces Southern Command
COMUSARSPACE	Commander, U.S. Army Space Command
COMUSARTF	Commander, United States Army Task Force
COMUSASOC	Commander, U.S. Army Special Operations Command
COMUSFOR KOREA	Commander, U.S. Forces Korea
COMUSFK	Commander, U.S. Forces, Korea
COMUSFORAZ	Commander, U.S. Forces, Azores
COMUSFORCARIB	Commander, U.S. Forces, Caribbean
COMUSFORCNTY	Commander US Forces Country
COMUSJ	Commander, U.S. Forces, Japan
COMUSJAPAN	Commander, U.S. Forces, Japan (also COMUSJ)
COMUSJTF	Commander, United States Joint Task Force
COMUSJUWTF	Commander, United States Joint Unconventional WarfareTask Force

COMUSKOREA	Commander, U.S. Forces, Korea (also COMUSK)
COMUSLANDFOR	Commander, United States Land Forces
COMUSMACTHAI	Commander, United States Military Assistance Command, Thailand
COMUSMARCENT	Commander, U.S. Marine Forces Central Command
COMUSMARDEZLANT	Commander, U.S. Maritime Defense Zone, Atlantic
COMUSMARDEZPAC	Commander, U.S. Maritime Defense Zone, Pacific
COMUSMARFOR	Commander, United States Marine Forces
COMUSMARTF	Commander, United States Marine Task Force
COMUSMILGP	Commander, United States Military Group
COMUSNAVAK	Commander, U.S. Naval Forces, Alaska
COMUSNAVCENT	Commander, U.S. Naval Forces, Central Command
COMUSNAVEUR	Commander, U.S. Naval Forces, Europe
COMUSNAVFOR	Commander, United States Naval Forces
COMUSNAVPHIL	Commander, U.S. Naval Forces, Philippines
COMUSNAVSO	Commander, U.S. Naval Forces South
COMUSNAVTF	Commander, United States Naval Task Force
COMZEALAND	Commander, Allied Land Forces, New Zealand
CON	Control(led)
CONAD	Continental Air Defense Command
CONDECA	Central America Defense Council
CONF	Confidential
CONFIG	Configuration
CONG	Congress
CONGEN	Consul General
CONGINT	Congressional Interest
ConNMJIC	Contingency NMJIC
CONOBJTR	Conscientious Objector
CONOP(S)	Concept of Operation(s)
CONOPS	(1) United States Army Intelligence Command Continental (United States) Operations; (2) Concept of Operations
CONPG	Chairman, Operational Nuclear Planning Group
CONPLAN	(1) Concept Plan; (2) Contingency Plan
CONR	CONUS NORAD Region
CONTEXT	Conferencing and Text Manipulation System
CONTRA-	Against, Opposite (Prefix)
CONUS	Continental United States
CONUSA	Continental United States Army
CONVL	Conventional
COOP	Continuity of Operations Plan
COORD	Coordination
COP	(1) Command Observation Post; (2) Crashout Package
COPG	Chairman, Operational Planners Group
COPRA	Comparative Postwar Recovery Analysis
COPRL	Command Operations Priority Requirements List

COPSTRAT	Continuity of Operations Plan (USSTRATCOM)
COR	(1) Command Operationally Ready; (2) Central Office of Record; (3) Contracting Officer's Representative
CORCEN	Correlation Center
CORE	Contingency Response (Program)
CORL	(1) Collection Opportunity Requirements List; (2) Chief of Receive Location
CORM	Commission on Roles and Missions
CORPS SAM	Corps Surface-to-Air Missile
CORTRAIN	Corps/Division Training Coordination Program
COS	(1) Combat Operations Staff; (2) Chief of Station; (3) Chief of Staff; (4) Communications Segment
cos	Cosine
COSAL	Consolidated Ship/Squadron Allowance
COSCOM	Corps Support Command
COSIN	Control Staff Instructions
COSA	Commander, Oceanographic Systems, Atlantic
COSP	Commander, Oceanographic Systems, Pacific
COSPO	Community Open Source Program Office Cotangent
COTP	Captain of the Port
COTR	Contracting Officer's Technical Representative
COTS	(1) Commercial Off-the-Shelf; (2) Container Offloading Transfer System
COUNTERMASINT	Counter Measurements and Signature Intelligence
COVCOM	Covert Communications
CoVRT	Commanders (and Staff) Visualization Research Tool
CP	(1) Contingency Planning; (2) Command Post; (3) Character Position; (4) Communications Processor; (5) Central Processor; (6) Career Program; (7) Counterproliferation
C&P	Characteristics and Performance
C-P	Counterproliferation
CPA	(1) Chairman's Program Assessment; (2) Collection Planning Aid; (3) CJCS Preparedness Assessment
CPAT	Collection Planning and Targeting
CPB	Charged Particle Beam
CPBS	(1) Capabilities Programming and Budgeting System; (2) Consolidated Program and Budgeting System
CPC	(1) Coastal Patrol Boat; (2) Collection and Processing Center; (3) Central Processing Center
CPE	(1) Circular Probable Error; (2) Central Production Element
CPFL	Contingency Planning Facilities List
CPI	Communications Processor and Interface
CPIA	Chemical Propulsion Information Agency
CPIC	Coastal Patrol and Interdiction Craft
CPM	Cycles Per Minute
CPMIEC	China Precision Machinery Import Export Corporation
CPNET	Custom Product Network

CPO	(1) Command Project Officer; (2) Chief Petty Officer
CPP	Communist Party of the Philippines
CPR	(1) Cardio-Pulmonary Resuscitation; (2) Chairman's Program Recommendations
CPS	(1) Collection Problem Set; (2) Correlation Processing Subsystem; (3) Characters Per Second; (4) COMSEC Parent Switch; (5) Craft Positioning System
CPSB	Career Program Selection Board
CPSS	Computer Systems Squadron
CPSU	Communist Party of the Soviet Union
CPT	Command Post Terminal
CPU	(1) Central Processing Unit; (2) Communications Processing Unit; (3) Computer Processing Unit
CPX	Command Post Exercise
CP OSCAR	Command Post Operations Support Center and Rear
CP TANGO	Command Post Tactical Air, Naval, Ground Operations
CQB	Close Quarter Battle
C-QUIP	Combined Quarterly Intelligence Production Listing
CR	(1) Crisis Relocation; (2) Combat Radius; (3) Collection Request; (4) Close Range; (5) Collections Requirement
CRAF	Civil Reserve Air Fleet
CRB	Contingency Reference Book
CRBIF	Crisis Basis Imagery File
CRC	(1) Command and Reporting Center; (2) Control and Reporting Center; (3) CONUS Replacement Center
CRDC	United States Army Chemical Research & Development Center
CRDL	Collateral Recurring Document Listing
CRE	(1) Combat Readiness Evaluation; (2) Control and Reporting Element
CREST	Covert Reconnaissance/Strike
CRF	(1) Crisis Response Force; (2) Cable Reports File
CRIMP	Crisis Management Plan
CRIS	Command Resources Information System
CRISCON	Crisis Condition (I&W System)
C-RISTA	Counter-Reconnaissance, Intelligence, Surveillance, and Target Acquisition
CRITIC	(1) Critical Intelligence; (2) Critical Intelligence Message; (3) Critical Intelligence Communication
CRITICOM	Critical Intelligence Communications Network
CRJOIC	Central Region Joint Operational Intelligence Center
CRL	Certificate Revocation List
CRM	Collection Requirements Management
CRMA	Collection Requirements Management Architecture/Application
CRMO	Collection Requirements Management Office(r)
CRMP	Collection Requirements Management Program or Plan
CRMS	Collection Requirements Management System
CRN	Combat Radio Net

CROF	Crete Remote Operating Facility
CROM	Continuous Read-Only Memory
CRP	(1) Control and Reporting Post; (2) COMSEC Resources Program
CRRC	Combat Rubber Raiding Craft
CRRES	Combined Release and Radiation Effects Satellite
CRRS	Customer Requirements Registration System
CRS	(1) COMIREX Requirements Structure; (2) Combined Recording Site; (3) Comprehensive Retrieval Subsystem; (4) Catholic Relief Service; (5) Congressional Research Service; (6) Community Relations Service
CRT	(1) Cathode Ray Tube (Terminal); (2) Combat Readiness Training; (3) Crisis Response Team
CRTA	Chief of Rocket Troops and Artillery
CRUDESGRU	Cruiser-Destroyer Group
CRWG	Current Requirements Working Group
CRYPTO	(1) Cryptography/Cryptographic; (2) Cryptologic
CS	(1) Combat Support; (2) Communications Subsystem; (3) Constant Source; (4) Chief of Staff; (5) Central Servers; (6) Coalition Support
CS1	Critical-Sensitive Level 1
CSA	(1) Chief of Staff, U.S. Army; (2) Central Supplies Agency of NATO; (3) Corps Support Activity; (4) Combat Support Agency(ies)
CSABE	Central and South African Basic Encyclopedia
CSAF	Chief of Staff, U.S. Air Force
CSAFM	Chief of Staff, Air Force Memorandum
CSAM	Chief of Staff, Army Memorandum
CSAR	Combat Search and Rescue
CSAW	Cryptologic Support to Amphibious Warfare
CSB	(1) Close Silo Basing; (2) Collection Support Brief (HUMINT); (3) Current Situation Branch
CSBR	Commander, Special Boat Squadron
CSC	(1) Community Support Center; (2) Customer Support Center; (3) Combat Support Cell
CSCE	Conference on Security and Cooperation in Europe
CSCG	Communications Security Control Group
CSCI	(1) Commercial Satellite Communications Initiative; (2) Computer Software Configuration Interface
CSCR	Computer System Change Request
CSDS	Command Spatial Display System
CSCT	Combat Support Coordination Team
CSE	(1) Cryptologic Support Element(s); (2) Command Support Element; (3) Client Server Environment; (4) Canadian SIGINT Establishment; (5) Communi-cations Security Element
CSE-SS	Client Server Environment-System Services
CSEL	Combat Survivor-Evader Locator
CSENCNET	Satellite Education Network
CSF	Command Support Functions

CSFOCI	Force Protection Operations
CSG	(1) Cryptologic Support Group; (2) Chairman's Staff Group; (3) Combat Support Group; (4) Corps Support Group
CSG-SOCOM	Cryptologic Support Group/USSOCOM
CSGN	Nuclear Strike Cruiser
CSI	Commercial Satellite Interconnectivity
C-SIGINT	Counter Signals Intelligence
CSIS	Canadian Security and Investigative Service
CSMA/CD	Carrier Sense Multiple Access with Collision Detection
CSMO	Cryptologic Support to Military Operations
C3SMP	Command, Control, Communications System Master Plan
CSMR	Coarse Spatial Resolution, Multispectral
CSOC	Consolidated Space Operations Center
CSP	(1) Communications Support Processor; (2) Crisis Staffing Procedures; (3) Contingency Support Package
CSP/HOL	Communications Support Processor/High Order Language
CSPAR	(1) Central Strategic Processing, Analysis, and Reporting; (2) CINC's Preparedness Assessment Report
CSPO	Consolidated SAFE Project Office
CSR	(1) Current Situation Room; (2) Coastal Surveillance Radar; (3) Controlled Supply Rate; (4) Collection Support Requirement; (5) Combat Search & Rescue
CSRD	Communication-Computer Systems Requirement Document
CSRS	Civil Service Retirement System
CSS	(1) Communications Security System; (2) Communications Support System; (3) Central Security Service; (4) Combat Service Support; (5) Collateral Support System; (6) Contingency Support Study; (7) Communications System Segment; (8) Common Sensor System; (9) COMSEC Subordinate Switch; (10) Combat Surveillance Service; (11) Continuous Signature Service; (12) Coded Switch System; (13) Command Specific Server
CSSA	Cryptologic Shore Support Activity
CSSCS	(1) Combat Service Support Control System; (2) Combat Service Support Computer System
CSSD	Combat Service Support Detachment
CSSE	Combat Service Support Element
CSSO	Contractor Special Security Officer
CSSP	Combined Services Support Program
CSSOC	Combat Service Support Operations Center
CSSR	CSS Replacement
CSST	Combat Service Support Team
CST	(1) Central Standard Time; (2) Coastal Survey Team; (3) Coalition Support Team
CSTC	Consolidated Space Test Center
CSTIP	Combined Strategic Intelligence Training Program
CSTOL	Cargo Short Take-Off & Landing
CSTVRP	Computer Security Technical Vulnerability Reporting Program
CT	(1) Training Cruiser; (2) Counterterrorism; (3) Combating Terrorism; (4) Cryptologic Technician

CTA	(1) Central Technical Authority; (2) Common Table of Allowances
CTAI	Continuous-Tone Aerial Imagery
CTAK	Cypher-Text Auto-Key
CTAPS	Contingency Theater Automated Planning System
CTB	Comprehensive Test Ban
CTBT	Comprehensive Test Ban Treaty
CTC	(1) Combat Targeting Center; (2) Counterterrorism Center; (3) Combat Training Center
CTD	(1) Collective Training Directorate; (2) Charge Transfer Device
CTDR	Commercial Training Device Requirements
CT&E	Certification Test and Evaluation
CTE	Coefficient of Thermal Expansion
CTEA	Cost and Training Effectiveness Analysis
CTF/JTF	(1) Crisis Task Force; (2) Commander Task Force; (3) Central Training Flight; (4) Combined Task Force; (5) Joint Task Force; (6) Consolidated Training Facility
CTF-B	Combined Task Force-Bomber
CTF-BM	Combined Task Force-Battle Management
CTF-C2	Combined Task Force Director of Intelligence
CTF PC II	CTF Provide Comfort II
CTG	Commander, Task Group
CTH	Aviation Training Cruiser
CTIA	Counter Technical Intelligence Activities
CTIS	Commander's Tactical Information System
CTL	Critical Task List
CTLZ	Control Zone
CTOC	Corps Tactical Operations Center
CTOCSE	CTOC Support Element
CTOL	Conventional Take-Off and Landing
CTP	Consolidated Telecommunications Program
CTR	Center
CTRL	Control
CTS	(1) Course Training Standards; (2) Communications Technology Satellite
CTSCR	Critical Time-Sensitive Collection Requirement
CTT	(1) Commanders' Tactical Terminal; (2) Common Task Test; (3) Combat Control Team
CTTA	Certified TEMPEST Technical Authority
CTT-H	Commanders' Tactical Terminal-Hybrid
CTTP	(1) USCENTCOM Tactics, Techniques, and Procedures Manual; (2) Component Tactics, Techniques, and Procedures Manual
CTU	Commander Task Unit
CU	Channel Unit
CUBB	Collateral Users Bulletin Board
CUBIC	Common User Baseline for the Intelligence Community
CUCV	Commercial Utility Cargo Vehicle

CUDIXS	Common-User Digital Information Exchange System
CUL	Combined User Language
CURR	Current
CUSRPG	Canadian-U.S. Regional Planning Group (NATO)
CUWTF	Combined Unconventional Warfare Task Force
CV	(1) Multipurpose Aircraft Carrier; (2) Carrier Vehicle; (3) Aircraft Carrier
CUP	COMSEC Utility Program
CVA	Clandestine Vulnerability Analysis
CVAN	CINCPAC Voice Alert Network
CVBF	Carrier Battle Force
CVBG	Carrier Battle Group
CVG	Guided-Missile Aircraft Carrier
CVGN	Nuclear-Powered Guided-Missile Aircraft Carrier
CVH	V/STOL Aircraft Carrier
CVHG	Guided-Missile V/STOL Aircraft Carrier
CVHGN	Nuclear-Powered Guided-Missile V/STOL Aircraft Carrier
CVHN	Nuclear-Powered V/STOL Aircraft Carrier
CVIC	Carrier-Based Intelligence Center
CVL	Light Aircraft Carrier
CVLGN	Nuclear-Powered Guided-Missile Light Aircraft Carrier
CVLN	Nuclear-Powered Light Aircraft Carrier
CVN	Nuclear Powered Aircraft Carrier
CVRT	Combat Vehicle (Reconnaissance, Tracked)
CVS	(1) Antisubmarine Aircraft Carrier; (2) Commercial Vendor Services
CVSD	Continuously Variable-Slope Delta Modulation
CVT	Training Aircraft Carrier
CVTS	Compressed Video Transmission Service
CVW	Carrier Air Wing
CW	(1) Chemical Warfare; (2) Carrier Wave; (3) Continuous Wave; (4) CONSTANT WATCH; (5) Composite Wing; (6) Commonwealth
C/W	Crisis/Wartime
CWC	(1) Composite Warfare Commander; (2) Conventional Weapons Guide
CWG	Coordinates Working Group
CWI	Conventional Weapons Index
CWIS	Crisis Window Information System
CWO	(1) Communications Watch Office; (2) Chief Warrant Officer
CWS	(1) Compartmented Work Station; (2) Collateral Workstation (ASAS)
CWT	Chemical Weapons Treaty
C2X	CCTF C2 OBI/CI Support Element
CY	Calendar Year
CYCLOPS	Fleet Support Message
CZ	(1) Combat Zone; (2) Convergent Zone

D

5D	Demand-Driven Direct Digital Dissemination
D	(1) Deciduous; (2) Density
D2	Data Distribution
DA	(1) Department of the Army; (2) Long-Range Aviation (USSR); (3) Double Agent; (4) Direct Action
D/A	Digital/Analog
DAA	Designated Approval Authority
DAB	Defense Acquisition Board
DABM	Defense Against Ballistic Missiles (Now SDI)
DABS	Dynamic Air Blast Simulator
DAC	(1) Development Assistance Committee of OECD; (2) Department of Army Civilian; (3) Discretionary Access Control
DACCO	Department of the Army Central Control Office
DACCS	Digital Access Cross-Connect System/Switch
DACOM	Data Communications
DACOS	Deputy Assistant Chief of Station
DACOS/I	Deputy Assistant Chief of Staff-Intelligence
DACT	Dissimilar Air Combat Tactics
DACU	(1) Device Access Control Unit; (2) Device Attachment Control Unit
DAD	Dual Air Density
DAES	Defense Acquisition Executive Summary
DAF	Department of the Air Force
DAG	(1) Defense Special Security Communications Systems Address Group; (2) Divisional Artillery Group (FSU)
DAIRSDIA	Advanced Imagery Reproduction System
DAISY	Daily Summary
DAJDIA	Office Symbol for JMITC
DALASP	Defense Advanced Language and Area Studies Program
DALATS	Data Logging and Transmission System
DAMA	Demand Assigned Multiple Access
DAMI	Department of the Army Military Intelligence
DAMPL	Department of the Army Master Priority List
DAO	Defense Attache Office
DAP	Designated Acquisition Program
DAPA	Drug and Alcohol Program Advisor
DAR	Designated Area for Recovery
DARC	District Area Command
DARO	Defense Airborne Reconnaissance Office
DARP	Defense Airborne Reconnaissance Program
DARPA	Defense Advanced Research Projects Agency
DARS	(1) Daily Aerial Reconnaissance and Surveillance; (2) Daily Apportionment and Reconnaissance Scheduling; (3) Daily Aerial Reconnaissance Syndicate

DARSC	Defense Airborne Reconnaissance Steering Committee
DARSP	Defense Academic Research Support Program
DART	(1) Developmental Air Reports Tracker; (2) Deployable Automated Remote Terminal
DARTS	Digital Antijam Radio Teletype System
DAS	(1) Defense Attache System; (2) Data Acquisition Segment
DASC	Direct Air Support Center
DASD	(1) Deputy Assistant Secretary of Defense; (2) Direct Access Storage Device
DASD(I&S)	Deputy ASD (Intelligence and Security)
DASH	Deployable Automated Support Host
DASPA	Defense Attache System Property Accounting
DASR	Defense Analysis Special Report
DASVA	Defense Attache System Vehicle Accounting
DAT	Direct Action Team
DATAINT	Data Intelligence
DATEXT	Data Extract
DATPS	Diver Active Thermal Protection System
DATS	Data Automated Tower Simulation
DATT	Defense Attache
DAWN	Defense Attache Worldwide Network
DAWS	Defense Automated Warning System
DAYLT	Daylight
dB	Decibel
DB	Data Base
DBA	Data Base Administrator
DBAS	Data Base Applications System
DBBL	Dismounted Battlespace Battle Lab
DBC	Data Base Correlation
DBCTRL	Data Base Control
DBD	Data Burst Device
dBi	Decibel (referenced to isotropic radiator)
DBIDI	Data Base of Imagery-Derived Information
DBK	Dominant Battlefield Knowledge
dB/K	Decibels per Degrees Kelvin
dBm	Decibels (referred to 1 milliwatt)
DBMAINT	Data Base Administrator
DBMS	Data Base Management System
DBQ	Data Base Query
DBS	(1) Data Broadcast System (also known as SCAMPI); (2) Direct Broadcast Service
dBSM	Decibels Per Square Meter
dBw	Decibels Referenced to One Watt of Power
DC	(1) District Commissioner; (2) Damage Control; (3) Defense Council; (4) Direct Current

DCA	(1) Defense Communications Agency; (2) Defense Cooperation Agreement; (3) Defensive Counter Air
DCAEUR	Defense Communications Agency Europe
DCAOC	DCA Operations Control Center
DCAPSS	Dual Criteria Aimpoint Selection System
DCAS	(1) Deployable Consolidated Applications Server; (2) Deployable Communications Applications Shelter
DCCC	Defense Collection Coordination Center
DCE	(1) Defensive Counter Espionage; (2) Data Communications Equipment
D-Cell	Deployment Cell
DCF	DOCS Certification Facility
DCG	Deputy Commanding General
DCGS	Distributed Common Ground System
DCI	Director of Central Intelligence
DCIA	Director, Central Intelligence Agency
DCIB	Defense Counterintelligence Board
DCID	Director of Central Intelligence Directive
DCII	Defense Central Index of Investigations
DCI&S	Director of Counterintelligence and Security
DCIIS	Defense CI Integrated Information System
DCINC	Deputy Commander in Chief
DCIP	Defense Counterdrug Intelligence Program
DCL	Direct Communications Link
DCM	Deputy Chief of Mission
DCMM	Database Creation and Management Module
DCMS	Database Creation and Management Segment
DCN	Defense Communications Network
DCO	(1) Defense Communications Office; (2) Deputy Commander for Operations (USAFE); (3) Dial Central Office; (4) Deputy Commanding Officer
DCOS	Deputy Chief of Staff
DCOSIPR	Deputy Chief of Staff, Intelligence Plans and Requirements
DCP	(1) Disaster Control Plan; (2) Decision Coordinating Paper; (3) Defense Cryptologic Program
DCR	Data Change Request
DCRSI	Digital Cassette Recording System (Improved)
DCS	(1) Defense Communications System; (2) Deputy Chief of Staff; (3) Defense Courier Service
DCS/I	Deputy Chief of Staff Intelligence
DCS/IN	Deputy Chief of Staff for Intelligence
DCSCA	Defense Communications System Central Area
DCSEC	Deputy Chief of Staff, Security
DCSI	Deputy Chief of Staff, Intelligence
DCSIM	Deputy Chief of Staff, Information Management
DCSI/DCSINT	Deputy Chief of Staff Intelligence (USAREUR)
DCSINT	Deputy Chief of Staff for Intelligence (U.S. Army)

DCSLOG	Deputy Chief of Staff for Logistics
DCSO	Deputy Commander for Space Operations
DCSOPS	Deputy Chief of Staff for Operations & Plans
DCSP	Design Controlled Spare Part(s)
DCSPER	Deputy Chief of Staff for Personnel
DCS/SSI	Deputy Chief of Staff for Safety, Security, and Intelligence
DCSTOP	Damage Criteria Study Target Data Base
DCTN	Defense Commercial Telecommunications/Teleconferencing Network
DD	(1) Destroyer; (2) Deputy Director; (3) Department of Defense; (4) Differential Doppler
D&D	Denial and Deception
DDAC	Foreign Denial and Deception Analysis Committee
D/DARO	Director, DARO
D-Day	Day in which a particular operation begins
DDC	(1) Defense Documentation Center; (2) Data Distribution Center
DDCI	Deputy Director of Central Intelligence
DDCMP	Digital Data Communications Message Protocol
DDDDD	Demand-Driven Direct Digital Dissemination System
DDG	Guided Missile Destroyer
DDGN	Nuclear-Powered Guided-Missile Destroyer
DDH	Aviation Destroyer (ASW)
DDHG	Guided-Missile Aviation Destroyer
DDHGN	Nuclear-Powered Guided-Missile Aviation Destroyer
DDHN	Nuclear-Powered Aviation Destroyer
DDI	Deputy Director of Intelligence
DDL	Direct Data Link
DDN	(1) Defense Data Network; (2) Defense Dissemination Network
DDO	(1) Deputy Director of Operations; (2) Deputy Duty Officer
DDP	Defense Dissemination Program
DDPO	Defense Dissemination Program Office
DDR&E	Director, Defense Research and Engineering
DDRS	Defense Data Repository System
DDS	(1) Defense Dissemination System; (2) Dry Deck Shelter; (3) Dual Driver Service (courier)
DDS/RL	Defense Dissemination System/Receive Location
DDSP	Defense Development Sharing Project
DDSS	Document Dissemination and Storage Segment
DDT	(1) Training Destroyer; (2) Distributed Decision-Aid Terminal
DDU	Distant Device Unit
DE	(1) Damage Expectancy; (2) Directed Energy; (3) Directorate for Estimates (DIA)
DE-U	Dissemination Element-Upgrade
DE/EW	Directed Energy/Electronic Warfare
DEA	Drug Enforcement Administration
DEACON	Defense Estimates Analytical Computer On-Line Network

DEB	(1) Digital European Backbone; (2) Defense Estimative Brief; (3) Debris (Orbital)
DEC	Digital Equipment Corporation
DEC (VAX)	Digital Equipment Corporation (Virtual Address Extension)
DECCO	Defense Commercial Contracting Office (now DITCO)
DECM	(1) Defense Electronic Countermeasures; (2) Deceptive Electronic Countermeasures
DECON	Decontaminate(ion)
DEDAC	Deception and Denial Analysis Committee
DEDDF	Digital Elevation Data Dubbing Facility
DEF	Defense
DEFCON	(1) Defense Condition; (2) Defense Readiness Condition
DEFCOS	Defense Courier System
DEFPLAN	Defense Plan
DEFSMAC	Defense Special Missile and Astronautics Center
Deg	Degree
DEGRAD	Degradation
DELORME	a Digital Mapping Computer Program
DEMEX	Demonstration Exercise
DEMOD	Demodulator
DEMONS	Demonstration System
DEMPC	Data Exploitation, Mission Planning, Communications/Center
DENAS	Daily European Naval Activity Summary
DEP	(1) Deflection Error Probable; (2) Defense Estimate for Production; (3) Deployed
DEPCOMNAVCENT	Deputy COMNAVCENT
DEPCOMUSNAVCENT	Deputy Commander, U.S. Naval Forces Central Command
DEPREP	Deployment Report
DEPSECDEF	Deputy Secretary of Defense
DEPT	Department
DES	(1) Digital Exploitation System; (2) Data Encryption Standard
DESA	Defense Evaluation Support Activity
DESC	Defense Electronics Supply Center
DESIGN	Designator (U.S. Navy)
DESIST	Decision Support and Information System for Terrorism
DESS	Defense Exploitation Support System
DESRON	Destroyer Squadron
DET/Det	Detachment
DEW	(1) Distant Early Warning; (2) Directed Energy Weapon
DEWLINE	Distant Early Warning Line
DF	(1) Direction Finding; (2) Disposition Form; (3) Deuterium Floride
DFAD	Digitized Feature Analysis Data
DFDS	Data Facility Dataset Services
DFED	Digitized Features Data
DFH	Deployed Forward Headquarters

DFLP	(1) Defense Foreign Language Program; (2) Democratic Front for the Liberation of Palestine
DFM	Deterrent Force Modules
DFOV	Dual Field of View
DFRIF	Defense Freight Railway Interchange Fleet
DFS	Direction Finding Subsystem
DFT	(1) Deployed for Training Team; (2) Deployment for Training
DG	Defense Guidance
DGCL	Ground Mobile Forces Control Link
DGCS	Downsized Ground Control Station
DGCT	Downsized Ground Control Terminal
DGIAP	Defense General Intelligence Applications Program
DGIF	Deployable Ground Intercept Facility
DGIS	Director General Intelligence and Security
DGITS	Digital Graphics Information Tailoring System
DGS	Deployable Ground Station
DGU	Downgrade to Unclassified
DGZ	(1) Desired Ground Zero; (2) Designated Ground Zero
DH-7	deHavilland Dash 7 (Drug Interdiction Aircraft)
DHCA	Data Handling Capability Analysis
DHFN	Direct Hire Foreign National
DHS	Defense HUMINT Service
DI	(1) Director of Intelligence (USEUCOM); (2) Directorate for Foreign Intelligence (DIA)
DIA	(1) Defense Intelligence Agency; (2) Defense Intelligence Assessment
DIA/CS	Defense Intelligence Agency/Command Support
DIAAPR	Defense Intelligence Agency Appraisal
DIAC	Defense Intelligence Analysis Center
DIAI	DIA Instruction
DIAIAPPR	DIA Intelligence Appraisal
DIAL	Defense Intelligence Agency Liaison
DIAL-J	DIA Liaison Office for Japan
DIALO	DIA Liaison Office
DIALOG	DIA Information Retrieval System
DIAM	Defense Intelligence Agency Manual
DIAMCP	DIA Master Contingency Plan
DIANM	DIA Analytical Memorandum
DIAOB	Defense Intelligence Air Order of Battle
DIAOLS	DIA On-Line System
DIAPF	DIA Part File
DIAR	DIA Regulation
DIATP	DIA Tactical Program
DIATS	DIA Terrorism Summary
DIB	(1) Defense Intelligence Board; (2) Defense Intelligence Brief; (3) Directory Information Base

DIC	(1) Defense Intelligence Community; (2) Difference in Condition; (3) Defense Intelligence College (Now JMIC); (4) Defense Intelligence Commentary
DICBM	Depressed Intercontinental Ballistic Missile
DICP	Defense Intelligence Counterdrug Program
DID	(1) Data Line Description; (2) Defense Intelligence Digest (Now Military Intelligence Digest); (3) Data Item Description
DIDHS	Deployable Intelligence Data Handling System
DIDOP	Digital Image Data Output Product
DIDS	Defense Intelligence Dissemination System
DIDSRS	Defense Intelligence Dissemination, Storage and Retrieval System
DIE	Defense Intelligence Estimate
DIEB	Defense Intelligence Executive Board
DIEC	Deployable Imagery Exploitation Capability
DIEPS	Digital Imagery Exploitation and Production System
DIEM	Defense Intelligence Estimates Memorandum
DIEOB	Defense Intelligence Electronic Order of Battle
DIFAR	(1) Directional Frequency Analysis and Recording System; (2) Directional Frequency and Ranging
DIFAX	(1) Defense Intelligence Facsimile; (2) Defense Intelligence Security Facsimile Network
DIFM	Defense Intelligence Functional Manager
DIFR	Defense Intelligence Facility Report
DIGITS	Digital Geographic Information Tailoring System
DIGOB	Defense Intelligence Ground Order of Battle
DIH	Daily Intelligence Highlights
DIHEST	Direct Induced High-Explosives Simulation Technique
DII	Defense Information Infrastructure
DIIN	Defense Imagery Intelligence Notice
DIIP	Defense Intelligence Interoperability Panel
DIIPS	Digital Imagery Interactive Processing System
DIIS	DIA Integrated Intelligence System
DILC	Dedicated Intelligence Loop Circuit
DIM	Defense Intelligence Memorandum
DIMES	Digital Image Manipulation & Enhancement System
DIMMD	Diver Integral Magnetic Mine Detector
DIMOB	Defense Intelligence Missile Order of Battle
DIMSS	DSN Integrated Management Support System
DIN	(1) Defense Intelligence Notice; (2) Defense Intelligence Network; (3) AUTODIN
DINAH	Desktop Interface to AUTODIN Host
DINOB	Defense Intelligence Naval Order of Battle
DINSUM	Defense Intelligence Summary

DIO	(1) Defense Intelligence Officer (DIA); (2) District Intelligence Officer (U.S. Navy); (3) Defence Intelligence Organisation (Australian)
DIOB	Defense Intelligence Order of Battle
DIOBS	Defense Intelligence Order of Battle System
DIOP	Defense Intelligence Objectives and Priorities
DIP	(1) Defense Intelligence Plan; (2) Defense Imagery Program
DIPC	Defense Intelligence Production Council/Conference
DIPFAC	(1) U.S. Diplomatic Facilities Graphic; (2) Diplomatic Facility
DIPOLES	Defense Intelligence Photoreconnaissance On-Line Exploitation System
DIPP	Defense Intelligence Projection for Planning
DIPS	(1) Defense Intelligence Production Schedule; (2) Digital Imagery Processing System; (3) Def Intelligence Production Study
DIR	(1) Defense Intelligence Report; (2) Directive; (3) Defense Imagery Report; (4) Director; (5) Direction
DIRCM	Direct Infrared Countermeasures
DIRES	Defense Imagery Requirements and Exploitation System
DIRINT	Director of Intelligence
DIRLAUTH	Direct Liaison Authorized
DIRNSA	Director, National Security Agency
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DIROI	Directorate Operating Instruction
DIRS	(1) Defense Intelligence Reference Series; (2) Defense Imagery Reference Series
DIS	(1) Defence Intelligence Staff (U.K.); (2) Defense Investigative Service; (3) Defense Intelligence Summary; (4) Daily Intelligence Summary; (5) Distributive Interactive Simulation; (6) Data Integration System; (7) Defense Information System
DISA	Defense Information Systems Agency
DISA-EUR	Defense Information Systems Agency-Europe
DISA-PAC	DISA-Pacific
DISA WESTHEM	DISA Western Hemisphere
DISAM	Defense Institute of Security Assistance Management
DISC	Daily Intelligence Summary Cable
DISC4	Director of Information Systems Command, Control, Communications and Computers
DISCAS	Defense Intelligence Special Career Automated System
DISE	Deployable Intelligence Support Element
DISECS	Defense Intelligence Space Exploitation and Correlation System
DISES	Defense Intelligence Senior Executive Service
DISIDS	Display and Information Distribution System/Subsystem
DISMOB	Defense Intelligence Strategic Missile Order of Battle
DISN	Defense Information Systems Network
DISNET	Defense Integrated Secure Network
DISO	Defense Intelligence Support Office

DISOB	Defense Intelligence Space Order of Battle
DISP	Defense Industrial Security Program
DISPEWT	Defense Intelligence Space Electronic Warfare Threat Data Base
DISR	(1) Daily Indicator Status Report; (2) Defense Indications Status Report
DISS	(1) Digest of Intelligence and Security Services; (2) Dissemination
DISSEM	Dissemination
DISSO	Deputy Information Systems Security Officer
DIST	Digital Imagery Support Terminal
DISTAFF	Directing Staff (NATO Commands, JECG)
DISTS	Defense Intelligence Secure Telephone System
DISTP	Defense Intelligence Special Technologies Program
DISUM	(1) Daily Intelligence Summary; (2) Defense Intelligence Summary
DIT	Defense Intelligence Thesaurus
DITB	Digital Imagery Test Bed
DITCO	Defense Information Technology Contracting Office (formerly DECCO)
DITDS	Defense Intelligence Threat Data System
DITEQ	Defense Intelligence Thesaurus Equivalency List
DITFOR	Defense Intelligence Technical Forum
DITS	Digital Imagery Transmission System
DITSUM	Defense Intelligence Terrorism Summary
DIV	(1) Division; (2) Defense Intelligence Videocassette
DIVARTY	Division Artillery
DIVISION	Enciphered Television
DIW	Dead in Water
DIWO	Duty Intelligence Watch Officer
DIWS	(1) Digital Imagery Workstation Suite; (2) Defense Indications and Warning System; (3) DOD Intelligence Warning System
DJ2	Deputy Director of Intelligence
DJS	Director, Joint Staff
DJSM	DJS Memorandum
DJTF	Deployable Joint Task Force
DJTFAC	DJTF Augmentation Cell
DLA	Defense Logistics Agency
DLAB	Defense Language Aptitude Battery
DLEA	Drug Law Enforcement Agency
DLED	Dedicated Loop Encryption Device
DLI	Defense Language Institute
DLIFLC	Defense Language Institute, Foreign Language Center
DLO	Defense Liaison Office
DLPT	Defense Language Proficiency Test
DLTV	Daylight Television
D&M	Detection and Monitoring

DM	(1) Dissemination Manager; (2) Decompression Monitor
DMA	(1) Defense Mapping Agency; (2) Direct Memory Access
DMAAC	Defense Mapping Agency Aerospace Center
DMACSC	Defense Mapping Agency Combat Support Center
DMAHTC	DMA Hydrographic and Topographic Center
DMAI	Defense Mapping Agency Instruction
DMAL	Defense Mapping Agency Liaison
DMAR	Deferred Maintenance and Repair
DMB	DODIIS Management Board
DMC&GP	Defense MC&G Program
DMD	Digital Message Device
DMDG	Digital Message Device Group
DME	Distance Measuring Equipment
DMED	Digital Message Entry Device
DMFE	DAWS Message Front End
DMI	Directorate of Military Intelligence
DMOB	Defensive Missile Order of Battle
DMOS	Daily Maritime OPINTEL Summary
DMPC	Deployment Media Production Center Project
DMPI	Desired Mean Point of Impact
DMS	(1) Data Management System; (2) Defense Message System
DMSP	Defense Meteorological Satellite (or Support) Program
DMZ	Demilitarized Zone
DN	(1) Data Net; (2) Duplicate Negative; (3) Department of the Navy
DNA	(1) Defense Nuclear Agency; (2) Deoxyribonucleic Acid
DNAS	(1) DODIIS Network Access System; (2) Data Network Access System
DNC	(1) Director, Naval Communications; (2) Digital Nautical Chart
DNCC	Data Network Control Center
DND	Department of National Defence (Canada)
DNI	Director of Naval Intelligence
DNSIX	DODIIS Network Security for Information Exchange
DNVT	Digital Non-Secure Voice Terminal
DO	Director of Operations
DOA	(1) Department of the Army; (2) Date of Arrival; (3) Director of Administration; (4) Dead on Arrival
DOAT	JAC Counterterrorism/Counterintelligence Analysis Branch
DOB	(1) Depth of Burst; (2) Date of Birth; (3) Defense Order of Battle
DOC	Department of Commerce
DOCC	(1) Defense Communications Agency Operations Center Complex; (2) Deep Operations Coordination Cell; (3) DISA Operational Control Complex
DOCEX	(1) Document Exploitation; (2) Document Exploitation Center
DOCKLAMP	Defense Attache System Message Channel
DOCS	DSCS Operations Control System

DoD, DOD	(1) Department of Defense; (2) Date of Death; (3) Date of Departure
DODCI	DoD Computer Institute
DODCSC	Department of Defense Computer Security Center
DODD	DoD Directive
DODEX	DoDIIS Extended
DODFCIP	DoD Foreign Counterintelligence Program
DODFDCO	Department of Defense Foreign Disclosure Coordinating Office
DODFIP	DoD Futures Intelligence Program
DODIIS	DoD Intelligence Information System
DODIIS SCINET	DoDIIS Sensitive Compartmented Information Network
DODIMS	DoD Intelligence Management System
DODIPP	DoD Intelligence Production Program
DODNACC	Department of Defense National Agency Check Center
DODSATCOM	DoD Satellite Communications Program
DOD SAT COM	DOD Satellite Communications
DODSI	Department of Defense Security Institute
DODSPECREP	DoD Special Representative
DOD TCSEC	DOD Trusted Computer System Evaluation Criteria
DOE	Department of Energy
DOF	Disposition of Forces
DOI	(1) Date of Information; (2) Duration of Illumination; (3) Director of Intelligence; (4) Imagery Division (JAC); (5) Director of Operations and Intelligence; (6) DSSCS Operating Instruction; (7) Date of Intercept
DOJ	Department of Justice
DOMS	Directorate of Military Support
DOMSAT	Domestic Satellite
DON	Department of the Navy
DOO	Daily Operations Order (NATO)
DOPS	DIA Outline Plotting System
DOS	(1) Department of State; (2) Date of Separation; (3) Disk Operating System; (4) Direct Operating System
DOSCOM	Division Support Command
DoSIP	Department of State Intelligence Program
DOSTN	Department of State Telecommunications Network
DOT	Department of Transportation
DP	(1) Duplicate Positive; (2) Development Program; (3) Displaced Person; (4) Delegated Production; (5) Directorate of Production; (6) Data Processing; (7) Decision Point; (8) Director of Personnel
DPAC	Defense Program Analysis Center
DPAE	Director, Program Analysis and Evaluation
DPAS	(1) Digital Patch and Access System; (2) Defense Priorities and Allocations System
DPC	Defense Planning Committee (NATO)
DPF	Digital Processing Facility

DPG	Defense Planning Guidance
DPI	Desired Point of Impact
DPIC	(1) Decentralized Pacific Imagery Processing and Interpretation Center; (2) Defense Photographic Interpretation Center
DPICM	Dual-Purpose Improved Conventional Munitions
DPKO	Department of Peacekeeping Operations
DPL	Degausser Products List
DPM	Dissemination Program Manager
DPOB	Date, Place of Birth
DPOM	Directorate of Plans, Operations, and Mobilization
DPOMIS	Directorate of Plans, Operations, Mobilization, Intelligence, and Security
DPP	(1) Delegated Production Program; (2) Deliberate Planning Process; (3) Distributed Production Program
DPPC	Deployable Print Production Center
DPPDB	Digital Point Positioning Database
DPPG	Defense Policy and Planning Guidance
DPQ	Defense Planning Questionnaire (NATO)
DPRB	Defense Planning and Resources Board
DPRK	Democratic People's Republic of Korea
DPS	(1) Delegated Production System; (2) Data Processing Set; (3) Department of Public Safety
DPSK	Digital Pulse Shift Key
DR	(1) Director; (2) Dissemination Requirement; (3) Directorate of Resources; (4) Detection Radar
DRA	Defense Research Assessment
DRAM	Dynamic Random Access Memory
DRASH	Deployable Rapid Assembly Shelters
DRB	Defense Resources Board
DRC	(1) Defense Review Committee (NATO); (2) Defense Research Comment; (3) Data Reduction Center
DR&E	Defense Research and Engineering
DRIC	Defense Resource Identification Code
DRM	Defense Research Memorandum
DRO	Departmental Requirements Officer
DRP	Disaster Relief Program
DRS	(1) Data Relay Satellite; (2) DoD Imagery Requirements Structure; (3) Data Retrieval Subsystem; (4) Data Reconstruction System
DRSA	Defense Reconnaissance Support Activities
DRSEM	Deployable Receive Segment Engineering Model
DRSN	Defense Red Switch Network

DRSP	(1) Defense Reconnaissance Support Program; (2) Defense Red Switched Program
DRU	Direct Reporting Unit
DRZ	Deep Reconnaissance Zone
DS	(1) Defense Suppression; (2) Direct Support
DS&T	Director of Science and Technology
DSA	(1) Defense Supply Agency; (2) Direct Service Activities (SIGINT); (3) Directed Search Area; (4) Division Support Area; (5) Defense Security Agency (ROK); (6) Digital Signature Algorithm
D&SA	Depth & Simultaneous Attack
DSAA	Defense Security Assistance Agency
D&SABL	Depth & Simultaneous Attack Battle Lab
DSARC	Defense Systems Acquisition Review Council
DSAT	(1) Developmental Submarine Analysis Terminal; (2) Defense Satellite
DSB	Defense Science Board
DSC	Defense Satellite Communications
DSCIS	Daily Space Command Intelligence Summary
DSCS	Defense Satellite Communications System
DSC-SLEP	Defense Satellite Communications System Service Life Enhancement Program
DSCSOC	Defense Satellite Communications System Operations Center
DSDIO	Director, Strategic Defense Initiative
DSE	(1) Direct Support Element; (2) Division Support Element
DSEC	Directorate of Security
DSFOB	Daily Strategic Forces Order of Battle
DSG	Defense Steering Group
DSI	Defense Simulation Internet
DSIATP	Defense Sensor Imagery Application Training Programs
DSIIB	Direct Support Imagery Interpretation Brief
DSIMS	Deployable SouthCom Intelligence Management System
DSI/TCCS	Defense Simulation Internet/Theater Command and Control System
DSM	Data Systems Modernization
DSN	(1) Defense Switched Network; (2) Deep Space Network
DSNET	Defense Integrated Secure Network
DSNET 1	Defense Integrated Secure Network 1 (SECRET level)
DSNET 2	Defense Integrated Secure Network 2 (TOP SECRET level)
DSNET 3	Defense Integrated Secure Network 3 (TS/SCI level)
DSO	Direct Support Operator/Operations
DSP	Defense Support Program
DSPO	Defense Special Projects Office
DSR	(1) Defense Source Register; (2) Data Service Request
DSRA	DODSPECREP-Alameda
DSRP	Defense Space Reconnaissance Program
DSRV	Deep Submergence Rescue Vehicle

DSS	(1) Decision Support System; (2) Devices, Simulators and Simulations
DSSCC	Defense Special Security Communications Center
DSSCS	Defense Special Secure Communications System
DSSCS/DIN	Defense Special Security Communications System/Digital Intelligence Network
DSSR	Deep Space Surveillance Radar
DSSS	Defense Special Security System
DST	(1) Daylight Savings Time; (2) Decision Support Template; (3) Decision Support Tools; (4) Direct Support Team; (5) Digital Support Team
DSTE	Digital Subscriber Terminal Equipment
DSTF	Decision Support Task Force
DSTP	Director, Strategic Target Planning
DSTS	Deep Space Tracking System
DSU	(1) Direct Support Unit; (2) Disk Storage Unit; (3) Data Service Unit (DCTN)
DSV	Deep Submergence Vehicle
DSVT	(1) Digital Subscriber Voice Terminal; (2) Digital Secure Voice Terminal
DT	(1) Developmental Test; (2) Directorate for Science and Technology
DTA	Directorate of Threat Analysis
DTC	(1) Digital Tape Cassette; (2) Desktop Computer
DTC-2	Desktop Computer-2 (Navy)
DTD	Digital Terrain Data
DT&E	Developmental Test and Evaluation
DTE	Data Terminal Equipment
DTED	Digital Terrain Elevation Data
DTG	Date-Time Group
DTI	Doppler-Time-Intensity
DTIC	Defense Technical Information Center
DTIO	Deputy Target Intelligence Officer
DTIR	Defense Technical Intelligence Report
DTLOMS	Doctrine, Training, Leadership, Organization, Material, Soldiers
DTLS	Descriptive Top-Level Specification
DTM	(1) Data Transfer Module; (2) Digital Transfer Module; (3) Digital Target Materials
DTMF	Dual-Tone Multi-Frequency
DTNSRDC	David W. Taylor Naval Ship Research & Development Center
DTOC	Division Tactical Operations Center
DTOCSE	Division Tactical Operations Center Support Element
DTOLM	Doctrine, Training, Organization, Leader Development and Material
DTD	Data Transfer Device
DTP	Drug Testing Program

DTS	(1) Diplomatic Telecommunications System/Service; (2) Data Transmission System; (3) Direct Transmission System; (4) Dedicated Transmission Service
DTSA	Defense Technology Security Administration
DTSG	Digital Technology Subworking Group
DTSS	Digital Topographic Support System
DTU	Data Transfer Unit
DTUC	Data Transfer Unit Cartridge
DUCA	Distributed Users Coverage Antennas
DUG	Deep Underground
DUPLEX	Simultaneous Transmit and Receive
DVO	Direct View Optics
DVM	Digital Voice Module
DVTC	Digital Voice Transmit Communications
D/TWP	Director, Tactical Warfare Programs
DTWS	Digital Topographic Work Station
DU	(1) Decision Unit; (2) Depleted Uranium
DUA	Directory User Agent
DUSD(AT)	Deputy Under Secretary of Defense (Advanced Technology)
DUSD(P)	Deputy Under Secretary of Defense (Policy)
DV	Distinguished Visitor
DVI	Digital Video Interactive
DVITS	Digital Video Imagery Transmission System
DVO	Defense Visit Offices
DWIO	Duty Watch Intelligence Officer (Canadian)
DWIP	Defense-Wide Intelligence Plan
DWS	Disaster Warning System
DWT	(1) Deadweight Ton; (2) Division Wing Team
DZ/LZ	Drop Zone/Landing Zone
DZ/LZ/RZ	Drop/Landing/Recovery Zone
DZS	Drop Zone Study

E

e	Elipticity
E	Evaporites (soil type)
EA	(1) Emergency Action(s); (2) Electronic Attack; (3) Executive Agent
E&A	(1) Exploitation and Analysis; (2) Engineering and Administration
E3	(1) End-to-End Encryption; (2) Emergency and Extraordinary Expenses
EAC	(1) Emergency Action Console; (2) Echelons Above Corps
EACTPC	Echelon-Above-Corps Theater Production Center
EACIC	Echelon-Above-Corps Intelligence Center
EAD	(1) Echelon Above Division; (2) Earliest Arrival Date; (3) Extended Air Defense
EADSIM	Extended Air Defense Simulation
EAM	(1) Emergency Action Message; (2) Event Analysis Matrix
EAMA	African States Associated with the EEC
EAMAS	Emergency Action Message Authentication System
EAP	(1) Emergency Action Procedure; (2) Emergency Action Plan
EAS	Emergency Action System
EASTLANT	Eastern Atlantic Command (NATO)
EASTPAC	Eastern Pacific
EATTG	Enhanced Automated Tactical Target Graphics
EBS	Emergency Broadcast System
EC	(1) European Community; (2) Expenditure Center; (3) Electronic Combat
ECA	(1) Enemy Capability Assessment; (2) Earth Central Angle; (3) Enemy Courses of Action
ECAC	Electromagnetic Compatibility Analysis Center
ECB	Echelons Corps and Below
ECC	(1) Eurasian Communist Countries; (2) European Communist Countries; (3) European Community Commission
ECCM	Electronic Counter-Countermeasures
ECDB	EISS Consolidated Database
ECG	Emergency Coordination Group
ECI	External Communications Interface
ECM	(1) Electronic Countermeasures; (2) European Common Market
ECMA	European Computer Manufacturer's Association
ECMC	Enhanced Crisis Management Capability
ECMO	European Collection Management Office
ECO	Electronic Collection Outstations
ECOA	Enemy Courses of Action
ECOWAS	Economic Community of West African States
ECP	(1) Emergency Communications Plan; (2) Entry Control Point
ECPL	Endorsed Data Encryption Standard Products List

ECS	(1) Electronic Combat Support; (2) European Communications Satellite
ECSC	European Coal and Steel Community
ECSM	(1) Special Assistant for Security Matters; (2) Enhanced Capability Stand-Off Munition
ECSO	European Command Special Operations
ECU	Environmental Control Unit (GSM)
ED	(1) European Capability Datum; (2) EUCOM Directive
EDA	Emergency Dissemination Authority(ies)
E-DAY	Start Day of an Exercise
EDI	European Defense Initiative
EDL	Electric Discharge Laser
EDM	Engineering Development Model
EDMS	Electronic Dissemination Management System
EDN	Emergency Data Network
EDP	(1) Electronic Data Processing; (2) ELINT Data Processor
EDPSELINT	Data Processing System
E-DRB	Expanded Defense (Planning &) Resources Board
EDRE	Emergency Deployment Readiness Exercises
E&E	Escape and Evasion
EEA	Essential Elements of Analysis
EEC	(1) European Economic Community; (2) East European Countries; (3) Enhanced Explosives Charge
EECT	End of Evening Civil Twilight
EEFI	Essential Elements of Friendly Information
EEI	Essential Elements of Information
EELS	Early Entry Lethality and Survivability
EELV	Evolved Expendable Launch Vehicle
EENT	End Evening Nautical Twilight
EEO	Equal Employment Opportunity
EEOB	Enemy Electronic Order of Battle
EEOC	Equal Employment Opportunity Commission
EES	Emergency Evacuation Study
EFCS	Electronic Filmless Camera System
EFD	Electronic Fill Device
EFS	(1) Electronic Filing System; (2) Proper Name of System
EFTA	European Free Trade Association
EFTO	Encrypted for Transmission Only
EFVS	Electronic Fighting Vehicle System
EGA	Enhanced Graphics Adapter
EGADS	Electronic Generation, Accounting, and Distribution System
EGIS	East German Intelligence Service
EHF	Extremely High Frequency
EI	Effectiveness Index
EIA	Electronics Industry Association

EIB	(1) European Investment Bank; (2) External Intelligence Bureau
EIC	Economic Intelligence Committee
EIDB	EISS Integrated Database
EIDS	Electronic Information Delivery System
EIF	(1) ECMC Interface Facility; (2) Enhanced Interface Facility
EIG	Explosive Incendiary Grenade
EIP	ELINT Improvement Program
EIRP	Effective Isotropic Radiated Power
EIS	Enhanced Imagery System
EISI	(1) Electrical Interface-SWPS/IDHS 2000; (2) Electrical IDHS-90/SWPS Interface
EISS	EUCOM Intelligence Support System
EITO	EUCOM Intelligence Training Office EKIP Enhanced Korean Information Package
EKMS	Electronic Key Management System
ELDO	(1) European Space Vehicle Launcher Development Organization; (2) European Launcher Development Organization
ELECTRO-OPINT	Electro-Optical Intelligence Element
ELECTRO-OPTINT	Electro-Optical Intelligence
ELEV	Elevation
ELF	Extremely Low Frequency
ELI	Emitter Location & Identification
Elm	Element
ELMT	Element
ELINT	Electronic Intelligence
ELISA	Electronic Intelligence Search & Analysis
ELNET	European Liaison Network
ELNOT	ELINT Notation
ELOS	Extended Line of Sight
ELS	Emitter Location System
ELSEC	Electronic Security
ELSET	(1) Element Set; (2) Proper Name of System
ELT	(1) Emergency Locator Transmitter; (2) Electronic Light Table
ELT 3000	Electronic Light Table for UNIX-based system
ELV	Expendable Launch Vehicle
EM	(1) Electromagnetic; (2) Enlisted Member; (3) Environmental Monitoring
E-Mail	Electronic Mail
EMA	European Monetary Agreement
EMAP	Electromagnetic Analysis Program
EMATS	Emergency Message Automatic Transmission System
EMC	Electromagnetic Compatibility
EMCS	ELINT Mission Control System
EMCON	Emission Control
EMCP	Electromagnetic Compatibility Program

EMD	Engineering and Manufacturing Development
E&MD	Engineering and Manufacturing Development
EMGTN	Equivalent Megatonnage
EMHS	EUCOM Message Handling System
EMI	Electromagnetic Interference
EMIDS	Experiment for Management Information Data Systems
EMINT	Emissions Intelligence
E-MIPE	Enhanced MIPE
EMIS	Early Mission Identification System
EMIT	Emergency Message Initiation Terminal
EMP	Electromagnetic Pulse
EMR	Electromagnetic Reconnaissance
EMSEC	Emanations/Emissions Security
EMT	(1) Emergency Management Team; (2) Equivalent Megatonnage
EMTR	Eastern Missile Test Range
EMUT	Enhanced Manpack UHF Terminal
En	Enemy
ENDEX	End Date of an Exercise
E-NET	Ethernet
Engr	Engineer
ENL	Enlisted
ENMCC	Expanded National Military Command Center
ENSCD	Enemy Situation and Correlation Division
ENSCE	Enemy Situation Correlation Element
ENSIT	Enemy Situation
ENTNAC	Entrance National Agency Check
EO	(1) Electro-Optical; (2) Executive Order; (3) Escape Orbit; (4) End Office
EOA	Early Operational Assessment
EOB	(1) Electronic Order of Battle; (2) Executive Office Building; (3) Enemy Order of Battle
EOBS	Electronic Order of Battle Server
EOC	Emergency Operations Center
EOD	(1) Explosive Ordnance Disposal; (2) Erasable Optical Disks
EOINT	Electro-Optical Intelligence
EOP	Emergency Operating Procedures
E-OPTINT	Electro-Optical Intelligence
EORSAT	ELINT Ocean Reconnaissance Satellite
EOS	Earth Observation Satellite
EOSAT	Earth Observation Satellite
EOSS	Electro-Optic Sensor System
EOTDA	Electro-Optical Tactical Decision Aids
EOW	Electro-Optic Warfare
EP	(1) ELINT Processor; (2) Electronic Protection
EP-3	U.S. Navy Reconnaissance Aircraft

EPA	(1) Environmental Protection Agency; (2) Evasion Plan of Action
EPAC	Eastern Pacific
EPAMS	Exercise Planning and Message System
EPAT	Earliest Possible Arrival Time
EPDS	(1) Electronic Processing and Dissemination System; (2) ELINT Processing and Dissemination System
EPF	Exploitation Products File
EPIC	El Paso Intelligence Center
EPIRB	Emergency Position-Indicating Radio Beacon
EPL	(1) ELINT Parameters List; (2) Evaluated Products List
EPLRS	Enhanced Position Location and Reporting System
EPMO	European Production Management Office
EPR	(1) Extended Planning Annex; (2) Enlisted Performance Report
EPROM	Erasable Programmable Read-Only Memory
EPS	(1) ELINT Processing System; (2) Electronic Publication System; (3) Exploitation Problem Set; (4) Encapsulated Postscript
EPW	(1) Earth Penetrator Weapon; (2) Enemy Prisoner of War
EPWG	Exploitation Plans Working Group
EPUU	Enhanced PLRS User Units
EQV	Equivalent
ER	(1) Enhanced Radiation; (2) Electronic Reconnaissance; (3) Eastern Region; (4) EAGLE REACH
ERA	(1) Extended Range Ammunition; (2) Equal Rights Amendment
ERADCOM	Electronic Research and Development Command
ERAST	Environmental Research Aircraft and Sensor Technology
ERBM	Extended Range Ballistic Missile
ERCS	Emergency Rocket Communications System
ERADCOM	Electronic Research and Development Command
ERDAS	Earth Resources Data Analysis System
ERF	Early Reinforcing Force
ERIN	Electronic Radio Intercept Network (USCS)
ERINT	Extended Range Intercept Missile
ERIR	Electronic Reconnaissance Intercept Report
ERIS	Exo-atmospheric Reentry Vehicle Interception System
EROS	Earth Resources Observational System
ERP	Effective Radiated Power
ERPHO	Earth Resources Photographic Satellite
ERRS	Emergency Regional Reporting System
ERS	(1) Emergency Relocation Site; (2) Earth Resources Satellite
ERSSO	Emergency Reaction Special Security Officer
ERT	Executive Reference Time
ERTM	Electronic Intelligence Request Tasking Message
ERTS	Earth Resources Technology Satellite
ERTZ	Equipment Radiation TEMPEST Zone
ERW	Enhanced Radiation Weapon

ES	(1) Emplacement Site; (2) Exploitation Support; (3) Electronic Warfare Support; (4) Expert System; (5) Electronic Support
ESA	(1) European Space Agency; (2) Electronically Steered Antenna
ESAA	European Special Activities Area (U.S. Air Force)
ESAC	El Salvador Analysis Cell
ESAF	European Special Activities Facility
ESAMS	Enhanced Surface-to-Air Missile Simulation
ESAR	Enhanced Synthetic Aperture Radar
ESC	Electronic Security Command (U.S. Air Force)
ESD	(1) Electronic Systems Division; (2) Ephemeris Support Data; (3) Exploitation Support Section (JSIPS)
ESF	(1) Environmental Scale Factor; (2) Extended Superframe Formatted
ESG	(1) Electronic Security Group; (2) Exploitation Steering Group
ESI	Extremely Sensitive Information
ESIAC	Electronic Satellite Image Analysis Center
ESJ	Escort Jamming
ESM	(1) Electronic Warfare Support Measures: (2) Electronic Support Measures; (3) Electronic Security Measures
ESMC	Eastern Space and Missile Center
ESMT	External Supply Management Tools
ESP	Emergency Special Measures
ESR	ELINT Summary Report
ESRO	European Space Research Organization
ESS	(1) Electronic Security Squadron; (2) ELINT Support System; (3) Exploitation Support Segment; (4) Exercise Support Subsystem; (5) Electronic Switching System; (6) Exploitation Support Section (JSIPS)
ESSA	(1) Expert System for Situation Assessment; (2) Environmental Satellite Service Administration
ESSM	Electronic Shop, Shelter-Mounted
Est	Estimated
ESV	Earth Satellite Vehicle
ESW	Electronic Security Wing
ET	(1) Enhanced Terminal; (2) Earth Terminal; (3) Embedded Training
ETA	(1) Estimated Time of Arrival; (2) Equivalent Target Area
ETAC	Enlisted Terminal Attack Controllers
ETAP	Education Training Awareness Program
ETAWG	ELINT Technical Analysis Working Group
ETC	(1) Estimated Time of Completion; (2) Et Cetera
ETD	(1) Estimated Time of Departure; (2) Effective Transfer Date
ETDS	Elapsed Time Distribution System
ETF	Enhanced Tactical Fighter
ETHICS	European Theater High Capacity Intelligence Communications System
ETI	Estimated Time of Impact

ETIBS	Enhanced Tactical Information Broadcast Service
ETII	External-to-Internal Interface
ETIWCS	European Theater Intelligence Warning and Communications System
ETL	(1) Endorsed Tools List; (2) Engineer Topographic Laboratories
ETO	(1) European Theater of Operations; (2) Earth-To-Orbit
ETP	(1) Extended Tether Program; (2) Enhanced Thermal Protection
ETPL	Endorsed TEMPEST Products List
ETR	(1) Estimated Time of Return; (2) Eastern Test Range
ETRAC	Enhanced Tactical Radar Correlator
ETRO	Estimated Time Return to Operation
ETS	(1) European Telephone System; (2) Estimated Time of Separation; (3) Expiration of Term of Service; (4) Earth Technology Satellite; (5) Engineer Test Satellite
ETSC	Electronic and Telecommunications Subcommittee
ETSS	Electronic Telecommunications Switching System
ETTP	EUCOM Tactics, Techniques and Procedures
ETUT	Enhanced Tactical User Terminal
EU	Expenditure Unit
EUCI	Endorsed for Unclassified Cryptographic Information
EUCOM	U.S. European Command
EUCOM/JIC	(1) U.S. European Command/Joint Intelligence Command; (2) EUCOM Joint Intelligence Center
EUDAC	European Defense Analysis Center
EUF	ECME User Facility
EUL	Economically Useful Life
EUMETSAT	European Meteorological Satellite (Organization)
EURATOM	European Atomic Energy Community
EUSA	Eighth U.S. Army (Korea)
EUSC	Effective United States Controlled
EUTE	Early User Test & Evaluation
EUTELSAT	European Telecommunications Satellite (Organization)
EUV	Extreme Ultraviolet
EUVE	Extreme Ultraviolet Explorer
EV	Enforcement Vector
EVA	Extra-Vehicular Activity
EVC	DoD Evasion Chart
EVO	Event Verification Officer
EVR	Enemy Vulnerability Report
EVS	Electronic Visual Communications
EW	(1) Electronic Warfare; (2) Early Warning
EW/GCI	Early Warning/Ground Control Intercept
EWAC	Electronic Warfare Anechoic Chamber
EWAS	Electronic Workorder Accounting System

EWC	(1) Electronic Warfare Center; (2) Electronic Warfare Coordinator
EWCC	Electronic Warfare Coordination Center
EWCM	Electronic Warfare Coordination Module
EWCS	Electronic Warfare Control System
EWIR	Electronic Warfare Integrated Reprogramming
EWIRS	Electronic Warfare Integrated Reprogramming System
EWMIS	Electronic Warfare Management Information System
EWMS	EW Mission Summary
EWO	(1) Electronic Warfare Officer; (2) Emergency War Order
EWOPFAC	Electronic Warfare Operating Facility
EWR	(1) Early Warning Radar; (2) Electronic Warfare Reprogramming
EWRL	Electronic Warfare Reprogrammable Library
EWS	Electronic Warfare Support
EWSE	EW Support Element
EWSM	Electronic Warfare Support Measures
EWSO	EW Staff Officer
EXCRIT	Exercise Critique System
EXDEF	Exercise Deficiency Program
EXCAP	Exercise Capability (simulator)
EXCOM	Community Executive Committee
ExDir/ICA	Executive Director for Intelligence Community Affairs
EXDIS	Exclusive Distribution (Pneumatic Tube Message Precedence)
EXEC	Executive
EXERTAS	Exercise Timeline Analysis System
EXFIL	Exfiltration
EXO	Exoatmosheric
EXOPLAN	Exercise Operations Plan
EXPER	Experience
EXPL	Exploitation
EXPLAN	Exercise Plan
ExPReS	Expoitation Process Reengineering Study
EXRAND	Exploitation Research and Development (COMIREX)
EXSCEN	Exercise Scenario System
EXSUBCOM	Exploitation Subcommittee (COMIREX)
EXSUM	Executive Summary
EXTAC	Experimental Tactics

F

F	(1) Fahrenheit; (2) Frequency
FA	(1) Frontal Aviation (FSU); (2) Field Artillery; (3) Forward Area; (4) Functional Architecture; (5) Frequency Agile; (6) Full Accounting; (7) Feasibility Assessment
FAA	(1) Federal Aviation Agency; (2) Federal Aviation Administration; (3) Foreign Assistance Act
FAAD C3I	Forward Area Air Defense Command, Control, Communications and Intelligence
FAADS	Forward Area Air Defense System
FAAR	Forward Area Alerting Radar
FAARP	Forward Area Armament and Refuel Point
FAAS	Foreign Affairs Administrative Support
FAC	(1) Forward Air Control (Controller); (2) Facilities
FACP	(1) Forward Air Control Post; (2) Forward Air Control Party
FACSFAC	Fleet Air Control and Surveillance Facility
FAD	(1) Fleet Air Defense; (2) Force Activity Designator; (3) Field Arbitrary Designators
FADOC	Future Air Defense Operation Concept
FADS	Foreign Area Data System
FAE	Fuel Air Explosive
FAF	Fast Access Format
FAFIC	Federal Armed Forces Intelligence Center (FRG)
FAI	Fuel Air Incendiary Concussion Bomb
FAIO	Field Artillery Intelligence Officer
FAISA	FORSCOM Automated Intelligence Support Activity
FAISS	FORSCOM Automated Intelligence Support System
FALD	Field Administration and Logistics Division
FAM	Functional Area Model
FAME	FORSCOM Automated Modernization Effort
FAMP	Foreign Army Materiel Production
FAMS	Fleet Ocean Surveillance Information Center Analytical Maritime Summary
FAMSIM	Family of Simulation
FANS	Friendly Allied Nation Support Network
FANT	French Atmospheric Nuclear Test
FAO	(1) Foreign Area Officer; (2) Forward Area of Operations; (3) Food and Agricultural Organization (UN)
FAPC	Food and Agriculture Planning Committee (NATO)
FARP	Forward Area Refuel Point
FARRFAA	Air Replacement Radar
FARRP	Forward Area Rearming and Refueling Point
FAS	(1) (U.S.) Foreign Agriculture Service; (2) Frequency Assignment Subcommittee
FAST	(1) Fleet Antiterrorist Support Teams; (2) Forward Area Support Team; (3) Forward Area Support Terminal
FAST-I	Forward Area SID and TRAP-Improved

FAST/I2	Improved FAST/I
FASTC	Foreign Aerospace Science and Technology Center (archaic, now NAIC)
FASTFAX	Tactical Digital Facsimile
FASTL	Future Analytic Strategic Target List
FAV	(1) Field Assistance Visit; (2) Fast Attack Vehicle
FAX	Facsimile
FB	Fighter Bomber
FBA	Fighter Bomber Attack
FBH	Force Beachhead
FBI	Federal Bureau of Investigation
FBIS	Foreign Broadcast Information Service
FBM	Fleet Ballistic Missile
FBR	Fast Breeder Reactor
FBS	(1) Forward-Based Systems; (2) Federal Border Service
FC	(1) Fire Control; (2) Fractional Coverage
FCA	Foreign Counterintelligence Activity
FCB	Functional Control Board
FCC	(1) Fleet Command Center; (2) Federal Communications Commission; (3) Fighter Control Center; (4) Fire Coordination Center
FCE	Forward Control Element
FCFS	First Come, First Served
FCG	Foreign Clearance Guide (military)
FCG2	FORSCOM G2
FCI	Foreign Counterintelligence
FCIAD	FORSCOM Component Intelligence Architecture Document
FCIP	Foreign Counterintelligence Program
FCISD	FORSCOM Component Intelligence Strategy Document
FCITP	Foreign Counterintelligence and International Terrorism Program (FBI)
FCITTP	FORSCOM Component Intelligence Tactics, Techniques and Procedures
FCLP	FORSCOM Command Language Program
FCO	Facility Control Office
FCRC	Federal Contract Research Center
FCS	(1) Fire Control System; (2) Flight Control System; (3) (U.S.) Foreign Commercial Service
FCSE	Forward Control Support Element
FCT	Foreign Comparative Test
FCZ	Forward Combat Zone
FD	Functional Design
F/d	Ratio of focal-length to diameter (of reflector type antennas)
FDB	Fleet Database
FDBM	Functional Data Base Manager
FDBPS	Fleet Data Base Production System

FDC	Fire Direction Center
FDDAC	Foreign Denial and Deception Analysis Committee
FDDI	Fiber Distributed Data Interface
FDDS	Flag Data Display System
FDIU	Fill Device Interface Unit
FDM	Frequency Division Multiplexing
FDMA	Frequency Division Multiple Access
FDO	Foreign Disclosure Officer
FDOA	Frequency Difference of Arrival
FDR	Foreign Disclosure Representative
FDT&E	Force Development Test & Experimentation
FDU	Force Design Update
FDW	Forward Deployed Workstation
FDX	Full Duplex
FEA	Front End Analysis
FEAF	Far Eastern Air Forces
FEBA	Forward Edge of the Battle Area
Fed	Federal Reserve System
FEDS	Front End Distribution System
FEDSIM	Federal Computer Performance Evaluation and Simulation Center
FEL	Free Electron Laser
FEMA	Federal Emergency Management Agency
FEMD	Far East Military District
FEMP	Front End Message Processors
FEP	(1) Front End Processor; (2) FLTSATCOM EHF Package
FERS	Federal Employees Retirement System
FET	Field Effect Transistor
FETVD	Far East Theater of Military Operations
FEWS	Future Early Warning System
FEWSG	Fleet Electronic Warfare Support Group
FF	Frigate
FFA	Free-Fire Area
FFAR	Folding-Fin Aerial Rocket
FFED	FIREFINDER Elevation Data
FFG	Guided-Missile Frigate
FFGH	Guided-Missile Aviation Frigate
FFGN	Nuclear-Powered Guided-Missile Frigate
FFH	Aviation Frigate
FFHGN	Nuclear-Powered Guided-Missile Aviation Frigate
FFHN	Nuclear-Powered Aviation Frigate
FFL	Corvette
FFLG	Guided-Missile Corvette
FFM	Full Face Mask
FFN	Fleet Flash Net

FFR	Radar Picket Frigate
FFS	(1) Fixed Field Site; (2) Formatted File System
FFT	Training Frigate
FGHQ	Fighter Group Headquarters (Canada)
FGN	Foreign
FH	Frequency Hopping
FH/DS	Frequency Hopping/Direct Sequence
FI	(1) Finished Intelligence; (2) Foreign Intelligence
FI&SS	Foreign Intelligence and Security Service(s)
FIA	Foreign Intelligence Agency
FIC	(1) Fleet Intelligence Center; (2) FORSCOM Intelligence Center
FICEURLANT	Fleet Intelligence Center, Europe and Atlantic
FICM	Fleet Intelligence Collection Manual
FICPAC	Fleet Intelligence Center, Pacific
FID	(1) Foreign Internal Defense; (2) Force Integration Division
FIDB	Fundamental Intelligence Database
FIE	Foreign Intelligence Element
FIG	Figure
FIIC	Force Imagery Interpretation Center
FIIU	Force Imagery Interpretation Unit
FIM	Force Integration Master Planner
FIN	(1) Fixed-Site Intelligence Network; (2) Financial
FINPLAN	Financial Plan
FIO	Foreign Intelligence Officer
FIP	(1) Force Improvement Plan; (2) Federal Information Processing
FIPC	Foreign Intelligence Priorities Committee
FIPS	(1) Federal Information Processing Standard; (2) Fleet Intelligence Production System
FIR	Field Investigative Region
FIRCAP	Foreign Intelligence Requirement Capabilities and Priorities
FIRE	Fused Intelligence Report in Europe
FIRF	Future Information Requirements Forecast
FIRMS	Foreign Intelligence Relations Management System
FIROPS	Freedom of Air Operations
FIRST	Fleet Intelligence Reserve Support Team
FIRSTEURLANT	Fleet Intelligence Reserve Support Team, Atlantic
FIRSTPAC	Fleet Intelligence Reserve Support Team, Pacific
FIS	(1) Foreign Instrumentation Signals; (2) Foreign Intelligence Service
FISA	Foreign Intelligence Surveillance Act
FISAP	FMFPac Intelligence Sub-Architecture Plan
FISINT	(1) Foreign Instrumentation and Signature Intelligence; (2) Foreign Instrumentation Signals Intelligence
FISS	Foreign Intelligence and Security Services
FIST	(1) Fleet Imagery Support Terminal; (2) Fire Support Team

FIST-T	Transportable FIST
FITCPAC	Fleet Intelligence Training Center, Pacific
FITD	FORSCOM Intelligence Training Detachment
FITWING	Fighter Wing
FLA	Foreign Launch Assessment
FLAGE	Flexible Lightweight Agile Guided Experiment
FLC	Foreign Language Committee
FLEETSATCOM	Fleet Satellite Communications
FLENUMOCEANCEN	Fleet Numerical Oceanography Center (U.S. Navy)
FLEX	Force-Level Execution System
FLI	Force-Level Information
FLIR	Forward-Looking Infrared (Radar)
FLO	Foreign Liaison Office
FLOT	Forward Line of Troops
FLR	Forward-Looking Radar
FLRA	Federal Labor Relations Authority
FLSG	Force Logistics Support Group
FLT	Fleet; Flight
FLTBCST	Fleet Broadcast
FLTCINC	Fleet Commander in Chief
FLTSAT	Fleet Satellite
FLTSATCOM	Fleet Satellite Communications System
FLTSEVOCOM	Fleet Secure Voice
FM	(1) Frequency Modulation; (2) Foreign Materiel; (3) File Maintenance; (4) Factory Marking(s); (5) Functional Manager; (6) Field Manual; (7) From; (8) Comptroller
FMA	(1) Foreign Materiel Acquisition; (2) Foreign Media Analysis
FMAO	Foreign Materiel Acquisition Operation
FMAR	Foreign Materiel Acquisition Requirement
FMAS	Foreign Media Analysis Subsystem
FMC	(1) Field Maintenance Center; (2) Force Mobile Command
FME	Foreign Materiel Exploitation
FMEC	Foreign Materiel Exploitation Catalogue
FMEP	Foreign Materiel Exploitation Program
FMF	Fleet Marine Force(s)
FMFLANT	Fleet Marine Force, Atlantic
FMFM	Fleet Marine Field Manual
FMFPAC	Fleet Marine Force, Pacific
FMIB	Foreign Materiel Intelligence Board
FMIG	Foreign Materiel Intelligence Group
FMIS	Force Management Information System
FMLM	French Military Liaison Mission
FMOCC	Fleet Mobile Operations Command Center
FMP	Foreign Materiel Program
FMPCP	Foreign Military Personnel Contact Program

FMPRB	Foreign Military Program Review Board
FMRL	Foreign Materiel Requirements List
FMs	Defense Intelligence Functional Managers
FMS	Foreign Military Sales
FMSF	Foreign Military Sales Financing
FMTV	Family of Medium Tactical Vehicles
FN	Foreign National
FNOC	Fleet Numerical Oceanographic Center
FNU	First Name Unknown
FO	Forward Observer
F/O	Fiber-Optics
FOA	(1) Field Operating Agency; (2) Forward Operating Area
FOAMP	Foreign Aerospace Materiel Production
FOAP	Foreign Aircraft Production
FOB	(1) Forward Operating Base; (2) Foreign Order of Battle
FOBS	Fractional Orbital Bombardment System
FOC	(1) Final Operational Capabilities; (2) Full Operational Capability; (3) FORSCOM Operations Center; (4) Full Operating Capacity
FOCI	Foreign Owned, Controlled or Influenced
FOCUS	(1) Interagency Review of Defense Attache Offices; (2) FORSCOM Objective Communications System
FOD	Foreign Object Damage
FOFA	Follow-on Forces Attack
FofF	Field of Fire
FOG	Fiber-Optics Guided
FOGM	Fiber-Optic Guided Missile
FOI	Freedom of Information
FOIA	Freedom of Information Act
FOL	(1) Forward Operating Location; (2) Family of Loudspeakers
FOLAN	Fiber-Optic Local Area Network
FOLPEN	Foliage-Penetrating
FOM	Figure of Merit
FOMA	Foreign Military Assistance
FOMCAT	Foreign Materiel Catalogue
FOMP	Foreign Missile Production
FONS	Fleet Operational Needs Statement for Intelligence
FOP	Forward Observation Post
FORDTIS	Foreign Disclosure Technical Information System
FORECON	Force Reconnaissance
FORGE	Force Generation
FORMAT	Foreign Materiel
FORMDEPS	FORSCOM Mobilization and Deployment Planning System
FORMICA	Foreign Military Intelligence Collection Activity
FORMMS	Foreign Materiel Management System

FORSCOM	U.S. Forces Command
FORSTAT	Force Status and Identity Report
FORT	Force Trends Data Base
FORTRAN	Formula Translator
FOSCAS	Foreign Ship Construction and Shipyards
FOSD	Family of Sabotage Devices
FOSIC	Fleet Ocean Surveillance Information Center
FOSIC-E	Fleet Ocean Surveillance Information Center, Europe
FOSICLANT	Fleet Ocean Surveillance Intelligence Center, Atlantic
FOSICPAC	Fleet Ocean Surveillance Information Center, Pacific
FOSIF	Fleet Ocean Surveillance Information Facility
FOSIF Rota	Fleet Ocean Surveillance Information Facility, Rota
FOSIF/WESTPAC	Fleet Ocean Surveillance Information Facility, Western Pacific
FOTARS	Follow-On Tactical Reconnaissance System
FOT&E	Follow-On Test and Evaluation
FOTELSYS	Foreign Telecommunications Systems
FOTRS	Follow-On Tactical Reconnaissance System
FOUO	For Official Use Only
FOV	Field of View
FP	(1) Fire Position; (2) Field Post; (3) Force Package
FPA	(1) Federal Preparedness Agency; (2) Focal Plane Array; (3) Force Projection Army
FPB	Fast Patrol Boat
FPE	Force Planning Estimate
FPF	Final Protection Fire
FPI	(1) Foreign Positive Intelligence; (2) Federal Process Improvement
FPIR	Force Protection Information Report
FPL	Fire Protective Line
FPN	Field Post Number
FPO	Fleet Post Office
fps	Feet Per Second
FPTOC	Force Projection Tactical Operations Center
FPU	Floating Point Unit
FQ&P	Flying Qualities and Performance
FRAG	Fragmentary Order
FRAGO	Fragmentary Order
FRD	(1) Federal Research Division (Library of Congress); (2) Formerly Restricted Data; (3) Functional Requirements Document
FREQ	Frequency
FRG	Federal Republic of Germany
FRIES	Fast Rope Insertion Extraction System
FRIF	Finished Recurring Intelligence File
FROG	Free Rocket Over Ground
FROKA	First Republic of Korea Army

FROSS	Foreign Reliance on Space Systems
FRPG	Facility Reference Point Graphic
FRR	Frequency Resource Records
FRS	(1) Fleet Readiness Squadron; (2) Federal Research Service; (3) Forward Recording Site
FRY	Former Republic of Yugoslavia
FRYM	Former Republic of Yugoslavia-Macedonia
FS	(1) File Server; (2) Fire Support
F3S	Field Station Support System
FSAIS	FICEURLANT SCI Analyst Information System
FSB	(1) Fleet Satellite Broadcast (of FLTSATCOM); (2) Forward Staging Base; (3) Fire Support Base
FSBS	Fleet Submarine Broadcast System
FSCC	Fire Support Coordination Center
FSCL	Fire Support Coordination Line
FSCOORD	Fire Support Coordinator
FSD	(1) Field Support Division; (2) Forward Support Detachment
FSE	Fire Support Element
FSHB	Fallout Safe Height of Burst
FSI	Foreign Service Institute
FSIC	Forward Sensor Interface and Control
FSK	(1) Field Station, Korea; (2) Frequency Shift Keying
FSM	Federated States of Micronesia
FSO	(1) Foreign Service Officer; (2) Fire Support Officer
FSOC	Fairchild Satellite Operations Center
FSOF	Forward Special Operations Facility
FSP	Fire Support Plan
FSRS	Functional Security Requirements Specification
FSS	(1) Fast Sealift Ship; (2) FAISS SID System; (3) Fixed Satellite Services
FSSG	Force Service Support Group (USMC)
FSST	Forward Space Support in Theater
FST	(1) Future Strategic Targets; (2) Future Soviet Tank
FSTC	Foreign Science and Technology Center (archaic; now NGIC)
FSTS	Federal Security Telephone Service
FSU	Former Soviet Union
FSV	Fire Support Vehicle
FSVS	Future Secure Voice System
FSWDS	Fixed-Site Warning & Detection System
FT	(1) Fort; (2) Foot
FT-1	Fractional T-1
FTA	(1) Field Training Area; (2) Functions, Tasks, and Activities
FTAM	File Transfer Access Management
FTC	(1) Fast Time Constant (ECCM); (2) Federal Trade Commission
FTD	Foreign Technology Division (USAF)

FTDB	Foreign Technology Data Base
FTI	Fixed Target Indicator
FTL	Future Target List
FTLS	(1) Future Target List-Strategic; (2) Formal Top-Level Specification
FTM	Full-Time Manning
FTP	File Transfer Protocol
FTPS	FORSCOM Topographic Production System (Facility)
FTR	Fighter
FTS	(1) Fleet Telecommunications System; (2) Federal Telecommunications System; (3) Federal Telephone System; (4) Flight Training Squadron
FTS 2000	Federal Telephone System 2000
FTSC	Fleet Technical Support Center
FTU	Forecast Tactical Unit
FTX	Field Training Exercise
FU	Forecast Unit
FUD	Full Unit Designator
FUE	First Unit Equipped
FUNT	French Underground Nuclear Test
FUSS	Fleet Undersea Surveillance System
FUWOB	Forward Unconventional Warfare Operations Base
FV	Fighting Vehicle
FVS	Foreign Visits System
FW	(1) Fighter Wing; (2) Fixed-Wing
FWAIS	Free-World Air Intelligence Study
FWAOB	Free-World Air Order of Battle
Fwd	Forward
FWE	Foreign Weapons Evaluation
FWIC	Fighter Weapon School Intelligence Course
FWVP	Fallout Wind Vector Plot
FY	Fiscal Year
FYDP	(1) Fiscal Year Defense Program/Plan; (2) Five-Year Defense Program; (3) Future Years Defense Program
FYI	For Your Information
FYIP	Five-Year Intelligence Plan
FYMOP	Five-Year Master Objectives Plan
FYP	Five-Year Plan (FSU)
FYROM	Federal Yugoslav Republic of Macedonia

G

G	Gain
G1	Assistant Chief of Staff, G1 (Personnel)
G2 or G-2	(1) Assistant Chief of Staff, G2 (Intelligence); (2) Army or Ground Directorate of Intelligence; (3) General Corps Staff Intelligence Officer
G3	Assistant Chief of Staff, G3 (Operations and Plans)
G4	Assistant Chief of Staff, G4 (Logistics)
G5	Assistant Chief of Staff, G5 (Civil Affairs)
G6	Director(ate) of C4
G8	Director(ate) of Resource Management
GA	Ground Attack
GaAs	Gallium Arsenide
GACC	Ground Attack Coordination Center
GAD	Guards Artillery Division
GADT	Ground/Air Defense Threat
GAF	Ground Alert Facility (of PAC ABNCP)
GAFIA	German Armed Forces Intelligence Agency
GALE	Generic Area Limitation Environment
GALS	FSU Satellite (“Horizon”)
GAMO	Ground and Amphibious Military Operations
GAO	General Accounting Office
GAS	(1) Gray Area Systems; (2) Getaway Special
GAT	(1) Government Acceptance Test; (2) Guidance, Apportionment, and Targeting
GATT	General Agreement on Tariffs and Trade (UN)
GB	(1) Gigabyte; (2) Guardband
GBCS(-L or -H)	Ground-Based Common Sensor (-Light or -Heavy)
GBI	Ground-Based Interceptor
GBL	Ground-Based Laser
GBMD	Global Ballistic Missile Defense
GBR	Ground-Based Radar
GBS	Global Broadcast System
GBU	Guided Bomb Unit
GC	Gun Camera
GCA	Ground Controlled Approach
GCC	(1) Government Control Center; (2) Ground Component Commander; (3) Gulf Cooperation Council; (4) Global Control Center
GCCS	(1) Ground Command and Control System; (2) Global Command and Control System
GCDCAL	Great Circle Distance Calculator
GCE	Ground Combat Element
GCI	Ground-Controlled Intercept
GCN	Ground Communications Network
GCNTTY	Ground Communications Network Teletype

GCP	Ground-Controlled Processor
GCP-E	Ground-Controlled Processor-ELINT
GCS	(1) Graphics Compatibility System; (2) Ground Control Station; (3) Global Connectivity Services; (4) Global Communications System
GCSS	Global Combat Support System
GDA	Gimbaled Dish Antenna
GDBI	Generic Data Base Interface
GDBMS	Generic Data Base Management Server
GDIC	General Defense Intelligence Community
GDIP	General Defense Intelligence Program
GDIPP	General Defense Intelligence Proposed Program
GDL	Gas Dynamic Laser
GDOP	Geometric Dilution of Precision
GDP	(1) General Defense Plan; (2) Gross Defense Product; (3) Ground Defense Position; (4) Gross Domestic Product
GDPS	Ground Data Processing System
GDRS	Ground Data Reduction System
GDS	(1) General Declassification Schedule; (2) FSU Guards; (3) Group Decision Support
GDSS	Global Decision Support System
GDT	Ground Data Terminal
Gen	General
GEM	Ground Effects Machine
GEN	(1) Generation; (2) General
GENIC	German National Intelligence Cell (NATO)
GENREP	General Reports
GENSER	General Service (Communications)
GEO	Geosynchronous Earth Orbit
GEODIS	Geographic Display
GEODSS	Ground-Based Electro-Optical Deep-Space Surveillance System
GEOFILE	(1) Geographic Locations Code File System; (2) Geolocation File (JOPES)
GEOREF	Global Reference System, a worldwide position reference system that may be applied to any map or chart graduated in latitude and longitude regardless of projection.
GEOSAT	Geological Satellite
GEP	Ground Entry Point
GEPS	Generic Electronic Publishing System
GES	Ground Entry Station
GFAC	Ground Forward Air Controller
GFCP	Generic Front-End Communications Package
GFE	Government Furnished Equipment
GFTD	Global Force Trends Data Base
GFR	Gap Filler Radar
GGI&S	Global Geospatial and Information Services
GHz	Gigahertz

GIGSTER	NSA Video Teleconferencing System
GIIPS	Geographic Installation Intelligence Production Specifications
GIITS	General Intelligence Imagery Training System
GIN	Greenland-Iceland-Norway
GIPD	(1) General Intelligence Production Detachment; (2) General Intelligence Production Division
GIPMIS	General Intelligence Production Management Information System
GIPS	Geographic Installation Intelligence Production Specifications
GIPSY	Graphics Information or Presentation System
GIS	Geographical Information System
GIST	Graphical Intelligence Support Terminal
GITAC	General Intelligence Training Advisory Committee
GITC	General Intelligence Training Center
GITS	General Intelligence Training System
GIUK	Greenland-Iceland-United Kingdom
GKNT	State Committee for Science and Technology (FSU)
GKS	Graphics Kernel System
GL	Grenade Launcher
GLCM	Ground-Launched Cruise Missile
GLLD	U.S. Ground Laser Locator Designator (for COPPERHEAD)
GLMX	Geological Multi-Source Exploitation (System)
GLOBIXS	Global Information Exchange System
GLOMR	Global Low-Orbiting Message Relay
GLONASS	Global Navigation Satellite System
GM	Guided Missile
GMD	Global Missile Defense
GMF	Ground Mobile Forces
GMFP	Global Military Force Policy
GMFSC	Ground Mobile Force Satellite Communications
GMI	(1) General Medical Intelligence; (2) General Military Intelligence
GMIPP	General Military Intelligence Production Plan
GMIT	Ground Military Intelligence Team (ROK)
GMRD	Guards Motorized Rifle Division (FSU)
GMS	(1) Ground Mobile System; (2) Geostationary Meteorological Satellite; (3) Ground Mission Supervisor
GMT	Greenwich Mean Time (Zulu)
GMTI	Ground Moving Target Indicator GNAS Gateway Network Access System
GNC	Global Navigation Chart
GND	Ground
GNP	Gross National Product
GNS	Global Network Segment
GNST	Glossary of Naval Ship Types
GO()	Government of (Name of Country)

G-O	Office of Law Enforcement and Defense Operations (USCG)
G-OINS	Intelligence Division (USCG/G-O)
G-OIS	Investigations and Security Division (USCG/G-O)
GOB	Ground Order of Battle
GOC	(1) General Officer Commanding (UK); (2) Government of Canada; (3) Global Operations Center
GOCO	Government Owned Contractor Operated
GOES	Geostationary Operational Environmental Satellites
GOLDS	General On-Line Display System
GOLDWING	Army HF Radio; HF communications system for meteorological and other operations
GOMS	Geostationary Operational Meteorological Satellite
GOP	Generated Option Plan
GOR	General Operational Requirement
GORB	General Officer Review Board
GOS	Grade of Service
GOSC	General Officer Steering Committee
GOSIA	Government Open System Interconnect Architecture
GOSIP	Government Open Systems Interconnected Profile
GOSPLAN	State Planning Committee (FSU)
GOSSNAB	State Committee for Material-Technical Supply (FSU)
GOTS	Government Off-the-Shelf
GP	(1) Group; (2) General Purpose
GPALS	Global Protection Against Limited Strikes
GPEE	General Purpose Encryption Equipment
GPF	(1) General Purpose Forces; (2) Ground Processing Facility
gph	Gallons Per Hour
GP NAF	General Purpose Numbered Air Force
GPNDS	Global Positioning & Nuclear Detection System
GPO	Government Printing Office
GPS	(1) Global Positioning System; (2) Grid Producing Source; (3) Geographical Positioning System; (4) Ground Processing Stations
GPSCS	General Purpose Satellite Communications System
GR	(1) Graphical Reporting; (2) Gateway Router
GRAD	Graduate
GRANITE SENTRY	Proper Name of System
GRID	Brand of Portable PC
GRIPF	GUARDRAIL Integrated Processing Facility
GRD	Ground Resolved Distance
GREEN FLAG	ACC live-fly electronic combat exercise
GRG	Gridded Reference Graphic
GRO	Gamma Ray Observatory
GROFIS	Ground Forces Intelligence Study
GRP	Glass Reinforced Plastic
GRT	Gross Registered Tonnage

GRU	FSU General Staff Intelligence Organization
GS	(1) General Staff, (2) General Support; (3) Geological Survey; (4) General Schedule; (5) General Service; (6) Government Service (Federal Civil Service); (7) Ground Station; (8) Government Civilian
GSA	General Services Administration
GSD	(1) Ground Sample Distance; (2) Graphical Situation Display
GSE	Ground Support Equipment
GSF	(1) Ground Support Fighter (FSU); (2) Group of Soviet Forces; (3) Ground Station Facility
GSFC	Goddard Space Flight Center
GSFG	Group of Soviet Forces Germany
GSFM	Group of Soviet Forces Mongolia
GSICS	General Support Interim Contractor Support
GSM	(1) Ground Support Module (JSTARS); (2) Ground Station Module
GSOAF	GGI&S Special Operations Applications Facility
GSP	General Strike Plan
GSR	(1) General Support Reinforcing; (2) Ground Surveillance Radar
GSRS	U.S. General Support Rocket System
GSS	(1) Global Support System; (2) General System Specification
GST	(1) Ground Sensor Terminal; (2) Ground Station Terminal; (3) Ground Support Terminal
GSTS	Ground-Based Surveillance and Tracking System
GSTN	General Switched Telephone Network
GSU	Geographically Separated Unit
G/T	Ratio of Antenna Gain to Noise Temperature
GTA	Government Training Aid
GTAB	Global Transportation Analysis Bulletin
GTD	Guards Tank Division (FSU)
GTN	Global Transportation Network
GTS	Global Telecommunications Service
GTC	Gas Turbine Compressor
GTTC	Goodfellow Technical Training Center
GUI	Graphics User Interface
GW	(1) Guided Weapon; (2) Gateway; (3) Guerrilla Warfare
G/W	Gateway
GWC	Global Weather Control
GWEN	Ground Wave Emergency Network
GWIC	Great Wall Industries Corporation (China)
GWIP	Global Weather Intercept Program
GWP	General Work Plan
GW/R	Gateway/Router
GWS	Gaps, Weaknesses, and Shortfalls (also GW&S)
GYRO	Gyroscope or Gyroscopic
GZ	Ground Zero

H

H	Symbol for the magnetic field of the propagated radio wave
H_2O	Critical life-essential liquid, commonly known as water
HA	Humanitarian Assistance
HAA	Helicopter Alighting Area
HAB	(1) High Altitude Burst; (2) High Altitude Bombing; (3) High Air Burst; (4) Hardened Aircraft Bunker
HAC	(1) House Appropriations Committee; (2) Historical Area Coverage
HACC	Humanitarian Assistance Coordination Center
HAE	High-Altitude Endurance
HAHO	High-Altitude High-Opening
HAIS	Hawaiian Air Intelligence System
HAL	Helicopter Light Attack
HALE	High-Altitude Long-Endurance
HALO	High-Altitude Low-Opening
HANE	High-Altitude Nuclear Effects
HANG	Hawaii Air National Guard
HARDLOOK	Special Data Analysis Product of NAVSPACECOM/N24
HARDS	High-Altitude Radiation Detection System
HARM	High-Speed Anti-Radiation Missile (AGM-88A)
HARV	Harassment Vehicle (Drone)
HAS	Hardened Aircraft Shelter
HASC	House Armed Services Committee
HATS	Heuristic Automated Transportation System
HATMD	High-Altitude Theater Missile Defense
HAV	(1) High Acceleration Vehicle; (2) Heavy Armored Vehicle (non-tactical)
HAWS	Hawaii Area Wideband System
HAZCON	Hazardous Condition
HAZMAT	Hazardous Materials
HB	High Burst
HBWP	Host-Based Word Processing
HC	HUMINT Committee
HCA	Humanitarian and Civic Assistance
HCC	HUMINT Contingency Cell
HCF	High Command of Forces
HCI/DV/AEX	Human-Computer Interface/Data Visualization/Automated Expansion
HCR	HUMINT Collection Requirement
HCS	Helicopter Combat/Search and Rescue
HCU	High Capacity Computer Unit
HD	Horizontal Ground Distance
HDL	Harry Diamond Laboratories
HDM	Hierarchical Development Methodology

HDO	Humanitarian Demining Operations
HDX	Half Duplex
HX	Half Duplex
HE	High Explosive
HEAT	High-Explosive AntiTank
HEC	Helicopter Element Coordinator
HEDI	High Endoatmospheric Defense Interceptor
HEF	Hostile Establishment File
HEI	High-Explosive Incendiary
HEL	High-Energy Laser
HELIP	HAWK European Limited Improvement Program
HELRATS	High Energy Laser Radar Acquisition & Tracking System
HELSTF	High-Energy Laser Systems Test Facility
HELW	High-Energy Laser Weapons
HELWING	Helicopter Wing
HEMP	High-Altitude Electromagnetic Pulse
HEMT	High-Electron-Mobility Transistor
HEO	(1) High-Earth-Orbit; (2) Highly Elliptical Orbit
HEP	High-Explosive Plastic
HERO	(1) Hazards of Electromagnetic Radiation To Ordnance; (2) Historical Evaluation and Research Organization
HERT	Headquarters Emergency Relocation Team
HES	Hardcopy Exploitation Systems
HESS	Hangul English Support System
HEST	High-Explosive Simulation Technique
HET	Heavy Equipment Transporter
HF	(1) High Frequency; (2) Height Finder; (3) Hydrogen Fluoride
HFE	Human Factors Engineering
HFA	High-Frequency Antenna
HF/DF	High-Frequency Direction-Finding
HFE	Heavy-Fuel Engine
HFEA	Human Factors Engineering Assessment
HFP	Host Front-End Protocol
HH	Hand-Held
HHC	Headquarters and Headquarters Company
HHD	Headquarters and Headquarters Detachment
HHS	(1) Headquarters and Headquarter Services; (2) Hasty Hide Shelter
HHW	Higher High Water
HIL	High Interest List
HI-PAR	High-Performance Precision-Approach Radar
HI-RES	High-Resolution
HIC	High-Intensity Conflict
HICOM	High Command (CINCPACFLT Voice Network)
HIDSS	Helmet-Integrated Display & Sight System

HIFAR	High-Frequency Fixed-Array Radar
HIMAD	(1) High- to Medium-Altitude Defense; (2) High to Medium Altitude Adjustment
HIMS	HUMINT Information Management System
HIP	Howitzer Improvement Program
HIRMS	Human Intelligence Requirements Management System
HIROCC	Hawaiian Islands Regional Operational Control Center
HIS	(1) Honeywell Information System; (2) Hostile Intelligence Services
HISP	Hostile Intelligence Service Profiler System
HIT	High-Interest Track
HITS	(1) Human Intelligence Tasking System; (2) Hawaii Information Transfer System
HJ	HONEST JOHN (U.S. Surface-to-Surface Rocket)
HL	Hand-Launched
HLA	Helicopter Landing Areas
HLA/DZ	Helicopter Landing Area/Drop Zone
HLA/DZS	Helicopter Landing Area/Drop Zone Study
HLLV	Heavy-Lift Launch Vehicle
HL-UAV	Hand-Launched Unmanned Aerial Vehicle
HLW	Higher Low Water
HLZ	Helicopter Landing Zone
HM	Helicopter Mine Warfare
HMC	HUMINT Management Center
HMCII	Higher Military Command, Interior and Islands (Greece)
HMF	Handbook of Military Forces
HMI	(1) Host-Message Interface; (2) Human-Machine Interface
HMMWV	High-Mobility Multipurpose Wheeled Vehicle
HMS	(1) Her Majesty's Ship; (2) HUMINT Management System
HMTV	Head-Mounted Thermal Vision
HN	Host Nation
HNAF	Host Nation Armed Forces
HNIS	Host Nation Intelligence Support
HNS	Host Nation Support
HNSC	House National Security Committee
HOB	Height of Burst
HOBO	Homing Optical Bomb
HOC	(1) History of Coverage; (2) HUMINT Operations Cell
HOCNET	HUMINT Operational Communications Network
HOE	Homing Overlay Experiment
HOIS	Hostile Intelligence Service(s)
HOJ	Home on Jam
HOL	High-Order Language
HOM	(1) Head of Media; (2) Head of Mission
HOTA	HUMINT Operational Tasking Authority

HOTOL	Horizontal Takeoff & Landing
HOTPHOTOREP	Hot Photographic Interpretation Report
HOTSIT	Hot Situation Message
how	Howitzer
HP	(1) Headquarters Pamphlet; (2) Horsepower
HPA	High-Power Amplifier
HPG	Hardcopy Products Group
HPM	High-Power Microwave
HPT	(1) High-Payoff Target; (2) High-Priority Target
HPSC	High-Performance Computing Research System
HPSCI	House Permanent Select Committee on Intelligence
HQ/HQS	Headquarters
HQDA	Headquarters, Department of the Army
HQJTF	Headquarters, Joint Task Force
HQMC	Headquarters, U.S. Marine Corps
HQMRHITS	Quarterly Management Report
HQ USAF	Headquarters, Department of the Air Force
HR	(1) High Resolution; (2) Humanitarian Relief Service
hr	Hour
HR/MR	Human Readable/Machine Readable (Data)
HRC	Human Resources Committee
HRCS	High-Resolution Camera System
HRMS	Human Intelligence Requirements Management System
HRPT	High-Resolution Picture Transmissions
HRR	High-Resolution Radar
HRS	(1) Hours; (2) Humanitarian Relief Service
HRTV	High-Resolution Television
HRU	Hardcopy Reconstruction Unit
HRV	High-Resolution Visible Range Instruments
HS	(1) Helicopter Squadron; (2) Home Station
HSD	HUMINT Support Detachment
HSE	HUMINT Support Element
HSE-E	HSE-Europe
HSE-SOCOM	HSE-USSOCOM
HSI	(1) Human Systems Integration; (2) Hyperspectral Imagery
H-SIP	H-Camera Spectral Improvement Program
HSLLADS	High Speed Low Level Aerial Delivery System
HSMS	Human Sources Management System
HSS	Health Service Support
HTACC	Hardened Tactical Air Control Center
HTKP	Hard-Target Kill Potential
HTLD	High-Technology Light Division
HTOHL	Horizontal Take-off and Horizontal Landing
HTML	Hypertext Markup Language
HUD	Heads-Up Display

HULTEC	Hull-to-Emitter Correlation
HUMINT	Human Resources Intelligence
HUMMV	High Utility Mobile Mechanized Vehicle
HUMRO	Humanitarian Relief Operations
HUS	Hardened Unique Storage
HUSK	Hardened Unique Storage Key
hv	Heavy
HVA	High Value Asset
HVAC	High-Voltage Air Conditioning
HVAP	High-Velocity Armor-Piercing
HVAPFSDS	High Velocity Armor-Piercing Fin-Stabilized Discarding-Sabot
HVAT	High-Velocity Antitank
HVF	Highly Volatile Fuel
HVIT	High Volume Information Transfer
HVT	High-Value Target
HW	(1) High Water; (2) Hardware
HWAS	High Wycombe Air Station
HWC	Hobart Walk-in Cooler
HW/SW	Hardware/Software
HWY	Highway
Hz	Hertz

I

i	Inclination
I2	Intelligence Information
IA	(1) Imagery Analyst; (2) Intelligence Assistant; (3) Initial Assessment; (4) Intelligence Analyst; (5) Intelligence Agent
IAA	Interagency Agreement
I&A	(1) Imagery and Analysis; (2) Identifcation and Authentication
IAB	Imagery Analysis Branch
IAC	(1) Intelligence Analysis Center; (2) Intelligence Advisory Committee; (3) Intelligence Analyst Course (DIA); (4) Information Analysis Centers
IAD	(1) Intelligence Analysis Division; (2) Integrated Air Defense
IADB	Inter-American Defense Board
IADS	Integrated Air Defense System
IAEA	International Atomic Energy Agency
IAG	(1) Intelligence Analysis Group (formerly ITAD); (2) Imagery Analysis Group
IAGC	Instantaneous Automatic Gain Control
IAGS	Inter-American Geodetic Survey
IAIPS	Integrated Automated Intelligence Processing System
IAM	Imagery Analysis Memorandum
IAMP	Imagery Acquisition and Management Plan
IAMS	Individual Aerial Mobility System
IAN	Imagery Analysis Notice
IAP	International Airport
IAPF	Inter-American Peace Force
IAR	Imagery Analysis Report
IAS	(1) Intelligence Access System; (2) Interactive Applications System; (3) Intelligence Analysis System
IAS WS	IAS Work Station
IASSA	INSCOM Automated Systems Support Activity
IAT	Intelligence Augmentation Team
IATA	International Air Transport Association
IAW	In Accordance With
IAWG	Interagency Working Group
IAWS	Improved Analyst Workstation
IBAC	Identity-Based Access Control
IBs	Issue Books
IBBS	Interim Brigade/Battalion Simulation
IBD	Intelligence Baseline Document
IBDTF	IBD Transaction Format
IBE	Field-Initiated BE Number
IBERLANT	Iberian Atlantic Area
IBIS	Imaging Background Limited Infrared System
IBM	International Business Machines

IBO	Intelligence Baseline Overview
IBOS	Intelligence Battlefield Operating System
IBS	(1) Interactive Beacon System; (2) Integrable Base Station; (3) Integrated Broadcast Service; (4) Intelsat Business Service; (5) Integrated Bridge System
IBSSIR	Background Signature Survey
IBTA	Integrated Battlefield Targeting Architecture
IBUR	Intelligence Bottom-Up Review
IC	(1) Intelligence Community; (2) Intelligence Collection; (3) Integrated Circuit; (4) Intelligence Center; (5) Irish Concern
IC/EC	Intelligence Community/Executive Committee
ICA	Intelligence Center Atlantic
ICAF	Industrial College of the Armed Forces
ICAO	International Civil Aviation Organization
ICAP	Improved Capabilities Program
ICARIS	Intelligence Communications Architecture and Requirements Information System
ICBM	Intercontinental Ballistic Missile
ICC	(1) Integrated Communications Center; (2) Intelligence Continuity Cell; (3) IMlNT Coordination Cell; (4) Intelligence Coordination Center (Coast Guard); (5) Initial Connectivity Capability
ICCC	International Council for Computer Communication
ICD	(1) Interface Control Document; (2) Intelligence Collection Division; (3) Initiative Communications Deception
ICDP	Intelligence Career Development Program
ICE	(1) Independent Cost Estimate; (2) Interface Control Element
ICEDEFOR	Iceland Defense Forces
ICES	International Cooperation in Ocean Exploration
ICF	(1) Intelligence Collection Flight; (2) Intelligence Contingency Funds; (3) Interconnect Facility
ICFTU	International Confederation of Free Trade Unions
ICIG	IDHSS CSSR Interface Guard
ICITAP	International Criminal Investigative Training and Assistance Program
ICL	Intelligence Coordination Cell
ICM	(1) Improved Conventional Munitions; (2) Intelligence Correlation Module; (3) Integrated Common Modules
ICMC	Intelligence Collection Management Course
ICOD	Intelligence/Information Cut-Off Date
ICOM	Integrated COMSEC (SINCGARS)
ICON	Image Communications and Operations Node
ICP	(1) Intelligence Collection Platform; (2) Interface Change Proposals; (3) Incremental Change Packages
ICPS	Intelligence Communications Processing Shelter
ICR	Intelligence Collection Requirement
ICRC	(1) Intelligence Contingency Readiness Center; (2) International Committee of the Red Cross
ICRS	Imagery Collection Requirements Subcommittee (COMIREX)

ICS	(1) Intercommunications System; (2) Intelligence Community Staff
ICTF	Interagency Crisis Task Force
ICTT	(1) Improved Commander's Tactical Terminal; (2) Interim Commander's Tactical Terminal
ICU	Interface Control Unit
ICV	Infantry Combat Vehicle
ICW	In Coordination With
ICWG	(1) Interface Control Working Group; (2) Imagery Coordination Working Group
ID	(1) Identification; (2) Infantry Division; (3) Intelligence Division
IDA	Institute for Defense Analysis
IDAD	Internal Defense and Development
IDB	(1) Integrated Data Base; (2) Inter-American Development Bank
IDB-II	PC-Based Integrated Data Base
IDBM	Integrated Data Base Maintenance
IDBR	Integrated Data Base Retrieval
IDBTF	Intelligence Data Base Transaction Format
IDC	Interagency Defector Committee
IDCSP	Initial Defense Communications Satellite Program
IDEAS	Intelligence Data Element Authorization Standards
IDES	Installation Damage Expectancy Summary
IDEX	Imagery Data Exploitation System
IDEX II	Imagery Data Exploitation System II
IDF	(1) Israeli Defense Force; (2) Installation Data File
IDHS	Intelligence Data Handling System
IDHS	IDHS for the mid-1990s
IDHS-2000	Intelligence Data Handling System for the Year 2000
IDHS-II	Intelligence Data Handling System, Second Iteration
IDHSC	Intelligence Data Handling System Communications
IDHSC-II	Intelligence Data Handling System Communications, Version II
IDIMS	Interactive Digital Image Manipulation System
IDIQ	Indefinite Delivery, Indefinite Quantity
IDIRA	Introduction to Defense Intelligence Research and Analysis (DIA)
IDL	Interoperable Data Link
IDM	Improved Data Modem
IDMS	IPAC Document Management System
IDN	Integrated Data Network
IDNX	Integrated Digital Network Exchange
IDP	Intelligence Data Processor
IDPS	(1) Imagery Data Processing System; (2) Integrated Deployable Processing System; (3) Interim Deployable Processing System
IDS	(1) Intrusion Detection System; (2) Infrared Detection Set
IDSCS	Initial Defense Satellite Communications System
IDSCP	Initial Defense Satellite Communication Program

IDSF	Intelligence Defector Source File
IDTT	Inactive Duty Training Travel
IDZ	Inner Defense Zone
IEA	International Energy Agreement
IEBL	Inter-Entity Boundary Line
IEC	(1) Imagery Exploitation Center; (2) Intelligence Exchange Conference
IED	(1) Improvised Explosive Device; (2) Imitative Electronic Deception
IEG	Imagery Exploitation Group
IEMATS	Improved Emergency Message Automated Transmission System
IEP	Independent Evaluation Plan
IEPG	Independent European Program Group
IEPR	Information Exchange and Processing Requirements Report
IER	Independent Evaluation Report
IES	Imagery Exploitation System
IESS	Imagery Exploitation Support Segment
IEW	Intelligence and Electronic Warfare
IEWCS	IEW Common Sensor
IEWD	Intelligence and Electronic Warfare Directorate
IEWFAM	IEW Functional Area Model
IEWSE	IEW Support Element
IEWTAC	IEW Technology Assessment Center
IEWTPT	IEW Tactical Proficiency Trainer
IF	(1) Interrogation Facility; (2) Identification Frequency; (3) Intermediate Frequency
IFAC	International Federation of Automatic Control
IFF	Identification, Friend or Foe
IFFN	Identification, Friend, Foe or Neutral
IFOR	Implementation Force (Operation JOINT ENDEAVOR)
IFOV	Instantaneous Field-of-View
IFPS	Interformation Position System
IFR	Instrument Flight Rules
IFRB	International Frequency Registration Board
IFS	Imagery File Server
IFTE	Integrated Family Test Equipment
IFV	Infantry Fighting Vehicle
IG	(1) Interagency Group; (2) Inspector General; (3) Intelligence Group (Air Force)
IGCP	Intelligence Guidance for COMINT Programming
IGD	Intelligence Guidance Document
IGR	Improved GUARDRAIL
IGRV	Improved GUARDRAIL V
IGS	Image Generation System
IGSM	Interim Ground Station Module
IGT	Interdepartmental Group on Terrorism

IGY	International Geophysical Year
IHC	Intelligence Information Handling Committee
IHE	Insensitive High Explosive
IHFR	Improved High Frequency Radio
IHO	(1) International Hydrographic Organization; (2) In Honor of
IHR	In-Extremis Hostage Rescue
II	(1) Imagery Interpretation; (2) Imagery Interpreter
IIC	Imagery Interpretation Center
IICT	Interagency Intelligence Committee on Terrorism
IID	Integrated Information Display
IIDP	Integrated Intelligence Development Plan (USCINCEUR)
IIE	Installation Identification Element
IIF	Imagery Interpretation Facility
IIG	(1) Imagery Intelligence Group (formerly USAIIC); (2) Intelligence Inspector General
IIM	Interagency Intelligence Memorandum
IIN	Imagery Interpretation Note
IINCOMNET	Intratheater Intelligence Community Network
IINS	Imagery Information Need Statement
IIPL	Integrated Intelligence Priority List
IIR	(1) Imaging Infrared; (2) Intelligence Information Report; (3) Imagery Interpretation Report
IIRES	Imagery Interpretation, Reporting, and Exploitation System
IIRK	Interarea Interswitch Rekeying Key
IIRS	Imagery Interpretability Rating Scale
IIS	(1) Indirect Identification System; (2) IPAC Intelligence Summary; (3) Imagery Interpretation Segment
IISE	Intelligence Information System Enhancement
IISS	Intelligence Information Subsystem
IITLPC	Inter/Intra Team Low Power Communications
IITS	(1) Intra-Theater Imagery Transmission System; (2) Installation Information Transfer Systems
IIU	(1) Imagery Interpretation Unit; (2) Imagery Interface Unit
IJMS	Interim JTIDS Message Standard
ILAM	Improved Limpet Assembly Modular
ILC	International Lines of Communication
ILD	Injection Laser Diode
ILE	Intelligence Liaison Element
ILEA	International Law Enforcement Academy
ILO	Intelligence Liaison Officer
ILP	Intelligence Liaison Party
ILS	(1) Instrument Landing System; (2) Integrated Logistic Support
ILSA	Improved Lightweight Satellite Antenna
IM	(1) Information Management; (2) Intermodulation
IM/GD	Intelligence Management/Guidance Document

IMA	(1) Institute for Military Assistance; (2) Intelligence Mobilization Augmentee; (3) Information Mission Area
I-MAE	Interim Medium Altitude Endurance UAV (formerly Tier I)
IMAF	1st Marine Amphibious Force
IMAP	Interim Mission Assessment Program
IMB	(USCENTCOM) Intelligence Management Board
IMC	The International Medical Corps
IMCO	Intergovernmental Maritime Consultative Organization
IMD	Intelligence Management Document
IMEF	First Marine Expeditionary Force
IMET	(1) International Military Education and Training; (2) Integrated Management Evaluation Team
IMETS	Integrated Meteorological System
IMF	International Monetary Fund
IMINT	Imagery Intelligence
IMIS	(1) Intelligence Management Information System; (2) Integrated Management Information System
IMLETT	International Maritime Law Enforcement Training Team
IMMP	Information Management Master Plan
IMNET	Imagery Network
IMOM	Intelligence Many-on-Many
IMOC	International Maritime Officer Course
IMP	(1) Interface Message Processor; (2) Input Message Processor; (3) Image Product; (4) Information Management Program
IMPs	Imagery Products
IMS	International Military Staff (NATO)
IMSAT	Imagery Satellite
IMSE	Imagery Management Support Element
IMSO	International Maritime Satellite Organization
IMTT	Intelligence Mobile Training Team
IN	(1) International Negotiations; (2) Intelligence; (3) Infantry; (4) Director of Intelligence (Air Force Component) (also A2)
INA	Information Not Available
INCA	(1) Intelligence Communications Architecture; (2) Integrated Nuclear Communications Assessment
INCOLLNOM	Intelligence Collection Requirement Nomination
INCOMNET	Intratheater Intelligence Communications Network
INCSEA	Incidents at Sea
INDICOM	(1) Indications Communication Network; (2) Indications and Warning Communications
INDICOMM	Indications Intelligence Communications
INEWS	Integrated Electronic Warfare System
inf	Infantry
INF	Intermediate-Range Nuclear Forces
INFIL	Infiltration
INFLIGHTREP	Inflight Reports
INFLTRPT	Inflight Reports

INFO	Information
INFOSEC	(1) Information Security; (2) Information Systems Security
INGO	International Nongovernmental Organizations
INI	Initiation
INL	International Narcotics and Law
INMARSAT	International Maritime Satellite
INMS	Integrated Network Management System
INR	Bureau of Intelligence and Research (State Department)
INS	(1) Inertial Navigation System; (2) Immigration and Naturalization Service
INSAT	Indian Satellite
INSICOM	Integrated Special Intelligence Communications
INSCOM	U.S. Army Intelligence and Security Command
INST	Instruction
INSTA	Automated Installations File (DIAOLS)
INSTAL	Installation
instl	Installation
INSUM	Intelligence Summary
INT/INTEL	Intelligence
INTACS	(1) Integrated Tactical Communications System; (2) Integrated Tactical Communications Study
INTCP	Intercept
INTEL	Intelligence
INTELCAST	Intelligence Broadcast
INTELCOM	Worldwide Intelligence Communication
INTELDATA	Intelligence Data
INTELINK	Proper Name of System
INTELSAT	International Telecommunications Satellite Organization
Intelink	Command server/client system that allows secure SCI connectivity to all commands on the network, and access to available files without additional log-on.
INTELNET	Intelligence Network
Internet	International Network
INTI	CI database
intg	Interrogation
INTRA	International Travel by Selected Foreign Officials
Intranet	Internet with local scope
INTREP	Intelligence Report
INREQ	Intelligence Request
INTSUM	Intelligence Summary
INUT	Indian Nuclear Underground Test
IO	(1) Indian Ocean; (2) Intelligence Officer; (3) Information Objectives; (4) Intelligence Objective; (5) Intelligence Operations (Division); (6) Information Operations; (7) Information Objectives
I/O	Input/Output
IOA	Indian Ocean Area

IOB	Intelligence Oversight Board
IOC	(1) Initial Operational Capability; (2) Intelligence Operations Center
IOCTL	Indian Ocean Conventional Target List
IOD	Intelligence Operations Division (USEUCOM)
IOF	Intelligence Operations Facility
IOIC	Integrated Operational Intelligence Center
IOM	Input/Output Module
IOMDWG	Interagency Offensive Missile Deployment Working Group
IONDS	Integrated Operational Nuclear Detection System
IOR	Individualized Operational Ration
IONDS	Integrated Operational Nuclear Detection System
IOS	(1) Intelligence Operations Specialist; (2) International Organization for Standards
IOSS	(1) Integrated Operational Support Study; (2) Intelligence Organization Stationing Study
IOT&E	Initial Operational Test and Evaluation
IP	(1) Initial Point; (2) Imagery Processing; (3) Intelligence Problem; (4) Instrumentation Point; (5) Immediate Permanent Incapacitation Dose; (6) Internet Protocol
IP/MP	Inphase/Midphase
IPA	(1) Intelligence Production Activity; (2) Imagery Product Archive
IPAT	Intelligence Planning/Programming Analysis Tool
IPB	Intelligence Preparation of the Battlefield/Battlespace
IPC	(1) Industrial Planning Committee; (2) Intelligence Producers' Council; (3) Intelligence Production Center
IPCP	Intelligence Production Campaign Plan
IPCS	Intelligence Producers Council Staff
IPD	(1) Intelligence Planning Document; (2) Intelligence Plans Division (USEUCOM); (3) Intelligence Production Division
IPDB	Intelligence Production Data Base
IPDS	Imagery Processing and Dissemination System
IPE	Intelligence Production Element
IPF	(1) Integrated Processing Facility; (2) Intelligence Processing Facility (Guardrail)
IPG	Implementation Planning Group
IPIR	(1) Immediate Photo Interpretation Report; (2) Initial Photographic Interpretation Report; (3) Initial Programmed Interpretation Report; (4) Initial Phase Interpretation Report
IPR	Integrated Personal Armor
IPIX	Interface Processor for Imagery Exchange

IPM	(1) Interface Processor for Imagery Exchange; (2) Intelligence Programs Management
IPMA	Intelligence Production Management Activity
IPMO	Intelligence Program Management Office
IPL	Integrated Priority List
IPM	Interpersonal Messaging
IPOIC	Interagency Prisoner of War Ad Hoc Committee
IPOM	Intelligence Program Objective Memorandum
IPP	(1) Intelligence Producer Profile; (2) Impact Point Prediction
IPR	(1) Intelligence Production Requirement; (2) In Process Review; (3) Impulse Response; (4) Internet Protocol Route
IPRG	(1) Intelligence Priorities Review Group; (2) Intelligence Program Review Board
IPS	(1) Integrated Program Summary; (2) Intelligence Production System; (3) Imagery Processing Segment (CARS); (4) Intelligence Production Section; (5) Instructions Per Second; (6) Imagery Processing System
IPSC	Information Processing Standards for Computers
IPSG	Intelligence Program Support Group (now CISA)
IPSO	Internet Protocol Security Option
IPSP	Intelligence Priorities for Strategic Planning
IPT	Integrated Product Team
IPU	Inter-Parliamentary Union
IPW	Interrogation of Prisoners of War
IPWG	Intelligence Priorities Working Group
IPX	Internet Packet Exchange
IR	(1) Infrared; (2) Intelligence Information Report; (3) Illumination Rate; (4) Impulse Response; (5) Information Requirement; (6) Intelligence Requirement; (7) Initial Radiation; (8) Induced Radiation; (9) Information Ratio
I2R	Imaging Infrared
IRA	Intelligence-Related Activities
IRAC	Interdepartmental Radio Advisory Committee
IRBM	Intermediate-Range Ballistic Missile
IRC	(1) International Red Cross; (2) International Rescue Committee
IRCM	Infrared Countermeasures
IRCS	Improved Radar Calibration System
IR&D	Independent Research & Development

IRD	(1) Independent Research & Development; (2) Intelligence Resources Division; (3) Intelligence Reserve Detachment
IRDB	Integrated Requirements Data Base
IRDC	Intelligence Research and Development Council
IRDHS	Imagery-Related Data Handling System (see AIRES)
IREMBASS	Improved Remotely Monitored Battlefield Surveillance System
IRDS	Infrared Detection System
IREMBASS	Improved-Remotely Monitored Battlefield Sensor System
IREPS	Integrated Refractive Effects Prediction System
IRF	(1) Imagery Readiness Facility; (2) Intelligence Readiness Facility
IRG	Interdepartmental Regional Group
IRGM	Infrared Guidance Module
IRINT	Infrared Intelligence
IRIS	Infrared Imaging System
IRISA	Imagery Report Index Summary
IRISF	Intelligence Report Index Summary File
IRK	Interswitch Rekeying Key
IRLS	Infrared Line Scanner
IRM	(1) Intelligence Requirements Management; (2) Information Resource Management
IRMS	Imagery Requirements Management System
IROF	Imagery Reconnaissance Objectives File
IROL	Imagery Reconnaissance Objectives List
IROP	(1) Imagery Reconnaissance Objectives Plan; (2) Infrared Optical Intelligence; (3) Imagery Requirements Objectives Program
IRPG	Installation Reference Points Graphics
IRPIA	Intelligence Information Report Photo Index
IRR	(1) Individual Ready Reserve; (2) Intelligence Requirement Request; (3) Intelligence Readiness Report
IRS	(1) Intelligence Research Specialist; (2) Internal Revenue Service; (3) Interface Requirements Specification; (4) Intelligence Requirements Subcommittee
IRSCOM	Imagery Requirements Subcommittee
IS	(1) Information Systems; (2) Intelligence Specialists; (3) Intelligence Squadron
I&S	(1) Intelligence and Security; (2) Intelligence and Surveillance

ISA	(1) International Security Affairs; (2) Interservice Support Agreement; (3) Intelligence Support Activity; (4) Integration Support Activity; (5) International Support Agreement
ISAF	Israeli Air Force
ISAR	Inverse Synthetic Aperture Radar
ISARC	Intelligence, Surveillance, and Reconnaissance Cell
ISB	(1) Initial Staging Base; (2) Intermediate Staging Base; (3) Intelligence Systems Board; (4) Intelligence Support Base
ISC	(1) Information Systems Command; (2) Information Science Center; (3) Intelligence Support Cell
ISCO	Intelligence Support to Combined Operations
ISC/SC	Intelligence Specialist Chief/Senior Chief
ISD	(1) Intelligence Support Detachment; (2) Intelligence Security Division; (3) Intelligence Support Division
ISDB	Integrated Satellite Data Base
ISDN	(1) Integrated Services Data Network; (2) Intelligence Services Digital Network ISEIntelligence Support Element
ISEMS	Improved Spectrum Efficiency Modeling and Simulation
ISEW	Intelligence, Security, and Electronic Warfare
ISF	Intelligence Support Facility (U.S. Navy)
ISG	Intelligence Support Group (U.S. Navy)
ISHMRS	Improved SOF High Frequency Manpack Radio System
ISIC	Intelligence Support and Indications Center
ISID	Interim Secondary Imagery Dissemination System
ISIDS	Improved SIDS
ISINT	Instrumentation Signals Intelligence
ISIP	Intelligence Support Interface Program
ISIS	(1) Integrated Signals Intelligence System; (2) Interim SOCOM Intelligence Threat Data System
ISLES	Information Systems for Law Enforcement Support
ISM	Industrial Security Manual
ISMB	Intelligence Systems Management Board
ISO	(1) Information Systems Office; (2) International Standards Organization
ISOFAC	Isolation Facility
ISOPREP	Isolated Personnel Report
ISOS	Intelligence System of Systems
ISP	(1) Intelligence Support Plan; (2) Industrial Security Program; (3) Intelligence Support Processor; (4) Integrated Survey Program; (5) Intelligence Survey Program
ISP DCS	Integrated Survey Program Data Collection System
ISP CPE	Integrated Survey Program Central Production Element
ISPER	IPAC Special Reports
ISPO	Intelligence Support Program Office
ISPR	Information Systems Processing Request
ISPS	(1) ISP Server; (2) Improved SOF Power Sources
ISPT	Intelligence Support Processor Tool

ISR	(1) Imagery Support Requirement; (2) Inter-Agency Source Registry; (3) Intelligence, Surveillance and Reconnaissance
ISRD	Information Systems Requirement Document
ISS	(1) Intelligence Support System; (2) Intelligence Support Subsystem; (3) Intelligence Support Staff; (4) Information Security System; (5) Information Systems Security
I&SS	Intelligence and Security Service
ISSA	(1) Information Systems Support Activity; (2) Inter-service Support Agreement
ISSM	Information Systems Security Manager
ISSO	(1) Information Systems Security Officer; (2) Intelligence Systems Support Office
ISST	ICBM SHF Satellite Terminal
IST	(1) Imagery Support Terminal; (2) Intelligence Support Team; (3) Intelligence System Team
ISTA	Intelligence, Surveillance, Target Acquisition
ISWG	Intelligence Support Working Group
ISYSCON	Integrated System Control
IT	Immediate Transient Incapacitation Dose
ITA	(1) Intelligence Terrain Analyzer; (2) International Telegraph Alphabet
ITAAS	Intelligence Training Army Area Schools
ITAC	(1) Intelligence and Threat Analysis Center (U.S. Army); (2) Intelligence Tracking Analysis and Correlation
ITACIES	Interim Tactical Imagery Exploitation System (U.S. Army)
ITACS	Integrated Tactical Air Control System
ITAR	International Traffic in Arms Regulations
ITAS	Improved Target Acquisition System
ITC	Interagency Training Center
ITCT	Improved Tactical Commander's Terminal
ITD	(1) Interim Terrain Data; (2) Individual Training Directorate; (3) International Training Division
ITDB	Intercept Tasking Data Base
ITDN	Integrated Tactical Data Network
ITEP	(1) Interim Tactical ELINT Processor (U.S. Army); (2) Integrated Threat Evaluation Program
ITF	Intelligence Task Force
ITFN	Intra-Task Force Network
ITG	Interdiction Target Graphic
ITIBS	Improved TIBS
ITIC-PAC	INSCOM Theater Intelligence Center-Pacific
ITII	Internal-to-Internal Interface
ITL	Interagency Telephone Laboratory
ITO	(1) International Trade Organization; (2) Integrated Tasking Order
ITOC	Interrogation Translation Operations Center
ITP	(1) Intelligence Town Plan; (2) Interrogation/Translation Platoon
ITS	Imagery Transmission System

ITSS	Integrated Tactical Surveillance System
ITT	Interrogator Translator Team
ITU	(1) Interrogator-Translator Unit; (2) International Telecommunications Union
ITUT	Interim Tactical Users Terminal
ITW	(1) International Targeting Workstation; (2) Integrated Threat Warning
ITW&AA	Integrated Tactical Warning and Attack Assessment
IU	(1) Interface Unit; (2) Image Understanding
lUG	Intelligence Users' Guide
IUS	Inertial Upper Stage
IUSS	Integrated Undersea Surveillance System
IVAN	Intelligence Van
IVCS	Integrated Vehicle Communications System
IVD	Interactive Video Disk
IVIS	Inter-Vehicle Information System
IVSN	Initial Voice Switched Network
IW	(1) Information Warfare; (2) Intelligence Wing
I&W	(1) Indications and Warning; (2) Intelligence & Warning
IWC	Information Warfare Center
IWD	Intermediate Water Depth
IWG	Intelligence Working Group
IWO	Intelligence Watch Officer
IWS	(1) Intelligence Work Station; (2) Information Warfare Squadron
IWSDB	Integrated Weapon System Data Base
IWST	Information Warfare Support Team
IWT	Intelligence Watch Team
IWTS	Indications and Warning Training System
IWW	Inland Waterway
IX	Unclassified Miscellaneous Ship

J

J3	Director(ate) of Operations
J4	Logistics Directorate
J5	Director(ate) of Plans, Policy, and Programs
J6	(1) Director(ate) of Command, Control, Communications; (2) Director(ate) of Command, Control, Communications, and Computer Systems
J7	Joint Operational Plans Staff
J8	Director(ate) of Resource Management
JA	Judge Advocate (General)
JAADS	Joint Allied Air Defense System
JAAT	Joint Air Attack Team
JAC	Joint Analysis Center
JACC/CP	Joint Airborne Communications Center/Command Post
JAD	Joint Assessment Data
JAEIC	Joint Atomic Energy Intelligence Committee
JAG	Judge Advocate General
JAI	Joint Administrative Instruction
JAIEG	Joint Atomic Information Exchange Group
JAIS	Japan Air Intelligence System
JAIS-PAC	Joint Area Information system-USPACOM
JAMIP	Joint Analytic Model Improvement Program
JAN	Joint Army-Navy
JANAF	Joint Army, Navy, Air Force Publication
JANAP	Joint Army/Navy Publication
JAO	Joint Area of Operations
JAOC	Joint Air Operations Center
JAOP	Joint Air Operations Plan
JAPC	Joint Attrition and Penetration Committee
JAR	JIC Analysis Report
JARCC	Joint Air Reconnaissance Control Center
JARIC	(1) Joint Aerial Reconnaissance Intelligence Center; (2) Joint Air Reconnaissance Interpretation Center (UK)
JAROC	(B) Joint Allied Refugee Operations Center (Berlin)
JARP	Joint Aerospace Reserve Program
JASDF	Japanese Air Self-Defense Forces
JASORS	Joint Advanced Special Operations Radio System
JASPO	Joint Airborne SIGINT Program Office
JASS	Joint Airborne SIGINT System
JAST	Joint Advanced Strike Technology Program
JATCCCS	Joint Advanced Tactical C3 System
JAWS	(1) Joint Analytical Workstation; (2) Joint Advanced Weapons System; (3) JDISS-Army Workstation
JBS	(1) Joint Base Station; (2) Joint Broadcast Service
J2C	CIA Liaison

JC2WC	Joint C2 Warfare Center
JCAT	(1) Joint Crisis Action Team; (2) Joint Crisis Analysis Tool
JCC	Joint Coordination Center
JCCC	Joint Communications Control Center
JCCOC	Joint Communications & Control Operational Concept
JCCWC	Joint Command and Control Warfare Center
JCET	Joint/Combined Exercises for Training
JCEOI	Joint CEOI
JCF	Joint Communications Facility
JCISB	Joint Counterintelligence Support Branch
JCISOC	Joint CI Staff Officer's Course
JCMC	(1) Joint Crisis Management Capability; (2) Joint Crisis Management Center
JCMEC	Joint Captured Materiel Exploitation Center
JCMO	Joint Collection Management Office
JCMOTF	Joint Civil Military Operations Task Force
JCMPO	Joint Cruise Missile Project Office
JCMST	Joint Collection Management Support Tool (renamed JCMT)
JCMT	Joint Collection Management Tool
JCNJSIC	Center Cheyenne Mountain Air Force Base (CMAFB) Node
JCNICC	Joint Counternarcotics Intelligence Coordination Center
JCP	Joint Congressional Committee on Printing
JCPES	Joint Chiefs Planning and Execution System
JCPX	Joint Command Post Exercise
JCRC	Joint Casualty Resolution Center
JCS	Joint Chiefs of Staff
JCSAN	JCS Alert Network
JCSAR	Joint Combat Search and Rescue
JCSE	(1) Joint Communications Support Element; (2) Joint Contingency Support Element
JCSM	Joint Chiefs of Staff Memorandum
JCSS	(1) Japan Combat Support System; (2) Joint Communications Support Squadron
JCTG-ME	Joint Technical Coordinating Group for Munitions Effectiveness
J2D	DIA Liaison
JDA	(1) Joint Deployment Agency; (2) Japan Defense Agency; (3) Joint Duty Assignment
JDAC	Joint District Area Command
JDAL	Joint Duty Assignment List
JDAM	Joint Direct Attack Munition
JDC	Joint Debriefing Center
J-DEC	JICPAC-Detachment Japan
JDEC	Joint Document Exploitation Center
JDF	Joint Development Facility
JDGW	Joint Digital Geopositioning Workstation
JDIA	Joint Digital Intelligence Assessment

JDIPC	Joint Deployable Imagery Production Center
JDISS	(1) Joint Deployable Intelligence Support System; (2) Joint Defense Intelligence Support Services
JDISS-C	Joint Deployable Intelligence Support System-CENTCOM
JDISS-E	JDISS-EUCOM
JDISS-S	Joint Deployable Intelligence Support System-SOCOM or SOCRATES
JDIVS	Joint Deployable Intelligence Video/Data System
JDMAG	Joint Deployable Maintenance Analysis Group
JDS	Joint Deployment System
JDSS	Joint Decision Support System
JDSIR	Joint Deployment System Incident Reporting System
JDSSC	Joint Data System Support Center
JEAP	(1) Joint Electronic Analysis Program; (2) Joint Electronic Analysis Position
JEC	Joint Economic Committee
JECC(G)	Joint Exercise Control Center (Group)
JECG	Joint Exercise Control Group
JECM	Joint Electronic Countermeasures
JEEP	Joint Emergency Evacuation Plan
JEIO	Joint Engineering and Interoperability Organization
JEFPROS	JAC EUCOM Force Protection Summary
JEIR	JAC EUCOM Intelligence Review
JEL	Joint Electronic Library
JEM	Joint Exercise Manual
JES	JDISS Embedded Support
JESS	Joint Exercise Support System
JET	JWICS Earth Terminal
JETDS	Joint Electronics Designation System
JEWC	Joint Electronic Warfare Center
JFACC	Joint Force Air Component Commander
JFC	(1) Joint Fusion Center; (2) Joint Force Commander
JFFC	Joint Force Fires Coordinator
JFFSC	Joint Force Fire Support Coordinator
JFI	Joint Force Integrator
JFIC	Joint Force Interdiction Coordinator
JFITL	Joint Force Integrator Task List
JFK CTRMA	John F. Kennedy Center for Military Assistance
JFLCC	Joint Force Land Component Commander
JLOTS	Joint Logistics Over the Shore
JFM	Joint Force Memorandum
JFMCC	Joint Force Maritime Component Commander
JFMO	Joint Frequency Management Office
JFSOCC	Joint Force Special Operations Component Commander
JGITSS	Joint General Intelligence Training System Subarchitecture

JGSDF	Japanese Ground Self-Defense Forces
JIATF	Joint InterAgency Task Force
JIATF-E	Joint InterAgency Task Force - East
JIATF-W	Joint InterAgency Task Force - West
JIB	Joint Intelligence Bureau (Commonwealth Countries)
JIC	(1) Joint Intelligence Center; (2) Joint Interrogation Center; (3) Joint Intelligence Cell
JIC-E	Joint Intelligence Center-Europe
JIC-SOUTH	Joint Intelligence Center-U.S. SOUTHCOM
JIC-2000	Designation of JICSOUTH upon movement to CONUS
JICEUR	Joint Intelligence Center Europe
JICPAC	Joint Intelligence Center Pacific
JICREP	Joint Intelligence Center Report
JICTRANS	Joint Intelligence Center for Transportation
JIEO	Joint Interoperability Engineering Organization (DISA)
JIEP	Joint Intelligence Estimate for Planning
JIF	Joint Interrogation Facility
JIFF	Joint Interdiction of Follow-on Forces
JIIKS	Joint Imagery Interpretation Key Structure
JIIM	Joint Intelligence Information Management
JILE	Joint Intelligence Liaison Element
JIM	JESS Intelligence Model
JINTACCS	Joint Interoperability of Tactical Command and Control Systems
JINTC	Joint Intelligence Task Force
JIO	Joint Intelligence Organization
JIOC	Joint Intelligence Operations Center
JIPC	Joint Imagery Production Center
JIPTL	Joint Integrated Prioritized Target List
JISA	Joint Intelligence Support Architecture
JISAD	JTF Intelligence Support Architecture Document
JISC	(1) Joint Intelligence Support Center; (2) Joint Intelligence Support Concept
JISE	Joint Intelligence Support Element
JISI	Joint Intelligence System Integration
JISS	Japan Intelligence Support System
JITAP	Joint Intelligence Training Activity Pacific
JITC	Joint Interoperability Test Center (DISA)
JITF	Joint Integration Testing Facility
JIVA	Joint Intelligence Virtual Architecture
JLA	Joint Logistics Assessment
JLARG	Joint Logistics Assessment Review Group
JL-COE	Joint Logistics Center of Excellence
JLD	Joint Liaison Detachment
JLE	Jammer Locator Electronics
JLMIS	Joint Logistics Management Information System

JLOTS	Joint Logistics Over the Shore
JLPPG	Joint Logistics and Personnel Policy and Guidance
JLRC	Joint Logistics Readiness Center
J4/LRC	Joint Logistics Readiness Center
JLREID	Joint Long-Range Estimating Intelligence Document (JSPS)
JLRSA	Joint Long-Range Strategic Appraisal
JLSP	Joint Logistics Steering Panel
JM	Joint Mission
JMA	(1) Joint Mobilization Augmentation; (2) Joint Mission Analysis
JMAT	Joint Mobility Assistance Team
JMC	Joint Movement Center
JMCC	(1) Joint MC&G Coordination Center; (2) Joint Mobile Command Center
JMCIS	Joint Maritime Command Information System
JMEM	Joint Munitions Effectiveness Manual
JMENS	Joint Mission Element Needs Statement
JMETL	(1) Joint Mission Essential Target List; (2) Joint Mission Essential Task List
JMI	JTIDS Modular AOC Integration System
JMIC	Joint Military Intelligence College
JMICS	JWICS Mobile Integrated Communications System
JMIE	Joint Maritime Information Element
JMIE/JEM	JMIE Support System and Modernization
JMINI	Joint UHF MILSATCOM Network Integrated
JMIP	Joint Military Intelligence Program
JMISE	Joint Military Intelligence Support Element
JMITC	Joint Military Intelligence Training Center
JMNS	Joint Mission Needs Statement
JMO	Joint Management Office
JMOCC	Joint Mobile Operations Command Center
JMP	(1) Joint Manpower Program; (2) Joint Mobilization Program
JMPAB	Joint Material Priorities Allocation Board
JMPP	Joint Munitions Production Panel
JMRR	Joint Military Readiness Review
JMSDF	Japan Maritime Self-Defense Force
JMSIP	Joint Modeling and Simulation Integration Program
JMSNS	Justification for Major System New Start
JMST	Joint Management Support Tool
JMTB	Joint Military Transportation Board
JMTG	(1) Joint Military Terminology Group; (2) Joint Master Training Guide
JMTK	Joint Mapping Tool Kit
JNACC	Joint Nuclear Accident Coordinating Center
JNAF	Yugoslavia National Air Force
JNC	Jet Navigation Chart

JNC-A	Jet Navigation Chart-Air
JNIDS	(1) Joint National Intelligence Dissemination System; (2) Joint National Intelligence Development Staff
JNPE	Joint Nuclear Planning Element
JOA	Joint Operations Area
JOC	Joint Operations Center
JOC/INT	Joint Operations Center/Intelligence Team
JOG	Joint Operations Graphic
JOG-A	Joint Operations Graphic-Air
JOG-C	Joint Operations Graphic-Combined
JOG-G	Joint Operations Graphic-Ground
JOG-R	Joint Operations Graphic-Radar
JOIC	Joint Operational Intelligence Center/Cell
JOIN	Joint Operations Intelligence Network
JOINT REDTRAIN	Joint Readiness Training
Joint STARS	Joint Surveillance Target Attack Radar System
JOP	Joint Operating Procedure
JOPES	Joint Operations Planning and Execution System
JOPS	Joint Operational Planning System
JOS	Joint Operational Stocks
JOSE	Joint Operations Support Element
JOTS	Joint Operational Tactical System
JP	(1) Jet Petroleum; (2) Joint Publication
JPAM	Joint Program Assessment Memorandum
JPAT	Joint Planning and Assistance Team
JPD	Joint Planning Document
JPEA	Joint Planning and Exercise Activity
JPEC	Joint Planning and Execution Community
JPL	Jet Propulsion Laboratory
JPM	Joint Program Manager
JPMIE	Joint Program for Military Intelligence Education
JPMO	Joint Program Management Office
JPN	JSIC Peterson Node
JPO	Joint Project Office
JPOTF	Joint Psychological Operations Task Force
JPOTG	Joint Psychological Operations Task Group
JPPR	Joint Planning and Program Review
JPRS	Joint Publications Research Service
JPSD	Joint Precision Strike Demonstration
JPSS	Joint Planning Staff for Space
JPSIO	Joint Precision Strike Integration Office
JRA	Joint Rear Area
JRB	Joint Reconnaissance Board
JRC	(1) Joint Reconnaissance Center; (2) Joint Recovery Center
JRCB	Joint Reconnaissance Coordination Board

JRCC	Joint Rescue Coordination Center
JRCP	Joint Readiness Command Program
JRDC	Joint Regional Defense Command
JRDOD	Joint Research and Development Objectives Document
JRFL	Joint Restricted Frequency List
JRIP	Joint Reserve Intelligence Program
JRMB	Joint Requirements and Management Board
JRO	Joint Reconnaissance Office
JROC	Joint Requirements Oversight Council
JROC-B	Joint Refugee Center, Berlin
JRS	Joint Reporting System/Structure
JRSC	Jam-Resistant Secure Communications
JRTC	(1) Joint Readiness Training Center; (2) Joint Regional Training Center
JRTC-IS	JRTC Instrumentation System
JRX	Joint Readiness Exercise
JRX MILES	JRX Milestone System
JS	Joint Staff
J/S	Ratio of received power level of a jamming signal and a desired signal
JSAJAC	Security Activity
JSAC	Joint State Area Command
JSAM	Joint Security Assistance Memorandum
JSAMSA	Joint Security Assistance Memorandum Supporting Analysis
JSB	Joint Synthetic Battlespace
JSC	(1) Lyndon B. Johnson Space Center; (2) Joint Spectrum Center
JSCP	Joint Strategic Capabilities Plan
JSCS	Joint Strategic Connectivity Staff
JSDF	Japanese Self-Defense Forces
JSEAD	(1) Joint Surveillance Enemy Air Defense; (2) Joint Suppression of Enemy Air Defenses
JSFC	Joint Space Fundamentals Course
JSIC	Joint SPACECOM Intelligence Center
JSIMS	Joint Simulation System
JSIOC	Joint Space Intelligence Operations Course
JSIOPC	Joint Space Intelligence Operations Policy Course
JSIP	Joint Services Imagery Processor
JSIPS	Joint Service Imagery Processing System
JSIPS-N	Joint Service Imagery Processing System-Navy
JSMB	Joint Space Management Board
JSO	(1) Joint Staff Office; (2) Joint Support Office
JSOA	(1) Joint Special Operations Agency; (2) Joint Special Operations Area
JSOACC	Joint Special Operations Air Component Commander
JSOC	(1) Joint Special Operations Center; (2) Joint Strategic Operations Center; (3) Joint Special Operations Command

JSODC	Joint Special Operations Deception Course
JSOFI	Joint Special Operations Forces Institute
JSOIC	Joint Special Operations Intelligence Course
JSOIT	Joint Special Operations Intelligence Training
JSOIO	Joint Special Operations Intelligence Orientation
JSOP	Joint Strategic Objectives Plan
JSOPW	Joint Special Operations Planning Workshop
JSOR	Joint Service Operational Requirement
JSOSOC	Joint Special Operations Staff Officer Course
JSOTF	Joint Special Operations Task Force
JSOTFSO	Joint Special Operations Task Force South
JSOTP	Joint Special Operations Training Project
JSOW	Joint Standoff Weapon
JSPD	Joint Strategic Planning Document
JSPDSA	Joint Strategic Planning Document Supporting Analysis
JSPO	Joint System Program Office
JSPS	Joint Strategic Planning System
JSR	(1) Joint Strategy Review; (2) Joint Special Reports
JSRC	Joint Search and Rescue Center
JSS	(1) Joint Surveillance System; (2) JMIE Support System
JSST	(1) Joint Space Support Team; (2) Joint Special Support Team
JSTARS	Joint Surveillance and Target Attack Radar System
JSTPS	Joint Strategic Target Planning Staff
JSWG	(1) J-TENS Special Working Group; (2) Joint Service Working Group
JT	Joint
JTA	(1) Joint Task Analysis; (2) Joint Table of Allowances
JTAGS	Joint Tactical Ground Station
JTAO	Joint Tactical Air Operations
JTARS	Joint Tactical Aerial Reconnaissance System
JTASC	Joint Training, Analysis and Simulation Center
JTB	(1) Joint Transportation Board; (2) Joint Targets Board
JTC	(1) Joint Target Committee; (2) Joint Technology Center; (3) JFACC Target Cell
JTC3A	Joint Tactical Command, Control, and Communications Agency
JTCAE	Joint Tactical Control and Analysis Element
JTCB	Joint Targets Coordination Board
JTCG	Joint Technical Coordinating Group
JTCG(ME)	Joint Technical Coordinating Group (For Munitions Effectiveness)
JTC/SIL	Joint Technology Center/ Systems Integration Laboratory
JTD	Joint Table of Distribution (Manning Authorization for a Joint Organization)
JTDA	Joint Table of Distribution and Allowances
JTEB	Joint Test and Evaluation Board
J-TENS	Joint Tactical Exploitation of National Systems

JTENS	Joint-Service Tactical Exploitation of National Systems
JTF	(1) Joint Tactical Fusion; (2) Joint Task Force
JTF-6	Joint Task Force-6
JTF-B	USSOUTHCOM JTF in Honduras
JTFCEM	Joint Task Force Contingency Engineer Manager
JTF-FA	Joint Task Force-Full Accounting
JTF-LOCE	Joint Tactical Fusion-Limited Operational Capability Europe
JTF-PM	Joint Task Force-Panama
JTFPO	Joint Tactical Fusion Program Office
JTF-PP	Joint Task Force PROVIDE PROMISE
JTF-SWA	Joint Task Force-South West Asia
JTFHQ	Joint Task Force Headquarters
JTFP	Joint Tactical Fusion Program
JTFPMO	Joint Tactical Fusion Program Management Office
JTFSO	Joint Task Force South
JTG	Joint Task Group
JTIC	Joint Transportation Intelligence Center
JTID	Joint Digital Team Information Device
JTIDS	Joint Tactical Information Distribution System
JTL	Joint Target List
JTMD	(1) Joint Theater Missile Defense; (2) Joint Table of Mobilization and Distribution
JTN	Joint Targeting Network
JTOSS	Joint Task-Organized Software Subsystem
JTP	Joint Training Plan
JTR	Joint Travel Regulation
JTRU	Joint Transportation Reserve Unit
JTSC	Joint Technology Steering Committee
JTSG	Joint Targets Steering Group
JTT	Joint Tactics Terminal
JTTP	Joint Tactics, Techniques and Procedures
JTWS	Joint Threat Warning System
JTX	Joint Training Exercise
JUAVTC	Joint UAV Training Center
JUDI	Joint Universal Data Interpreter
JULL	Joint Universal Lessons Learned
JULLS	Joint Universal Lessons Learned System
JUMPS	Joint Uniform Military Pay System
JUSMAG	Joint United States Military Advisory Group
JUWC	Joint Unconventional Warfare Command
JUWTF	Joint Unconventional Warfare Task Force
JVIDS	Joint Visual Integrated Display System
JWAC	Joint Warfare Analysis Center
JWARS	Joint Warfare Simulation
JWBCA	Joint Whole Blood Control Agency

JWC	(1) Joint Warfare Center; (2) Joint Working Group
JWCA	Joint Warfighting Capability Assessment
JWFC	Joint Warfighting Center
JWG	Joint Working Group
JWICS	(1) Joint Warning Indications Communications System; (2) Joint Worldwide Intelligence Communications System
JWID	Joint Worldwide Interoperability Demonstration
J2X	JTF J2 Support Element

K

K	Kelvin (absolute temperature scale)
KAC	Korea Analysis Center
KADIZ	Korean Air Defense Identification Zone
KAIS	Korean Air Intelligence System
KAK	Key-Auto-Key
KAL	Key Asset List
KALCC	Korean Airlift Control Center
KAPP	Key Asset Protection Program
KAWS	Korean Analyst Workstation
KB	(1) Kilobyte; (2) Knowledgeability Brief
Kbps	Kilobits Per Second (also KPS)
KBS	Knowledge-Based System
KBYTES	Kilobytes
KCG	Korean Consultative Group
KCIA	Korean Central Intelligence Agency
KCOIC	Korean Combat/Combined Operations Intelligence Center
KCSS	Korean Combat Support System
KDC	Key Distribution Center
KDEI	Key Defense Estimates Issues
KDIA	Korean Defense Intelligence Agency
KDII	Key Defense Intelligence Issues
KE	Kinetic Energy
KEK	Key Encryption Key
KELP	Kaleidoscope Elint Processor
KEW	Kinetic Energy Weapon
KG	(1) Kilogram; (2) Key Generator
KGB	Committee for State Security (FSU)
KH	Keyhole
KHA	Killed by Hostile Action
KHz	Kilohertz
KIA	Killed in Action
KIA-BNR	Killed in Action, Body Not Recovered
KIAS	Knots Indicated Air Speed
KIES	Kodak Imagery Exploitation System
KIEWS	Kodak Imagery Edit Workstation
KILLREP	Kill Report
KILLSUM	Kill Summary
KILOD	Killed in the Line of Duty
KIP	(1) Key Intelligence Position; (2) Key Indigenous Personnel
KIPPL	Key Intelligence Program Priorities List
KISS	Korean Intelligence Support System
KIWS	KISS Intelligence Workstation
KJ	(1) Kilojoules; (2) Key Judgments

KM	Kilometer
KMASE	Key Management Application Service Element
KMC	Key Management Center
KM/HR	Kilometers Per Hour
KMODC	Key Management Ordering and Distribution Center
KMID	Key Management Identification Number
KMP	Key Management Protocol
KMPDU	Key Management Protocol Data Unit
KMR	Kwajalein Missile Range
KMS	Key Management System
KMSA	Key Management System Agent
KMUA	Key Management User Agent
KN	Knot
knots	Nautical Miles per hour
KP	Key Processor
KPH	Kilometers Per Hour
KPK	Key Production Key
KS	South Korea (ROK)
KSA	Knowledge, Skills, and Abilities
KSC	Kennedy Space Center
KSOS	Kernelized Secure Operating System
KT	(1) Kiloton; (2) Knot
KTAS	Knots True Airspeed
KTO	Kuwait Theater of Operations
KTTP	Korean Tactics, Techniques, and Procedures
Ku	A Satellite Frequency Band
KUSLO	U.S. Liaison Office-Kenya
KW	Kilowatt
KWH	Kilowatt Hours
KVG	Key Variable Generator

L

LAAIB	Latin American Air Intelligence Brief
LAAM	Light Anti-Aircraft Missile
LAB	Laboratory
LABS	Laboratories
LAD	Launch Assist Device
LADD	Low Angle Drogue Delivery
LAEO	Low-Altitude Electro-Optical
LAEWWING	Light-Airborne Early Warning Wing
LAF	Launch Alert Folder
LAFTA	Latin America Free Trade Association
LAGEOS	Laser Geodynamic Satellite
LAI	(1) Light Armored Infantry; (2) Look-Down Air Intercept
LAL	Library Accessions List
LALO	Low-Altitude Low-Opening
LAM	Louisiana Maneuvers
LAMM	Land Armament and Manpower Model
LAMP	Lockwood Analytical Method for Prediction LAMPS (1) Light Airborne Multipurpose System; (2) LANTCOM Message Processing System
LAN	Local Area Network
LANDCENT	Land Forces Central Region
LANDSAT	Land Satellite (Commercial Multi-Spectral)
LANDSOUTH	Land Forces Southern Region
LANFORSIXTHFLT	Landing Force Sixth Fleet
LANL	Los Alamos National Laboratory
LANT	Atlantic
LANTAF	Atlantic Command Air Forces
LANTAREA	Atlantic Area
LANTCOM	Atlantic Command (now ACOM)
LANTCOMDIS	Atlantic Command Deployable Intelligence System
LANTCOM JIC	Atlantic Command Joint Intelligence Center (AIC)
LANTDAC	Atlantic Command Defense Analysis Center
LANTDIS	USACOM Deployable Intelligence System
LANTFLT	U.S. Atlantic Fleet
LANTIRN	Low-Altitude Navigation and Targeting Infrared System for Night
LANTIS	Atlantic Intelligence Supplement
LANUP	Local Area Network Upgrades
LANWAN	Local Area Network/Wide Area Network
LAR	Laser-Aided Rocket

LARB	Light Amphibious Reconnaissance Battalion
LARS	Light Artillery Rocket System
LAS	Land Analysis System
LASA	Light Armed Surveillance Attack
LASER	Light Amplification by Stimulated Emission of Radiation
LASERFAX	Secure System for Transmitting Photos
LASH	Lighter Aboard Ship
LASINT	Laser Intelligence
LASTE	Low-Altitude Safety Targeting Enhancement
LAT	Latitude
LATAM	Latin America
LATIN	Atlantic Command Theater Intelligence Network
LATS	Large Aperture Tracking System
LATWING	Light Attack Wing
LAV	Light Armored Vehicle (non-tactical)
LAW	Light Antitank Weapon
LAWS	Long-Range Cruise Missile Analysis and Warning System
LB	Live Broadcast
Lb	Pound
L-BAND	1 to 2 GHz
LBR	Laser Beam Recorder
lbs (LB)	Pounds
LBSR	Lightweight Battlefield Surveillance Radar
LC	(1) Library of Congress; (2) Line of Contact
LCAC	Landing Craft, Air Cushion
LCC	(1) Amphibious Command Ship; (2) Logistics Coordination Center; (3) Launch Control Center; (4) Land Component Commander
LCC-IC	Amphibious Command Ship-Intelligence Center
LCD	Liquid Crystal Display
LCE	Liaison Coordination Element (Special Operations Liaison Team in Coalition Operations)
LCF	Launch Control Facility
LCM	(1) Medium Landing Craft; (2) Life Cycle Management
LCP	(1) Personnel Landing Craft; (2) Launching Control Post
LCPR	Ramped Personnel Landing Craft
LCS	Low-Cost Satellite
LCSMM	Life Cycle Support Management Model
LCSR	Swimmer Reconnaissance Landing Craft
LCU	(1) Utility Landing Craft; (2) Launch Correlation Unit
LCW	Special Warfare Support Craft
LCWS	Low-Cost Workstation
LD	(1) Line of Departure; (2) Laser Defense
LDC	(1) Less-Developed Country; (2) Local Data Concentrator; (3) Light-Weight Deployable Communication; (4) Land Defense of CONUS

LDEF	Long Duration Exposure Facility
LDF	Lightweight Digital Facsimile
LDIS	Library Document Inventory System
LDM	Limited Distance Modems
LDMX	Local Digital Message Exchange
LDR	Low Data Rate
LDS	Laser Detection System
LDSD	Lookdown/Shootdown
LDT	Large Diameter Target
LDX	Long-Distance XEROX
LEA	Law Enforcement Agency
LEAD	(1) Low-Cost Encryption/Authentication Device; (2) List of Emerging Activations and Dispositions
LEAF	Law Enforcement Access Field
LEASAT	(1) Leased Satellite; (2) Leased System
LED	Light Emitting Diode
LEDS	Link 11 Display System
LEM	Land Engagement Model
LEN	Large Extension Node
LENSCE	Limited Enemy Situation Correlation Element
LEP	Linear Error Probable
LEPCU	Lightweight Environmental Protection Combat Uniform
LEO	Low Earth Orbit
LEO COM	Low Earth Orbit Data Communications
LERTCON	Alert Condition
LES	(1) Leading Edge Services; (2) Land Earth Station; (3) Limited Effects Submunition
LEW	Limited Effects Weapons
LEXIS	Meade Data Central Legal Service
LF	(1) Low Frequency; (2) Launch Facility; (3) Landing Force
LF6F	Landing Force 6th Feet
LFC	Large Format Camera
LFICS	Landing Force Integrated Communications System
LFM	Landing Force Manual
LFOC	Landing Force Operations Center
LFOV	Limited Field of View
LFR	Inshore Fire Support Ship
LFRSV	Launch-Fly-Recover Space Vehicle
LFS	Amphibious Warfare Fire Support Ship
LG	ACC Director of Logistics
LGB	Laser-Guided Bomb
LHA	Amphibious Assault Ship (General Purpose)
LHA-IC	Amphibious Assault Ship (General Purpose)-Intelligence Center
LHD	Multi-Purpose Amphibious Assault Ship
L-HOUR	Hour on C-Day when deployment begins

LHR	Low Hop Rate
LHW	Lower High Water
LHX	Lightweight Helicopter
LIC	Low-Intensity Conflict
LIDAR	Light Detection and Ranging
LIGHTSAT	Lightweight Satellite
LIMDIS	(1) Limited Dissemination; (2) Limited Distribution
LIME	Laser-Induced Magnetic Emissions
LIMMER	Limited Control of Merchant Shipping
LIN	LANTCOM Intelligence Network
LINCS	Long-Range Intelligence Networked Communications Service
LIR	Launch and Impact Report
LISS	LANTCOM Intelligence Support System
LITE	Laptop Imagery Transmission Equipment
LITES	Laser Intercept and Technical Exploitation System
LITINT	Literature Intelligence
LIVID	Language Identification and Voice Identification
LIWA	Land Information Warfare Activity
LJ	Laser Jet
LKA	Amphibious Cargo Ship
LKG	Loop Key Generator
LL	(1) Landline; (2) Latent Lethal Dose
LLLTV/IR	Low-Light-Level TV/Infrared
LLSO	Low-Level Source Operations (CI/HUMINT)
LLTV	Low-Light-Level Television
LLNL	Lawrence Livermore National Laboratory
LLO	Land Liaison Office
LLW	Lower Low Water
LLVI	Low-Level Voice Intercept
LMBB	GENSER Intelligence Broadcast
LMCC	LOCE Mobile Correlation Center
LMD	Local Management Device
LMD-KP	Local Management Device/Key Processor
LME	Layer Management Entry
LMI	Layer Management Interface
LMR	Land Mobile Radio
LMRDFS	Lightweight Man-Transportable Radio Direction Finding System
LMS	(1) Local Monitor Station; (2) Least Means Squared
LMSR	Large Medium Speed RO/RO
LNA	Low Noise Amplifier
LNE	Liaison Element
LNG	Liquefied Natural Gas
LNIS	Atlantic Command Naval Intelligence Summary
LNO	(1) Limited Nuclear Option; (2) Liaison Officer

LNU	Last Name Unknown
LO	(1) Liaison Officer; (2) Low Observables
LO/LO	Lift-On/Lift-Off
LOA	(1) Letter of Agreement; (2) Lead Operational Authority; (3) Letter of Assist
LOAC	Law of Armed Conflict
LOB	Line of Bearing
LOC(S)	(1) Line(s) of Communication; (2) Library of Congress; (3) Launch Operations Center; (4) Liaison Officer Coordinator; (5) Location; (6) ILS Localizer
LOCD	Lines of Communication Designators
LOCE	(1) Limited Operational Capability, Europe; (2) Linked Operations-Intelligence Centers Europe
LOCK	Logical Co-Processing Kernel
LOD	Low-Observable Demonstrations
LOFAR	Low-Frequency Analysis and Recording
LOG	Logistics
LOGCAP	Logistics Civil Augmentation Program
LOGEX	Logistics Exercise
LOGS	Logistics
LOI	(1) Letter of Instruction; (2) Location of Interest
LON	Longitude
LONG	Longitude
LORAD	Long-Range Air Defense
LORAN	Long-Range Navigation
LOROP	Long-Range Oblique Photography
LOROPS	(1) Long-Range Optical System; (2) Long-Range Oblique Photographic Sensor
LOS	(1) Line of Sight; (2) Law of the Sea
LOTS	(1) Lighter Over the Shore; (2) Logistics Over the Shore
LOW	(1) Laws of War; (2) Launch on Warning
LOX	Liquid Oxygen
LP	Listening Post
LPA	Amphibious Personnel Transport
LPAR	Large Phased-Array Radar
LPC	Linear Predictive Coding
LPD	(1) Amphibious Assault Transport Dock; (2) Low Probability of Detection
LPD/I	Low Probability of Detection/Intercept
LPF	Low Pass Filter
LPG	Liquefied Natural Gas
LPH	Amphibious Assault Ship (Helicopter)
LPI	(1) Low Probability Intercept; (2) Lines per Inch
LPO	Leading Petty Officer
LPR	Amphibious Transport (Small)
LPS	(1) Logistics Planning Study; (2) Large Processing Station

LPSS	Amphibious Transport Submarine
LPT	Logistics Preparation of the Theater
LRA	Long-Range Aviation (FSU)
LRAA	Long-Range Air Army (FSU)
LRAACA	Long-Range Air-ASW Capable Aircraft
LRAAM	Long-Range Air-to-Air Missile
LRC	(1) Logistics Readiness Center; (2) Logistics Resupply Center; (3) Lesser Regional Contingency; (4) Limited Regional Conflict; (5) Limited Regional Contingency
LRCM	Long-Range Cruise Missile
LRCS	Light-Reaction Communications System
LRE	Launch and Recovery Element
LREO	Long Range Electro-Optical
LRINF	Longer Range Intermediate-Range Nuclear Forces
LRIP	Limited/Low-Rate Initial Production
LRL	Low-Cost Receive Location
LRM	Low-Rate Multiplexer
LRP	(1) Low-Rate Production; (2) Long-Range Plan; (3) Limited Response Package
LRR	Long-Range Reconnaissance
LRRP	Long-Range Reconnaissance Patrol
LRSC	Long-Range Surveillance Company
LRSO	Long-Range Surveillance Out-Post
LRSP	(1) Long-Range Surveillance Plan; (2) Long-Range Systems Plan
LRSPRAC	Long-Range Special Reporting and Coordination
LRSTIA	Long-Range Scientific and Technical Intelligence Assessment
LRSU	Long-Range Surveillance Unit
LRTNF	Long-Range Theater Nuclear Forces
LRU	Line-Replaceable Unit
LSA	(1) Logistics Support Analysis; (2) LAN Systems Administrator
LSB	Lower Sideband
LSC	Linear Shaped Charge
LSCS	Logistics Support Command, Somalia
LSD	(1) Landing Ship, Dock; (2) Lease Separation Distance
LSDV	Swimmer Delivery Vehicle
LSE	Logistic Support Element
LSG	Large-Scale Graphics
LSI	Large-Scale Integration
LSM	Medium Amphibious Assault Landing Ship
LSP	Launch Sequence Plan
LSS	Library Support System
LSSA	Logistic System Support Activity
LSSC	Light Seal Support Craft
LST	(1) Amphibious Vehicle Landing Ship; (2) Local Standard Time
LST-5C	Deployable Satellite Terminal

LSV	Light Strike Vehicle
LT	(1) Light Table (2) Light
LTAC	Land Terminal Access Control
LTAS	Lightweight Tactical Army Satellite Communications System
LTBT	Limited Test Ban Treaty
Ltd	Limited
LTDP	NATO Long-Term Defense Program
LTDS	Laser Target Designator System
LTI	Lightweight Thermal Imager
LTID	Laser Target Interface Device
LTIOV	Latest Time Information of Value
LTMS	Light Table Mensuration System
LTOE	Living Table of Organization and Equipment
LUA	Launch Under Attack
LUT	Limited User Test
LVDS	Low-Volume Dissemination System
LW	Low Water
LWA	Light Weight Aircraft
LWIR	Long-Wavelength Infrared
LWM	Lightweight Motor
LWOP	Leave Without Pay
LWR	Lutheran World Relief, Inc
LWT	Amphibious Warping Tug
LZ	Landing Zone
LZCT	Landing Zone Control Team

M

3M	Material, Maintenance, Management
M	(1) Meter; (2) Mach; (3) Mega (Million)
M1A1	M1A1 ABRAMS Tank
MA	Mission Assessment
MAA	Mission Area Analysis
MAAG	Military Assistance Advisory Group
MAAP	Master Air Attack Plan
MAB	Marine Amphibious Brigade
MAC	(1) Military Airlift Command (now AMC); (2) Mobile Inshore Undersea Warfare Attack Craft; (3) Multi-Array Correlator; (4) Missile Analysis Center; (5) Mandatory Access Control; (6) Message Authentication Code; (7) Military Areas of Coordination
MAC-IN	Military Airlift Command-Director of Intelligence
MACA	Military Assistance to Civil Authorities
MACCOM	MAC Communications (Network)
MACCS	Marine Aviation Command and Control System
MACDIS	Military Assistance to Civil Disturbances
MACLO	MAC Liaison Officer
MACOM	(1) Major Army Command; (2) Major Command
MACSAT	Multiple Access Communications Satellite
MAD	(1) Magnetic Anomaly Detector; (2) Mutual Assured Destruction
MADP	Military Attache for Defense Programs
MAE	(1) Mean Area of Effectiveness; (2) Medium Altitude Endurance UAV (formerly Tier II)
MAEO	Medium-Altitude Electro-Optical
MAE-UAV	Medium-Altitude Endurance Unmanned Aerial Vehicle
MAF	Marine Amphibious Force
MAFC	MAGTF All-Source Fusion Center
MAG	(1) Marine Aircraft Group; (2) Military Assistance Group; (3) Military Advisory Group; (4) Magnetic
MAGIC	Maritime Air-Ground Intelligence Cell
MAGIIC	Mobile Army Ground Imagery Interpretation Center
MAGIS	Marine Air-Ground Intelligence System
MAGR	Miniature Airborne GPS Receiver
MAG Tape	Magnetic Tape
MAGTF	(1) Marine Air-Ground Task Force; (2) Marine Amphibious Ground Task Force
MAINT	Maintenance
MAIS	Military Airlift Intelligence System
MAISRC	Major Automated Information System Review Council
MAJCOM	(1) Major Air Force Command; (2) Major Command
MAMS	MASINT Automated Management System
MAN	(1) Mandatory Modification; (2) Metropolitan Area Network

MANPADS	Manportable Air Defense System
MANPRINT	Manpower and Personnel Integration
MAO	Major Attack Option
MAOC	Modular Air Operations Center
MAP	(1) Military Assistance Program; (2) Ministry of Aviation Industry (USSR); (3) Multiple Aim Point; (4) Master Attack Plan; (5) Materiel Acquisition Process
MAPREQ	Map Requisition System
MARAD	Maritime Administration
MARC	MAC ALCE Reaction Communications System
MARCENT	Marine Forces Central Command
MARCORSYSCOM	Marine Corps Systems Command
MARE	Mission Analysis Report-Electrical
MARECS	Maritime European Communications Satellite
MARDEZ	Maritime Defense Zone
MARDEZLANT	Maritime Defense Zone, Altantic
MARDIV	Marine Division
MARFOR	Marine Forces
MARFOREUR	Marine Forces Europe
MARFOR-K	Marine Forces Korea
MARFORCENT	Marine Forces, Central Command
MARFORLANT	Marine Forces Atlantic
MARFORPAC	Marine Forces Pacific
MARFORSOUTH	Marine Forces, Southern Command
MARG	(1) Marine Amphibious Readiness Group; (2) Marginal
MARINETERP	Westlant Maritime Intelligence Report
MARINTSUM	Maritime Intelligence Summary
MARISAT	Maritime Satellite (COMSAT)
Mark-Up	Detailed Budget Recommendation from a Congressional Committee
MARPAC	Marine Forces Pacific
MARREP	Maritime Report
MARS	(1) Man-hour Accounting and Reporting System; (2) Military Affiliate Radio System; (3) Monthly Aerial Reconnaissance Summary
MART	Mobile Autodin Record/Remote Terminal
MARV	Maneuverable Reentry Vehicle
MAS	(1) Military Airlift Squadron; (2) Measurement and Signature; (3) Message Analysis Server; (4) Military Agency for Standardization
MASDR	Measurement and Signature Data Requirements
MASH	Mobile Army Surgical Hospital
MASINT	Measurement and Signature Intelligence
MASS	(1) Matrix Analysis Subsystem; (2) Missile and Space Summary
MASST	Major Ship Satellite Terminal
MAST	(1) Mobile Ashore Support Terminal; (2) Manual Acquisition Satellite Track; (4) MILSTAR Advanced Satellite Terminals

MAT	Medium Assault Transport
MATB	Multi-Spectral Analyst Test Bed
MATC	Armored Troop Carrier, Mini
MATDEV	Materiel Developer
MATRIX	Multi-source Automatic Target Recognition with Interactive Exploitation
MATS	Mobile Automatic Telephone System
MATSYM	Material Symbol
MATT	Multi-Mission Advanced Tactical Terminal
MATWING	Medium Attack Wing
MAU	Marine Amphibious Unit
MAVUS	Maritime Vertical Takeoff and Landing Unmanned Aerial Vehicle System
MAW	(1) Military Airlift Wing; (2) Marine Aircraft Wing
MAWTS	Marine Aviation Weapons and Tactics Squadron
MAXI	Modular Architecture for the Exchange of Intelligence
MB	(1) Megabit; (2) Meteor Burst; (3) Megabits
Mb	Megabyte
MBA	(1) Main Battle Area; (2) Multiple Beam Antennae
MBB	Modular Building Block (of EIF/ECMC)
MBC	Meteor Burst Communications
MBFR	Mutual and Balanced Force Reduction
MBITR	Multiband Inter Team Radio
MBO	Management by Objective
MBMR	Multiband Multimode Radio
MBPS	Megabytes per Second
MBRADIO	Multiband Radio
MBT	Main Battle Tank
MBYTES/Mbyte	Megabytes
MC	(1) Military Committee; (2) Mobility Corridor; (3) Joint Military Intelligence College; (4) Multi-Channel MC&G Mapping, Charting and Geodesy
MCA	(1) Maritime Collection Assets; (2) Military Capabilities Assessment; (3) Military Civil Action; (4) Mission Concept Approval
MCAR	Multi-Channel Acoustic Relay
MCAS	Marine Corps Air Station
MC ASI	Marine Corps Assistant Chief of Staff Intelligence
MCB	(1) Markings Center Brief; (2) Marine Corps Base
MCC	(1) Mobile Command Center; (2) Movement Control Center; (3) Mission Control Complex; (4) Military Coordination Center; (5) Mission Control Cell; (6) Mission Control Center
MCCB	Modification/Configuration Control Board
MCCC	Mobile Consolidated Command Center (USSPACECOM)
MCCP	Marine Corps Campaign Plan
MCCS	Mobile Command and Control System
MCCT	Mobile Command Communications Team
MCDN	Marine Corps Data Network

MCDS	Multilateral Counterterrorism Data System
MCE	(1) Mission Control Element; (2) Modular Control Equipment
MCEB	Military Communications Electronics Board
MCG	(1) Magneto Cumulative Generator; (2) Minimum Character Grid; (3) Monitor Control Group; (3) Mapping, Charting, and Geodesy
MCG&I	Mapping, Charting, Geodesy, and Imagery
MCIA	Marine Corps Intelligence Activity
MCM	(1) Mine Countermeasures; (2) Military Committee Memorandum; (3) Multi-Command Manual; (4) Chairman of the Joint Chiefs of Staff Memorandum (Designator)
MCMIP	Marine Corps Master Intelligence Plan
MCO	MASINT Control Officer
MCOO	Modified Combined Obstacles Overlay
MCP	Mobile Command Post
MCR	Military Command Region
MCRB	Military Costing Review Board
MCRC	Master Control and Reporting Center
MCRD	Marine Corps Recruit Depot
MCRP	Mobilization Command Readiness Program
MCS	(1) Mine Countermeasures Support Ship; (2) Military Capabilities Study; (3) Maneuver Control System; (4) Master Control Station; (5) Mission Control Segment
MCSF	Mobile Cryptologic Support Facility
MCSFBN	Marine Corps Security Force Battalion
MCSP	Mobile Communications Support Package
MCST	Magnetic Card Selectric Typewriter (IBM)
MCT	Mobile Communications Terminal
MCTL	(1) Mediterranean Contingency Target List; (2) Military Critical Technologies List
MCU	Mobile Communications/Command Unit
MCW	Modulated Continuous Wave
MD	(1) Military District; (2) Map Distance; (3) Mission Director
MDA	Missile Defense Act of 1991
MDAP	Major Defense Acquisition Program
MDC	(1) Manipulation Detection Code; (2) Message Distribution Center
M-Day	Day on which mobilization begins
MDI	Multidiscipline Interaction
MDCI	Multidisciplinary Counterintelligence
MDCISUM	Multidisciplinary Counterintelligence Summary
MDDS	Modular Digital Dissemination System
MDID	MSE Data Interface Device
M-DITDS	Migration Defense Intel Threat Data System
MDJCS	Memorandum by the Director, Joint Staff for the Joint Chiefs of Staff
MDLX	Military Demarcation Line Extended

MDPS	Mission Data Preparation System
MDO JAPAN	Military Defense Office, Japan
MDR	(1) MASINT Data Request; (2) Medium Data Rate
MDS	(1) Mission Dependent Segment; (2) Modular Dissemination System
MDT	Message Distribution Terminal
MDU	(1) Mine Disposal Unit; (2) Mission Data Update
MDW	Military District of Washington
MDZ	Maritime Defense Zone
ME	(1) Middle East; (2) Munitions Effectiveness
MEA	Munitions Effectiveness Assessment
MEAP	Military Economic Advisory Panel
MEB	Marine Expeditionary Brigade
MEBE	Middle East Basic Encyclopedia
MEC	Main Evaluation Center
MECD	Military Equipment Characteristics Document (NATO)
MECH	Mechanized
MECL	Mission Essential Circuits List
MECO	Main Engine Cutoff (Shuttle and Expendable Launch Vehicles)
MECS	Manual ELINT Collection System
Med	Mediterranean
MED	(1) Message Element Dictionary (JINTACCS); (2) Manipulative Electronic Deception; (3) Medical
MED-RES	Medium Resolution
MEDCAP	Medical Civic Action Project
MEDCOM	Medical Command
MEDEVAC	Medical Evacuation
MEDRETE	Medical Readiness Training Exercises
MEDINT	Medical Intelligence
MEECN	Minimum Essential Emergency Communications Network
MEF	(1) Marine Expeditionary Force; (2) Maximum Elevation Figure
MEFCG	MEF Command Group
MEFTL	Middle East Force Target List
MEIF	Master ELINT Intercept File
MECL	Mission Essential Circuits List
MELOS	Mediterranean Littoral OPINTEL Summary
MELT	Maximum Efficiency Language Training
MEM	Mission Effectiveness Model
MENA	Middle East (and) North Africa
MENS	Mission Element Needs Statement
MEO	Medium Earth Orbit
MEP	(1) Ministry of Electronics Industry (FSU); (2) Mission Enhancement Program (AWACS); (3) Management Engineering Plan
MER	(1) Maximum Effective Range; (2) Minimum Essential Requirements

MERADCOM	Mobility Equipment Research and Development Command (U.S. Army)
MERCAST	Merchant Ship Broadcast System
MERCO	Merchant Ship Reporting and Control
MERCOSUR/MERCOSUL	Common Market of the South (South American Southern Cone Customs Union)
MERIT	Military Exploitation of Reconnaissance and Intelligence Technology
MERSHIP	Merchant Ship
MESA	Mechanically Steered Antenna
MET	(1) Mobile Exploitation Team; (2) Meteorology; (3) MILSTAR Engineering Development Model Terminal
METCOM	Control of Meteorological Information
METEOSAT	Meteorological Satellite
METL	Mission Essential Task List
METOC	Meteorological and Oceanographic
METSAT	Meteorology Satellite
METT-T	Mission, Enemy, Terrain, Troops and Time Available
MEU	Marine Expeditionary Unit
MEU(SOC)	Marine Expeditionary Unit (Special Operations Capable)
MEWSS	Mobile Electronic Warfare Support System
MEWSS PIP	Marine Electronic Warfare Support System-Product
MF	Medium Frequency
MFC	Multinational Force Commander
MF IDB	Mainframe Integrated Data Base
MFLOPS	Millions of Floating Point Operations per Second
MFO	Multinational Force and Observers
MFP	Major Force Program
MFP2	Major Force Program 2
MFR	(1) Memorandum for Record; (2) Mutual Force Reduction
MFS	(1) Ministry of State Security (East German); (2) Multifunction Switch
MFT	Mission, Functions and Tasks
MG	Machinegun
MGID	Military Geographic Information and Documentation
MGMT	Management
MGPS	Mobile Ground Processing System
MGR	Manager
MGRS	Military Grid References System
MGS	(1) Mission Ground Station; (2) Mobile Ground Station
MGT	(1) Mobile Ground Terminal; (2) Management
MHC	Coastal Mine Hunter
MHD	Magnet-to-Hydrodynamic
MHE	(1) Mechanized Handling Equipment; (2) Message Handling Enhancement; (3) Materiel Handling Equipment
MHOP	Multiple-Hop
MHS	Message Handling System

MHV	Miniature Homing Vehicle
MHW	Mean High Water
MHz	Megahertz
mi	Miles
MI	(1) Military Intelligence; (2) Message Indicator
MIA	Missing in Action
MIB	(1) Military Intelligence Board; (2) Military Intelligence Battalion; (3) Management Information Base
MIBNLI	Military Intelligence Battalion, Low Intensity
MIBWG	Military Intelligence Board Working Group
MIC	(1) Mid-Intensity Conflict; (2) Multinational Intelligence Cell; (3) Monolithic Integrated Circuit; (4) Maritime Intelligence Center
MICEP	Military Intelligence Civilian Excepted Career Program
MICNS	Modular Integrated Communications and Navigation System
MICOM	Missile Command (U.S. Army)
MICON	Military ICON
micro	one millionth
MICFAC	Mobile Integrated Command Facility Ashore Center
MICS	MIIDS/IDB Interface to Client/Server
MICV	Mechanized Infantry Combat Vehicle
MID	(1) Military Intelligence Detachment (2) Military Intelligence Digest MIDB Modernized Integrated Data Base; Migratory Integrated Data Base
MID(S)	(1) Military Intelligence Detachments (Strategic); (2) Mobile Imagery Dissemination System
MIDAS	MAXI Intelligence Desktop Application Software
MIDE	Mean Installation Damage Expectancy
MIDEASTFOR	Middle East Force
MI DET	Military Intelligence Detachment
MIDL	Miniature Interoperable Data Link
MIDLANT	Mid-Atlantic
MIDPAC	Mid-Pacific
MIDMS	Machine Independent Data Management System
MIEF	Master Imagery Exchange Format
MIERS	Modernized Imagery Exploitation & Reporting System
MIES	Modernized Imagery Exploitation System
MIFASS	Marine Integrated Fire and Air Support System
MIG	(1) Mikoyan (FSU) Aircraft; (2) Military Intelligence Guide; (3) Military Intelligence Group
MIGP	Military Intelligence Group
MIIA	Medical Intelligence Information Agency (now AFMIC)
MIIDS	Military Intelligence Integrated Data System
MIIDS/IDB	Military Intelligence Integrated Data System/Integrated Database
MIIPS	Military Intelligence Information Processor Subsystem
MIJI	Meaconing, Intrusion, Jamming, and Interference

MIJIFEEDER	Meaconing, Intrusion, Jamming, and Interference Report Feeder
MIL	Military
MILAN	International Antitank Guided-Missile System
MILCOM	Military Communications
MILCOMSAT	Military Communications Satellite
MILCON	Military Construction
MILDEP	Military Department
MILGP	Military Group
MILGRPS	Military Advisory Groups
mili	one thousandths
MILNET	(1) Military Logistics Equipment; (2) Military Network
MILOBS	Military Observer(s)
MILPERS	Military Personnel
MILSAT(COM)	Military Satellite (Communications)
MILSPEC	Military Specification
MILSTAR	(1) U.S. Military Communications Satellite Program; (2) Military Strategic and Tactical Relay
MILSTD	Military Standard
MIMES	Multi-Spectral Imagery Materials Exploitation System
MIMI	Multi-Level Interactive Man/Machine Interface
MIMIC	Monolithic Microwave/Millimeter Wave Integrated Circuit
MIMS	Multiple Independent Maneuvering Submissile
min	Minutes
MIN-O	Minimum Weapon for Damage
MINI-DISE	Compact Version of Deployable Intelligence Support Element
MINTERM	Miniature Terminal
MINURSO	United Nations Mission for the Referendum in Western Sahara
MINX	Multi-Media Information Exchange
MIPE	Mobile Intelligence Processing Element
MIO	(1) Missile Intelligence Officer; (2) Counter-Terrorism Database
MIP	(1) Management Implementation Plan; (2) Message Input Processor
MIPE	Mobile Intelligence Processing Element
MIPIR	(1) Multi-Mission Imagery Photographic Interpretation Report; (2) Multi-Source Photo Interpretation Report
MIPR	Military Interdepartmental Purchase Request
MIPS	Million Instructions per Second
MIR	(1) Mission Intercept Report; (2) Morning Intelligence Report
MIRA	Medium-Wave Infrared Acquisition Array
MIRACL	Mid-Infra-Red Advanced Chemical Laser
MIRADCOM	United States Army Missile Research & Development Command
MIRE	Mission Intercept Report-Electrical
MIRF	Mission Information Recording Facility
MIRGS	Multi-Intelligence Reconnaissance Ground Station
MIRS	Miniaturized Imagery Receive System

MIRV	Multiple Independently-Targetable Reentry Vehicle
MIS	(1) Management Information System; (2) Military/Monthly Intelligence Summary; (3) Mission Integration Segment
MISE	Military Information Support Element
MISREP	Mission Report
MISSI	Multilevel Information System Security Initiative
MIST	(1) MCCS Intelligence Support Team; (2) Modular Interoperable Support Terminal; (3) Military Information Support Team
MISTE	Miniature Integrated Satellite Terminal Equipment
MIT	Mobile Interrogation Team (HUMINT)
MITASK	Mission Tasking
MITS	(1) Monthly International Terrorism Summary; (2) MAC Imagery Transmission System; (3) Multimedia-Intelligence Tracking Subsystem
MITT	Mobile Integrated Tactical Terminal
MITTS	Mobile Intelligence Tactical Transmission (System)
MIUW	Mobile Inshore Undersea Warfare
MIW	Mine Warfare
MJCS	Memorandum for the Joint Chiefs of Staff
MK-5O	Advance Lightweight Torpedo
MK V	Mark V Special Operations Craft
MLA	Multispectral Linear Array
MLBM	Modern Large Ballistic Missile
MLE	Mobile Logistics Element
MLLW	Mean Lower Low Water
MLM	Military Liaison Mission
MLNIS	Modified Atlantic Naval Intelligence Summary
MLO	Military Liaison Office
MLP	Multi-Line Phone
MLPP	Multilevel Precedence Preemption
MLRP	Marine Corps Long-Range Plan
MLRS	Multiple Launch Rocket System
MLS	(1) Microwave Landing System; (2) Multi-Level Security; (3) Multi-Level Simulcast
MLSATCOM	Military Satellite Communications
MLST	Mobile Logistics Support Team
MLW	Mean Low Water
MM	(1) Millimeter; (2) Million; (3) Manual Morse; (4) Minelayer
MMB	Miniature Multiband Beacon
MMI	Man/Machine Interface
MMIC	Monolithic Microwave Integrated Circuit
MMIS	Military Man in Space
MMP	MAGTF Master Plan
MMS	Multimission Modular Spacecraft
MMU	Manned Maneuvering Unit

MMW	Millimeter Wave
MN	Multinational
MNAS	MAXI Network Access System
MNC	Major NATO Command (NATO)
MND	Multi-National Division
MNF	Multi-National Force
MNIC	Multinational Intelligence Cell
MNMIC	Modernized NMIC
MNS	Mission Needs Statement
MNTHS	Months
MNU	Middle Name Unknown
MO	Counter-Terrorism Database
MOA	(1) Memorandum of Agreement; (2) Military Operating Area
MOAF	Mission-Oriented Assessment Framework
MOB	(1) Main Operating Base; (2) Missile Order of Battle; (3) Mobilization
MOBDES	Mobilization Designee (now IMA)
MOBEX	Mobilization Exercise
MOBS	Multiple-Orbit Bombardment System
MOBSTA	Mobilization Station
MOBTDA	Mobilization Table of Distribution and Allowances
MOC	(1) Minister of Communications; (2) Mission Operations Center; (3) Mission Operations Chief
MOD	(1) Ministry of Defense; (2) Mobile Obstacle Detachment
MODA	Ministry of Defense and Aviation
MODCOM	Modular Communications
MODEMS	Modulation/Demodulation Equipment
MODS	Multiple Object Data System
MOE	Measure of Effectiveness
MOGAS	Motor Gasoline
MOICPAC	Maritime Operational Intelligence Center, Pacific
MOJT	Managed On-the-Job Training
MOL	Manned Orbital Laboratory
MOLINK	Moscow/Washington Emergency Communications Link
MOLNIYA	Soviet (FSU) satellite
MOM	Ministry of General Machine Building (FSU)
MOMCOMS	Man-on-the-Move Communications System
MOOTW	Military Operations Other Than War
MOP	(1) JCS Memorandum of Policy; (2) Ministry of Defense Industry (FSU)
MOPOT	Mobile PSYOP Transmitter
MOPP	Mission-Oriented Protective Posture
MOPS	Million Operations per Second
MORL	Manned Orbital Research Laboratory
mort	Mortar

MORTREP	Mortar Bombing Report
MOS	(1) Military Occupational Specialty; (2) Maritime Operational Intelligence Summary; (3) Marine Observation Satellite
MOSFET	Metal-Oxide Semiconductor Field-Effect Transistor
MOSS	Manned Orbital Space Station
MOST	Mosaic Optical Sensor Technology
MOSW	Military Operations Short of War
MOT	Military Ocean Terminal
MOTIF	Maui Optical Tracking and Identification Facility
MOU	Memorandum of Understanding
MOUT	Military Operations in Urban Terrain
MOV	Military Owned Vehicle
MP	(1) Military Police; (2) Military Personnel
MP&B	Mission Planning and Briefing
MPA	(1) Maritime Patrol Aircraft; (2) Mission and Payload Assessment; (3) Mission Planning Agent
MPARE	Mission Planning, Analysis, Rehearsal, and Execution System
MPC	(1) Mobile Processing Center; (2) Manpower and Personnel Center; (3) Message Processing Center; (4) Media Production Center
MPDS	Message Processing and Distribution System
MPDT	Message Processing Distribution Terminal
MPEG	Motion Picture Experts Group
MPF	(1) Maritime Prepositioned Force; (2) Message Processing Facility; (3) Mission Planning Folder; (4) Media Production Center
MPF-E	Maritime Prepositioning Force Enhanced
MPI	Mean Point of Impact
MPM	Mission Planning Module
MPN	MSE Packet Network
MPP	Massively Parallel Processing
MPRS	Mission Planning and Rehearsal Segment
MPS	(1) Maritime Prepositioned Ships; (2) Message Processing System; (3) Master Personnel System; (4) Modular Printing System
MPSOC	Multi-Purpose Satellite Operations Center
MPSS	Ministry of Communications Equipment Industry (FSU)
MPWS	Mobile Protected Weapon System
MQS	Military Qualification and Standards System
MR	(1) Military Region; (2) Medium Range; (3) Motorized Rifle
MRB	Motorized Rifle Battalion
MRBM	Medium-Range Ballistic Missile
MRC	(1) Movement Report Center; (2) Military Region Command; (3) Motorized Rifle Company; (4) Major Regional Contingencies; (5) Major Regional Conflict
MRCA	Multirole Combat Aircraft
MRCS	Medium-Resolution Camera System

MRD	(1) Mission Rehearsal Device; (2) Motorized Rifle Division
MRDBS	(1) MASINT Requirements Data Base System; (2) Measurement and Signature Intelligence Requirements Database
MRDFS	Man-Transportable Radio Direction-Finding System
MRDC	Missile Research and Development Command (U.S. Army)
MRF	Ministry of Radio Industry (FSU)
MRI	Military-Related Intelligence
MRK	Manual Remote (re)Keying
MRL	(1) Multiple Rocket Launcher; (2) Master Requirements List
MRLS	Multiple Rocket Launcher System
MRLOGAEUR	Minimum Required Logistics Augmentation Europe
MROC	(1) Multiple-Command Required Operational Capability; (2) Minimum Required Operational Capabilities
MRP	Mobilization Readiness Project
MRPE	Mobile Receive Processing and Exploitation
MRR	Motorized Rifle Regiment
MRS	Movement and Reinforcement Study
MRT	(1) Mobile Remote Terminal; (2) Miniature Receiver Terminal
MR-UAV	Medium-Range Unmanned Airborne Vehicle
MRV	Multiple Reentry Vehicle
MRVC	Multi-Rate Voice Card (Red Switch)
ms	Millisecond
MS	(1) Multispectral; (2) Mobilization Station
M&S	Modeling and Simulation
m/s	Meters per Second
MS-DOS	Microsoft Disk Operating System
MSA	(1) Military Strength Assessment; (2) Minimum Safe Altitude
MSAM	Medium Surface-to-Air Missile
MSB	Minesweeping Boat
MSC	(1) Military Sealift Command; (2) Coastal Minesweeper; (3) Major Subordinate Command (NATO); (4) Military Staff Committee
MSCD	Military Support to Civil Defense
MSCS	Multiple Source Correlation System
MSCT	Training Coastal Minesweeper
MSD	(1) Minesweeping Drone; (2) Mensuration Support Data
MSDF	Maritime Self-Defense Force (Japan)
MSE	Mobile/Multi Subscriber Equipment (Network) (U.S. Army)
MSEL	Master Scenario Events List
MSF	(1) Fleet Minesweeper; (2) Mobile Strike Force; (3) Medicines Sans Frontiers
MSG	(1) Marine Security Guard; (2) Military Support Group
Msg	Message
MSGGEN	Message Generator
MSH	Mine Hunter

MSI	(1) Inshore Minesweeper; (2) Multi-Spectral Imagery; (3) Multisensor Interpretation
MSIC	Missile and Space Intelligence Center
MSID	Message Identifier
MSIP	(1) Multi-Spectral Image Processor; (2) Multisensored Intelligence Processor
MSK	Minimum Shift Keying
MSL	(1) Missile; (2) Mean Sea Level
MSM	(1) Minesweeper (River); (2) Ministry of Medium Machine Building (FSU)
MSN	Mission
MSO	(1) Ocean Minesweeper; (2) Marine Safety Office; (3) MILSATCOM Systems Office
MSP	Ministry of Shipbuilding Industry (FSU)
MSPB	Merit System Protection Board
MSPF	Marine Special Purpose Forces
MSR	(1) Patrol Minesweeper; (2) Main Supply Route; (3) Missile Site Radar
MSRT	(1) Mobile Subscriber Radio Telephone; (2) Mobile Subscriber Remote Terminal
MSS	(1) Message Support Subsystem; (2) Specialized Minesweeper; (3) Moored Sonobuoy System; (4) Mission-Management Support System; (5) Mission Support System; (6) Multispectral Scanner
MSSC	(1) Medium SEAL Support Craft; (2) Specialized Coastal Minesweeper; (3) MEU Service Support Group
MSSI	Master of Science of Strategic Intelligence
MSSP	Multi-Functional Smart Sensor Packages
MSSS	Maui Space Surveillance System
MST	(1) Mutual Security Treaty; (2) Maintenance Support Team; (3) Miniature Satellite Transceiver; (4) Multiband Satellite Terminal
MSTS	(1) Multisource Tactical System; (2) Multisource Transceiver System
MSU	(1) Major Subordinate Unit; (2) Ministry of the Soviet Union
MSW	MASINT Server/Workstation
MT	(1) Metric Ton; (2) Megaton; (3) Motor Transport; (4) Maintenance Trainer; (5) Machine Translation
MT-LB	Soviet (FSU) Tracked Vehicle
MTA	Maritime Threat Analysis
MTACCS	(1) Marine Tactical Command and Control System; (2) Marine Tactical Air Command Center System
MTAS	Multisensor Target Acquisition System
MTB	Motor Torpedo Boat
MTBF	Mean Time Between Failures
MTBSP	Mobilization Troop Basis Stationing Plan
MTCACS	Marine Corps Tactical Command and Control System
MTCR	Missile Technology Control Regime
MTDS	Military Tactical Data System
MTF	Message Test Format

MTG	Master Training Guide
MTH	Memorandum To Holder
MTI	Moving Target Indicator
MTIB	Soviet (FSU) Amphibious Armored Tractor
MTIC	Military Target Intelligence Committee
MTIMS	Military Target Intelligence Management Structure
MTIT	Military Technical Intelligence Team
MTL	Mean Tide Level
MTLR	Moving Target-Locating Radar
MTL(S)	Material(s)
MTMC	Military Traffic Management Command
MTN	(1) Mountain; (2) M22 Tactical Network
MTO	Mission Type Order
MTO&E	Modified Table of Organization & Equipment
MTP	(1) Mission Training Plan; (2) Master Training Plan
Mtr	Motor
MTS	(1) Maritime Tactical Schools (NATO); (2) Man-Transportable SOCRATES; (3) Masked Target Sensor
MTST	Magnetic Tape Selectric Typewriter (IBM)
MTT	(1) Military Training Team; (2) Mobile Training Team
MTTR	Mean Time To Repair
MTZ	Motorized Infantry
MULE	Modular Universal Laser Equipment
MUSARC	Major United States Army Reserve Command
MUSIC	Multi-User Special Intelligence Communications
MUSE	MC&G Utility Software Environment
MUTES	Multiple Threat Emitter System
MUX	Multiplexer
Mvr	Maneuver
MV	Magnetic Variation
MVS	Multiple Virtual Storage
MVS/XA	Multiple Virtual System/Extended Architecture
MW	(1) Mine Warfare; (2) Millimeter Wave; (3) Microwave; (4) Missile Wing
MW/AA	Missile Warning/Attack Assessment
MWC	Missile Warning Center
MWDS	Missile Warning Display Subsystem
MWHQ	Mobile War Headquarters
MWIR	Medium Wavelength Infrared
MWL	Mean Water Level
MWR	Morale, Welfare, and Recreation
MWS	Missile Warning System
MWTGM	Millimeter Wave Terminal Guided Missile
MX	(1) Missile, Experimental; (2) Peacekeeper Ballistic Missile; (3) Mechanized; (4) Mexico; (5) Mission; (6) Maintenance

N

N	North
N2	(1) Director of Intelligence (Naval Component); (2) Navy Staff Intellligence Officer
N/A	Not Applicable
NA	Navy
NAA	North Atlantic Alliance
NAADM	North American Air Defense Modernization
NAASW	Nonacoustic Antisubmarine Warfare
NAAWS	NATO Antiair Warfare System
NAB	(1) NATO Air Base Satellite (System); (2) Naval Amphibious Base; (3) Naval Air Base
NAC	(1) North Atlantic Council (NATO); (2) No Apparent Change; (3) National Agency Check; (4) Network Access Controller
NACA	National Advisory Committee for Aeronautics
NACAA	National Advisory Committee for Aeronautics and Astronautics
NACAM	National COMSEC Advisory Memorandum
NACC	Net Assessment Coordinating Committee
NACDF	National Area Coverage Data File
NACIC	National CI Center
NACIPB	National CI Policy Board
NACOB	National CI Operations Board
NACSI	National COMSEC Instruction
NACSIM	National COMSEC Information Memorandum
NADGE	NATO Air Defense Ground Environment
NADS	North Atlantic Defense System
NAEW	NATO Airborne Early Warning (System)
NAF	(1) Numbered Air Force; (2) Naval Air Facility
NAFI	Non-Appropriated Fund Instrumentality
NAFIS	Naval Forces Intelligence Study
NAI	Named Areas of Interest
NAIC	National Aerospace Intelligence Center
NAK	Negative Acknowledge
NALE	Naval Liaison Element
NAM	(1) Non-Aligned Movement; (2) Naval Armaments Model
NAMSO	NATO Maintenance and Supply Organization
nano	one billionth
NAOB	Naval Air Order of Battle
NAOC	National Airborne Operations Center
NAOS	North Atlantic Ocean Station
NARA	National Archives and Records Administration
NARRS	NORTHAG Reconnaissance Reporting System

NAS	(1) Naval Air Station; (2) Network Access System; (3) National Academy of Science
NASA	National Aeronautics and Space Administration
NASACOM	NASA Communications Network
NASF	NIC Analyst Support Facility
NASIC	North American Air Sovereignty Intelligence Capability
NASP	National Aerospace Plane
NAT	Not Air-Transportable
NAT'L	National
NATO	North Atlantic Treaty Organization
NATO ASWCS	Anti-Surface Warfare Combat System
NAV	(1) Navigation; (2) Navy
NAVAIR	Naval Air Systems Command
NAVAL AIRSHIP	Naval AIRSHIP Radar Surveillance System
NAVASTROGRU	Naval Astronautics Group
NAVATAC	Navy Antiterrorist Alert Center
NAVCAMS	Naval Communications Area Master Station
NAVCENT	U.S. Naval Forces Central Command
NAVCOMDET	Naval Communications Detachment
NAVCOMPARS	Naval Communications Processing and Routing System
NAVCOMTELCOM	Naval Computer and Telecommunications Command
NAVCOMSTA	Naval Communication Station
NAVDAC	Naval Data Automation Command
NAVELEX	Naval Electronic Systems Command
NAVEUR	U.S. Naval Forces, Europe
NAVFAC	(1) Naval Facility; (2) Naval Shore Facilities
NAVFOR	Naval Forces
NAVFORK	Naval Forces Korea
NAVIDS/SIS	Navigational Aids/Selective Identification System
NAVINTCOM	Naval Intelligence Command
NAVLGRU	Naval Liaison Group
NAVMACS	Navy Modular Automated Communications System
NAVMIC	Naval Maritime Intelligence Command
NAVMAP	Navy Missile Analysis Program
NAVMARINTCEN	Naval Maritime Intelligence Center
NAVMAT	Naval Material Command
NAVNET	Navy Data Network
NAVOCEANCOMDET	Naval Oceanography Command Detachment
NAVOCEANO	Naval Oceanographic Office
NAVOCFORMED	Naval On-Call Force for the Mediterranean (NATO)
NAVOPINTCEN	Naval Operations Intelligence Center
NAVPGSCHOOL	Naval Postgraduate School
NAVRADSTA	Naval Radio Station
NAVRES	Naval Reserve
NAVS	Navigators

NAVSAT	Navigation Satellite
NAVSATCOMFAC	Naval Satellite Communications Facility
NAVSEA	Naval Sea Systems Command
NAVSEC	Naval Ship Engineering Center
NAVSECGRU	Naval Security Group
NAVSECGRUACT	Naval Security Group Activity
NAVSECGRUCOM	Naval Security Group Command
NAVSECSTA	Naval Security Station
NAVSO	Naval Forces, South
NAVSOC	Naval Special Operations Command
NAVSOF	Naval Special Operations Forces
NAVSOUTH	Naval Forces, Southern Command
NAVSPACECOM	Naval Space Command
NAVSPASUR	Naval Space Surveillance Activity
NAVSPAWAR	Naval Space and Warfare Systems Command
NAVSPECWARCEN	Navy Special Warfare Center
NAVSPECBOATRON	Navy Special Boat Squadron
NAVSPECWARCOM	Naval Special Warfare Command
NAVSPECWARDEVGRU	Naval Special Warfare Development Group
NAVSPECWARGRU	Naval Special Warfare Group
NAVSPECWARUNIT	Naval Special Warfare Unit
NAVSPOC	Naval Space Operations Center
NAVSTA	Naval Station
NAVSTAR	Navigation and Satellite Timing and Ranging
NAVSTAR USER EQUIP	NAVSTAR User Equipment
NAVSUPACT	Naval Support Activity
NAVTECHINTCEN	Naval Technical Intelligence Center
NAVTELCOM	Naval Telecommunications Command
NAVWARCOL	Naval War College
NAWAS	National Attack Warning System
NAWC-AD	Naval Air Warfare Center-Aircraft Division
NAWS	NORAD Attack Warning System
NB	Naval Base
NBC	(1) Nuclear/Biological/Chemical; (2) National Broadcasting Corporation
NBCE	Nuclear, Biological, Chemical Element
NBCWRS	NORAD - Nuclear, Biological, and Chemical Warning Reporting
NBK	Non-Battle Killed
NBRG	National Basic Reference Graphic
NBS	National Bureau of Standards
NC	(1) No Change; (2) Node Center; (3) Narrow Coverage
NCA	National Command Authority(ies)
NCAPS	Naval Controls and Protection of Shipping
NCB	Nuclear Contingency Branch

NCC	(1) Naval Component Command; (2) Navy Command Center; (3) Net Control Center
NCCD	Nuclear Command and Control Document
NCCOSC	Naval Command, Control, and Ocean Surveillance Center
NCCS	Naval Command and Control System
NCDU	Naval Combat Demolition Unit
NCEUR	NSA/CSS Europe
NCIC	National Crime Information Center
NCIS	(1) Non-Communications Intercept System; (2) National Counterintelligence Strategy; (3) Naval Criminal Investigative Service
NCIS-E	NCIS-Europe
NCISFO	NCIS Field Office
NCISRA	NCIS Resident Agent
NCISRU	NCIS Resident Unit
NCMA	National Command and Military Authority
NCMC	National Collection Management Cell
NCMP	Navy Capabilities and Mobilization Plan
NCO	Non-Commissioned Officer
NCOA	(1) Non-Commissioned Officers' Academy; (2) Non-Commissioned Officers' Association
NCOC	NORAD Combat Operations Center
NCOES	Non-Commissioned Officers' Educational System
NCOIC	Non-Commissioned Officer in Charge
NCOS	Naval Control of Shipping
NCP	Nuclear Contingency Plan
NCPS	Nuclear Contingency Planning System
NCR	(1) National Capital Region; (2) NSA/Cryptologic Support Service Representative; (3) National Cryptologic Representative; (4) NSA/Central Security Service Representative
NCS	(1) National Communications System; (2) NMIC Control Subsystem; (3) Naval Control of Shipping; (4) Network Control Station; (5) Node Center Switch; (6) National Cryptologic School; (7) Net Control Station
NCSC	(1) Navy Command Support Center; (2) National Computer Security Center
NCSE	NIST Communications Support Element
NCSO	Naval Control of Shipping Office
NCSRT	Non-Communications Signal Recognition Trainer
NCTAMS	Navy Computer and Telecommunications Area Master Station
NCTC	Naval Computer and Telecommunications Center
NCTR	Non-Cooperative Target Recognition
NCTS	Naval Computer and Telecommunications Station
NCWA	NATO Civil Wartime Agency
NCWG	National Correlation Working Group
NCWR	Non-Codeword Reporting
ND	Deputy CINCNORAD

NDA	Nondisclosure Agreement
NDAA	Non-Developmental Airlift Aircraft
N-Day	Days Before D-Day
NDB	Non-Direction Beacon
NDCDB	National Digital Cartographic Database
NDCP	Navy Decision Coordinating Paper
NDD	Nuclear Detection Device
NDDS	Nuclear Detonation Detection System
NDGZ	National Desired Ground Zero
NDHQ	National Defense Headquarters (Canada)
NDI	Non-Developmental Item
NDIC	National Drug Intelligence Center
NDL	(1) Network Data Language; (2) National DGZ List
NDOC	National Defense Operations Center
NDP	(1) National Disclosure Policy; (2) Naval Doctrine Publication
NDPC	National Disclosure Policy Committee
NDPO	National Disclosure Policy Office(r)
NDRF	National Defense Reserve Fleet
NDS	(1) Nuclear Detection Satellite; (2) NPIC Data System; (3) Nuclear Detection System
NDU	National Defense University
NEA	(1) Northeast Asia; (2) National Education Association
NEACP	National Emergency Airborne Command Post
NEADS	Northeast Air Defense Sector
NEANMCC	Navy Element Alternate National Military Command Center
NEC	(1) Naval Enlisted Code; (2) Northern European Countries; (3) Navy Enlisted Classification
NEIC	USAFE NATO Equipment Interpretation Course
NEMVAC/NISH	Non-combatant Emergency Evacuation/NEO Intelligence Support Handbook
NEL	National Exploitation Laboratory
NEO	Noncombatant Evacuation Operation
NEOPACK	NEO Package
NEPA	National Environmental Policy Act
NEREP	Nuclear Execution and Reporting Plan
NES	Network Encryption System
NESDIS	National Environmental Satellite Data and Information Service
NESEA	Naval Electronic Systems Engineering Activity
NESN	NATO English-Speaking Nations
NESP	Navy EHF SATCOM Program
NET	(1) Not Earlier Than; (2) New Equipment Training
NETS	Nationwide Emergency Telecommunications Service
NETT	New Equipment Training Team
NEXIS	Meade Data Center News Service
NF	No Foreign Dissemination, NOFORN

NFA	(1) New Fighter Aircraft; (2) No Forwarding Address; (3) No-Fire Area
NFAC	National Foreign Assessment Center
NFCS	Nuclear Forces Communications Satellite
NFD	No Foreign Dissemination
NFDP	National Foreign Disclosure Policy
NFE	Network Front End
NFI	(1) Not Further Identified; (2) No Further Information
NFIB	National Foreign Intelligence Board (formerly USIB)
NFIC	National Foreign Intelligence Council
NFIP	National Foreign Intelligence Program
NFL	New Foreign Launch
NFM	Near-Full-Motion
NFS	Network File System
NFSN	NATO French-Speaking Nations
NFWS	Navy Fighter Weapons School
NFZ	Nuclear Free Zone
NG	National Guard
NGA	NATO Guidelines Area
NGAZ	NATO Gazetteer
NGB	National Guard Bureau
NGF	Northern Group of Forces (Soviet Forces in Poland)
NGFS	Naval Gunfire Support
NGIC	National Ground Intelligence Center
NGL	Natural Gas Liquids
NGO	Non-Governmental Organization(s)
NGS	National Ground Site
NHCD	National HUMINT Collection Directive(s)
NHCP	National HUMINT Collection Plan
NHO	Naval Hydrographic Office
NHRTC	National HUMINT Requirements Tasking Center
NIA	National Imagery Agency
NIAC	(1) National Information & Analysis Center; (2) Naval Intelligence Automation Command
NIAG	NATO Industrial Advisory Group
NIC	(1) Naval Intelligence Command; (2) National Intelligence Council; (4) Naval Intelligence Cell; (5) National Intelligence Cell/Community
NICCIA	National CI Coordinating Authority
NICKA	Nickname and Exercise Term System
NICOLS	NIC On-Line System
NICS	NATO Integrated Communications System
NICSCOA	NATO Integrated Communications System Central Operating Authority
NID	National Intelligence Daily
NIDS	NMCC Information Display System

NIE	National Intelligence Estimate
NIEO	New International Economic Order
NIETB	National Imagery Exploitation Target Base
NIETS	National Imagery Exploitation Tasking Study
NIEX	No-notice Interoperability Exercise
NIG	National Input Group
NIHS	NAVEUR Intelligence Highlights Summary
NII	National Information Infrastructure
NIIC	NORAD Intelligence Indications Center
NIIDTS	Naval Intelligence Imagery Data Transmission System
NIIRS	National Imagery Interpretability Rating Scale
NILS	Naval Intelligence Locating Summary
NIM	NORAD Intelligence Memorandum
NIMA	National Imagery and Mapping Agency
NIO	National Intelligence Officer
NIP	(1) Notice of Intelligence Potential; (2) National Intelligence Priorities; (3) NATO Interoperability Plan
NIPIR	Nuclear Immediate Photo Interpretation Report
NIPRNET	Unclassified-but Sensitive (N) Internet Protocol Router Network
NIPS	(1) NMCC Information Processing System; (2) Naval Intelligence Processing System
NIPSSA	Naval Intelligence Processing Systems Support Activity
NIPSTRAFAC	Naval Intelligence Processing Systems Training Facility
NIS	(1) National Intelligence Summary; (2) National Intelligence Survey; (3) Naval Investigative Service; (4) NATO Identification System; (5) NPIC Information System (former NDS); (6) Newly Independent States; (7) National Imagery Segment; (8) National Input Segment; (9) NIPCImagery System; (10) Network Information System
NISAC	National Industrial Security Advisory Committee
NISAM	Naval Intelligence Systems Architecture Manual
NISC	Naval Intelligence Support Center (U.S. Navy) (now NIC)
NISCOM	Naval Investigative Service Command
NISHQ	Naval Investigative Service Headquarters
NISO	Naval Investigative Service Office
NISP	Nuclear Weapons Intelligence Support Plan
NISR	National Intelligence Situation Report
NIST	(1) National Intelligence Support Team; (2) National Institute of Standards and Technology
NIT	National Intelligence Topic
NITF	National Imagery Transmission Format
NITFS	NITF Standard
NIU	Network Interface Unit
NKIL	North Korea Installation List
NKSR	Nonkernel Security Related Software
NLC	National Logistical Command
NLI	Natural Language Interface

NLM	Netware Loadable Module
NLP	Natural Language Processing
NLOS	Non-Line-of-Sight Weapon System
NLS	Non-Lethal Submunitions
NLT	Not Later Than
NLZ	No-Loan Zone
NM	Nautical Mile
NMC	(1) Naval Materiel Command; (2) NATO Military Council
NMCC	National Military Command Center
NMCC(A)	National Military Command Center (Alternate)
NMCS	National Military Command System
NMCSSC	National Military Command Systems Support Center
NMD	National Military Defense
NMI	No Middle Initial
NMIC	(1) National Military Intelligence Center (archaic, now NMJIC); (2) National Maritime Intelligence Center
NMICC	NATO Maritime Intelligence Coordination Center
NMICSS	NMIC Support System
NMIS	National Military Intelligence Support
NMIST	National Military Intelligence Support Team
NMITC	(1) Navy-Marine Corps Intelligence Training Center; (2) National Military Intelligence Training Center
NMJCC	National Military Joint Command Center
NMJIC	National Military Joint Intelligence Center
NMN	No Middle Name
NMOSS	NATO Maritime Operational Support System
NMRL	National MASINT Requirements List
NMS	National Military Strategy
NMSD	National Military Strategy Document
NMIC	National Military Intelligence Center
NMICC	National Military Intelligence Collection Center
NMJIC	National Military Joint Intelligence Center
NN	Neural Network
NNA	Neutral and Non-Aligned
NNAG	NATO Naval Armaments Group
NNBIS	National Narcotics Border Interdiction System
NNICP	National Nuclear Intelligence Collection Plan
NNWS	Non-Nuclear Weapons States
NOAA	National Oceanic and Atmospheric Administration
NOB	(1) Naval Order of Battle; (2) Nuclear Order of Battle
NOBS	Naval Operations Bases
NOBTS	Naval Order of Battle Textual Summary

NOC	(1) Naval Operations Center; (2) Network Operations Center NOCONTRACT Not Releasable to Contractors or Contractor Consultants
NOD	Night Observation Device
NOE	Nap-of-the-Earth
NOFORN	Not Releasable to Foreign Nationals
NOIAN	National Operations and Intelligence Analysts Net
NOIC	Naval Operational Intelligence Center
NOIWON	National Operations and Intelligence Watch Officers Network
NOK	Next Of Kin
NOMS	Nuclear Operations Monitoring System
NOPF	Naval Ocean Processing Facility
NOR	Norway
NORAD	North American Aerospace Defense Command
NORD	Nordic
NORIP	NORAD Intelligence For Planning Document
NORLANT	North Atlantic
NORMIB	NORAD Missile Intelligence Bulletin
NORSAR	Norwegian Seismic Array
NORSIB	NORAD Weekly Space Intelligence Bulletin
NORTHAG	Northern Army Group
NORTIC	NORAD Tactical Intelligence Cell
NOSC	Naval Ocean Systems Center
NOSG	Naval Operations Support Group
NOSIC	Naval Ocean Surveillance Information Center
NOTAL	Not To All (message distribution restriction)
NPA	New People's Army
NPB	Neutral Particle Beam
NPE	Nuclear Planning and Execution
NPES	Nuclear Planning and Execution System
NPGS	Naval Postgraduate School
NPHR	National Foreign Intelligence Plan for Human Resources
NPIC	National Photographic Interpretation Center
NPR	Nuclear Posture Review
NPS	Nuclear Planning System
NPT	Non-Proliferation (of Nuclear Weapons) Treaty
NR	(1) Research Submarine (Nuclear); (2) Naval Reserve; (3) Non-Recurring; (4) Number
NRAD	NCCOSC Research, Development, Test and Evaluation Division
NRC	National Research Council
NRCC	NORAD Region Combat Center
NRDL	Naval Radiological Defense Laboratory
NRF	Naval Reserve Force
NRFI	Non-Recurring Finished Intelligence
NRI	Net Radio Interference

NRIP	Naval Reserve Intelligence Program
NRIS	National Radar Interpretability Scale
NR JOIC	Northwestern Region Joint Operational Intelligence Cell
NRL	(1) Naval Research Laboratory; (2) NUWEP Reconnaissance List; (3) National Receive Location
NRO	National Reconnaissance Office
NROSS	Navy Remote Ocean Surveillance Satellite
NRP	(1) National Reconnaissance Program; (2) Net Radio Protocol
NRT	(1) Near Real Time; (2) Net Registered Tonnage
NRTEM	Near-Real-Time Exploitation Module
NRTI	Near-Real-Time Information
NRTS	Naval Reconnaissance and Technical Support
NSA	(1) National Security Agency; (2) National Shipping Authority; (3) National Standards Association; (4) Naval Support Activity
NSAD	Network Security Architecture and Design
NSA/CSS	National Security Agency/Central Security Service
NSAM	National Security Action Memorandum
NSARC	Navy Systems Acquisition Review Council
NSC	(1) National Security Council; (2) Naval Supply Center
NSC/DC	Deputies Committee of the NSC
NSCID	National Security Council Intelligence Directive
NSCIG	National Security Council Interdepartmental Group
NSD	National Security Directive
NSDD	National Security Decision Directive
NSDM	National Security Decision Memorandum
NSE	(1) Naval Support Element; (2) National Support Element
nsec	Nanosecond
NSEP	National Security Emergency Preparedness
NSF	National Science Foundation
NSFS	National Surface Fire Support
NSG	Naval Security Group
NSGA	Naval Security Group Activity
NSGC	Naval Security Group Command
NSGD	Naval Security Group Detachment
NSI	National Security Information
NSIC	Naval Security and Investigative Command
NSN	National Stock Number
NSNF	Non-Strategic Nuclear Forces
NSO	(1) Non-SIOP Option; (2) Network Security Officer
NSOC	(1) National Security Operations Center (formerly National SIGINT Operations Center); (2) Naval Special Operations Command
NSOF	Naval Status of Forces
NSP	NORAD/USSPACECOM
NISPC	National In-Service Production Centers
NSPG	National Security Planning Group

NSRB	National Security Resources Board
NSRDB	National SIGINT Requirements Data Base
NSRDC	Naval Ship Research and Development Center
NSRL	National SIGINT Requirements List
NSRS	National SIGINT Requirements System
NSS	(1) NMIC Support System; (2) National Seismic Station; (3) National Security Strategy; (4) Network Support Server
NSSD	National Security Study Directive
NSSM	(1) Navy Spread Spectrum Modem; (2) National Security Study Memorandum
NSST	(1) Navy Space Command Space Support Team; (2) National Special Support Teams
NSTAC	National Security Telecommunications Advisory Committee
NSTD	(1) National Strategic Target Database; (2) Non-System Training Device
NSTG	Nuclear Strike Target Graphic
NSTGFE	Naval Scientific and Technical Group, Far East
NSTISSAM	National Security Telecommunications and Information Systems Security Advisory/information Memorandum
NSTISSC/D/I/P	National Security Telecommunications and Information Systems Security Committee/Directive/Instruction/Policy
NSTL	National Strategic Target List
NSTS	NSA/CSS Secure Telephone System
NSV	Netted Secure Voice
NSVN	NATO Secure Voice Network
NSW	Naval Special Warfare
NSWC	(1) Navy Surface Weapons Center; (2) Navy Special Warfare Command
NSWDG	Naval Special Warfare Development Group
NSWG	Naval Special Warfare Group
NSWP	Non-Soviet Warsaw Pact
NSWTG	Naval Special Warfare Task Group
NSWTG/U	Naval Special Warfare Task Group/Unit or (Unconventional)
NSWTU	Naval Special Warfare Task Unit
NSWU	Naval Special Warfare Unit
NTA	National Tasking Authority
NTB	(1) National Targeting Base; (2) Nuclear Test Ban
NTBS	National Target Base Server
NTC	(1) National Territorial Command; (2) National Tasking Center; (3) Naval Training Center; (4) Network Terminal Concentrator; (5) National Training Center
NTCB	Network Trusted Computing Base
NTCC	Naval Telecommunications Center
NTCS-A	Naval Tactical Communications System-Afloat
NTDI	NATO Target Data Inventory
NTDS	Naval Tactical Data System
NTF	National Test Facility

NTI	(1) National Tactical Interface; (2) Near-Term Initiative
NTIA	National Telecommunications & Information Administration/ Agency
NTIB	NATO Tactical Intelligence Broadcast
NTIC	Naval Technical Intelligence Center
NTIS	National Technical Information Service
NTISSAM	National Telecommunications and Information Systems Security Advisory/information Memorandum
NTISSC/D/I/P	National Telecommunications and Information Systems Security Committee/Directive/Instruction/Policy
NTM	National Technical Means
NTMWG	Nuclear Test Monitoring Working Group
NTP	National Tasking Plan
NTPC	National Telemetry Processing Center
NTPR	Nuclear Targeting Policy Review
NTPS	Near-Term Maritime Pre-Positioning Ships
NTS	(1) Nuclear Test Site; (2) Naval Telecommunications System
NTSC	National Television Standard Code/Committee
NTSDS	National Target/Threat Signatures Data System
NTSS	National Time-Sensitive System
NTU	New Threat Upgrade
NTZ	No Transgression Zone
NUAC	Nicaragua Analysis Cell
NUCAP	Nuclear Capabilities Data Base
NUCDEF	Nuclear Defense
NUCDETS	Nuclear Detonation Detection & Reporting System
NUCINT	Nuclear Intelligence
NUCREP	Nuclear Damage Report
NUCWPN	Nuclear Weapon(s)
NUICCS	NORAD/USSPACECOM Integrated Command and Control System
NUDET	(1) Nuclear Detection; (2) Nuclear Detonation
NUIS	NORAD/USSPACECOM Intelligence Systems
NURAD	Nuclear Radiation Detection
NUREP	Nuclear Weapons Report
NUSC	Naval Underwater Systems Center
NUT	Naval Upper Tier
NUTEX	Nuclear Tactical Exercise
NUWEAMP	Nuclear Weapons Employment and Acquisition Master Plan
NUWEP	Nuclear Weapons Employment Policy/Plan (NCA)
NVDEP	Network Virtual Data Entry Protocol
NVDET	Network Virtual Data Entry Terminal
NVG	Night Vision Goggles
NVIS	(1) Near-Vertical Incidence Skywave; (2) Night Vision Imaging System
NVS	Night Vision System

NW	(1) Nuclear Warfare; (2) Northwest (region)
NWB	Nuclear Weapons Branch
NWC	(1) National War College; (2) Naval War College; (3) Naval Weapons Center; (4) NORAD Weather Center
NWFZ	Nuclear Weapons Free Zone
NWIP	Naval Warfare Information Publication
NWIS	Naval Weaponeering Information Sheet
NWL	Naval Weapons Laboratory
NWP	Naval Warfare Publication
NWR	Northwest Region
NWRS	Nuclear Weapons Requirement Study
NWS	(1) Nuclear Weapons State; (2) North Warning System; (3) National Weather Service
NWSS	Nuclear Weapons Storage Site
NWWCSS	Naval Worldwide Command Support System
NX	Non-Expendable

O

O/A	On or About
OA	(1) Office Automation; (2) Operations Analysis; (3) Operational Area
OAC	Objective Architecture Center
OAD	(1) Operational Availability Date; (2) Objective Architecture Document
OAD-2	Objective Architecture Document, 2nd Iteration
OADR	Originating Agency's Determination Required
OALAN	Office Automation Local Area Network
OAMP	Optical Airborne Measurements Program
OAP	(1) Organizational Assessment Package; (2) Offset Aim Point
OAPEC	Organization of Arab Petroleum-Exporting Countries
OAS	(1) Organization of American States; (2) Offensive Air Support
OASA(RDA)	Office of the Assistant Secretary of the Army (Research, Development, and Acquisition)
OASD	Office of the Assistant Secretary of Defense
OASD(C3I)	OASD (Command, Control, Communications, and Intelligence)
OASIS	(1) Operational Application of Special Intelligence Systems; (2) Office Automation System for Intelligence Support
OATS	(1) Operations Analysis for Tactical Support; (2) Online AIF Transaction System
OAU	Organization of African Unity
OB	Order of Battle
OBC	Optical Bar Camera
OBE	Overtaken By Events
OBI	Observable Human Resources Intelligence
OBI-OC	OBI Operations Center
OBIS	Order of Battle Intelligence System
Obj	Object
OBP	On-Board Processing
OBO	Official Business Only
OBS	(1) Ocean Baseline System; (2) Orders of Battle System; (3) Observations (Optical Tracking)
OBSS	(1) Off-Board Sensor Systems; (2) Operational Briefing Support System
OBSUM	Order of Battle Summary
OBU	OSIS Baseline Upgrade
OC	(1) Dissemination and extraction of Information Controlled; (2) Optical Carrier
O&C	Operations & Control
OCA	(1) Ocean Control Authority; (2) Operational Control Authority; (3) Offensive Counterair
OCAC	Operational Control and Analysis Center
OCAM	Afro-Malagasy and Mauritian Common Organization

OCAR	Office, Chief of Army Reserve
OCCIS	Operational Command and Control Information System
OCCULT	Optical Covert Communications Using Laser Transceivers
OCEANLANT	Ocean Atlantic Area (NATO)
OCJCS	Office of the Chairman, Joint Chiefs of Staff
OCM	Operational Coordination Message
OCMA	Objective Collection Management Architecture
OCMC	Overhead Collection Management Center
OCNO	Office of the Chief of Naval Operations
OCOKA	Observation and Fields of Fire, Concealment and Cover, Obstacles, Key terrain, Avenues of Approach, and Mobility Corridors
OCONUS	Outside CONUS
OCR	(1) Office of Collateral Responsibility; (2) Optical Character Reader
OCS	(1) Officer Candidate School; (2) Offensive Counterspace
OCS3	Optical Carrier 3 Communications
OCSA	Office of the Chief of Staff of the Army
OCSURV	Ocean Surveillance
OCU	Operational Conversion Unit
OD	Operating Directive(s)
ODA	Operational Detachment Alpha
ODC	Office of Defense Cooperation
ODCSINT	Office of the Deputy Chief of Staff, Intelligence
ODCSLOG	Office of Deputy Chief of Staff for Logistics
ODCSPER	Office of Deputy Chief of Staff for Personnel
ODECA	Organization of Central American States
ODIN	Operations Dedicated Imagery Network (LOCE)
ODISC4	Office of Director Information Systems Command, Control, Communications, Computers
ODJS	Office of the Director, Joint Staff
ODP	(1) Officer Distribution Plan; (2) Office of Defense Planning
ODRP	Office of the Defense Representative - Pakistan
ODS	(1) Open Data Server; (2) Operation DESERT STORM; (3) Output Data Server
OE	Operational Effectiveness
OECD	Organization for Economic Cooperation and Development
OEE	Operational ELINT Exploitation
OEF	Operational Exploitation Facility
OEG	Operational Exposure Guide
OEIC	Overseas Economic Intelligence Committee
OER	(1) Officer Evaluation Report; (2) Officer Efficiency Report; (3) Operational ELINT Requirements
OET	Office of Emergency Transportation
OFC	Office
OFCO	Offensive Counterintelligence Operation
Off	Officer

OFM	Office of Foreign Mission
OGOOI	Operations Group Operations Officer Intelligence (Air Force)
OGS	Overseas Ground Station
OGSI	Operations Group Support Intelligence (Air Force)
OHD	Over-the-Horizon Detection Radar
OHD-B	Over-the-Horizon Detection Radar-Backscatter
OI	(1) Operating Instruction; (2) Operational Interest
O&I	Operations & Intelligence
OIA	(1) Office of Imagery Analysis; (2) Operations Intelligence Automation
OIC	Officer in Charge
OICC	(1) Operational Intelligence Crisis Center; (2) Operational Intelligence Coordination Center
OICS	Operational Intelligence Collection System
OII	Operations-Intelligence Interface
OILO	Operations Intelligence Liaison Officer
OIP	(1) Offset Instrumentation Point; (2) Operator Interface Processor
OIR	Operational Intelligence Requirement
OISS	Operational Intelligence Support System
OIW	OII Workstation
OJCS	(1) Organization of the Joint Chiefs of Staff; (2) Office of the Joint Chiefs of Staff
OJT	On-the-Job Training
OL	Operating Location
OLC	Oak Leaf Cluster
OM	Operations Module
O&M	Operation and Maintenance
OMA	(1) Office of Military Affairs (CIA); (2) Operations and Maintenance, Army
OMAR	Operations and Maintenance Army Reserve
OMAT	Ocean Measurements and Array Technology
OMB	Office of Management and Budget
OMC	Office of Military Cooperation
OMC-K	Office of Military Cooperation-Kuwait
OMG	Operational Maneuver Group (FSU)
OMNG	Operation and Maintenance, National Guard
OMOB	Offensive Missile Order of Battle
OMV	Orbital Maneuvering Vehicle
ON	Original Negative (film)
ONA	Australia Office of National Assessments
ONC	Operational Navigation Chart
ONI	Office of Naval Intelligence
ONIR	Overhead Non-Imaging Infrared
ONLEXKED	On-Line Five Year Exercise Schedule System
ONOO	Outline NATO Operational Objective

ONPG	Operational Nuclear Planning Group
ONR	Office of Naval Research
ONS	Operational Needs Statement
ONUC	United Nations Operations in the Congo
ONUMOZ	United Nations Operations in Mozambique
ONUSAL	United Nations Observer Mission in El Salvador
OOA	Out of Area
OOB	Order of Battle
OODA	Observation, Orientation, Decision and Action
OOK	On/Off Keying
OOP	Object Oriented Programming
OOTW	Operations Other Than War
OP	(1) Observation Post; (2) Operation; (3) Operational
OPA	Other Procurement Activity
OP3	Overt Peacetime PSYOP Program
OPCC	Offutt Processing and Correlation Center
OPCEN	Operations Center
OPCODES	Operational Codes
OPCOM	Operational Command
OPCON	Operational Control
OPDEC	Operational Deception
OPEC	Organization of Petroleum-Exporting Countries
OPELINT	Operational Electronic Intelligence
OPF	Orbiter Processing Facility
OPFAC	Operational Facilities
OPFIS	Operational Foreign Instrumentation Signals
OPFOR	Opposing Forces
OPG	Operations Planning Group
OPI	Office of Primary Interest
OPIC	(1) Overseas Processing and Interpretation Center; (2) Overseas Private Investment Corporation
OPIC-A	Overseas Processing and Interpretation Center - Asia
OPINT	Optical Intelligence
OPINTEL	Operational Intelligence
OPLAN	Operations Plan
OPM	Office of Personnel Management
Opn(s)	Operation(s)
OPNAV	Office of the Chief of Naval Operations
OPNAVINST	OPNAV Instruction
OPNOTES	Operational Notes
OPORDER/OPORD	Operations Order
OPPAR	Opposing Army
OPR	Office(r) of Primary Responsibility; Officer Performance Report
OPREP	Operations Report
OPREPS	Operational Reporting System

OPS/OPNS/OP	Operations
OPS/INTEL	Operations Intelligence
OPSDEPS	Operations Deputies (JCS)
OPSCO	Operations Coordinator
OPSCOM	Operations Committee
OPSCOMM	Operations Secure Communications
OPSEC	Operations Security
OPSKAN	Open Skies Advanced Notice
OPSNOTE	Operations Note
OPT	(1) Optional Modification; (2) Operations Planning Team
OPTEMPO	Tempo of Operations
OPTEVFOR	Operational Test and Evaluation Force
OPTINT	Optical Intelligence
OPTIR	Optical Infrared
OPUS	OBU Program Upgrade System
OR	(1) Operational Requirements; (2) Operationally Ready
ORBINT	Orbital Intelligence
ORBIT	System Development Corporation Data Search Service
ORCON	(1) Dissemination and Extraction of Information Controlled by Originator; (2) Originator Controlled
ORD	Operational Requirements Document
ORE	Operational Readiness Exercise
ORF	Official Representation Fund
Org	Organization
ORI	Operational Readiness Inspection
OS	(1) Operating System; (2) Cryptologic Officer
O&S	Operations & Support
OSA	Open Systems Architecture
OSAP	Ocean Surveillance Assessment Program
OSAS	Operational Space Application System
OSC	(1) Office of the Security Council; (2) Operational Support Company; (3) Operations Support Center; (4) On-Scene Commander
OSCAR	Optical Submarine Communications by Aerospace Relay
OSCARCP	Operations Support Center and Rear Command Post (Korea)
OSD	Office of the Secretary of Defense
OSD(C)	OSD (Comptroller)
OSF	Open Systems Foundation
OSI	(1) Operating Systems Incorporated (Contractor); (2) On-Site Inspection; (3) Off-Shore Islands; (4) Office of Special Investigations; (5) Open System Interconnect; (6) Office of Special Investigations; (7) Open System Interconnect
OSIA	On Site Inspection Agency
OSINT	Open Source Intelligence
OSIS	(1) Ocean Surveillance Information System; (2) Open Source Information Service
OSP	(1) Ocean Surveillance Product; (2) Operational Support Package

OSPRA	Ocean Surveillance Pattern Recognition Algorithm
OSO	Operational Support Office
OSP	Operational Support Packages
OSS	(1) Operational Storage Site; (2) Operations Support Squadron; (3) Operations Support System
OSSC	On-Line System Support Center
OST	Outer Space Treaty
OSTP	Office of Science and Technology Policy
OT	(1) Overseas Territories; (2) Overtime; (3) Operational Test; (4) One Time; (5) Operations Team
OT&E	Operational Test and Evaluation
OTA	(1) Operational Tasking Authority; (2) Office of Technology Assessment
OTAD	Over-The-Air Key Distribution
OTAR	Over-The-Air Rekeying
OTAT	Over-The-Air Transmission/Transfer
OTAU	Over-The-Air Updating
OTC	(1) Officer in Tactical Command; (2) Over-the-Counter
OTCIXS	(1) Officer in Tactical Command Information Exchange Subsystem; (2) OTC Information Exchange System
OTE	See OT&E
OTEA	Operational Test and Evaluation Agency (U.S. Army)
OTH	Over-the-Horizon
OTH-B	Over-the-Horizon Backscatter
OTH-R	Over-the-Horizon Radar
OTH-T	Over-the-Horizon Targeting
OTIS	Operational Targeting Intelligence System
OTM	On the Move
OTP	One-Time Pad
OTS	(1) One-Time Source; (2) Officer Training School; (3) Oahu Telecommunications System
OTT	One-Time Tape
OTU	Operational Training Unit
OUO	Official Use Only
OUSDRE	Office of the Under Secretary of Defense, Research & Engineering
OUTS	Operational Unit Transportable System
OVOP	Overt Operational Proposal
OVPF	Object-Oriented Vector Product Format

P

P	Peacetime
P2E2I	Pre-Planned Essential Elements of Information
P-3H	Land-Based Anti-Submarine Warfare Patrol Aircraft (re-engined)
P3I	Pre-Planned Product Improvement
PA	(1) Pulse Amplitude; (2) Probability of Arrival; (3) Public Affairs; (4) Preliminary Assessment; (5) Proper Authority
PAA	(1) Primary Aircraft Authorized; (2) Peer Access Approval
PA ANG	Pennsylvania Air National Guard
PAATS	Precision Approach Area Tracking System
PABX	Private Access Branch Exchange
PAC	Pacific
PACAF	Pacific Air Forces
PACCAAT	USPACOM Command and Control AUTODIN Access Terminal
PACCS	Post-Attack Command and Control System
PACE	Portable Acoustic Collection Equipment
PACFAST	Pacific Forward Area Support Team
PACFLT	Pacific Fleet
PACOM	U.S. Pacific Command
PACOPS	Pacific Air Force Operations
PACTAIS	Pacific Theater Air Intelligence System
PACTIDS	PACOM Theater Intelligence Data System
PACVTCN	Pacific Video Teleconferencing Network
PAD	Program Action Directive
PADAR	Passive Airborne Detection & Ranging
PA&E	Program Analysis and Evaluation
PAE	Peer Access Enforcement
PAF	Production Analysis and Fusion
PAI	Project Assignment Instruction
PAIDS	PACOM Area Imagery Distribution System
PAIS	(1) Personnel Authentication Identification System; (2) Prototype Advanced Indicator System; (3) Pacific Air Intelligence System
PAL	Permissive Action Link
PALAPA	Indonesian Satellite
PALS	Photo Area & Location System
PAM	(1) Payload Assist Module; (2) Penetration Augmented Munition
PAMIS	Psychological Operations Automated Management Information System
PANAMSAT	PAN American Satellite (Communications System)
PANMAN	Panama Metropolitan Area Network
PAO	(1) Product Activity/Operational Code; (2) Public Affairs Officer
PAOC	PACAF Air Operations Center

PAR	(1) Precision Approach Radar; (2) Perimeter Acquisition Radar; (3) Phased-Array Radar; (4) Population at Risk; (5) Program Assessment Review
PARCS	(1) Perimeter Acquisition Radar Attack; (2) Perimeter Acquisition Characterization System
PARINT	Partial Intercept
PARIS	Pacific Army Intelligence System
PARMIS	Peacetime Airborne Reconnaissance Management Information System
PARPRO	(1) Peacetime Aerial Reconnaissance Program; (2) Preplanned Application of Reconnaissance Programs
PAS	(1) Plans and analysis Staff; (2) Pan American Satellite
PASEP	Passed Separately
PASS	(1) Photo Interpretation Analyst Support System; (2) PACOM IPAC Intelligence Computer System Analyst Support System; (3) PACOM ADP Server Site
PASS-E	USPACOM ADP Server Site-EASTPAC
PASSEX	Passing Exercise (Naval)
PASS-H	USPACOM ADP Server Site, Hawaii
PASS-J	USPACOM ADP Server Site, Japan
PASS-K	USPACOM ADP Server Site, Korea
PAT	(1) Payload Associated Transporter; (2) Planning Assistance Team; (3) Process Action Team
PATREP	Patrol Report
PATRIOT	Phased Array Tracking to Intercept of Target
PATRIOT PAC III	Phased Array Tracking to Intercept of Target Advanced Capability III
PATRON	Patrol Squadron (Navy)
PATWING	Patrol Wing
PAVE	USAF Programs Connected (Night) Avionics, Target Designators, Vision
PAWS	(1) Portable Analyst Work Station; (2) Prototype Analytical Workstation; (3) Portable ASAS Workstation
PAX	Passengers
PB	(1) Particle Beam; (2) Patrol Boat
PB(A)(H)	Patrol Boat (Air Cushion) (Hydrofoil)
PBAC	Program Budget Activity Committee
PBC	Program and Budget Committee
PBD	(1) Program Budget Decision; (2) Patrol Boat Drone
PBEIST	Planning Board for European Inland Surface Transport
PBL	Patrol Boat, Light
PBN	Public Broadcasting Network
PBOS	Planning Board for Ocean Shipping
PBR	(1) River/Roadstead Patrol Boat (Navy); (2) Precision Bombing Range
PBTN	Panama Backbone Transport Network
PBV	Post-Boost Vehicle
PBW	Particle Beam Weapon

PBX	Private Branch Exchanges
PC	(1) Patrol Craft; (2) Positive Control; (3) Production Control; (4) Personal Computer; (5) Project Coordinator; (6) Parallel Computing; (7) Provide Comfort; (8) Patrol Coastal
PCA	Point of Closest Approach
PCAC	Primary Collection and Analysis Center
PCC	(1) POADS Computer Center; (2) Program Coordinating Committee
PCD	(1) Program Change Decision; (2) Positive Control Document
PCE	Patrol Escort
PCF(A)(H)	Fast Patrol Craft (Air Cushion) (Hydrofoil)
PCFS	Fire Support Patrol Craft
PCH	Patrol Craft (Hydrofoil)
PC II	PROVIDE COMFORT II
PCL	Parallel Communications Link
PCM	Pulse Code Modulation
PCMCIA	Personal Computer Memory Card International Association
PCN	(1) Production Control Number; (2) Packet Switching Node; (3) Personal Communications Networking
PCP	(1) Project Concept Proposal; (2) Program Change Proposal
PCR	(1) Performance and Cost Report; (2) Program Change Request
PCS	(1) Publication Control Sheet; (2) Permanent Change of Station; (3) Submarine Chaser; (4) Personal Communications System; (5) Primary Control Station
PCS/UPT	Personal Communications Services/Universal Personal Telecommunications
PCSF	Fire Support Patrol Craft
PCT	Training Patrol Craft
PCTN	Pacific Consolidated Telecommunications Network
PCTCS	Pentagon Center Telecommunications System
PCZ	Protected Communications Zone
PD	(1) Probability of Damage; (2) Presidential Directive; (3) Pulse Duration; (4) Passive Detection; (5) Point Detonation (Fuse)
PDA	Personal Digital Assistant
PDB	PSYOP Dissemination Battalion
PDC	Propaganda Development Center
PDD	Presidential Decision Directive
PDI	Principal Deputy for Intelligence
PDF	Panamanian Defense Force
PDL	Program Design Language
PDM	(1) Program Decision Memorandum; (2) Pulse Duration Modulation
PDMS	Point Defense Missile Systems
PDMT	Pursuit Deterrent Munition Trainer
PDOP	Position Dilution of Precision

PDP	(1) Program Decision Paper; (2) Programmable Data Processor
PDR	Preliminary Design Review
PDS	(1) Passive Detection System; (2) Power Distribution System; (3) Production Deconfliction System; (4) Protected Distribution System PDSC PACOM Data Systems Center
PDSS	Post-Deployment Software Support
PDU	Protocol Data Unit
PDUSD(A&T)	Principal Deputy Under Secretary of Defense (Acquisition & Technology)
PE	(1) Probable Error; (2) Personnel Equipment; (3) Program Element; (4) Preliminary Exploitation; (5) Peace Enforcement
PEAD	Presidential Emergency Affairs Documents
PEAS	(1) Psychological Operations Effectiveness Analysis Subsystem; (2) PSYOP Effects Analysis System
PEC	(1) Pacific Command Electronic Intelligence Center; (2) Program Element Code
PEG	(1) Photo Exploitation Group; (2) Priority Exploitation Group; (3) Priorities for ELINT Guidance; (4) Program Element Group
PEH	Probable Error in Height
PEI	Production Enhancement Initiative
PEILS	PACOM Executive Intelligence Summary
PEM	(1) Purchased Equipment Maintenance; (2) Program Element Monitor
PEO	Peace Enforcement Operation
PEOC4I	Program Executive Officer for Command, Control, Communications, Computers, and Intelligence
PEP	Photographic Exploitation Products
PER	Personnel
PERIGEE	Perspective Image Generation and Exploitation System
PERINTREP	Periodic Intelligence Report
PERINTSUM	Periodic Intelligence Summary
PERM	Processless Electron Recording Media
PERMCERT	Permanent Certification
PERSCON	Personal Contact
PEO	Program Executive Officer
PEO-CCS	PEO Command and Control Systems
PERSEC	Personnel Security
PERT	Program Evaluation and Review Technique
PES	Positive Enable System
PESM	Passive Electronic Support Measures
PF	Protection Factor
PFADS	Psychological Operations Foreign Area Data Subsystem
PFD	Power Flux Density
PFIAB	President's Foreign Intelligence Advisory Board
PFLP	Popular Front for the Liberation of Palestine
PFM	Production Functional Manager

PFOD	Presumptive Finding of Death
PG	(1) Patrol Combatant; (2) Persian Gulf; (3) Precision Guidance
PGDR	Portable Data Reduction System
PGF	Patrol Ship
PGG	Guided-Missile Patrol Combatant
PGH	Patrol Gunboat (Hydrofoil)
PGIP	Postgraduate Intelligence Program
PGM	Precision-Guided Munitions
PGR	Reconnaissance Patrol Combatant
PGW	Precision Guided Weapon
PGSS	Publications and Graphics Subsystem
PHD	Phase History Data
PHIBGRU	Amphibious Group
PHIBRON	Amphibious Squadron
PHIGS	Programmer's Hierarchical Interactive Graphics
PHM	Patrol Combatant Missile (Hydrofoil)
PHOTOINT	Photographic Intelligence
PHOTORECON	Photographic Reconnaissance
PHS	Public Health Service
PHYSEC	Physical Security
PI	(1) Photographic Interpretation/Interpreter; (2) Principal Investigator
PIAC	PACOM Intelligence Architecture Committee
PIB	(1) PACOM Intelligence Board; (2) Photo Interpretation Brief
PIC	(1) Pacific Imagery Processing and Interpretation Center; (2) Parent Indicator Code; (3) Processing and Interpretation Center
PICON	Portable ICON
PIF	(1) Processing and Interpretation Facility; (2) Project Investment Fund
PIGS	Passive Infrared Guidance System
PIICS	PACOM - Intelligence Computer System
PILOT	Phased Integrated Laser Optics Technology
PIM	Path of Intended Movement
PIN	(1) Preliminary Imagery Nomination File; (2) Photographic Intelligence Note; (3) Personal Increment Number; (4) Plan Identification Number; (5) Personal Identification Number; (6) PACOM Intelligence Net
PINES	PACAF Interim National Exploitation Segment/System

PIP	(1) Project Implementation Plan; (2) Product Improvement Package
PIR	(1) Photo Interpretation Report; (2) Priority Intelligence Requirement
PIRATE	Portable Imagery Receive and Transmission Equipment
PIREP	Pilot Report
Pixel	Picture Element
PJ	Pararescue Jumper
PK	(1) Probability of Kill; (2) Soviet (FSU) Light Machinegun; (3) Peacekeeping
PKA	Public Key Algorithm
PKC	Public Key Cryptography
PKK	Kurdistan Worker's Party
PKO	Peace-Keeping Operation
PKSD	Programmable Key Storage Device
PL	(1) Phase Line; (2) Plans and Operations Division; (3) Public Law
PLA	(1) Plain Language Address; (2) People's Liberation Army (China)
PLARS	Position Locating and Reporting System
PLGR	Precision Lightweight GPS Receiver
PLL	Prescribed Load List
PLNG	Planning
PLRS	Position Location Reporting System
PLO	Palestinian Liberation Organization
PLP	PSYOP Leaflet Payload
PLS	Pre-Launch Survivability
PLSDU	Physical Layer Service Data Unit
PLSS	U.S. Precision Location Strike System
PLT/Plt	Platoon
PM	(1) Preventive Maintenance; (2) Post Meridian (after noon); (3) Prime Mover; (4) Preventive Medicine; (5) Program Manager; (6) Prime Minister; (7) Provost Marshall; Project Manager; (8) Production Manager; (9) Peacemaking
PMATS	Program Management Automated Tool Set
PMB	Program Management Board
PME	Professional Military Education
PMF	Project Management File
PMGM	Program Manager's Guidance Memorandum
PMIS	(1) Personnel Management Information System; (2) PSYOP Management Information Subsystem
PMO	(1) Program Management Office; (2) Project Management Office
P Model	Preproduction Model
PMP	Program Management Plan
PMPTS	Program Management Performance Tracking System
PMR	Primary Mission Readiness
PMRP	Program Manager's Recommended Program

PMS	(1) Project Management System; (2) Preventive Maintenance System; (3) Precision Mensuration Software
PMSP	Preliminary Message Security Protocol
PMTC	Pacific Missile Test Center (Navy)
PN	Packet Network
PNAF	Prime Nuclear Airlift Force
PNCC	PASS Network Control Center
PNEK	Post-Nuclear-Event Key
PNE(T)	Peaceful Nuclear Explosion (Treaty)
PNG	Persona Non Grata
PNL	Prescribed Nuclear Load
PNUTS	Possible Nuclear Underground Test Site
PNVS	Pilot Night Vision System
PO	(1) Petty Officer; (2) Peace Operations
POA&M	(1) Plan of Action and Milestones; (2) Plan of Attack and Milestones
POADS	Psychological Operations Automated Data System
POAS	Psychological Operations Automation System
POB	(1) Place of Birth; (2) Psychological Operations Battalion
POC	(1) Point of Contact; (2) Program of Cooperation; (3) Psychological Operations Company
POC/ET	Proof of Concept/Experimental Testbed
POCS	Portable Oxygen Charging System
POD	Port of Debarkation
POE	(1) Plan of Execution; (2) Point of Entry; (3) Port of Embarkation
POES	Polar Orbiting Environmental Satellite
POG	Psychological Operations Group
POI	Program of Instruction
POL	(1) Petroleum, Oils, and Lubricants; (2) Political
POL-MIL	Political-Military
POLAD	Political Advisor
POM	(1) Program Objective Memorandum; (2) Preparation for Overseas Movement
POMCUS	Prepositioned Organizational Materiel Configured in Unit Sets
POOS	Parachute Offset Oxygen System
POP	Point of Presence
POR	Preparation for Oversees Replacement
PORTS (JOPES)	(1) Portable Remote Telecommunications System; (2) Seaports Files; (3) Portable Receive and Transmit System
PORTS-1N	Portable Receive and Transmit System - 1N
PORTSREP	Ports Report File (JCS/J-3)
Pos	Position
POSIX	Preliminary Open System Interface Standard
Pos-Nav	Positioning and Navigation
POST	Prototype Ocean Surveillance Terminal

POTBI	Places, Organizations, Things, Biographics, Intangibles
POTF	Psychological Operations Task Force
POV	Privately Owned Vehicle
POW	Prisoner of War
POWERR	Prototype Workstation for Electronic Warfare and Radio
PP	Preprogramed
PPO	Pilot and Payload Operator
PPBES	Planning, Programming, and Budgeting Execution System
PPBS	Planning, Programming, and Budgeting System
PPC	Printing and Publications Center
PPDB	Point Positioning Data Base
PPF	Photographic Processing Facility
PPGM	Planning and Programming Guidance Memorandum
PPI	Pulse Position Indicator
PPIF	Photographic Processing and Interpretation Facility
PPL	Preferred Products List
PPM	(1) Parts Per Million; (2) Pulse Position Modulation
PPMS	Power Pattern Measurement System
PPS	Precision and Positioning Service
PR	(1) Production Requirement; (2) Personnel Recover
PRA	(1) Permanent Restricted Area; (2) Population Reception Area (NATO)
PRAM	Allied Mine
PRB	Program Review Board
PRBAC	Partition Rule Base Access Control
PRC	(1) Policy Review Committee; (2) People's Republic of China
PRC(I)	Policy Review Committee (Intelligence) (now SIG(I))
PRCSO	Peacetime Reconnaissance and Certain Sensitive Operations
PRD	(1) Production Responsibilities Document; (2) Presidential Review Directive
PRDA	Photo Reconnaissance Damage Assessment
PREMSS	Photo Reconnaissance and Exploitation Management Support System
PREP/RAMP	Pre-Edit Processor/Report and Message Processor
PRF	Pulse Repetition Frequency
PRG	Program Review Group
PRGB	Point Reference Guild Book
PRI	(1) Pulse Repetition Interval; (2) Primary Rate Interface
PRIMAC	Production and Inventory Management and Control System
PRM	Presidential Review Memorandum
PROC	Processing/Process
PROCOMM	Terminal Emulation Software for DOS Workstations
PROD	Production
PROG	Program
PROM	Programmable Read-Only Memory

PROPIN	Caution — Proprietary Information Involved
PRP	Portable Radio Program
PRPG	Preliminary Reference Point Graphic
PRS	PACOM Remote System
PRSCO	Peacetime Reconnaissance and Sensitive Collection Operations
PRT	Personal Rapid Transit
PRTB	Soviet (FSU) Mobile Rocket Technical Base
PRU	Photographic Reconnaissance Unit
PS	(1) Processing Station; (2) Processing Segmext; (3) Policy Support
Ps	Permanent snowfields
PSAA	Pacific Special Activities Area
PSAC	President's Scientific Advisory Committee
PSB	Harbor Patrol Boat
PSC	Principal Subordinate Command (NATO)
PSDU	Physical Layer Service Data Unit
PSI	(1) Pounds Per Square Inch; (2) Personnel Security Investigation
PSK	Phase Shift Keying
PSL	Protected Services List
PSN	(1) Packet Switching Node; (2) Public Switched Network; (3) Packet Switched Network
Psns	Positions
PSO	(1) Protective Structure Only; (2) Personnel Security Office; (3) Post Security Officer
PSP	(1) Pierced Steel Planking; (2) Planning Support Package
PSPS	PSYOP Studies Program Subsystem
PSR	(1) Post-Attack Status Report; (2) Periodic Status Report
PSRC	Presidential Selected Reserve Call-Up
PSS	Packet Switched Service
PST	Pacific Standard Time
PSTN	Public Switched Telecommunications Network
PSYOP	Psychological Operations
PSYOPGP	Psychological Operations Group
PSYWAR	Psychological Warfare
PT	(1) Torpedo Boat; (2) Part Time; (3) Physical Training
Pt	Peat
PTADB	Planning Terrain Analysis Data Base
PTG	Missile Attack Boat
PTGP	Part-Time Graduate Program
PTIAP	PACOM Theater Intelligence Architecture Program
PTL	Small Torpedo Boat
Ptl	Patrol
PTN	Pacific Tributary Network
PTP	(1) Probability to Penetrate; (2) Point-to-Point
PTR/P	Paper Tape Reader/Punch

PTS	Predicasts Terminal System
PTSR	Postmobilization Training Support Requirement
PTSS	Passive Thermal Suppression Suit
PTT	(1) Training Torpedo Boat; (2) Postal, Telephone, and Telegraph; (3) Push to talk
PTTP	USPACOM Tactics, Techniques, and Procedures
PTTDS	Projected Target Trends Data Sheet (FTL)
PTTP	USPACOM Tactics, Techniques, and Procedures
Pub	Publication
PUG	Partially Underground
PUP	(1) Performance Upgrade Program; (2) Pop-Up Point
PV	Physical Vulnerability
PVDS	Physical Vulnerability Data Sheets
PVITS	Portable Video Imagery Transmission System
PVST	Port Visit
PVO	(1) Air Defense (FSU); (2) Private Voluntary Organization
PVTM	Physical Vulnerability Technical Memorandum
PW	(1) Prisoner(s) of War; (2) Pulse Width
PWDS	Protected Wireline Distribution System
PWHQ	Primary War Headquarters
PWI	PACOM Warning Intelligence
PWIPS	Pre-Launch Warning Intelligence Processing System
PWRS	Prepositioned War Reserve Stock
PZ	Pick-Up Zone

Q

QA	Quality Assessment
Q&A	Question and Answer
QBE	Query by Example
QC	Quality Control
QEA	Quick Erect Antenna
QM	Quartermaster
Q-MESSAGE	Classified Message on Navigational Hazard
QOL	Quality of Life
QPQ	Quid Pro Quo
QPSK	Quadrature Phase Shift Keying
Q/R	Query/Response
QRA	Quick Reaction Alert
QRC	Quick Reaction Capability
QRF	Quick Response Force
QRG	Quick Response Graphic
QRLS	Quick Reaction Launch System
QRMP	Quick Response Multicolor Printer
QRP	Quick Reaction Package
QRRC	Quarterly Readiness Report to Congress
QRT	(1) Quick Reaction Task; (2) Quick Reaction Terminal
QRSA	Quick Reaction Satellite Antennae
QRSP	Quick Reaction Shuttle Payload
QSR	Quick Strike Reconnaissance
QSTAG	Quadripartite Standardization Agreement
QUICKSAT	Modified AN/FSC-78
QUIP	Quarterly Intelligence Production Listing

R

R	(1) Rock Outcrops; (2) Receiver
RA	(1) Restricted Area; (2) Responsible Agency; (3) Resident Agent
RAAF	Royal Australian Air Force
RAAP	Rapid Application of Air Power
RAC	Resident Agent in Charge
RACE	Rapid Automatic Cryptographic Equipment
RAF	Royal Air Force
RABFAC	Radar Beacon Forward Air Controller
RAC	Research and Analysis Company
RACO	Rear Area Combat Operations
RAD	Radiation Absorbed Dose
RADAR	Radio Detection and Ranging
RADAREXREP	Radar Exploitation Report
RADAY	Radio Day
RADBN	Radio Battalion
RADC	Rome Air Development Center
RADCM	Radar Countermeasures
RADCOM	Radio Communications
RADCON	Radiological Control
RADIAC	Radioactive Detection, Indication, and Computation
RADINT	Radar Intelligence
RADREL	Radio Relay
RAF	Royal Air Force (U.K.)
RAG	(1) River Assault Group; (2) Regimental Artillery Group (FSU)
RAIDS	Rapid Access Imagery Dissemination System
RAILS	Relational Analyses of Internetted Linkages System
RAM	(1) Rolling Airframe Missile; (2) Random Access Memory; (3) Radar Absorbing Materials; (4) Reliability, Availability, and Maintainability
RAMP	Rating Maintenance Program
RAMPART	Radar Advanced Measurement Program for Analysis of Reentry Techniques
RAOC	(1) Rear Area Operations Center; (2) Regional Air Operations Center
RAOWG	Radar and Optical Intelligence Working Group
RAP	(1) Rocket Assisted Projectile; (2) Remedial Action Projects
RAPIDE	Relocatable Army Processors for Intelligence Data-Europe
RAPIER	Rapid Emergency Reconstitution
RAPTOR	Responsive Aircraft Program for Theater Operations
RAS	(1) Record Assigned Systems; (2) Replenishmest at Sea; (3) Regional Analysis Section; (4) Rear Area Security; (5) Remote Access Support
RASC	Required Automated Services Center

RASS	Random Access Storage System
RAST	Regional Analyst Support Team
RATO	Rocket-Assisted Takeoff
RATT	Radio Teletypewriter/Teleprinter
RATV	Rescue All Terrain Vehicle
RAU	Radio Access Unit
RAWS	RAPIDE Analyst Workstation
RAWSII	Raw Statement of Intelligence Interest
RB/ER	Reduced Blast/Enhanced Radiation
RBIF	Red Basic Intelligence File
RBS	(1) Regional Broadcast System; (2) Remote Base Server
RC	(1) Radio-Controlled; (2) Required Capability; (3) Reserve Component; (4) Riverine Craft
RCA	(1) Riot Control Agent; (2) Royal Canadian Army; (3) Requirements Control Authority
RCAF	Royal Canadian Air Force
RCAS	Reserve Component Automated System
RCC	(1) Regional Control Center; (2) Rescue Coordination Center
RCF	Remote Collection facility
RCM	Radar Countermeasures
RCOC	Regional Communications Operations Center
RCMP	Royal Canadian Mounted Police
RCP	Remote Communications Processor
RCS	(1) Radar Cross Section; (2) Remote Collection System
RCSS	(1) Reconnaissance Cargo; (2) RC-135 Support Service
RCST	RC-135 Support Team
RCU	Reserve Component Unit
RCV	Receive
RCW	Reconfigurable Workstation
RCZ	Rear Combat Zone
RD	(1) Restricted Data; (2) Radius of Damage; (3) Replacement Detachment; (4) Readiness Division
R&D	Research and Development
RD&A	Research, Development, and Acquisition
RDA	Research, Development, Acquisition
RDAISA	United States Army Research, Development & Acquisition Information Systems Agency
RDB	Requirements Data Base
RDBMS	Relational Data Base Management System
RDC	Rapid Deployment Capability
RDD	Required Delivery Date
RDE	Radiation Detection Experiment
RDEC	Research Development Engineering Center
RDF	(1) Radio Direction Finding; (2) Rapid Deployment Force
RDI	Reconnaissance, Detection & Identification
RDIT	Rapid Deployment Imagery Terminals

RDJTF	Rapid Deployment Joint Task Force
RDL	Recurring Document Listing
RDMSS	Rapidly Deployable Mobile SIGINT Systems
RDS	(1) Remote Display System; (2) Rapid Dissemination System
RDSS	Rapidly Deployed Surveillance System
RDT&E	Research, Development, Test and Evaluation
RDV	Rapid Deployment Vehicles
RE	Receive Element
READ	Readiness
READYCAP	Fighter Aircraft in Standby Condition
REC	Radio-Electronic Combat
RECA	Residual Capabilities Assessment
RECA(T)	Residual Capability Assessment (Team)
RECAP	Requirements and Capabilities System
RECAS	Residual Capabilities Assessment System
RECC	Regional Emergency Communications Coordinator
RECCE	Reconnaissance
RECCEXREP	Reconnaissance Exploitation Report
RECI	Radar Emitter Classification Identification
RECLAU	Reconnaissance Launch Report
RECON	Reconnaissance
RECONBN	Reconnaissance Battalion
RECONT	Reconnaissance Intentions Report
REDCOM	Readiness Command
REDCON	Readiness Condition
RED Cell	Rapid Exploitation and Dissemination Cell
RED FLAG	ACC Combat Flying Exercise at Nellis AFB
RED HORSE	Deployable Civil Engineering Group
REDTRAIN	Readiness Training
REFORGER	Return of Forces to Germany (Exercise)
RFC	Request for Collection
REG	Regulation
REGT/Regt	Regiment
REL	Releasable
RELCAN	Releasable to Canada
RELROK	Releasable to the Republic of Korea
REM	Route Evaluation Module
REMAB	Remote Marshalling Base
REMBASS	Remotely Emplaced Battlefield Surveillance System
REMS	Remote Employed Sensors
REMT	Regional Emergency Management Team
RENS	Reconnaissance, Electronic Warfare & Naval Intelligence System
REP	(1) Range Error Probable; (2) Reserve Exploitation Program; (3) Representative

RES	Remote Earth Sensing
Res	Reserve
RESDAT	Restricted Data
RESTA	Reconnaissance, Surveillance & Target Acquisition
RETRANS	Retransmission
RETS	Remoted Target System
REUTERS	A News Service
REW(S)	Radio Electronic Warfare (Service)
REWSON	Reconnaissance, Electronic Warfare, Special Operations & Naval Intelligence Processing System
RF	(1) Radio Frequency; (2) Representative Fraction
RF-4	Designator for Reconnaissance Aircraft (USAF/USMC)
RFA	Restricted Fire Area
RFC	Request for Collection
RFD	Radio Frequency Distribution
RFE/RL	Radio Free Europe/Radio Liberty
RFI	(1) Radio Frequency Interference; (2) Request for Information
RFIS	Reserve Forces Intelligence School
RFL	Restrictive Fire Line
RFMETS	Radio Frequency Mobile Electronics Test Set
RFP	(1) Remaining Force Potential; (2) Radio Frequency Pulse; (3) Request for Proposal; (4) Request for Production
RFPI	Rapid Force Projection Initiative
RFPW	Radio Frequency Pulse Weapon
RFR	Request for Requirements
RFS	Request for Service
RFTB	Reserve Force Target Base
RFTL	Reserve Forces Target List
RGB	Red-Green-Blue
RGR	(1) Ranger; (2) Roger
RGS	Relay Ground Station
RGT	Regiment
RHAW	Radar Homing and Warning
RHIB	Rubber Hull Inflatable Boat
RI	Routing Indicator
RIB	Rigid Inflatable Boat
RIC	(1) Regional Intelligence Center; (2) Resource Identification Code
RIF	Reduction in Force
RII	Request for Intelligence Information
RIM	ROTHR Interface Module
RIMPAC	U.S. Naval Exercise
RIMS	Requirements Inventory Management System
RINT	Unintentional Radiation Intelligence
RIO	Radar Intercept Officer

RIP	(1) Register of Intelligence Publications; (2) Reconnaissance Information Point
RIPL	Reconnaissance and Interdiction Planning Line (NATO)
RIPSO	Revised IP Security Option
RISC	Reduced Instruction Set Computer
RISOP	Red Integrated Strategic Operations Plan
RISP	Reserve Intelligence Support Project
RIT	Remote Imagery Transceiver
RITS	Remote Imagery Transceiver System
RJITF	Regional Joint Intelligence Training Facility
RL	(1) Rocket Launcher; (2) Radio Liberty; (3) Receive Location
RLG	Ring Laser Gyro
RM	(1) Requirements Management; (2) Resource Management
RMBUX	Rocky Mountain Basic UNIX
RMEC	Regional Military Emergency Coordinator
RMG	Resource Management Group
RMO	(1) Records Management Officer; (2) Requirements Management Office
RMS	(1) Requirements Management System; (2) Remote Monitoring System
RNAV	Area Navigation
RNO	Regional Nuclear Option
RNP	(1) Radio Navigation Point; (2) Remote Network Processor
RO	(1) Reporting Officer; (2) Radar Operation; (3) Receive Only; (4) Resident Office
RO/RO	Roll-On/Roll-Off (Ship)
ROB	Radar Order of Battle
ROC	(1) Required Operational Capability; (2) Republic of China; (3) Reconnaissance Operations Center; (4) Required Operational Capability; (5) Regional Operations Center
ROCC	Regional Operations Control Center
ROD	Reconnaissance Operations Division
RODCA	(1) Reporting of DoD HUMINT Collection Activities; (2) Message Caveat
ROE	Rules of Engagement
ROF	(1) Rate of Fire; (2) Remote Operating Facility
ROFA	Remote Operating Facility Airborne
ROIPB	Rear Operations Intelligence Preparation of the Battlefield
ROK	Republic of Korea
ROKA	Republic of Korea Army
ROKAF	Republic of Korea Air Force
ROKN	Republic of Korea Navy
ROKUSCFC	Republic of Korea and U.S. Combined Forces Command
ROM	Read Only Memory
RON	Remain Overnight
ROP	Remote Operating Position
RORSAT	Soviet (FSU) Radar Ocean Reconnaissance Satellite

ROSE	Remote Optical Sensing of the Environment
ROSS	Refinement of SIGINT Support
ROT	Rotating Position
ROTC	Reserve Officer Training Corps
ROTHR	Relocatable Over-the-Horizon Radar
ROU	Radius of Uncertainty
ROW	Rest-of-World
RP	(1) Reference Point; (2) Release Point
RPA	Reserve Personnel Allotment
RPB	Regional Preparedness Board
RPC	(1) Regional Preparedness Committee; (2) Regional Reporting Center; (3) Remote Procedure Calls; (4) Rapid Positioning Capability
RPE	Reconnaissance Planning Element
RPG	(1) Soviet (FSU) Shoulder-Fired Antitank Grenade Launcher; (2) Report Program Generator
RPK	Soviet (FSU) Light Machinegun (similar in design to the AK rifle)
RPM	(1) Revolutions per Minute; (2) Rounds per Minute
RPT	Report
RPTG	Reporting
RPV	Remotely Piloted Vehicle
RQS	Rescue Squadron
RQT	(1) Reliability Qualification Tests; (2) Requirement
RQMTS	Requirements
RR	(1) Railroad; (2) Radio Relay
R&R	Rest and Recreation
RRC	Regional Reporting Center
RRDB	Rapidly Reconfigurable Data Base
RRF	(1) Ready Reserve Force; (2) Rapid Reaction Force (ACE)
RRG	Remote Receive Group
RRI	Response to Request for Information
RRICS	Rapid Response Imagery Capability System
RRII	Response to Request for Intelligence Information
RRM	Red Resource Monitoring
RRP	Rapid Reinforcement Plan
RRS	Remote Receive Station
RRT	Radio Receive/Transmitter
RRTP	Rail-to-Road Transfer Point
RS	Reconnaissance/Surveillance
R&S	Reconnaissance and Surveillance
RSB	PSYOP Regional Support Battalion
RSBN	Short-Range Navigation System (FSU)
RSDN	Long-Range Navigation System (FSU)
RSC	(1) Regional Support Commands; (2) PSYOP Regional Support Company
R&SC	Reconnaissance and Surveillance Center

RSE	Ranger Support Element
RSI, R/S/I	Rationalization, Standardization and Interoperability
RSN	Red Switched Network
RSO	(1) Reconnaissance & Survey Officer; (2) Regional Security Officer
RSOC	Regional SIGINT Operations Center
RSOD	Remote Satellite Operations Demonstration
RSOG	Reserve Special Operations Group
RSR	(1) Resource Status Report; (2) Required Supply Rate; (3) Radar Service Request
RSSC	Regional Space Support Centers
RSSP	Reconnaissance Support Survivability Program
RST	(1) Recovery Support Team; (2) Regional Survey Team
RSTA	Reconnaissance, Surveillance, & Target Acquisition
RSW	Reflected Shockwave
RT	(1) Real Time; (2) Radio Telephone; (3) Relocatable Target; (4) Radius of Target
RTA	Residual Threat Assessment
RTAPS	Relocatable Target Adaptive Planning Support
RTASS	Remote Tactical Airborne SIGINT System
RTCE	Rapid Targeting Capability Europe
RTG	Reconnaissance Technical Group (TAC, USAFE, PACAF)
RTIC	(1) Regional Threat Information Cell; (2) Real-Time Information to the Cockpit
RTIP	Real-Time Interactive Processor
RTM	Receiver/Transmitter/Modem
RTOS	Real-Time Optical System
RTP	Rail Transfer Point
RTS	(1) Reconnaissance Technical Squadron; (2) Real-Time Simulator
RTS-I	Regional Training Site(s)-Intelligence
RTSP	Real-Time Signal Processor
RU	(1) Roundup; (2) Resident Unit
RUNT	Russian Underground Nuclear Test
RURPOP	Rural Population File
RV	(1) Reentry Vehicle; (2) Radius of Vulnerability; (3) Reconnaissance Vehicle
RVT	Remote Video Terminal
RW	(1) Radiological Warfare; (2) Rotary Wing; (3) Reconnaissance Wing
RWH	Radar Warning & Homing
RWI	Radio Wireline Interface/Integration
RWO	Reconnaissance Watch Officer
RWR	Radar Warning Receiver
RWS	Remote Workstation
RX	Receive
RZ	Recovery Zone

S

S	Secret
/s/	Signature
S-1	Personnel Staff Officer
S-2	Intelligence Staff Officer; Brigade, Battalion, and Armored Cavalry
S-3	Operations Staff Officer
SA	(1) Logistics Staff Officer; (2) Special Access; (3) Situational Awareness (4) Signals Analysis; (5) Surface-to-Air; used to identify FSU Surface-to-Air Missiles, e.g., SA-7/GRAIL; (6) Situation Assessment; (7) Security Assistance; (8) Special Agent; (9) Stand Alone; (10) Secretary of the Army; (11) Systems Administrator; (12) Strategic Attack
SAA	(1) Special Area Assessments; (2) Strategic Air Army
SAAC	Strategic Analysis Applications Center
SAAM	Special Assignment Airlift Mission
SAASE	Standard Data Element-Based Automated Architecture Support Environment
SACC	Supporting Arms Coordination Center
SACCS	Strategic Air Command Automated Command & Control System
SACS	(1) Secure Access Control System; (2) STU-III Access Control System
SAE	Service Acquisition Executive
SAB	Subject as Above
SAC	(1) Strategic Air Command; (2) Scientific Advisory Committee; (3) Senate Appropriations Committee
SACDIN	SAC Digital Network
SACEUR	Supreme Allied Commander, Europe (NATO)
SACLANT	Supreme Allied Commander, Atlantic (NATO)
SACLANTREPEUR	SACLANT Representative in Europe
SACOM	Southern Area Command
SACOS	SAC Operational Staff
SACWARNS	(1) Strategic Air Command Indications and Warning; (2) SAC Warning System
SADARM	Sense and Destroy Armor
SADF	South African Defense Force
SADO	Senior Air Defense Officer
SADT	Structured Analysis Design Technique
SAEDA	Subversion and Espionage Directed Against the Army
SAF	(1) Soviet (FSU) Air Force; (2) Source Acquisitions File; (3) Secretary of the Air Force; (4) US Air Force Staff
SAFE	(1) Support for the Analysts' File Environment; (2) Selected Area for Evasion
SAFF	Safing, Arming, Fuzing, and Firing
SAF/O/T	Security Assistance Force/Organization/Team
SAG	(1) Study Advisory Group; (2) Surface Action Group; (3) Strategic Advisory Group

SAGE	Semiautomatic Ground Environment (Radar)
SAI	Strategic Command Administrative Instruction
SAIB	Safe Area Intelligence Brief
SAID	Safe Area Intelligence Description
SAIS	Strategic Aerospace Intelligence System
SAL	(1) Strategic Arms Limitation; (2) Submarine Alerting and Locating
SALT	(1) Strategic Arms Limitation Talks; (2) Supporting Arms Liaison Team
SALUTE	Size, Activity, Location, Unit, Time, Equipment (spot report format)
SAM	(1) Surface-to-Air Missile; (2) Summary Assessment Matrix
SAMOB	Surface-to-Air Missile Order of Battle
SAMSO	Space And Missile System Organization
SAMT	State of the Art Medium Terminals
SAO	(1) Special Access/Activities Office; (2) Select Attack Option; (3) Special Access Only; (4) Security Assistance Organization; (5) Security Assistance Office
SAOB	FSU Air Order of Battle
SAOC	(1) Space Actions Officers Course; (2) Sector Air Operations Center
SAOCS	Submarine/Aircraft Optical Communications System
SAP	(1) Special Access Program; (2) System Acquisition Plan
SAPAS	Semiautomatic Population Analysis System
SAR	(1) Search and Rescue; (2) Synthetic Aperture Radar; (3) Special Access Required; (4) Sea-Air Rescue
SARC	Surveillance and Reconnaissance Center
SARDA	Secretary of the Army for Research, Development and Acquisition
SARP	Storage and Retrieval Processor
SARPF	Strategic Air Relocatable Processing Facility
SARSAT	Search and Rescue Satellite-Aided Tracking
SART	Strategic Aircraft Recovery Team
SARV	Strategic Aerospace Reconnaissance Vehicle
SAS	(1) Strategic Area Study; (2) Strategic Aerospace Summary; (3) Special Activities Squadron; (4) Support to Analyst Subsystem; (5) Survivable Adaptive Systems
SASC	Senate Armed Services Committee
SASM	Strategic Air-to-Surface Missile
SASS	(1) Small Aerostat Surveillance System; (2) Systems Acquisition Support Services
SAT	(1) Satellite; (2) Staff Augmentation Team; (3) Satisfactory
SATCOM	Satellite Communications
SATCOMA	Satellite Communications Agency (U.S. Army)
SATKA	Surveillance, Acquisition, Tracking, and Kill Assessment
SATRAN	(1) Satellite Reconnaissance Advanced Notice; (2) Satellite Transmission
SATS	Southwest Asia Telecommunications System
SATVUL	Satellite Vulnerability

SAVE	Situation Analysis and Vulnerability Estimate
SAVI	Systems Analysis of Vulnerability to Intrusion
SAWC	Special Air Warfare Center
SAWG	Simulation and Analysis Working Group
SAWIC	Strike and Amphibious Warfare Intelligence Center
SAWS	Submarine Analyst Work Station
SAWVS	Satellite Attack Warning and Verification System
SB	Sentinel Byte
S-BAND	2 to 4 GHz
SBB	Sustained Bare Base
SBI	(1) Special Background Investigation; (2) Space-Based Interceptor
SBIRS	Space-based Infrared Radar System
SBIS	Sustaining Base Information Services
SBKKV	Space-Based Kinetic Kill Vehicle
SBL	Space-Based Laser
SBM	Single-Point Mooring Buoy
SBR	(1) Special Boat Squadron; (2) Space-Based Radar
SBS	Site Backbone Segment
SBSS	Space-Based Surveillance System
SBU	(1) Special Boat Unit; (2) Sensitive but Unclassified
SBWASS	Space-Based Wide-Area Surveillance System
SC	(1) Science Committee (NATO); (2) Signal Corps; (3) Security Code; (4) Signal Company; (5) System Center; (6) Structural Category; (7) Screen Commander or Coordinator; (8) Air Force Communications-Computers Directorate; (9) Submarine Conversion
SCA	Service Cryptologic Agency
SCAD	Subsonic Cruise Armed Decoy
SCAMP	Sensor Control and Management Platoon
SCAMPI	SOF C3I Telecommunications System
SCARE	Standard Collection Asset Request Format
SCATANA	Security Control of Air Traffic and Air Navigation Aids
SCC	(1) Special Coordination Committee; (2) Standing Consultative Commission (SALT); (3) Surveillance Coordination Center; (4) System Control Center; (5) Space Control Center; (6) Service Component Commander
SC CAT	SOUTHCOM Crisis Action Team
SCC(I)	Special Coordination Committee (Intelligence)
SCCP	Single-Channel Command Post
SCCS-R	Single-Channel Collection System - Rear
SCCTV	Secure Closed-Circuit Television
SCDL	Surveillance and Control Data Link (JSTARS)
SCE	Service Cryptologic Element
SCF	Satellite Control Facility
SCF-UK	Save the Children Federation-UK
SCG	Special Consultative Group (NATO)

SCI	(1) Sensitive Compartmented Information or Information Programs; (2) Source Code Indicator
SCIBS	Sensitive Compartmented Information Billet System
SCIC	State Crime Information Center
SCIF	Sensitive Compartmented Information Facility
SCIM	Subject Codes for Intelligence Management
SCIMITAR	System for Countering Interdiction Missiles and Target Radars
SCINET	Sensitive Compartmented Information Network (DoDIIS)
SCIP	Special Communications Intelligence Package
SCIPMIS	Standard Civilian Personnel Management Information System
SCIPS	Sensitive Compartmented Information Processing System
SCIS	Survivable Communication Information System
SCISS	SOUTHCOM Intelligence Support System
SCI-VTC	Sensitive Compartmented Information-Video Teleconferencing
SC J2	USSOUTHCOM J2
SCL	Standard Conventional Load
SCLNO	SOUTHCOM Liaison Officer
SCM	Security Countermeasures
SCN	Satellite Control Network
SCO	(1) Service Cryptologic Organizations; (2) Sub-Control Office
SCOLA	Satellite Communications for Learning
SCORE	Signal Communications by Orbiting Relay Equipment
SCOTT	Single-Channel Objective Tactical Terminal
SCP	Secure Conferencing Project
SCPC	Single Channel per Carrier
SCS	(1) Signal Collection System; (2) Satellite Control Squadron
SCSC	SOUTHCOM Support Center
SCSI	Small Computer Systems Interface
SCT	(1) Single-Channel Terminal; (2) Single-Channel Transponder
SCUBA	Self-Contained Underwater Breathing Apparatus
SCUD	Nickname of a Missile System
SD	(1) Space Director; (2) Standard Displacement; (3) Senior Director; (4) Security Division; (5) Strategic Command Directive
SDA	(1) Ships Destination Authority; (2) Strike Damage Assessment
S&DA	Strike and Damage Assessment
SDB	Space Data Base
SDC	(1) Strategic Dissemination Company; (2) Strategic Defense Command
SDD	Secure Data Device
SDF	Structured Data Fields
SDHS	Satellite Data Handling System
SDI	Strategic Defense Initiative
SDIE	Special Defense Intelligence Estimate

SDIN	(1) Secure Digital Information Network; (2) Special Defense Intelligence Notice
SDIO	Strategic Defense Initiative Organization
SDIS	Switched Digital Integrated Service
SDLC	Synchronous Data Link Control
SDM	Standoff Destructive Munition
SDMA	Spaced Division Multiple Access
SDMS	SINET Data Management System
SDNRIU	Secure Digital Network Radio Interface Unit
SDNS	Secure Data Network System
SDO	System Development Office
SDOB	Scaled Depth of Burst
SDR	(1) Source-Directed Requirements; (2) System Design Review
SDS	(1) Satellite Data System; (2) SIGINT Direct Support; (3) Satellite Dissemination System; (4) Secondary Dissemination System; (5) Strategic Defense System; (6) Switched Data Services; (7) Spatial Data Server; (8) Small Digital Switch
SDV	(1) Swimmer Delivery Vehicle; (2) SEAL Delivery Vehicle
SDVT	SEAL Delivery Vehicle Team
SDYS	Studies
SE	Southeastern
SEA	(1) Southeast Asia; (2) Senior Enlisted Advisor
SEABEE	Navy Construction Battalion Personnel
SEALANCE	Anti-Submarine Warfare Standoff Weapons (ASW/SOW)
SEAD	Suppression of Enemy Air Defense
SEADS	Southeast Air Defense Sector
SEAGA	Selective Employment Air Ground Alert Forces
SEAL	Sea/Air/Land
SEASTAG	SEATO Standardization Agreement
SEATO	Southeast Asia Treaty Organization
SEAWATCH	NOSIC On-Line Computer System
SEC	(1) Second; (2) Section; (3) Submarine Element Coordinator
SECAF	Secretary of the Air Force
SECARMY	Secretary of the Army
SECC	Survivable Enduring Command Center
SECCLEAR	Security Clearance (Management System)
SECDEF	Secretary of Defense
SECNAV	Secretary of the Navy
SECOM	Security Committee
SECS	Survivable and Enduring Communications System
SECSTATE	Secretary of State
SECTY	Security
SED	Simulated Electronic Deception
SEDSCAF	Standard ELINT Data System Codes and Formats

SEE	(1) System Engineering and Evaluation; (2) Softcopy Exploitation Environment
SEEI	Special Essential Elements of Information
SEEK	Soviet Emigre Exploitation Kit
SEI	Specific Emitter Identification
SEIP	Senior Enlisted Intelligence Program
SEIS	Survivable and Enduring Intelligence System
SELA	Latin American Economic System
SELORS	Ship Emitter Locating Reports
SELMON	Selective Monitoring
SEMA	Special Electronic Mission Aircraft
SEMEC	SOF Enhanced Moldable Explosive Change
SEN	(1) Small Extension Node; (2) Space Engagement Node
SEOS	SIGINT/Electronic Warfare Operating System
SEP	(1) Selective Employment Plan (NATO); (2) Separate
SEPA	FSU Extended Planning Annex
SEPS	NATO Selective Employment Plan
SERE	Survival, Evasion, Resistance, and Escape
SERER	Survival, Evasion, Resistance, Escape, and Recovery
SERNO	Serial Number
SES	(1) Surface Effects Ship; (2) Systems Engineering Study; (3) Senior Executive Service; (4) Sensor Employment Squadron; (5) Softcopy Exploitation System; (6) Societe European Des Satellites
SESOCC	Southeastern Sector Operations Control Center
SESS	Space Environment Sensor Suite
SET	Sensor Employment Teams
SETAF	Southern European Task Force
SEVOCCS	Secure Voice Command and Control System
SEVOX	Secure Voice
SEWC	Space and Electronic Warfare Commander
SEWCC	SIGINT/Electronic Warfare Coordination Center
SEWS	(1) Satellite Early Warning System; (2) SIGINT Electronic Warfare Subsystem
SF	(1) Special Forces; (2) Standard Form
SFA	Security Fault Analysis
SFAT	Strategic Forces Advisory Team
SFD	Saturated Flux Density
SFEM	Space Forces Engagement Model
SFG	Special Forces Group
SFG-A	Special Forces Group-A
SFG(A)	Special Forces Group (Airborne)
SFOA	Special Forces Operations Area
SFOB	(1) Special Forces Operating Base; (2) Soviet (FSU) Forces Order of Battle
SFOD	Special Forces Operational Detachment

SFODA	Special Forces Operational Detachments-A
SFOD-D	First Special Forces Operational Detachment-Delta
SFOS	Special Forces Operating System
SFQC	Special Forces Qualification Course
SFR	Statement of Functional Requirement
SFRD	Safe Functional Requirements Document
SFT	Secure Fault Tolerant
SFTL	Strategic Future Targets List
SFUG	Security Features Users Guide
SGB	SOUTHCOM Ground Order of Battle
SGDPS	Second Generation Data Processing System
SGEMP	System Generated Electromagnetic Pulse
SGF	(1) Southern Group of Forces (Soviet Forces in Hungary); (2) Synthetic Aperture Radar Ground Facility
SGS	(1) Secretary to the General Staff; (2) Squadron Ground Station
SGT	(1) Satellite Ground Terminal; (2) Sergeant
SHA	Secure Hast Algorithm
SHAPE	Supreme Headquarters Allied Powers Europe (NATO)
SHARES	Shared HF Resources
SHC	Supreme High Command
SHF	Super High Frequency
SHED	Special Handling and Evaluation Detachment
SHELREP	Shell Report
SHF	Super High Frequency
SHOP	Special Handling for Operations Purposes
SHORAD	Short-Range Air Defense
SI	(1) Special Intelligence; (2) Special Instructions
S&IA	Security and Investigative Activities
SIAB	Senior Imagery Advisory Board
SIAD	Strategic Imagery Analysis Detachment
SIAP	Strategic Intelligence Architecture Program
SIB	Special Intelligence Brief
SIC	(1) Subject Indicator Code (NATO message code); (2) System Integration Configuration
SICAM	SIGINT Control and Analysis Module
SICR	Specific Intelligence Collection Requirement
SID	(1) Secondary Imagery Dissemination; (2) Subscriber Identification
SID(S)	Selective Imagery Dissemination (System)
SIDA	Single Integrated Data Base
SIDAC	Single Integrated Damage Assessment Code
SIDPAC	Strategic Imagery Detachment Pacific
SIDS	Secondary Imagery Dissemination System
SIE	Space Intelligence Element
SIF	Special Interrogation Facility

SIFR	Special Intelligence Functional Requirement
Sig	Signal
SIGCEN	U.S. Army Signal Center
SIG-I	Senior Interagency Group for Intelligence
SIGINT	Signals Intelligence
SIGSEC	Signals Security
SIGSUM	SIGINT Summary
SII	Statement of Intelligence Interest
SIIR	Special Imagery Interpretation Report
SIL	Systems Integration Laboratory
SIM	(1) Sensor Interface Module; (2) Systems Integration Management
SIMIR	USSTRATCOM IDHS Monthly Integration Review
SIMM	Single Inline Memory Module
SIMNET	Single Channel Ground/Airborne Radio Sub-Systems
SIMO	SIM Office
SIMP	Space Intelligence Master Plan
SIMS SOUTHCOM	Intelligence Management System
SINCGARS	(1) Single Integrated Channel Ground and Airborne Radio Subsystems; (2) Single Channel Ground-to-Air Radio System
SINET	Strategic Intelligence Network
SINTER	SIGINT/IMINT Interaction
SIO	(1) Senior Intelligence Officer; (2) Space Intelligence Officer; (3) Ship's Intelligence Officer
SIOP	Single Integrated Operational Plan
SIORI	Self-Initiated Operational Readiness Inspection
SIPE	Strategic Intelligence Processing Element
SIPRNET	Secret Internet Protocol Router Network
SIR	(1) Shuttle Imaging Radar; (2) Specific Information Requirements; (3) Spectrum Interferance Resolution
SIRADS	Shared Imagery Repository and Dissemination System
SIRCS	Shipborne Intermediate-Range Combat System
SIREP	Sensitive Information Report
SIRVES	SIGINT Requirements Validation and Evaluation Subcommittee (of SIGINT Committee)
SIS	(1) Significant Indications Summary; (2) Space Intelligence System; (3) Special Intelligence Support; (4) Selective Inquiry System; (5) Special Information System
SISOCS	Army Logistics/Maintenance Depot Data Network
SISR	SIGINT Security Regulation
SISS	(1) Survivable Intelligence Support to SlOP; (2) Subcommittee on Information Systems Security of the NSTISSC
SISUM	Sensitive Information Summary
SIT	Specialized Investigations Team
SITAS	Strategic Industrial Target Analysis Systems
SITDEV	Situation Development
SITMAP	Situation Map

SITREP	Situation Report
SITS	Secondary Imagery Transmission System
SITSUM	Situation Summary
SITTP	(US)STRATCOM Intelligence Tactics, Techniques, and Procedures for Strategic Operations
SIW	Strategic Intelligence Wing
SJA	Staff Judge Advocate
SJCS	Secretary, Joint Chiefs of Staff
SKCATL	South Korea Conventional Air Target List
SKE	Station-Keeping Equipment
SKYLINK	Communications System Provided by the Diplomatic Telecommunications System
SKYNET	United Kingdom Military Communications Satellite
SL	Sea Level
SLA	Special U.S. Liaison Advisor
SLAM	Standoff Land Attack Missile (Navy)
SLAR	Side-Looking Airborne Radar
SLAT	Surface-Launched Air-Targeted
SLBM	Submarine-Launched Ballistic Missile
SLC	Space Launch Complex
SLCM	(1) Submarine-Launched Cruise Missile; (2) Sea-Launched Cruise Missile
SLDCOM	Satellite Launch Dispenser Communications
SLED	Safe Low-Energy Detonators
SLEP	Service Life Extension Program
SLF	Super Low Frequency
SLFCS	Survivable Low Frequency Communications System
SLGR	Small Lightweight Global Positioning System Receiver
SLIP	Serial Line Interface Protocol
SLMM	U.S. Submarine-Launched Mobile Mine
SLO	Space Liaison Officer
SLOC	Sea Lines of Communication
SLOC(S)	Sea Line(s) of Communication
SLR	Side-Looking Radar
SLS	Space Launch Squadrons
SLSSM	Submerged-Launched Surface-to-Surface Missile
SLV	Space Launch Vehicle
SM	(1) Memorandum by the Secretary, JCS; (2) Statute Mile; (3) Service Member; (4) Security Monitor; (5) Smart Modules
SMAA	Submarine Movement Advisory Authority
S/MANCO	Space/Missile Analyst NCO
SMANCO	Space/Missile Analyst NCO
SMART-T	Secure Mobile Antijam Reliable Tactical Terminal
SMCC	Survivable Mobile Command Center
SMDPS	Strategic Mission Data Preparation System
SME	Subject Matter Expert

SMEB	Significant Military Exercise Brief
S/MEO	Space/Missile Event Office
SMG	Standard Mail Guard
SMIOC	Senior Military Intelligence Officers' Conference
SMLM	Soviet (FSU) Military Liaison Mission
SMM	(1) Spatial Model Matching; (2) Special Mission Mandatory Modification
SMO	(1) Support to Military Operations; (2) Senior METOC Officer; (3) Special Mission Optional Modification
SMOB	Strategic Missile Order of Battle
SMOTEC	Special Missions Operational Test and Evaluation Center
SMP	Soviet Military Power (the publication)
SMPAS	Space Mission Payload Assessment System
SMR	Sources, Methods, and Rationale
SMS	Stand-Alone Analysis Subsystems
SMTP	Single Mail Transfer Protocol
SMU	Secure Mobile Unit
SNA	(1) Soviet Naval Aviation; (2) System Network Architecture
SNAP	Soviet (FSU) Nuclear Artillery Projectile
SNCCDIPP	Selected Non-Communist Countries DIPP
SNDV	Strategic Nuclear Delivery Vehicles
S/NF	Secret/NOFORN
SNF	(1) Short-Range Nuclear Forces; (2) Secret NOFORN
SNI	Soviet (FSU) Naval Infantry
SNIE	Special National Intelligence Estimate
SNIP	Soviet (FSU) Naval Imagery Panel
SNM	Special Nuclear Materials
SNMS	Security and Network Management Segment
SNO	Special Naval Operations
SNR	Signal-to-Noise
SNS	Shared Network Server
SNUTR	SIGINT Numerical Tasking Register
SO	Special Operations
SO/LIC	Special Operations/Low Intensity Conflict
SOA	(1) Special Operations Aviation; (2) Special Operations Area; (3) Speed of Advance
SOAB	(1) Special Operations Aviation Battalion; (2) Special Operations Aviation Brigade
SOAC	(1) Special Operations Aviation Command; (2) Special Operations Aviation Company; (3) Special Operations Acquisition Center
SOAD	Special Operations Aviation Detachment
SOADS	Special Operations Automated Data System
SOAE	Deputy for Acquisition and Acquisition Executive
SOAG	Special Operations Aviation Group
SOAR	(1) Special Operations Aviation Regiment; (2) Special Operations Analytical Reports

SOARS	Satellite On-Board Attack Reporting System
SOB	Space Order of Battle
SOC	(1) Special Operations Command; (2) Special Operations Capable; (3) Sector Operations Center; (4) Special Operations Craft
SOCACOM	Special Operations Command-Atlantic Command
SOCC	(1) Sector Operational Control Center; (2) Special Operations Control Center
SOCCE	(1) Special Operations Command Communications Element; (2) Special Operations Command and Control Element
SOCCENT	(1) Special Operations Command Center; (2) Special Operations Command Component, CENTCOM
SOCCMO	Special Operations Command Collection Management Office
SOCCS	Special Operations Combat Control Squadron
SOCCT	Special Operations Combat Control Team
SOCDSS	Special Operations Command Deployable Support Set
SOCET	Special Operations Command Extraction Tool
SOCEUR	Special Operations Command, Europe
SOCJIC	United States Special Operations Command Joint Intelligence Center
SOCKOR	Special Operations Command, Korea
SOC-K	Special Operations Command, Korea
SOCLANT	Special Operations Command, Atlantic
SOCLITE	Special Operations Command Laptop
SOCOM	Special Operations Command
SOCOORD	Special Operations Coordination Element
SOCOS	Special Operations Command Operating Staff
SOCPAC	Special Operations Command, Pacific
SOCRATES	Special Operations Command Research, Analysis, and Threat Evaluation System
SOCSIDS	Special Operations Command - Secondary Imagery Dissemination System
SOCSO	Special Operations Command, South
SOCSOUTH	Special Operations Command, South
SOD	Special Operations Detachment
SODARS	Special Operations Debriefing and Retrieval System
SOEAID	Special Operations Executive Aide
SOF	Special Operations Forces
SOF-IV	Special Operations Forces-Intelligence Vehicle
SOF C4I	Special Operations Forces Command, Control, Communications, Computers, and Intelligence
SOF-MOSS	SOF Modular Remote Sensing System
SOFA	Status of Forces Agreement
SOFATS	Special Operations Forces Aircrew Training System
SOFCOM	Special Operations Forces Command
SOF EW	Special Operations Forces Enhanced Weapons
SOFPAC	Special Operating Forces, Pacific
SOFI	Special Operations Forces Improvements

SOF IRIS	Special Operations Forces Imagery Receiver and Intelligence System
SOFIST	Foreign Instrumentation Signals Requirement (a collection management software application)
SOFLAM	Special Operations Forces Laser Acquisition Marker
SOFPARS	Special Operations Forces Planning and Rehearsal System
SOF PLD	Special Operations Forces Protection Laser Defense
SOFPREP	Special Operations Forces Planning, Rehearsal and Execution Preparation
SOF PSA	Special Operations Forces Power Supply Assembly
SOFSA	Special Operations Forces Support Activity
SOFTACS	Special Operations Forces Tactical Assured Connectivity System
SOG	Special Operations Group
SOH	SOF Offensive Handgun
SOHFRAD	Special Operations HF Radio
SOHI	Seminar on Human Intelligence
SOI	(1) Signal Operating Instructions; (2) Signal of Interest; (3) Space Object Identification
SOIC	(1) Space Operational Intelligence Center; (2) Senior Official of the Intelligence Community; (3) Special Operations Intelligence Center
SOICS	Special Operations Improved Cryptographic System
SOIF	Special Operational Intelligence Folders
SOIN	Special Operations Intelligence Notes
SOINT	Staff Officer Intelligence
SOIPS	Special Operations Imagery Production System
SOIS	Special Operations Intelligence System
SOISUM	Space Object Identification Summary
SOIT	Seminar on International Terrorism
SOIWSD	Special Operations Information Warfare Support Demonstration
SOJ	(1) Sea of Japan; (2) Stand-Off Jamming
SOJTF	Special Operations Joint Task Force
SOLANT	South Atlantic
SOLARS	SAC On-Line Analysis and Retrieval System
SOLE	Special Operations Liasion Element
SOLIS	SIGINT On-Line Intelligence (or Information) System
SOLL	Special Operations Low Level
SOLOG	Special Operations Logistics System
SOMA	Status of Mission Agreement
SOME	Satellite Orbit Mission Evaluation
SOMOB	Strategic Offensive Missile Order of Battle
SOMPF	Special Operations Mission Planning Folder
SOMS	Special Operations Media System
SON	Statement of Need
SONAR	Sound Navigation and Ranging
SONET	Synchronous Optical Network

SONI	Seminar on National Intelligence
SONMET	Special Operations Naval Mobile Environmental Teams
SOO	Space Operations Officer
SOP	(1) Standard Operating Procedure(s); (2) Senior Officer Present
SOPE	Special Operations Planning Exercise
SOPEO	Special Operations Program Executive Officer
SOPIF	Special Operations Photographic Interpretation Facility
SOPM	Special Operations Program Manager
SOPPC	Special Operations Photo Processing Cell
SOPPREP	Special Operation Forces Planning, Rehearsal, and Execution System
SOPS	(1) Space Operations Squadron; (2) Special Operations Power Sources
SOR	(1) Specific Orders and Requests; (2) Statement of Requirements
SORD	System Operational Requirements Document
SORDAC	Special Operations Research, Development and Acquisition Center
SORFMS	Special Operations Radio Frequency Management System
SORS	(1) Specific Order or Requests; (2) SIGINT Overhead Reconnaissance Subcommittee
SORTIEALOT	Sortie Allotment
SORTIC	Seminar on Reconnaissance and Technical Information Collection
SORTS	Status of Resources and Training System
SOS	(1) International Distress Signal (2) Squadron Officers' School; (3) Special Operations Squadron
SOSC	Special Operations Support Command
SOSS	Satellite Ocean Surveillance System
SOSST	Special Operations Small Secure Transceiver
SOST	Special Operations Special Technology
SOSTI	Seminar on Scientific and Technical Intelligence
SOSOS	U.S. Sound Surveillance System
SOT-A	Special or Support Operations Team-Alpha
SOTA	SIGINT Operational Tasking Authority
SOTAS	Standoff Target Acquisition System
SOT-B	Special or Support Operations Team-Bravo
SOTF	(1) Special Operations Task Force; (2) Security Operations Training Facility
SOTSE	Special Operations Theater Support Element
SOTVS	Special Operations Tactical Video System
SOTW	Special Operations Training Wing
SOUTHAM	South America
SOUTHCOM	Southern Command
SOVPACFLT	Soviet Pacific Fleet
SOW	(1) Statement of Work; (2) Special Operations Wing
SOW/TE	Special Operations Weather/Technical Element
SOWG	Special Operations Working Group

SOWT	Special Operations Weather Team
SP	(1) Self-Propelled; (2) Shore Patrol; (3) Security Police
SPA	(1) Special PSYOP Analysis; (2) Special PSYOP Assessment
SPACDEFENSE	Space Defense and Operations/Anti-Satellite (ASAT) Missile System
SPACC	Space Command Center
SPACEAF	Space Air Force (14 AF)
SPACECOM	Space Command (See AFSPACECOM and USSPACECOM)
SPACING	Space Processing and Collection Internals Group
SPAD	Special Advisor
SPADATS	Space Detection and Tracking System
SPADCCS	Space Defense Command and Control System
SPADOC	Space Defense Operations Center
SPADVOS	Spaceborne Direct View Optical Scanner
SPAF	Special Airfield File
SPAIS	South Pacific Air Intelligence System
SPAN	Security Policy Automation Network
SPATS	Strategic Posture and Aerospace Threat Summary
SPB	Special Projects Branch (NATO)
SPC	SIGINT Processing Center
SPCL	Special Purpose Communications Link
SPD	Strategic Posture Display
SPEAR	(1) Signal Processing, Evaluation, Alert and Reporting; (2) SOF Personal Equipment Advanced Requirements
SPEC	Counterterrorism Database
Spec Nav	Special Navy Program
SPECAT	Special Category (Pneumatic Tube Message Precedence)
SPECBOATRON	Special Boat Squadron
SPECBOATUNIT	Special Boat Unit
Spectre	AC-130 H/U Gunship
SPECWAR	Special Warfare
SPETSNAZ	Soviet (FSU) Special Purpose Forces
SPF	(1) Special Purpose Forces; (2) Single Point of Failure
SPG	(1) Self-Propelled Gun; (2) Softcopy Products Group
SPIES	Special Insertion and Extraction System
SPIN	Space Intelligence Notes
SPINS	Special Instructions
SPINTCOM	Special Intelligence Communications (Network)
SPIREP	Spot Intelligence Report
SPIRES	Special Intelligence Reports
SPIRIT	Special Purpose Integrated Remote Intelligence Terminal
SPK	Single Point Key(ing)
SPO	Special Project Officer
SPOC	Space Operations Center
SPOD	Sea Ports of Debarkation

SPOE	Sea Ports of Embarkation
SPOT	Satellite Pour l'Observation de la Terre (French)
SPOTREP	Spot Report
SPP	Shared Production Program
SPR	Strategic Petroleum Reserve
SPRAA	Strategic Plans and Research Analysis Agency
SPS	Scratch Pad Store
SPS	Special PSYOP Study
SPSS	Secured Packet Switched Service
SPT	Support
SPTCONF	Support Confirmation
SPTD	Supported
SPTG	Supporting
SPTREQ	Support Request
SQ	(1) Square; (2) Squadron
SQD	Squad
SQDN	Squadron
SQL	(1) Standard Query Language; (2) Structured Query Language
SQN	Squadron
SR	(1) Special Reconnaissance; (2) Short Range; (3) Southern Region; (4) Senior
SRBM	Short-Range Ballistic Missile
SRF	SIGINT Readiness Facility
SRHIT	Small Radar-Homing Intercept Technology (BMD Missile)
SRIG	Surveillance, Reconnaissance, and Intelligence Group
SRIS	Surface Range Imaging System
SROC	Southern Region Operations Center
SRIG	Surveillance, Reconnaissance, and Intelligence Group
SRJOIC	Southern Region Joint Operations Intelligence Center
SRAM	U.S. Short-Range Attack Missile
SRAMII	U.S. Short-Range Attack Missile (XAGM-131A; formerly AASM)
SRAM-T	Short Range Attack Missile - Tactical
SRB	Senior Review Board
SRBM	Short-Range Ballistic Missile
SRC	Strategic Reconnaissance Center
SRCU	SINCGARS Remote Control Unit
SRD	(1) System Requirements Document; (2) Special Research Detachment (U.S. Army)
SRF	(1) Strategic Rocket Forces (USSR); (2) Strategic Reserve Forces; (3) Secure Reserve Force (U.S.); (4) Selected Reserve Force; (5) SIGINT Readiness Facility; (6) SPIRIT Remote Facility (TROJAN)
SRFTL	Secure Reserve Force Target List
SRI	Surveillance, Reconnaissance and Intelligence
SRIG	Surveillance/Reconnaissance Intelligence Group

SRINF	Short-Range, Intermediate-Range Nuclear Forces
SRJOIC	Southern Region Joint Operational Intelligence Center
SRMIS	Southern Region Maritime Intelligence Summary
SRO	Sensitive Reconnaissance Operations
SROE	Standing Rules of Engagement
SRP	(1) Sealift Readiness Program; (2) SIOP Reconnaissance Plan
SRR	(1) Survival, Recovery and Reconstitution; (2) Security Requirements Review
SRS	(1) Strategic Reconnaissance Squadron; (2) Software Requirements Specification
SRSG	Special Representative to the Secretary-General
SRT	(1) Strategic Relocatable Target; (2) Standard Remote Terminals
SRW	Strategic Reconnaissance Wing
SRWG	Standing Requirements Working Group
SS	Attack Submarine
SSA	(1) Security Supporting Assistance; (2) Diesel-Powered Auxiliary Submarine; (3) Special Support Activity; (4) SIGINT Support Activity; (5) Soviet (FSU) Strategic Aviation
SSAN	(1) Social Security Account Number; (2) Nuclear-Powered Auxiliary Submarine
SSB	(1) Ballistic Missile Submarine; (2) Standard Software Base; (3) Single Sideband
SSB	Ballistic Missile Submarine
SSBN	Nuclear-Powered Ballistic Missile Submarine
SSBSC	Single Sideband, Suppress Carrier
SSC	(1) Coastal Submarine; (2) Space Surveillance Center; (3) Surface Support Craft
SSCC	Special Security Communications Center
SSCI	Senate Select Committee on Intelligence
SSD	Strategic Studies Detachment
SSE	Special Security Element
SSES	Ships Signal Exploitation Space
SSF	(1) Software Support Facility; (2) Special Service Force
SSG	(1) Cruise Missile Attack Submarine; (2) Special Security Group
SSGN	Nuclear-Powered Cruise Missile Attack Submarine
SSI	(1) Specialty Skill Identifier; (2) Safety, Security and Intelligence
SSIXS	Submarine Satellite Information Exchange Subsystem
SSJ	Self-Screening Jamming
SSLP	Transport Submarine
SSLSM	Single-Source Logistics Support Manager
SSM	(1) Surface-to-Surface Missile; (2) Midget Submarine
SSM/I	Sensor System Microwave Imager
SSM/T	Sensor System Microwave/Temperature
SSMA	Spread Spectrum Multiple Access
SSME	Spread Spectrum Modulation Equipment

SSMO	SIGINT Support to Military Operations
SSMOB	Surface-to-Surface Missile Order of Battle
SSMP	Security System Management Plan
SSN	(1) Nuclear-Powered Attack Submarine; (2) Social Security Number; (3) Space Surveillance Network
SSO	(1) Special Security Office; (2) Special Security Office(r)
SSO-INT	Senior Staff Officer-Intelligence (Canadian)
SSP	(1) SIGINT Support Plan; (2) Scheduled Strike Program (NATO); (3) Single-Shot Probability of Damage; (4) Single-Source Processor; (5) SIOP Support Program
SSP-S	Single Source Processor-SIGINT
SSQ	Auxiliary Submarine, Communications
SSQN	Nuclear-Powered Auxiliary Submarine, Communications
SSR	(1) Radar Picket Submarine; (2) Secondary Surveillance Radar; (3) Special Security SSRS Representative SIGINT Surveillance and Reporting System
SSS	(1) Staff Summary Sheet; (2) Systems Science and Software; (3) System Support Segment; (4) Special Support Section
SSSP	Single-Source SIGINT Processor
SST	(1) Training Submarine; (2) System Specific Threat; (3) Supersonic Transport; (4) Single Subscriber Terminal; (5) Safe Secure Transport; (6) Strategic Support Team; (7) Space Support Team
SSTO	Single-Stage-To-Orbit
SSTS	Space Surveillance and Tracking System
SSUS	Spin-Stabilized Upper Stage
ST	(1) SEAL Team; (2) Strategic Task; (3) Short Tons
S&T	Scientific and Technical
S&TI	Scientific and Technical Intelligence
ST&E	Security Test and Evaluation
STA	Surveillance and Target Acquisition
STACCS	Standard Theater Army Command and Control System
STAMIS	Standard Army Management Information System
STAMP	SOUTHCOM Topographic Augmentation Program
STAMPS	Stand-Alone Message Processing System
STANAG	Standardization Agreement (NATO)
STANAVFORLANT	Standing Naval Force, Atlantic (NATO)
STAN-EVAL	Standardization and Evaluation
STANS	(1) Soviet Tactical Nuclear Study; (2) Space Target Analysis and Networking System
STAP	Science and Technology Advisory Panel
STAR	(1) Surface-to-Air Recovery; (2) System Threat Assessment Report
STARC	State Area Command
STARS	Surveillance, Target Acquisition & Reporting System
STAR-T	SHF Tri-Band Advanced Range Extension Tactical Terminal
START	Strategic Arms Reduction Talks/Treaty

STARTEX	Start Date of an Exercise
STASS	Submarine-Towed Array Surveillance System
STATDM	Statistical Time Division Multiplex
Static RI	Static Infrared Workstation
STATS	Strategic Target Analysis and Tracking System
STATSIONAR	USSR/Russian COMSAT System
STC	(1) Sensitivity Time Control; (2) Short Time Constant (ECCM); (3) SHAPE Technical Center
STCFE	Science and Technology Center Far East
STD	(1) SIGINT Technical Data; (2) Standard
STEL	Stanford Telecommunications
STEP	Standardized Technical Entry Point
STEPS	Scientific and Technical ELINT Processing System
STEPS II	Scientific and Technical ELINT Processing System II
STG	Special Tactical Group
STEL	Secure Telephone
S&TI	Scientific and Technical Intelligence
STIC	(1) Scientific and Technical Intelligence Committee; (2) Scientific and Technical Intelligence Center
STICS	Scalable Transportable Intelligence Communications System
STIFF	Strategic Intelligence Forecast File
STIISP	Scientific and Technical Intelligence Information Services Program
STINT	Science and Technology (S&T) Intelligence
STIR	Scientific and Technical Intelligence Register
STITEUR	Scientific and Technical Information Team, Europe
STK	(1) Satellite Took Kit; (2) Strike
STO	Science and Technology Objectives
STOL	Short Takeoff and Landing
STON	Short Ton
STOPS	Stand-Off Optical System
STOVL	Short Takeoff, Vertical Landing
STP	(1) Space Test Program; (2) Site Transition Plan
Str	Strength
STRAM	Static Random Access Memory
STRAT	Strategic
STRATCOM	Strategic Command
STRATJIC	USSTRATCOM Joint Intelligence Center
STRATLAT	Strategic Command Liaison Assistance Team
STRATMAS	Strategic Message Analysis Server
STRATPAT	Strategic Planning and Analysis Tool
STRED	Standard-Tactical Receive Equipment Display STRICOM Simulations, Training, and Instrumentation Command
STRIKFORSOUTH	Strike Force South
S-TRED	Standard Tactical Receive Equipment Display
STRUM	Standard Technical Reporting Using Modules

STS	(1) Special Training Standard; (2) Special Tactics Squadron; (3) Subcommittee on Telecommunications Security of the NSTISSC
STT	(1) Small Tactical Terminal; (2) Special Tactics Teams; (3) Shore Targeting Terminal
STU	Secure Telephone Unit (STU II & III)
STU-III	Secure Telephone Unit III
STUR	Secure Telephone Unit/Remote
STVD	Southern Theater of Military Operations (FSU)
STW	Strike Warfare
STWC	Strike Warfare Commander
STX	Situational Training Exercise
SUAWACS	Soviet (FSU) AWACS
SUBACS	Submarine Advanced Combat System
SUBLANT	Submarine Forces, Atlantic
SUBOPAUTH	Submarine Operating Authority
SUBORD	Subordinate
SUBPAC	Submarine Forces, Pacific
SUCCESS	Secure UHF Computer Controlled Equipment Subsystems
SUG	SAFE Users Group
SUM	(1) Surface-to-Underwater Missile; (2) Structural Usage Monitor
SUMS	Structural Usage Monitor System
SUPCOM	Support Command
SUPINTREP	Supplementary Intelligence Report
SUPIR	(1) Supplemental Photographic Interpretation Report; (2) Supplemental Phase Interpretation Report
SUPNAVFOR	Supporting Naval Force
SUPPLOT	Supplemental Plot
SUPREMS	Supplemental Preliminary Mission Summary
SUPT	Superintendent
SURAN	Southeastern Universities
SURFSHIP	Surface Ship
SURFWARDEVGRU	Surface Warfare Development Group
SURTASS	Surveillance Towed Array Sonar System (U.S.)
SURV	Surveillance
SUSLAK	Special U.S. Liaison Activity Korea
SUSLO	Special U.S. Liaison Officer
SV	(1) Secure Voice; (2) Special View
SVC	Service
SVCN	Secure Voice Conferencing Network
SVD	Soviet Sniper Rifle
SVGA	Super Video Graphics Adapter
SVIP	Secure Voice Improvement Program
SVOD	Soviet Aircraft Navigation and Landing System
SVS	Secure Voice System
SVTC	Secure Voice Teleconferencing

SVTS	Secure Video Teleconferencing System
SW	(1) Short Wave; (2) Surface Warfare; (3) Software; (4) Strategic Wing
S&W	Surveillance and Warning
SWA	(1) Southwest Asia; (2) Southwest Africa; (3) Standoff Weapons Assembly; (4) Senior Warning Analyst; (5) Senior Weather Analyst; (6) Secure Work Area
SWADII	Southwest Asia Defense Information Infrastructure
SWAL	Shallow-Water Attack Craft, Light
SWAM	Shallow-Water Attack Craft, Medium
SWAT	SOCRATES WS/LAN Analysis Testbed
SWB	Southwest Border
SWC	(1) Special Warfare Center (U.S. Army); (2) Special Warfare Craft; (3) Strategic Warfare Center; (4) Strategic Warning Center; (5) Space Warfare Center
S&WC	Surveillance and Warning Center/Control
SWCL	Special Warfare Craft, Light
SWCM	Special Warfare Craft, Medium
SWCS	Special Warfare Center and School
SWE	Sweden
SWHQ	Static War Headquarters
SWI	Special Weather Intelligence
SWIR	Short Wave Infrared
SWIRTERCAT	SWIR Terrain Categorization
SWIS	Survivable Wartime Intelligence System
SWO	(1) Special Weapons Officer; (2) Staff Weather Officer; (3) Senior Watch Officer
SWORD	Submarine Warfare Operations Research Department
SWP	Standing Warning Program
SWPS	Space & Weapons Systems SIGINT Working Group
SWR	Southwest Region
SWRS	Slow-Walker Reporting System
SWSC	Space Warning Systems Center
SWTMO	SW Theater of Military Operations
SYBASE	A Collection Requirements Database
SYDET	Sympathetic Detonator
SYDP	Six-Year Defense Plan
SYG	Secretary General
SYNCOM	Synchronous Communications Satellite
SYRACUSE	Systeme de Radio Communication Utilisant un Satellite
SYRUP	System Resource Utilization Package
SYS	System(s)
SYSADM	System Administrator
SYSADMIN	Systems Administration Technical Assistant
SYSCON	Systems Control
SYSOPR	System Operator

T

T	(1) Tank; (2) Training; (3) Transmitter
T1	1.54 Megabits per Second Throughput
T2	Technology Transfer
T3	44.3 Megabits per Second Throughput
TA	(1) Traffic Analysis; (2) Tank Army; (3) Terrain Avoidance; (4) Theater Army; (5) Target Acquisition; (6) Target Analysis
T&A	Transcription and Analysis
TAA	(1) Tactical Air Army (FSU); (2) Total Army Analysis; (3) Tactical Assembly Area; (4) Theatre Army Area
TAACOM	Theater Army Area Command
TAB	(1) Target Acquisition Battery; (2) Theatre Air Base
TABNR	Table Number
TABS	Threat Assement Briefing System
TAC	(1) Tactical Air Command; (2) Terrain Analysis Center (U.S. Army); (3) Tactical Access Controller; (4) Tri-Service Tactical Digital Communication System; (5) Technology Assessment Center; (6) Terminal Access Control; (7) Tactical Command Post
TACAC-D	Technical Control and Analysis Center-Division
TACAIR	Tactical Air
TACAMO	(1) U.S. Air Relay Communication System; (2) Take Charge and Move Out
TACAN	Ultrahigh-Frequency Tactical Air Navigation
TACAWS	The Army Combined Arms Weapons System
TACC	(1) Tactical Air Control Center; (2) Tanker Airlift Control Center; (3) Theater Army Communications Command
TACC(A)	Tactical Air Control Center (Afloat)
TACCIMS	(1) Theater Army Command and Control Information Management System; (2) Tactical Command and Control Information Management System
TACCP	Tactical Command Post
TACCS	(1) Tactical Airborne Command and Control and Surveillance; (2) Tactical Air Control Center System
TACCSIMS	Theater Area Command and Control Information Management System
TACCS-K	Tactical Automated Command and Control Systems-Korea
TACCTA	Tactical Commander's Terrain Analysis
TAC-D	Tactical Deception
TACE	(1) Technical Analysis Cost Estimate; (2) Tactical Air Coordination Element
TACELINT	Tactical Electronic Intelligence (Report)
TACFAST	Tactical Forward Analysis Support Terminal
TACFIRE	Tactical Artillery Fire Control
TACIES	Tactical Imagery Exploitation System
TACINTEL	Tactical Intelligence
TACIT RAINBOW	Anti-Radiation Missile

TACM	Tactical Amphibious Collection Management
TACO	Tactical Command Post
TACO-2	Tactical Communications-Two
TACOMM	Tactical Communications
TACOMSIM	Tactical Communications Simulator
TACON	Tactical Control
TACOPS	Tactical Air Combat Operations Staff
TACP	Tactical Air Control Party
TACRECCE	Tactical Reconnaissance
TACREP	Tactical Report
TACRON	Tactical Air Control Squadron
TACS	(1) Tactical Air Control System; (2) Technology Acquisition Coordination Subcommittee; (3) Theater Air Control System
TACS/TADS	Tactical Air Control System/Tacticai Air Defense System
TACSAM	Tactical Surface-to-Air Missile
TACSAT	Tactical Satellite
TACSATCOM	Tactical Satellite Communications
TACSIM	Tactical Simulation (Simulator)
TACTAS	Tactical Towed Array System (U.S. Surface Warship)
TACTASS	Tactical Towed-Array Surveillance System (USN)
TACTED	Tactical Trunk Encryption Device
TACTEL	Tactical Telecommunications
TACTERM	Tactical Terminal
TACW	Tactical Air Control Wing
TACWINGSLANT	Tactical Wings Atlantic
TAD	(1) Temporary Additional Duty; (2) Theater Air Defense
TADIL	Tactical Data Information Link
TADIL-J	Tactical Digital Interface Link-Joint
TADIX-B	Tactical Data Exchange System-B
TADIXS	Tactical Data Information Exchange Subsystem
TADIXS-B	Tactical Data Information Exchange System Broadcast
TADS	(1) Tactical Air Defense System; (2) Target Acquisition and Designation System
TADSS	Training Aids, Devices, Simulations and Simulators
TADMS	TRS ASARS-2 Data Manipulation System
TAE	Transportable Applications Executive
TAF	Tactical Air Forces
TAFIC	Tactical Air Forces Intelligence Center
TAFIES	Tactical Air Force Intelligence Exploitation System
TAFIIS	Tactical Air Forces Integrated Information System
TAFLC	Tactical Air Force Limited Operational Capabilities Europe
TAFSM	Tactical Fire Support Model
TAG	(1) Target Actions Group; (2) The Adjutant General; (3) Theater Army Group; (4) Target Aimpoint Graphic; (5) TEMPEST Advisory Group
TAGS	Theater Air Ground System

TAH	Tactical Aviation Headquarters
TAI	Target Areas of Interest
TAISS	Telecommunication and Automated Information Systems Security
TALM	Tactical Air-Launched Missile
TALO	Tactical Airlift Liaison Officer
TALON	Theater Applicatiaon-Launch on Notice
TAOS	Thrust-Assisted Orbiter System
TALP	Total Army Linguist Program
TAMPS	(1) Threat Avoidance Mission Planning System; (2) Tactical Aircraft Mission Planning System
TANGO	Tactical Air, Naval, Ground Operations
TAO	Tactical Air Operations
TAOC	Tactical Air Operations Center
TAOR	Tactical Area of Responsibility
TAP	(1) Terrain Analysis Program; (2) Theater Analysis and Planning
TAPA	Target Analysis Pacific Area
TAPCOMP	Targeting and Analysis Program Computers
TAPS	Technical Analysis Processing System
TAR	Terrain Avoidance Radar
TARBUL	Target Bulletin
TARDEV	Target Development
TARE	Telegraph Automation Relay Equipment
TAREX	Target Exploitation
TARM	Tactical Antiradiation Missile
TARPS	Tactical Air Reconnaissance Pod System (USN)
TARRRS	Tactical Air Reconnaissance Results Reporting System
TARS	Tactical Air Reconnaissance System
TAS	(1) Tactical Airlift Squadron; (2) Traffic Analysis Survey; (3) Terminal Access System; (4) True Air Speed; (5) Timeline Analysis System; (6) Temporal Analysis System
TASE	Tactical Air Support Element
TASES	Tactical Airborne Signals Exploitation System
TASM	Tactical Air-to-Surface Missile
TASMO	Tactical Air Support of Maritime Operations
TASO	Terminal Area Security Officer
TASOC	Theater Army Special Operations Command
TASOSC	Theater Army Special Operations Support Command
TASS	(1) Towed Array Surveillance System; (2) Official News Agency of the FSU; (3) Tactical Air Support Squadron; (4) Tactical Automatic Switching System
TAT	(1) Terrorist Action Team; (2) Tactical Analysis Team; (3) Target Area Tactics
TATERS	TROJAN Air Transportable Electronic Reconnaissance System
TAV	(1) Total Asset Visibility; (2) Trans-Atmospheric Vehicle
TAVR	Territorial and Army Volunteer Reserve
TAW	Tactical Airlift Wing

TAWC	Tactical Air Warfare Center
TAWDS	Transportable Automated Weather Distribution System
TAXIS-A	Tactical Data Information Exchange Subsystem A
TB	(1) Tank Battalion; (2) Tuberculosis
TBA	To Be Announced
TBD	To Be Determined
TBM	(1) Tactical Ballistic Missile; (2) Theater Battle Management; (3) Theater Ballistic Missile
TBP	To be published
TC	(1) Tank Company; (2) Transportation Corps; (3) Transport Cradles
TC3	Theater Command, Control, and Communications
TCA	(1) Theater Collection Assets; (2) Theater Communications Architecture; (3) Tactical Communication Augmentation
TCAC	Technical Control and Analysis Center
TCAC-C	Technical Control and Analysis Center - Corps
TCAC PIP	Technical Control and Analysis Center-Product
TCAE	(1) Technical Control and Analysis Element; (2) Tactical Control and Analysis Element
TCAE C/D/B	Technical Control and Analysis Element Corps/Division/Brigade
TC-AIMS II	Transportation Coordinator Automated Information For Movements Systems II
TCB	Trusted Computing Base
TCC	(1) Telecommunications Center; (2) Tactical Command Center
TCCC	Theater Communications Control Center
TCCE/CA	Theater Contingency Communications Equipment, Central Area
TCCS	Theater Command and Control System
TCD	Time Compliance Data
TCICA	Theater Counterintelligence Coordinating Authority
TCIM	Tactical Communications Interface Module
TCJ2	TRANSCOM J2
TCM	Tactical Cruise Missile
TCMS	Tactical Communications Management System
TCO	(1) Test Control Officer; (2) Telecommunications Control Officer; (3) Telecommunications Contracting Office
TCOS	Tactical Combat Operations System
TCP	(1) Technological Coordinating Paper; (2) Tactical Cryptologic Program; (3) Transmission Control Protocol; (4) Traditional CINC Programs
TCP/IP	Transmission Control Protocol/Internet Protocol
TCR	Time Critical Requirements
TCS	(1) Tactical Computer System; (2) Test/Crisis Service
TCSEC	DOD Trusted Computer System Evaluation Criteria
TCT	(1) Tactical Commanders Terminal; (2) Tactical Computer Terminal(s)
TCU	Tactical Computer Unit

TD	(1) Tank Destroyer; (2) Tank Division; (3) Time Dominant (imagery); (4) Tactical Deception; (5) Training Detachment; (6) Target Designator; (7) Transfer Device
TDA	(1) Table of Distribution and Allowances; (2) Target Damage Assessment; (3) Tactical Decision Aids
TDAD	Training Development and Analysis Directorate
TDAR	Tactical Defense Alert Radar
TDC	(1) Tactical Digital Computer; (2) Theater Deployable Communications
TDD	Target DBZ Designator
TDDP	Tactical Defense Dissemination Program
TDDS	(1) Tactical Defense/Data Dissemination System; (2) TRAP Data Dissemination System
TDES	Theater Document Exploitation System
TDF	(1) Tactical Data Facsimile; (2) Tactical Digital Facsimile
TDFD	Time Delay Firing Device
TDI	(1) Target Data Inventory; (2) Target Data Inventory; (3) ETIBS Datalink Interface
TDM	Time Division Multiplex
TDMA	Time Division Multiple Access
TDOA	Time Difference of Arrival
TDP	(1) Threat Display & Projection; (2) Tactical Display Programmer; (3) Tactical Data Processor
TDRSS	Tracking and Data Relay Satellite System
TDS	(1) Target Data Sheet; (2) Training Device System; (3) Target Development System
TDSS	Theater Display Support System
TDT	Tactical Data Terminal
TDY	Temporary Duty
TE	(1) Tactical Exploitation; (2) Table of Equipment
T&E	Test & Evaluation
TEA	Tactical Exploitation Assessment
TEAMS	Trend and Error Analysis Methodology System
TEARR	Time, Elevation, Azimuth, Range, Range Rate
TEB	Tactical Exploitation Battalion
TEC	Topographic Engineering Center
TECCE	Tactical Exploitation Collection and Coordination Element
TECH	Technical
TECHELINT	Technical ELINT
TECHINT	Technical Intelligence
TECHLIB	Technical Library
TECHSUM	Technical Summary
TECRAS	Technical Reconnaissance and Surveillance
TED	Trunk Encryption Device
TEDB	Technical ELINT Data Base
TEDS	Tactical Expendable Drone System
TEG	Tactical Exploitation Group (JSIPS)

TEK	Traffic Encryption Key
TEL	Transporter-Erector-Launcher
TELAR	Transporter-Erector-Launcher and Radar
TELCON	Telephone Conversation
TELECOM	Telecommunications
TELEFAC	Telecommunications Facilities Vulnerability Study
TELINT	Telemetry Intelligence
TELNET	Telecommunications Network
TEMP	Test and Evaluation Master Plan
TEMPEST	(1) Unclassified Name for Compromising Emanations; (2) Compromising Electronic Emission Control Program; (3) Transient Electromagnetic Pulse Emanations
TENCAP	Tactical Exploitation of National Capabilities
TEOC	Technical Objective Camera
TEP	(1) Tactical ELINT Processor; (2) TEMPEST Endorsement Program
TEPP	Tomahawk Employment Planning Package
TERCAT	Terrain Categorization
TERCOM	Terrain Contour Matching
TEREC	(1) Tactical Electronic Reconnaissance; (2) Tactical ELINT Receiver
TERPES	Tactical Electronic Reconnaissance Processing and Evaluation System
TERS	(1) Tactical Electronic Reconnaissance System; (2) Tactical ELINT Reporting System; (3) Tactical Event Reporting System
TES	(1) Tactical Electronic Squadron; (2) Tactical Event System
TESAR	Tactical Endurance Synthetic Aperture Radar
TESS	Tactical Engagement Simulation System
TET	Transportable Electronic Tower
TEWS	Tactical Electronic Warfare System
TEXAS	Tactical Exchange Automation System
TF	(1) Task Force; (2) Transaction Format
TFAS	Task Force Able Sentry
TFC	Tactical Fusion Center
TFCICA	Task Force CI Coordinating Authority
TFCC	Tactical Flag Command Center
TFJ2	Task Force Director of Intelligence
TFM	Trusted Facility Manual
TFR	Terrain Following Radar
TFS	(1) Tactical Fighter Squadron; (2) Terrain and Feature Server; (3) Traffic Flow Security
TFT	(1) Tri-Band Field Terminal; (2) Tactical Facsimile Terminal
TF/TA	Terrian Following/Terrain Avoidance
TFU	Tactical Forecast Unit
TFW	Tactical Fighter Wing
TFWC	Tactical Fighter Weapons Center

TG	(1) Task Group; (2) Training Group
T&G	Tracking and Guidance
TGA	Target Analysis
TGCF	Tactical Ground Control Facility
TGIF	Transportable/Tactical Ground Intercept Facility
TGPF	Transportable Ground Processing Facility
TGS	(1) Transportable Ground Station; (2) Turkish General Staff
TGT	Target
TGTINT	Targeting Intelligence
TGTINFOREP	Target Information Report
TGW	Terminal-Guidance Warhead
THAAD	Theater High-Altitude Area Defense
THAAD/GBR	Theater High-Altitude Area Defense/Ground Based Radar
THEC	Theater HUMINT Exploitation Center
THMT	Tactical High Mobility Terminal
THREATCON	JCS Terrorist Threat Condition
THz	Terahertz
TI	(1) Technical Intelligence (TECHINT); (2) Target Intelligence; (3) Transition Increment
TI/TTR	Target Illumination/Target Tracking Radar
TIA	Target Implications Annex
TIAP	Theater Intelligence Architecture Program
TIAPCO	TIAP Communications Overlay
TIARA	Tactical Intelligence and Related Activities
TIARRA	Target Identification And Recognition Radar
TIAS	Target Identification & Acquisition System
TIB	Target Intelligence Branch
TIBS	Tactical Information Broadcast System
TIC	(1) Theater Intelligence Center; (2) Technical Information Center
TICANA	Tactical Imagery Communications and Network Alternatives
TICC	Tactical Information Communications Center
TICON	Tight Control
TID	Theater Intelligence Digest
TIDL	Tactical Imagery Data Link
TIDY	Teletype Integrated Display System
TIEC	Theater Imagery Exploitation Capability
TIES	Tactical Information Exchange System
TIF(S)	Theater Interrogation Facility(ies)
TIFA	Theater Intelligence Fusion Architecture
TIFF	Tagged Image File Format
TIG	Tactical Intelligence Group
TIHB	Target Intelligence Handbook
TIIF	Tactical Imagery Interpretation Facility
TIIMS	Text and Image Information Management System
TILO	Transportation Intelligence Liaison Officer

TIM	Target Intelligence Material
TIM-DIS	Time & Distance
TIMS	(1) Tactical Information Management System; (2) TFCC Information Management System
TIO	Target Intelligence Officer
TIP	(1) Target Intelligence Package; (2) Theater Intelligence Plan; (3) Tracking and Impact Prediction; (4) Tactical Imagery Program
TIPE	Tactical Intelligence Product Enhancement
TIPI	Tactical Information Processing and Interpretation System
TIPP	Target Intelligence Production Plan
TIPS	(1) Terrorist Incident Profile System; (2) Tactical Intelligence Processing System; (3) Target Intelligence Packages
TIR	Terminal Imaging Radar
TIROS	Television Infrared Observation Satellite
TIROS-N	Television Infrared Observation Satellite-National
TIRS	Thermal Infrared Scanner
TIRSAG	Tactical Intelligence, Reconnaissance, Surveillance Action Group
TIRSS	Theater Intelligence, Reconnaissance & Surveillance Study
TIS	(1) Tactical Intelligence Squadron; (2) Thermal Imaging Sight; (3) Tactical Input Segment
TISD	Tactical (Air Forces) Integrated Situation Display
TISEO	Target Identification System, Electro-Optical
TISL	Target Identification System, Laser
TISO	Theater Intelligence Support Officer
TISP	Transition Implementation Support Plan
TISS	Tactical Intelligence Support Staff
TITF	Theater Intelligence Training Facility
TIU	ETIBS Interface Unit
TJS	Tactical Jamming System
TK	Talent-Keyhole
Tk	Tank
TKR	Tanker
TLAM	Tomahawk Land Attack Missile
TLAR	Transporter-Launcher and Radar
TLC	(1) Telecommunication Link Controller; (2) Teleconferencing
TLCF	(1) TACINTEL Link Control Facility; (2) Teleconferencing
TLE	Target Location Error
TLS	Top-Level Specification
TLST	TACAMO Logistics Support Team
TM	(1) Tactical Missile; (2) Threat Manager; (3) Target Material; (4) Landsat Thematic Mapper; (5) Technical Manual; (6) Team Materials; (7) Team
TMA	Theater of Military Action
TMB	Technical Management Board
TMCN	Tactical Target Materials Change Notice

TMD	(1) Theater Missile Defense; (2) Tactical Map Depot
TMDE	Test Measurement and Diagnostic Equipment
TMD/GBR	Theater Missile Defense/Ground-Based Radar
TMET	Transportable Medium Earth Terminal
TMFU	Theater METOC Forecasting Unit
TMMRS	Trojan Mobile Remote Receiver System
TMO	(1) Technical Management Office; (2) Theater of Military Operations
TMP	Training Management Plan
TMPC	Theater Mission Planning Center
TMPG	Target Materials Producers Group
TMPO	Target Materials Program Office
TMPS	Theater Mission Planning System
TMRG	Terrain-Masked Radar Graphics
TMSR	Tactical Meteorological Satellite Receiver
TMS	Target Materials Squadron
TMT	Target Marking Technologies
TMUG	Target Materials Users Group
TMWG	Target Materials Working Group
TMWS	Target Materials Workstation
TNAPS+	Tactical Network Analysis and Planning System Plus
TNET	Teletraining Network
TNF	Theater Nuclear Forces
Tng	Training
TNI	Trusted Network Interpretation
TNIEG	Trusted Network Interpretation Environment Guideline
TNK	Tanker
TNL	Target Nomination List
TNT	Tunnel Neutralization Team
TNO	Theater Nuclear Option
T/O	Take Off
TO&E	Tables of Organization and Equipment
TOA	(1) Total Obligational Authority; (2) Time of Arrival; (3) Transportation Operation Agency; (4) Time of Attack; (5) Transfer of Authority; (6) Table of Organic Allowance
TOC	(1) Tactical Operations Center; (2) Theater of Operations Command
TOE	(1) Table of Organization and Equipment; (2) Time of Entry
TOF	Time of Flight
TOPCAT	Tactical Operations Planner for Collection, Analysis, and Tasking
TOPINS	Theater Operational Intelligence System
TOPO	Topographic
TOPS	Tactical Operations Support
TOR	(1) Terms of Reference; (2) Tactical Operations Room; (3) Tentative Operational Requirement; (4) Time of Receipt
TORP	Torpedo

TORPCM	Torpedo Countermeasures & Deception
TOS	(1) Tactical Ocean Surveillance; (2) Theater Operating System
TOSP	Tailored Ocean Surveillance Product
TOSS	(1) Tactical Operations Support System; (2) Technical Oriented Support System
TOT	(1) Time over Target; (2) Time of Transmission
TOVS	TIROS Operational Vertical Sounder
TOW	Tube-Launched Optically-Tracked Wire-Guided Missile
T/P	Terminal/Printer
TPA	Theater Production Assets
TPAS	Target Planning and Scheduling
TPC	(1) Tactical Pilotage Chart; (2) Tempest Personal Computer; (3) Two-Person Control
TPCS	Team Portable COMINT System
TPEP	(1) TEREC Portable Exploitation Processor; (2) Trusted Products Evaluation Program
TPF	Topographic Production Facility
TPFD	Time-Phased Force Deployment
TPFDD	Time-Phased Force Deployment Data
TPFD(L)	Time-Phased Force Deployment (List)
TPI	Two-Person Integrity
TPL	Time-Phased Line
TPN	Tactical Packet Network
TPP	Thermal Powerplant
TPS	(1) Thermal Protection System; (2) Telecommunications Prioritization System
TPSD	(1) Theater Planning Support Division (J-5); (2) Theater Planning Support Document
TPU	Troop Programs Units
TPV	Terrain Perspective Viewing
TQL	Total Quality Leadership
TQM	Total Quality Management
T/R	Transmit-Receive
TR	(1) Tank Regiment; (2) Transportation Request
TRA	Temporary Restricted Areas
TRAC	(1) Tactical Radar Correlator; (2) TRADOC Analysis Center
TRADOC	U.S. Army Training and Doctrine Command
TRAINS	Interactive Video Teletraining System
TRAM	Target Recognition and Attack-Multisensor
TRANSCOM	Transportation Command
TRANSEC	Transmission Security
TRANSIT	Navy Navigation Satellite System
TRANSNAT	Transnational
TRAP	(1) Threat Research and Analysis Program; (2) TRE and Related Applications; (3) Terrorist Research and Analysis Project; (4) Tactical Related Applications
TRAP-I	TRAP-Improved

TRAPS	TRE & Related Applications
TRB	Technical Review Board
TRDL	Tactical Reconnaissance Data Link
TRE	Tactical Receive Equipment
TRED	Tactical Receive Equipment Display
TREDS	(1) Tactical Reconnaissance Exploitation Demonstration System; (2) Tactical Receive Equipment (TRE) Display System
TREE	Transient Radiation Effects on Electronics
TRF	Topographic Readiness Facility
TRICOMS	Triad Computer System
TRI-MEF	Tri-Marine Expeditionary Force
TRI-MEFO	Tri-Marine Expeditionary Force Order
TRITAC	Tri-Service Tactical Communications System
TRI-TAC	(1) U.S. Joint Tactical Communications Program; (2) Tri-Service Tactical Communications
TRIES	Tactical Radar Imagery Exploitation System
TRIGS	TR-1 Ground Station
TRIMSS	TRANSCOM Imagery Management Support System
TRITAF	Tactical Air Forces of TAC, USAFE and PACAF
TRIX(S)	Tactical Reconnaissance Intelligence Exchange System
TRL	Target Recommendation List
TRML	USAFE Target Reference Material List
TRN	(1) Target Reference Number; (2) Target Reference Point
TROFA	Temporary Remote Operating Facility, Airborne (NSA)
TROJAN	Name of Technical Training System
TROJAN SPIRIT	TROJAN Special Purpose Integrated Remote Intelligence Terminal
TROKA	Third ROK Army
TROPO	Tropospheric Scatter Radio
TROSCOM	United States Army Troop Support Command
TRP	(1) Target Reporting Parameters; (2) Theater Response Package
Trp	Troops
TRRIP	(1) Theater Rapid Response Intelligence Package; (2) Tactical Rapid Reaction Intelligence
TRS	(1) Tactical Reconnaissance Squadron; (2) Tactical Reconnaissance System; (3) Trunked Radio System; (4) Telecommunications Service Request
TRSS	Tactical Remote Sensor System
TRT	TEREC Remote Terminal
TRUS	Tilting Wing/Rotor UAV System
TRV	Tank Recovery Vehicle
TRW	Tactical Reconnaissance Wing
TS	(1) Top Secret; (2) Transaction Services; (3) Target Spotting; (3) TROJAN SPIRIT
TSAR	Transmission Security Analysis Report
TSART	Test Support and Analysis Report Terminal
TSB	PSYOP Tactical Support Battalion

TSC	(1) Tactical Support Center; (2) Top Secret Control; (3) Technical Support Center; (4) Tactical Support Company; (5) TROJAN Switching Center; (6) Training Support Center
TSC2	Tactical/Strategic Command & Control
TSCA	Time-Sensitive Collection Actions
TSCE	Time-Sensitive Collection Emphasis
TSCIF	Tactical/Temporary Sensitive Compartmented Information Facility
TSCIXS	Tactical Support Center Information Exchange System
TSCM	Technical Surveillance Countermeasures
TSCO	Top Secret Control Officer
TSCR	Time-Sensitive Collection Requirement
TSCS	Transportable Satellite Communications System
TS/SCI	Top Secret/Sensitive Compartmented Information
TSCSI	Temporary Surface Cryptologic Support Installation
TSCW	Top Secret Codeword
TSDS	Tactical SIGINT Data Support
TSE	Target Support Element
TSEC	Telecommuncations Security
TSF	Technical Support Facility
TSG	Threat Steering Group
TSIT	Technical Service Intelligence Team
TSK	Transmission Security Key
TSM	Threat Spectrum Model
TSMA	Theater of Strategic/Military Action
TSOC	Theater Support Operations Cell
TSOR	Technical Standards of Readiness
TSP	(1) Transshipment Point; (2) Training Support Base; (3) Tactical Sensor Planner
TSR	(1) Time-Sensitive Requirement; (2) Telecommunications Support Request; (3) Trans-Siberian Railroad
TSRS	Tactical Support Reconnaissance System
TSS	(1) Telecommunications Security System; (2) Time-Sharing System; (3) Target Summary Sheets; (4) Target Selection Standards
TSSAM	Tri-Service Standoff Attack Missile
TSSR	Tropo Satellite Support Radio
TSSS (TS3)	(1) Tactical Simulator Study Support; (2) Time-Sensitive Support System
TSSTM	Tactical SIGINT Systems Training Module
TST	(1) Tactical Surveillance Technology; (2) Theater Support Team; (3) Tactical Support Team
T-STAR	TRANSCOM Situation Transportation Analysis Review
TS/TM	Target Support/Target Materials
TSWA	Temporary Secure Working Area
TSWG	Technical Support Working Group Of IG/T
TT	(1) Technology Transfer; (2) Target Track

TT&C	Telemetry Tracking and Command
TTAC	Technology Transfer Analysis Center
TTADB	Tactical Terrain Analysis Data Base
TTAP	Telemetry Technical Analysis Position
TTBT	Threshold Test Ban Treaty
TTC	(1) Transportation Terminal Command; (2) Tactical Telephone Central
TTD	Tactical Terrain Data
TTG	Technical Training Group
TTI	Tactical Target Illustration
TTIC	Technology Transfer Intelligence Committee
TTM	Tactical Target Materials
TTMC	Tactical Target Materials Catalogue
TTMP	Tactical Target Materials Program
TTMPD	Tactical Target Material Production Document
TTP	Tactics, Techniques, and Procedures
TTPI	Trust Territory of the Pacific Islands
TTR	Target Tracking Radar
TTSB	Theater Tactical Selection Board
TTU	(1) Transportation Terminal Unit; (2) Tape Transport Unit
TTY	(1) Teletypewriter; (2) Teletype
TU	Task Unit
TUDE	Teletype User Display Equipment
TUHTKP	Time Urgent Hard Target Kill Potential
TUSA	Third U.S. Army
TUT	Tactical User's Terminal
TUV	Task Unit Van
TV	(1) Television; (2) Theater of War (FSU); (3) Target Vulnerability
TVA	Target Value Analysis
TVD	Theater of Military Operations (FSU)
TVITS	Tactical Video Imagery Transmission System
TVSSC	TACCIMS VTC Support System
TW	Targeting and Weaponeering
TW/AA	Tactical Warning/Attack Assessment
TWAC	Tactical Weather Analysis Center
TWCS	(1) Tomahawk Weapon Control System; (2) Tactical Warfare Control System
TWG	(1) Threat Working Group; (2) Technology Working Group
TWI	Training With Industry
TWRL	Two-Way Radio Link
TWS/IPS	Topographic Workstation/Imagery Processing System
TWT	Traveling Wave Tube
TWTA	Traveling Wave Tube Amplifier
TYC	Tactical Message Central
TX	(1) Technology Exploitation; (2) Transmission

U

U	Unclassified
U-2	(1) Designator for a Military Reconnaissance Aircraft; (2) AF Reconnaissance Aircraft
UA	User Agent
UAAF	Unified Action Armed Forces
UAE	United Arab Emirates
UAM	Underwater-to-Air-Missile
UAMP	USIS Architecture Migration Plan
UARR	Universal Aerial Refueling Receptical
UATP	UNIX Advanced Tracking Prototype
UAV	Unmanned Aerial Vehicle
UAV-CR	Unmanned Aerial Vehicle-Close Range
UAV-E	Unmanned Aerial Vehicle-Endurance
UAV-H	Unmanned Aerial Vehicle-HUNTER
UAVJPO	Unmanned Aerial Vehicle Joint Program Office
UAV-M	Unmanned Aerial Vehicle-Maneuver
UAV-SR	Unmanned Aerial Vehicle-Short Range
UBA	Underwater Breathing Apparatus
UBR	Unassigned Bit Rate
UC	Under Construction
UCAB	USIS Customer Advisory Board
UCC	ULTRA-Compact Camera
UCG	Universal Communications Gateway
UCIB	USAFE Command Intelligence Brief
UCIRF	USAREUR Combat Intelligence Readiness Facility
UCMJ	Uniform Code of Military Justice
UCP	Unified Command Plan
UD	Deputy USCINCSPACE
UDEAC	Economic and Customs Union of Central Africa
UDF	United Democratic Front
UDIR	USAREUR Daily Intelligence Report
UDT	Underwater Demolition Team
UE	Unit Equipment
UEAC	Union of Central African States
UEC	USAREUR Exploitation Center
UFO	(1) Unidentified Flying Object; (2) UHF Follow-On Satellites
UFR	Unfunded Requirements
UGM	Underwater Guided Missile
UGS	Unattended Ground Sensors
UHF	Ultra High Frequency
UI	(1) Unidentified; (2) Unit of Issue

UIC	(1) USAREUR Interrogation Center; (2) Unit Identification Code
UIES	USAREUR Imagery Exploitation System
UIR	User Interface Requirements
UIRK	Unique Interswitch Rekeying Key
UIS	User Interface System
UJTL	Universal Joint Task List
UK	United Kingdom
UKADGE	United Kingdom Air Defense Ground Environment
UKAGE	United Kingdom Air Defense Ground Environment
UKAIR	United Kingdom Air Forces
UKLF	United Kingdom Land Forces
Ukn	Unknown
ULAN	Unit Local Area Network
ULANA	Universal Location Area Network Architecture
ULCC	Ultra Large Crude Carrier
ULCS	Unit-Level Circuit Switch
ULF	Ultra Low Frequency
ULO	USAREUR Liaison Office
ULV	Unmanned Launch Vehicle
UMD	Unit Manning Document
UMF	Unconventional Military Forces (NATO)
UMIES	USAREUR Modernized Imagery Exploitation System
UMO	Unconventional Military Operations
UMOP	Unintentional Modulation on Pulse
UN	United Nations
UNAAF	Unified Action Armed Forces
UNAMIR	United Nations Assistance Mission for Rwanda
UNAVEM	United Nations Angola Verification Mission
UNC	United Nations Command
UNCIVPOL	United Nations Civilian Police
UNCLAS	Unclassified
UNDERSEC	Under Secretary
UNDHA	United Nations Department of Humanitarian Affairs
UN-DMT	United Nations Disaster Management Team
UNDOF	United Nations Disengagement Observer Force
UNDP	United Nations Development Program
UNEF	United Nations Emergency Forces
UNESCO	United Nations Educational, Scientific & Cultural Organization
UNFICYP	United Nations Peacekeeping Force in Cyprus
UNGA	United Nations General Assembly
UNHCR	United Nations High Commissioner for Refugees
UNHQ	United Nations Headquarters
UNICEF	United Nations Childrens' Fund
UNIFIL	United Nations Interim Force in Lebanon

UNIKOM	United Nations Iraq-Kuwait Observer Mission
UNITA	National Union for the Total Independence of Angola
UNITAF	Unified Task Force
UNITAS	United International Antisubmarine Warfare Exercise (Joint U.S.-Latin American Naval Exercise)
UNITREP	Unit Report
UNITSITREP	Unit Situation Report
UNIX	Orginally UNICS, for Uniplex Information and Computing System
UNMIH	United Nations Mission in Haiti
UNMO	United Nations Military Observers
UNMOGIP	United Nations Military Observer Group in India and Pakistan
UNOMIG	United Nations Mission in Georgia
UNOMIL	United Nations Observer Mission in Liberia
UNOMUR	United Nations Mission for Uganda-Rwanda
UNOSOM	United Nations Operations in Somalia
UNMSC	United Nations Military Staff Committee
UNODIR	Unless Otherwise Directed
UNPROFOR	United Nations Protection Force
UNPP	UN Peace Plan
UNSAT	Unsatisfactory
UNSC	United Nations Security Council
UNTSO	United Nations Truce Supervision Organization
UQL	Universal Query Language
UNREF	United Nations Refugee Fund
UNRWA	United Nations Relief & Works Agency
UO	Using Organization
UPI	United Press International
UPP	User Partnership Program
UPS	(1) Uninterruptible Power Supply; (2) Universal Polar Stereographic
U2R	Reconnaissance Aircraft (U.S. Air Force)
URBBO	Urban Area Boundary File
URBPOP	Urban Population File
URD	User Requirements Document
URG	Underway Replenishment Group
URS	User Readout Simulator
US	United States
U&S	Unified and Specified (Archaic, now Unified) Commands
US MLO	U.S. Military Liaison Office
US/AIA	USEUCOM/ACE Interface Architecture
USA	(1) U.S. Army; (2) United States of America
USAABMDA	United States Army Advanced Ballistic Missile Defense Agency
USAADASCH	U.S. Army Air Defense Artillery School
USACAPOC	U.S. Army Civil Affairs and Psychological Operations Command

USACC	U.S. Army Communications Command
USACE	U.S. Army Corps of Engineers
USACID	U.S. Army Criminal Investigative Division Command
USACSLA	United States Army Communications Security Logistics Agency
USACOM	U.S. Atlantic Command
USAEIS	United States Army Electronic Intelligence & Security
USAF	U.S. Air Force
USAFE	U.S. Air Forces, Europe
USAFE/CC	Commander, U.S. Air Forces Europe
USAFINTEL	United States Air Force Intelligence
USAFISA	U.S. Army Force Integration Support Agency
USAFJ	U.S. Air Forces, Japan
USAFK	U.S. Air Forces, Korea
USAFLANT	U.S. Air Force, Atlantic
USAFR	U.S. Air Force Reserve
USAFRED	U.S. Air Force Readiness Command
USAFSO	U.S. Air Force Southern Command
USAFSOC	U.S. Air Force Special Operations Command
USAFSOS	U.S. Air Force Special Operations School
USAFSS	United States Air Force Security Service
USAFTAC	(1) U.S. Air Force Technical Applications Center; (2) U.S. Air Force Tactical Air Command
USAFWTC	U.S. Air Force Weapons and Tactics Center
USAIA	U.S. Army Intelligence Agency
USAICE	U.S. Army Intelligence Center, Europe
USAIC	U.S. Army Intelligence Center
USAICS	U.S. Army Intelligence Center and School
USAID	U.S. Agency for International Development
USAIIA	United States Army Imagery Interpretation Agency
USAINSCOM	U.S. Army Intelligence and Security Command
USAISC	U.S. Army Information Systems Command
USAISD	U.S. Intelligence School, Fort Devens
USAITAC	U.S. Army Intelligence Threat Analysis Center
USAITFG	United States Army Intelligence Threats & Forecasts Group
USAJFKWCS	U.S. Army John F. Kennedy Special Warfare Center and School
USAKA	U.S. Army Kwajalein Atoll
USAOG	U.S. Army Operational Group
USAR	U.S. Army Reserve
USARAK	U.S. Army Alaska
USARC	U.S. Army Reserve Command
USARCENT	U.S. Army Forces, Central Command
USARCO	U.S. Army Commercial Communications Office
USAREUR	U.S. Army, Europe
USARJ	U.S. Army, Japan
USARLANT	U.S. Army, Atlantic

USARPAC	U.S. Army, Pacific
USARSO	(1) U.S. Army, South; (2) U.S. Army Forces, South
USARSOC	U.S. Army Reserve, Special Operations Command
USARSPACE	U.S. Army Space Command
USARSPACECOM	U.S. Army Space Command
USASAALA	US Army Security Assistance Agency Latin America
USASACDA	United States Army Security Agency Combat Development Activity
USASACDSA	United States Army Security Agency Command Data Systems Activity
USASAE	United States Army Security Agency, Europe
USASAPAC	United States Army Security Agency, Pacific
USASASA	United States Army Security Agency Systems Activity
USASASSA	United States Army Security Agency Signal Security Activity
USASATCOMA	United States Army Satellite Communications Agency
USASATEC	United States Army Security Agency Test & Evaluation Center
USASEXC	United States Army Services Exploitation Center
USASFC	U.S. Army Special Forces Command
USASOA	U.S. Army School of the Americas
USASOC	U.S. Army, Special Operations Command
USASOF	U.S. Army, Special Operations Forces
USASOSC	U.S. Army Special Operations Support Command
USASSDC	U.S. Army Space and Strategic Defense Command
USASSG	U.S. Army Special Security Group
USATAC	U.S. Army Terrain Analysis Center
USATACOM	U.S. Army Tank Command
USATC	United States Air Target Chart
USATEC	U.S. Army Topographic Engineering Center
USATSC	U.S. Army Training Support Center
USB	Upper Sideband
USC	(1) Under Secretaries Committee; (2) United States Code
USCENTAF	U.S. Air Forces Central Command
USCENTCOM	U.S. Central Command
USCG	U.S. Coast Guard
USCG INT	U.S. Coast Guard Intelligence
USCGNET	U.S. Communications Grid Network
USCINCACOM	Commander in Chief, U.S. Atlantic Command
USCINCARRED	Commander in Chief, United States Army Forces, Readiness Command
USCINCCENT	Commander in Chief, U.S. Central Command
USCINCEUR	Commander in Chief, U.S. European Command
USCINCFOR	United States Commander in Chief, US Forces Command
USCINCLANT	Commander in Chief, U.S. Atlantic Command
USCINCMEAFSA	United States Commander in Chief Middle East, Southern Asia, & Africa South of the Sahara
USCINCPAC	Commander in Chief, U.S. Pacific Command

USCINCPACFLT	Commander in Chief, U.S. Pacific Fleet
USCINCRED	United States Commander in Chief, US Readiness Command
USCINCSO	Commander in Chief, U.S. Southern Command
USCINCSOC	Commander in Chief, U.S. Special Operations Command
USCINCSOINT	Commander in Chief, U.S. Special Operations Intelligence
USCINCSPACE	Commander in Chief, U.S. Space Command
USCINSTRAT	Commander in Chief, Strategic Command
USCINCTRANS	Commander in Chief, U.S. Transportation Command
USCMA	United States Court of Military Appeals
USCOB	United States Command Berlin
USCOMEASTLANT	U.S. Commander, Eastern Atlantic
USCS	(1) U.S. Customs Service; (2) Unified Soils Classification System; (3) U.S. Cryptologic System
USD	Under Secretary of Defense
USD(A&T)	Under Secretary of Defense (Acquisition & Technology)
USD(P)	Under Secretary of Defense for Policy
USDA	U.S. Department of Agriculture
USDAO	U.S. Defense Attache Office
USDE	Undesired Signal Data Emanations
USDR	United States Defense Representative
USELEMNORAD	U.S. Element NORAD
USEMB	United States Embassy
USEUCOM	U.S. European Command
USFJ	U.S. Forces, Japan
USFK	U.S. Forces, Korea
USFORAZ	U.S. Forces, Azores
USFORCARIB	U.S. Forces, Caribbean
USFORDOMREP	U.S. Forces, Dominican Republic
USFORSCOM	U.S. Forces Command
USFORSOM	U.S. Forces, Somalia
USG	United States Government
USGS	U.S. Geological Survey
USI	U.S. Intelligence
USIA	U.S. Information Agency
USIS	(1) U.S. Information Service (USIA abroad); (2) U.S. Imagery System
USIC	U.S. Intelligence Community
USILO	U.S. Imagery Liaison Officer
USIS	(1) U.S. Information Service; (2) U.S. Imagery System
USJTF	United States Joint Task Force
USLANTCOM	U.S. Atlantic Command
USLO	United States Liaison Officer
USM	Underwater-to-Surface Missile
USMAAG	U.S. Military Assistance Advisory Group
USMARCENT	U.S. Marine Forces Central Command

USMARDEZLANT	U.S. Maritime Defense Zone, Atlantic
USMARFORK	U.S. Marine Forces, Korea
USMARFORLANT	U.S. Marine Forces, Atlantic
USMC	U.S. Marine Corps
USMILGP	U.S. Military Group
USMLM	U.S. Military Liaison Mission
USMOG-W	U.S. Military Observer Group-Washington
USMS	U.S. Marshal Service
USMTF	(1) U.S. Message Text Formats; (2) U.S. Message Text Formatter
USMTM	U.S. Military Training Mission
USN	U.S. Navy
USNAVAK	U.S. Navy Alaska
USNAVCENT	U.S. Naval Forces, Central Command
USNAVEUR	U.S. Naval Forces, Europe
USNAVFORJAPAN	U.S. Naval Forces, Japan (also USNAVFORJ)
USNAVFORKOREA	U.S. Naval Forces, Korea (also USNAVFORK)
USNAVSO	U.S. Naval Forces, Southern Command
USNI	U.S. Naval Institute
USNR	U.S. Naval Reserve
USNS	U.S. Naval Ship
USO	(1) United Service Organization; (2) Unit Security Officer
USODC	U.S. Office of Defense Cooperation
USOMC	U.S. Office of Military Cooperation
USOUTHAF	United States Southern Command Air Forces
USOS	USAF Special Operations School
USP&FO	U.S. Property and Fiscal Officer
USPACOM	U.S. Pacific Command
USR	Unit Status Report
USREDCOM	U.S. Readiness Command
USREPMILCOMUN	United States Representative, UN Military Staff Committee
USRNMC	United States Representative To NATO Military Committee
USS	(1) User Support System; (2) U.S. Ship
USSID	U.S. Signals Intelligence Directive
USSIS	U.S. Signals Intelligence System
USSOCOM	U.S. Special Operations Command
USSOCPAC	U.S. Special Operations Command Pacific
USSOUTHAF	U.S. Southern Command Air Forces
USSOUTHCOM	U.S. Southern Command
USSPACECOM	U.S. Space Command
USSR	(1) Union of Soviet Socialist Republics (now FSU); (2) Union of Soviet Sovereign Republics
USSS	(1) U.S. SIGINT System; (2) U.S. Secret Service
USSTRATCOM	U.S. Strategic Command
USTRANSCOM	U.S. Transportation Command
USTS	UHF Satellite Terminal System

USW	Undersea Warfare
USYG	Under-Secretary General
UT	Users' Terminal
UTAIN	USAFE Tactical Air Intelligence Network
UTAIS	USAFE Tactical Air Intelligence System
UTC	(1) Unit Type Code; (2) Universal Coordinated Time
UTCB	USCENTCOM Transportable Communications Backbone
UTH	USAREUR Transportable Host
UTIC	USAREUR Tactical Intelligence Center
UTM	Universal Transverse Mercator (Grid)
UTTAS	Utility Tactical Transport Aircraft System
UV	Ultra Violet
UW	(1) Unconventional Warfare; (2) Underwater
UWB	Ultra Wide Band
UWOA	Unconventional Warfare Operational Area

V

V-22 OSPREY	Joint Advanced Vertical-Lift Aircraft (Formerly JVX)
VA	Veterans Administration
VAAP	Vulnerability Analysis and Assistance Program
VAB	French Front Armored Vehicle
VAC	Volts, Alternating Current
VAN	Value-Added Networks
VAR	Variable
VAX	Virtual Address Extension
VBR	Variable Bit Rate
VCA	Virginia Contracting Activity
VCINCNORAD	Vice Commander in Chief, NORAD
VCJCS	Vice Chairman, Joint Chiefs of Staff
VCR	Video Cassette Recorder
VCS	(1) Video Conference Server; (2) VLAN Common Server; (3) Voice Communications Services
VCSA	Vice Chief of Staff, Army
VDL	Video Down Link
VDP	Video Disk Player
VDS	Variable Depth Sonar
VDT	Video Display Terminal
VDU	(1) Video Display Unit (TV Monitor); (2) Video Docking Unit
VDV	Soviet (FSU) Airborne Forces
veh	Vehicle
VERT	Vertical
VF	Voice Frequency
VFR	Visual Flight Rules
VGA	Virtual Graphics Array
VGK	Supreme High Command (FSU)
VGW	Variable-Geometry Wing
VHF	Very High Frequency
VHS	Video Home System
VHSIC	Very High Speed Integrated Circuit
vic	Vicinity
VICE	Voice Interceptor Comprehensive Evaluation
VID	Visual Identification (Canadian)
VIDINT	Video Intelligence
VIDS	Visually Integrated Display System
VIN	Vehicle Identification Number
VIP	(1) Very Important Person; (2) Variable Incentive Payment; (3) Visual Input Processor
VISINT	Visual Intelligence
VISTA	Very Intelligent Surveillance & Target Acquisition

VIXS	Video Information Exchange System
VLAN	Very Local Area Network
VLAR	Vertical Launch and Recovery
VLCC	Very Large Crude Carrier
VLDS	Very Large Data Storage
VLF	Very Low Frequency
VLS	Vertical Launch System
VLSI	Very Large-Scale Integration
VM	Virtual Memory
VMAP	Vector Product Format
VMAQ	Marine Tactical Electronic Warfare Squadron
VMFP	Marine Tactical Reconnaissance Squadron
VMO	(1) Marine Observation Squadron; (2) Tactical Operations Squadron
V Model	Advanced Development Model
VMS	Virtual Memory System
VN	Vulnerability Number
VO	Validation Office
V/O	Vertical/Oblique
VOA	Voice of America
VOCOM	Voice Communications
VOD	Vertical On-Board Delivery
VOL	Volume
VOR	Very High Frequency Omnidirectional Range
VORTAC	Collocated VOR and TACAN
VP	(1) Patrol Aircraft (Navy); (2) U.S. Naval Patrol Squadron; (3) Maritime Patrol Squadron
VPCN	Virtual Personal Communications Networking
VPF	Vector Product Format
VPH	Video Phase History
VPK	Military Industrial Commission (FSU)
VPN	Voice Product Net
VQ	U.S. Naval Fleet Air Reconnaissance Squadron
VR	Virtual Reality
VRD	Virtual Retinal Display
VRBM	Variable-Range Ballistic Missile
VRHS	VIDMAR Robotic Hoist System
VRIT	Volume Reduced Imagery Transmission
VSAT	(1) Very Small Aperture Satellite Terminal; (2) Very Small Aperture Terminals
VSO	Vault Security Officer
VSS	VIDMAR STAK System
V/STOL	Vertical/Short Takeoff & Landing
VSWING	Anti-Submarine Wing
VT	(1) Variable Time (Fuse); (2) Video Terminal

VTA	Military Transport Aviation (FSU)
VTB	Video Telebroadcasting
VTC	(1) Video Teleconferencing; (2) Video Telegraph
VTOL	Vertical Takeoff and Landing
VTR	Tracked Recovery Vehicle
VTS	Vandenberg Tracking Station
VTT	Video Teletraining
VULREP	Vulnerability Report
VVS	FSU Air Forces

W

W	(1) A W prefix to any ship type designates it as subordinated to a quasi-military force; (2) Watt
WABNRES	WWMCCS Airborne Resources
WAC	(1) World Aeronautical Chart; (2) World Area Code
WADS	West Air Defense Sector
WAG	World Area Grid
W-CIOC	Wartime Combined Intelligence Operations Center
WAM	WWMCCS ADP Modernization
WAN	Wide-Area Network
WARC	World Administrative Radio Conference
WARLOG	Wartime Logistics
WARM	Wartime Reserve Mode
WAS	Wide-Area Search
WASAS	Weekly All-Source Algerian Situation Report
WASHFAX	Washington Area Secure Facsimile System
WASP	War Air Service Program
WARSIM	War Simulation
WASS	Wide-Area Surveillance System
WASSO	WWMCCS ADP System Security Officer
WATCHCON	Watch Condition
WATS	Wide Area Telecommunications System
WAWS	Washington Area Wideband System
WB	Wideband
WBIS	Wideband Intercept System
WBMS	Wideband Measurement System
WBST	Wideband Subscriber Terminals
WC	(1) Weather Center; (2) Weapon Control
WCCS	Wing Command and Control System
WCG	Workstation Computer Graphics
WDCS	Weapons Data Correlation System
WE	Weather Element
WEBE	Western European Basic Encyclopedia
WECON	Weather Control
WEFAX	Weather Facsimile
WES	WWMCCS Entry System
WESS	Weather Environmental Support System
WESTLANT	Western Atlantic Area (NATO)
WESTPAC/WPAC	Western Pacific
WESTLCF	WES Teleconferencing System
WETM	Cadre Weather Team
WEU	West European Union
WFC	World Food Council

WFOV	Wide Field of View
WFP	World Food Program
WG	(1) Wing; (2) Working Group
WGS	World Geodetic System
WH	White House
WHCA	White House Communications Agency
WHD	Western Hemisphere Defense
WHO	World Health Organization
WHQ	War Headquarters
WHSR	White House Situation Room
WIA	Wounded in Action
WIC	Worldwide Intelligence Conference
WICP	Wing Initial Communications Package
WICS	Worldwide Intelligence Communications System
WIDARSURV	Wide-Area Surveillance
WIFC	Wallops Island Flight Center
WIG	Wing-in-Ground Effect
WIMS	Warning and Indications Monitoring System
WIN	(1) WWMCCS Intercomputer Network; (2) WWMCCS Interconnected Network
WINCO	Warning Intelligence Non-Commissioned Officer
WINCS	WWMCCS Information Network Communications System
WINE	Warning and Indications in Europe
WINK	Warning in Korea
WINTEX	Winter Exercise
WIP	Weekly Intelligence Production Listing
WIR	Weekly Intelligence Review
WIS	(1) Weekly Intelligence Summary; (2) WWMCCS Information System; (3) Weaponeering Information Sheet
WISE	Warning Indicators System Europe
WISP	(1) Warning Improvement Study Plan; (2) Wartime Information Security Program; (3) Worldwide Intelligence Support Program
WISS	WESTCOM Intelligence Support System
WMD	(1) Western Military District; (2) Weapons of Mass Destruction
WMTR	Western Missile Test Range
WN	Warning-Intelligence Sources and Methods Involved
WNA	Would Not Answer
WN/WNINTEL	Warning Notice-Intelligence Sources and Methods Involved
WNY	Washington Navy Yard
WO	(1) Washington Office; (2) Warrant Officer
W/OAP	With Offset Aim Point
WOC	Wing Operations Center
WORM	Write Once/Read Many
WP	(1) Warsaw Pact; (2) Word Processing
WPAC	West PAC

WPC	(1) Warsaw Pact Countries; (2) Word Processing Center; (3) World Peace Council
WPM	Words Per Minute
Wpn	Weapon
WPNS	Weapons
WPNVG	Waterproof Night Vision Goggles
WPRS	War Powers Reporting System
WR	(1) Weapon Radius; (2) Western Range
WRA	Weapon Release Authority
WRM	War Reserve Materiel
WRMS	War Reserve Materiel Stocks
WRNC	Washington National Records Center
WRS	(1) Weapons Recommendation Sheet; (2) War Reserve Stocks
WRSA	War Reserve Stocks for Allies
WRSK	War Readiness Spares Kits
WS	(1) Workstation; (2) Weather Squadron; (3) Weapons School
WSAP	Weapons System Acquisition Program
WSEP	Weapon System Evaluation Program
WSI	Weapons School of Intelligence
WSI/L	War Supporting Industries and Logistics
WSMC	Western Space and Missile Center
WSMR	White Sands Missile Range
WSS	Workfile Support System
WSSIC	Weapon and Space Systems Intelligence Committee
WTM	World Target Mosaic
WTO	Warsaw Treaty Organization
WVRD	World Vision Relief and Development, Inc.
WWABNCP	Worldwide Airborne Command Post
WWCT	Worldwide Color TV
WWDMS	WWMCCS Data Base Management System
WWHFIBSN	Worldwide High Frequency Interlocking Base Station Network
WWIMS	Worldwide Warning Indicator Monitoring System
WWMCCS	Worldwide Military Command and Control System(s)
WWSVCS	Worldwide Secure Voice Conferencing System
WWW	Worldwide Web
WX	Weather
WXFCST	Weather Forecast

X

XDM/X Model	Experimental Development Model/Exploratory Development Model
Xfer	Transfer
XIDB	Extended Integrated Database
XMIT	Transmit
XMTR	Transmitter
XO	Executive Officer
XOI	USAFE Director of Intelligence
XOIN	USAFE Combat Operations Division
XOIX	USAFE Plans & Systems Division
XP	Director(ate) of Plans
XRL	X-Ray Laser
XTR	Transmitter
XVIII ABC	XVIII Airborne Corps

Y

YAG	Yttrium Aluminum Garnet
YAGE	Experimental Service Craft
YAM	Missile Support Craft
YAMM	Missile Support Barge
YC	Open Barge
YCF	Car Barge
YCK	Lighter Open Cargo
YCV	Lighter Aircraft Transport
YD	Floating Crane
YDG	Deperming/Degaussing Barge
YDT	Diving Tender
YE	Ammunition Lighter
YEN	Ammunition Barge
YF	Covered Lighter
YFB	Ferry
YFDB	Large Floating Drydock
YFDL	Small Floating Drydock
YFDM	Medium Floating Drydock
YFL	Launch
YFN	Covered Barge
YFNB	Large Covered Barge
YFND	Drydock Companion Barge
YFP	Floating Power Barge
YFR	Refrigerated Lighter
YFRN	Refrigerated Barge
YFU	Harbor Utility Transport
YG	Garbage Lighter
YGN	Garbage Barge
YGS	Survey Craft
YGT	Target Service Craft
YGTN	Target Barge
YH	Ambulance Craft
YM	Dredge
YMN	Non-Self-Propelled Dredge
YNC	Net Cargo Craft
YNG	Gate Craft
YO	Fuel Lighter
YON	Fuel Barge
YOS	Oil Storage Barge
YOSR	Nuclear Waste Disposal Barge
YOSS	Submersible Oil Storage Barge
YPD	Floating Pile Driver
YPL	Barracks Barge

YPT	Torpedo Retriever
YR	Floating Workshop Barge
yr	Year
YRC	Cable Tender
YRD	Auxiliary Repair Dock
YRG	Tank Cleaning Craft
YRRN	Radiological Repair Barge
YRS	Salvage Craft
YSR	Sludge Removal Craft
YSS	Service Submersible
YTB	Large Harbor Tug
YTL	Small Harbor Tug
YTM	Medium Harbor Tug
YTR	Fireboat
YTS	Sail Training Craft
YVS	Seaplane Service Craft
YW	Water Lighter
YWN	Water Barge
YXR	Hulk or Relic
YXT	Training Craft

Z

Z	Zulu Time (Greenwich Mean Time)
ZBB	Zero-Based Budget
ZF	Zone of Fire
ZG	Zero Gravity
ZI	Zone of the Interior
ZICON	(1) Zone of the Interior Consumers' Network; (2) Zone of Interior Communication Network
ZOS	Zone of Separation
ZPU	Soviet (FSU) Antiaircraft Machinegun
ZSU	Soviet (FSU) Self-Propelled Antiaircraft Gun
ZU	Soviet (FSU) Towed Antiaircraft Gun
ZULU	Greenwich Mean Time

CODES FOR GEOPOLITICAL AREAS

Abkhazia	AB
Adriatic Sea	8D
Aegean Sea	8G
Afghanistan	AF
Albania	AL
Algeria	AG
American Samoa	AQ
Andaman Islands	ZQ
Andorra	AN
Angola	AO
Anguilla	AV
Annobon (Pagulu)	YR
Antarctica	AY
Antigua and Barbuda	AC
Arabian Peninsula	A4
Arabian Sea	6R
Arctic Ocean	5A
Argentina	AR
Armenia	AM
Aruba	AA
Ashmore and Cartier Islands	AT
Asia	A
Atlantic Ocean	Z8
Atlantic Ocean, North	1A
Atlantic Ocean, South	2A
Australia	AS
Austria	AU
Azerbaijan	AJ
Azores Islands	AZ
Bahamas	BF
Bahrain	BA
Baker Island	FQ
Balearic Islands	BI
Baltic Sea	7B
Bangladesh	BG
Barbados	BB
Barents Sea	5B

Bassas Da India	BS
Belarus	BO
Belgium	BE
Belize	BH
Benin	BN
Bering Sea	5D
Bering Strait	5R
Bermuda	BD
Bhutan	BT
Black Sea	8B
Bolivia	BL
Bosnia and Herzegovina	BK
Botswana	BC
Bouvet Island	BV
Brazil	BR
British Indian Ocean Territory	I0
British Virgin Islands	VI
Brunei	BX
Bulgaria	BU
Burkina Faso (formerly Upper Volta)	UV
Burma	BM
Burundi	BY
Belarus	BO
Cabinda	VK
Cambodia (now Kampuchea)	CB
Cameroon	CM
Canada	CA
Canary Islands	ZZ
Cape Verde	CV
Caribbean Islands	N5
Caribbean Sea	1X
Caroline Islands	ZL
Caspian Sea	8C
Cayman Islands	CJ
Central African Republic	CT
Central America	N4
Chad	CD
Chile	CI
China (Peoples Republic of)	CH
Christmas Island	KT
Chukchi Sea	5C

Clipperton Island	IP
Cocos (Keeling Islands)	CK
Colombia	CO
Comoros	CN
Congo	CF
Cook Islands	CW
Coral Sea Islands	CR
Corsica	VP
Costa Rica	CS
Crete	VJ
Croatia	HR
Cuba	CU
Cyprus	CY
Czechoslovakia (former)	CZ
Czech Republic	EZ
Denmark	DA
Diego Garcia	YL
Djibouti	DJ
Dominica	DO
Dominican Republic	DR
Easter Island	XZ
Eastern Europe	E5
Ecuador	EC
Egypt	EG
El Salvador	ES
Elobey, Islas de	YU
Equatorial Guinea	EK
Eritrea	ER
Estonia	EN
Ethiopia	ET
Europa Island	EU
Falkland Islands	FK
Faroe Islands	FO
Fiji	FJ
Finland	Fl
France	FR
French Guiana	FG
French Polynesia	FP
French Southern and Antarctic Lands	FS
Gabon	GB
Gambia	GA

Gaza Strip	GZ
Georgia	GG
Germany	GM
Germany, Democratic Republic of (former)	GC
Germany, Federal Republic of	GE
Ghana	GH
Gibraltar	GI
Glorioso Islands	GO
Greece	GR
Greenland	GL
Grenada	GJ
Guadeloupe	GP
Guam	GQ
Guatemala	GT
Guernsey	GK
Guinea	GV
Guinea-Bissau	PU
Gulf of Mexico	1M
Guyana	GY
Haiti	HA
Heard Island and McDonald Islands	HM
Holy See	VT
Honduras	HO
Hong Kong	HK
Howland Island	HQ
Hungary	HU
Iceland	IC
India	IN
Indian Ocean	6A
Indian Ocean Islands	V2
Indonesia	ID
Iran	IR
Iraq	IZ
Iraq/Saudi Arabia Neutral Zone	IY
Ireland	El
Israel	IS
Italy	IT
Ivory Coast	IV
Jamaica	JM
Jan Mayen	JN
Japan	JA

Japan, Sea of	3J
Jarvis Island	DQ
Jersey	JE
Johnston Atoll	JQ
Jordan	JO
Juan De Nova Island	JU
Juan Fernandez Archipelago	YV
Kampuchea (formerly Cambodia)	CB
Kazakhstan	KZ
Kenya	KE
Kingman Reef	KQ
Kiribati	KR
Korea, Democratic Peoples Republic of (North Korea)	KN
Korea, Republic of (South Korea)	KS
Kuwait	KU
Kyrgyzstan	KG
Lakshadweep Islands (Laccadive Islands)	LD
Laos	LA
Latin America	L7
Latvia	LG
Lebanon	LE
Lesotho	LT
Liberia	LI
Libya	LY
Liechtenstein	LS
Lithuania	LH
Luxembourg	LU
Macau	MC
Macedonia	MK
Madagascar	MA
Madeira Islands	VD
Malawi	MI
Malaysia	MY
Maldives	MV
Mali	ML
Malta	MT
Man, Isle of	IM
Marshall Islands	VH
Marshall Islands, Republic of	RM
Martinique	MB
Mauritania	MR

Mauritius	MP
Mayotte	MF
Mediterranean, Eastern	8E
Mediterranean, Western	8W
Mediterranean Sea	Z9
Mexico	MX
Micronesia, Federated States of	FM
Middle East	F8
Midway Islands	MQ
Moldova	MD
Monaco	MN
Mongolia	MG
Montenegro	MW
Montserrat	MH
Morocco	MO
Mozambique	MZ
Namibia	WA
NATO Countries	N2
Nauru	NR
Navassa Island	BQ
Nepal	NP
Netherlands	NL
Netherlands Antilles	NT
New Caledonia	NC
New Hebrides (now Vanuatu)	NH
New Zealand	NZ
Nicaragua	NU
Nicobar Island	YZ
Niger	NG
Nigeria	NI
Niue	NE
Norfolk Island	NF
North Africa	F1
North Africa and Middle East	F9
Northern Island	WN
Northern Mariana Islands	CQ
Norway	NO
Norwegian Sea	5N
Okhotsk, Sea of	3Q
Okinawa	XG
Oman	MU

Pacific Islands (Palau), Trust Territory of the	PS
Pacific Ocean	Z7
Pacific Ocean Islands	V1
Pacific Ocean, North	3A
Pacific Ocean, South	4A
Pakistan	PK
Palmyra Atoll	LQ
Panama	PM
Papua New Guinea	PP
Paracel Islands	PF
Paraguay	PA
Pemba Island	PB
Persian Gulf	6P
Peru	PE
Philippines	RP
Pitcairn Islands	PC
Poland	PL
Portugal	PO
Puerto Rico	RQ
Qatar	QA
Red Sea	6E
Reunion	RE
Romania	RO
Russia	RS
Rwanda	RW
Sala y Gomez Island	WC
San Ambrosio, Isla	YX
San Felix, Isla	YK
San Marino	SM
Sao Tome and Principe	TP
Sardinia (Sardegna)	SD
Saudi Arabia	SA
Senegal	SG
Serbia	SR
Seychelles	SE
Sierra Leone	SL
Singapore	SN
Slovak Republic	LO
Slovenia	SI
Socotra	SJ
Solomon Islands	BP

Somalia	SO
South Africa	SF
South America	S
South Asia	A5
South China Sea	3U
Southeast Asia	A6
South Orkney Islands	WG
South Shetland Islands	WH
Southwest Asia	A7
Spain	SP
Spratly Islands	PG
Sri Lanka	CE
St. Christopher (Kitts) and Nevis	SC
St. Helena	SH
St. Lucia	ST
St. Pierre and Miquelon	SB
St. Vincent and the Grenadines	VC
Sub-Saharan Africa	F7
Sudan	SU
Suriname	NS
Svalbard	SV
Swaziland	WZ
Sweden	SW
Switzerland	SZ
Syria	SY
Taiwan	TW
Tajikistan	TI
Tanzania	TZ
Thailand	TH
Togo	TO
Tokelau	TL
Tonga	TN
Trinidad and Tobago	TD
Tromelin Island	TE
Tunisia	TS
Turkey	TU
Turkmenistan	TX
Turks and Caicos Islands	TK
Tuvalu	TV
Uganda	UG
Ukraine	UP

Union of Soviet Socialist Republics	UR
United Arab Emirates	TC
United Kingdom	UK
United Nations	UN
United States	US
United States (Miscellaneous Pacific Islands)	IQ
Upper Volta (now Burkina Faso)	UV
Uruguay	UY
Uzbekistan	UZ
Vanuatu (formerly New Hebrides)	NH
Vatican City (Holy See)	VT
Venezuela	VE
Vietnam	VM
Virgin Islands	VQ
Wake Island	WQ
Wallis and Futuna	WF
Walvis Baai	YA
West Bank	WE
Western Europe	E6
Western Sahara	WI
Western Samoa	WS
Worldwide	W
Yellow Sea	3Y
Yemen	YM
Yemen Arab Republic (North Yemen, arch.)	YE
Yemen, Peoples Democratic Republic of (South Yemen, arch)	YS
Yugoslavia (former)	YO
Zaire	CG
Zambia	ZA
Zanzibar	ZY
Zimbabwe	ZI

GEOPOLITICAL AREAS BY CODE

A4	Arabian Peninsula
A5	South Asia
A6	Southeast Asia
A7	Southwest Asia
1A	Atlantic Ocean, North
1M	Gulf of Mexico
1X	Caribbean Sea
2A	Atlantic Ocean, South
3A	Pacific Ocean, North
3J	Sea of Japan
3Q	Sea of Okhotsk
3U	South China Sea
3Y	Yellow Sea
4A	Pacific Ocean, South
5A	Arctic Ocean
5B	Barents Sea
5C	Chukchi Sea
5D	Bering Sea
5N	Norwegian Sea
5R	Bering Strait
6A	Indian Ocean
6E	Red Sea
6P	Persian Gulf
6R	Arabian Sea
7B	Baltic Sea
8C	Caspian Sea
8D	Adriatic Sea
8E	Mediterranean, Eastern
8W	Mediterranean, Western
8G	Aegean Sea
A	Asia
AA	Aruba
AB	Abkhazia
AC	Antigua and Barbuda
AF	Afghanistan
AG	Algeria
AL	Albania
AM	Armenia
AN	Andorra
AO	Angola

AQ	American Samoa
AR	Argentina
AS	Australia
AT	Ashmore and Cartier Islands
AU	Austria
AV	Anguilla
AY	Antarctica
AZ	Azores Islands
BA	Bahrain
BB	Barbados
BC	Botswana
BD	Bermuda
BE	Belgium
BF	Bahamas
BG	Bangladesh
BH	Belize
BI	Balearic Islands
BK	Bosnia and Herzegovina
BM	Burma
BN	Benin
BO	Belarus
BP	Solomon Islands
BQ	Navassa Island
BR	Brazil
BS	Bassas Da India
BT	Bhutan
BU	Bulgaria
BV	Bouvet Island
BX	Brunei
BY	Burundi
CA	Canada
CB	Kampuchea (formerly Cambodia)
CD	Chad
CE	Sri Lanka
CF	Congo
CG	Zaire
CH	China (Peoples Republic ofl
CI	Chile
CJ	Cayman Islands
CK	Cocos (Keeling Islands)
CM	Cameroon

CN	Comoros
CO	Colombia
CQ	Northern Mariana Islands
CR	Coral Sea Islands
CS	Costa Rica
CT	Central African Republic
CU	Cuba
CV	Cape Verde
CW	Cook Islands
CY	Cyprus
CZ	Czechoslovakia
DA	Denmark
DJ	Djibouti
DO	Dominica
DQ	Jarvis Island
DR	Dominican Republic
E5	Eastern Europe
E6	Western Europe
EC	Ecuador
EG	Egypt
El	Ireland
EK	Equatorial Guinea
EN	Estonia
ER	Eritrea
ES	El Salvador
ET	Ethiopia
EU	Europa Island
EZ	Czech Republic
F1	North Africa
F7	Sub-Saharan Africa
F8	Middle East
F9	North Africa and Middle East
FK	Falkland Islands
FG	French Guiana
FI	Finland
FJ	Fiji
FM	Micronesia, Federated States of
FO	Faroe Islands
FP	French Polynesia
FQ	Baker Island
FR	France

FS	French Southern and Antarctic Lands
GA	Gambia
GB	Gabon
GC	Germany, Democratic Republic of (arch.)
GE	Germany, Federal Republic of
GG	Georgia
GH	Ghana
Gl	Gibraltar
GJ	Grenada
GK	Guernsey
GL	Greenland
GM	Germany
GO	Glorioso Islands
GP	Guadeloupe
GQ	Guam
GR	Greece
GT	Guatemala
GV	Guinea
GY	Guyana
GZ	Gaza Strip
HA	Haiti
HK	Hong Kong
HM	Heard Island and McDonald Islands
HO	Honduras
HQ	Howland Island
HR	Croatia
HU	Hungary
IC	Iceland
ID	Indonesia
IM	Man, Isle of
IN	India
IO	British Indian Ocean Territory
IP	Clipperton Island
IQ	United States (Miscellaneous Pacific Islands)
IR	Iran
IS	Israel
IT	Italy
IV	Ivory Coast
IY	Iraq/Saudi Arabia Neutral Zone
IZ	Iraq
JA	Japan
JE	Jersey

JM	Jamaica
JN	Jan Mayen
JO	Jordan
JQ	Johnston Atoll
JU	Juan De Nova Island
KE	Kenya
KG	Kyrgyzstan
KN	Korea, Democratic Peoples Republic of (North Korea)
KQ	Kingman Reef
KR	Kiribati
KS	Korea, Republic of (South Korea)
KT	Christmas Island
KU	Kuwait
KZ	Kazakhstan
L7	Latin America
LA	Laos
LD	Lakshadweep Islands (Laccadive Islands)
LE	Lebanon
LG	Latvia
LH	Lithuania
LI	Liberia
LO	Slovak Republic
LQ	Palmyra Atoll
LS	Liechtenstein
LT	Lesotho
LU	Luxembourg
LY	Libya
MA	Madagascar
MB	Martinique
MC	Macau
MD	Moldova
MF	Mayotte
MG	Mongolia
MH	Montserrat
MI	Malawi
MK	Macedonia
ML	Mali
MN	Monaco
MO	Morocco
MP	Mauritius
MQ	Midway Islands

MR	Mauritania
MT	Malta
MU	Oman
MV	Maldives
MW	Montenegro
MX	Mexico
MY	Malaysia
MZ	Mozambique
N2	NATO countries
N4	Central America
N5	Caribbean Islands
NC	New Caledonia
NE	Niue
NF	Norfolk Island
NG	Niger
NH	Vanuatu (formerly New Hebrides)
NI	Nigeria
NL	Netherlands
NO	Norway
NP	Nepal
NR	Nauru
NS	Suriname
NT	Netherlands Antilles
NU	Nicaragua
NZ	New Zealand
PA	Paraguay
PB	Pemba Island
PC	Pitcairn Islands
PE	Peru
PF	Paracel Islands
PG	Spratly Islands
PK	Pakistan
PL	Poland
PM	Panama
PO	Portugal
PP	Papua New Guinea
PS	Trust Territory of the Pacific Islands (Palau)
PU	Guinea-Bissau
QA	Qatar
RE	Reunion
RM	Marshall Islands, Republic of

RO	Romania
RP	Philippines
RQ	Puerto Rico
RS	Russia
RW	Rwanda
S	South America
SA	Saudi Arabia
SB	St. Pierre and Miquelon
SC	St. Christopher (Kitts) and Nevis
SD	Sardinia (Sardegna)
SE	Seychelles
SF	South Africa
SG	Senegal
SH	St. Helena
SI	Slovenia
SJ	Socotra
SL	Sierra Leone
SM	San Marino
SN	Singapore
SO	Somalia
SP	Spain
SR	Serbia
ST	St. Lucia
SU	Sudan
SV	Svalbard
SW	Sweden
SY	Syria
SZ	Switzerland
TC	United Arab Emirates
TD	Trinidad & Tobago
TE	Tromelin Island
TH	Thailand
TI	Tajikistan
TK	Turks and Caicos Islands
TL	Tokelau
TN	Tonga
TO	Togo
TP	Sao Tome and Principe
TS	Tunisia
TU	Turkey
TV	Tuvalu

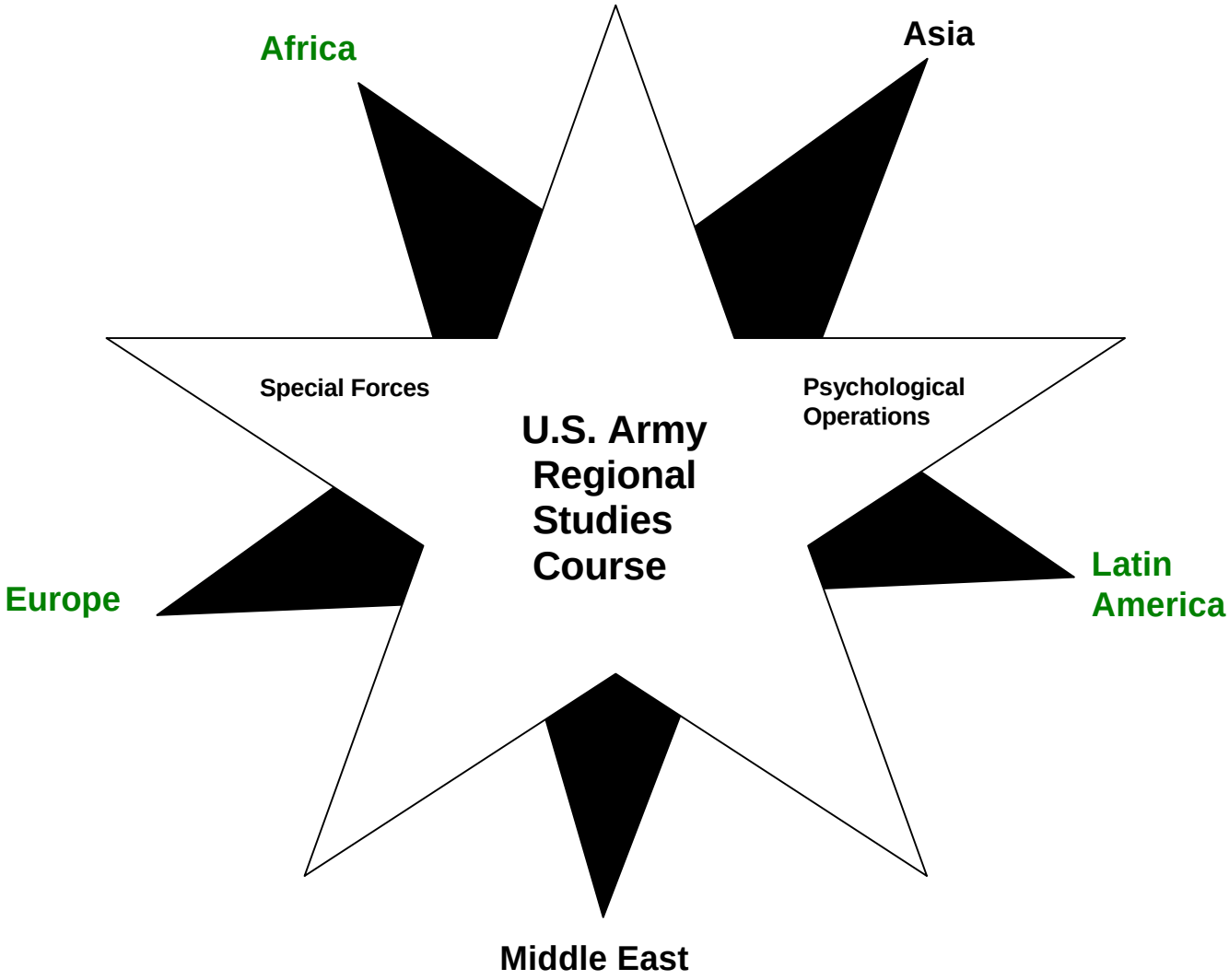
TW	Taiwan
TX	Turkmenistan
TZ	Tanzania
UG	Uganda
UK	United Kingdom
UN	United Nations
UP	Ukraine
UR	Union of Soviet Socialist Republics
US	United States
UV	Burkina Faso (formerly Upper Volta)
UY	Uruguay
UZ	Uzbekistan
V1	Pacific Ocean Islands
V2	Indian Ocean Islands
VC	St. Vincent and the Grenadines
VD	Madeira Islands
VE	Venezuela
VH	Marshall Islands
VI	British Virgin Islands
VJ	Crete
VK	Cabinda
VM	Vietnam
VP	Corsica
VQ	Virgin Islands
VT	Vatican City (Holy See)
W	Worldwide
WA	Namibia
WC	Sala y Gomez Island
WE	West Bank
WF	Wallis and Futuna
WG	South Orkney Islands
WH	South Shetland Islands
WI	Western Sahara
WN	Northern Island
WQ	Wake Island
WS	Western Samoa
WZ	Swaziland
XG	Okinawa
XZ	Easter Island
YA	Walvis Baai
YE	Yemen Arab Republic (North Yemen, arch.)

YK	San Felix, Isla
YL	Diego Garcia
YM	Yemen
YO	Yugoslavia
YR	Annobon (Pagulu)
YS	Yemen, Peoples Democratic Republic of (South Yemen, arch.)
YU	Eloby, Islas de
YV	Juan Fernandez Archipelago
YX	San Ambrosio, Isla
YZ	Nicobar Island
Z7	Pacific Ocean
Z8	Atlantic Ocean
Z9	Mediterranean Sea
ZA	Zambia
ZI	Zimbabwe
ZL	Caroline Islands
ZQ	Andaman Islands
ZY	Zanzibar
ZZ	Canary Islands

This Page Is Intentionally Left Blank

Special Operations and International Studies

Political Military Analysis Handbook



United States Army John F. Kennedy Special Warfare Center and School

Fort Bragg, North Carolina 28310
2004

FOREWORD

This handbook has been prepared by the faculty (appendix 1) of the “Regional Studies Course” (RSC) to support a program of study that prepares Army officers for Civil Affairs and Psychological Operations assignments abroad. In the course, students survey five world “regions” -- Africa, Asia, Europe, Latin America, and the Middle East -- and study one of them in some depth. The faculty uses the sixteen discrete “Political-Military Factors” discussed herein as common reference points for teaching the course's five regionally focused seminars. More important, they are introduced to the students as a reliable framework for analysis that, when applied judiciously, will lead to a sophisticated understanding of the dynamics within the foreign country or region of their assignment. Furthermore, the framework provides the start point for specific analyses of associated operational issues, questions, and problems. The theories, concepts, and insights developed in-conjunction with these sixteen factors are drawn from broadly accepted scholarship; but they are selected, organized, and presented to support the course's practical goal of preparing officers for challenging Civil Affairs and Psychological Operations assignments abroad.

We welcome your comments, ideas, and critiques. Address them to: Regional Studies Course Attn: Seminar Director, P.O. Box 74145, Ft. Bragg, NC . 28307.

INTRODUCTION

As a Civil Affairs or Psychological Operations officer conducting or planning for operations in foreign environments you will need a solid grasp of the military, political, and sociological dynamics at work within the “Area of Operation." Experience shows that developing a sophisticated understanding of the operational environment in another country or region is a very complex endeavor. Success requires a deliberate analytical approach using a well-vetted framework and solid methodology.

By analytical approach, or analysis, we mean the study of the whole by dividing it into discrete parts, examining the nature of each part, and determining how they function in relation to each other and the whole. The objective is not merely a multi-faceted description of a certain phenomenon, physical or social, but an **explanation** of how those facets relate to each other and create the whole. For example, we cannot explain how a Swiss watch works simply by disassembling it and describing the various parts. We must also determine how those parts fit and operate in conjunction with each other.

The "Pol-Mil" Factors

The sixteen Political-Military factors discussed in this handbook provide a carefully constructed framework for use in analyzing an operational environment. Each factor addresses an important aspect of that environment, nominally assumed to be that of a foreign country. When used collectively, and in conjunction with the research methodology reviewed in chapter 1, these factors will develop a comprehensive base of knowledge about the country or region of interest. When assessed in conjunction with each other, they form the start point for multi-discipline analyses of the issues and questions that are associated with Civil Affairs or Psychological Operations activity abroad. You will exercise with these factors in the Regional Studies Course with the intent that you apply them in your assignments after graduation.

The sixteen factors presented here have been selected to ensure that all the “parts” or dimensions of complex foreign environments are captured and brought under examination. While this specific list, or framework, is somewhat arbitrary, we consider it a comprehensive one that incorporates insights from a range of academic disciplines to ensure the development of a fully dimensioned understanding of the operational environment. Recently we have added “Media” and “Technology” to the mix of factors as their impact on operations abroad has clearly increased in the age of “globalization.”

How to Use the Handbook

Each chapter is devoted to an individual "factor" or dimension of a country or region. The chapters begin by defining important terms and introducing academic approaches that have been developed to help interpret data and explain events within the domain of that factor. The aim is to provide important fixed markers that are commonly used when examining the area under study through that chapter's particular domain or lens and, at the same time, alert you to the often broad scope of thought and approach within it. For

example, while "history" is succinctly defined early on in Chapter I, the review of literature that follows illuminates the multitude of approaches and perceptions that lurk just under the surface of the definition. The chapters then turn to a practical distillation of approaches, concepts, cautions, and questions. You should use these as guides to help you with the task of sorting through the voluminous available data and opinion relevant to the factor, or aspect, of the area under study. [1] This task, the selection and evaluation of data is the crucial start point for all analyses.

Understanding how each of these factors or dimensions are reflected or manifested in the area you are studying is, in most cases, just the first step in your analysis. Just as the mainspring and gears of a watch do not operate in isolation from each other, neither do the various discrete factors taken up by the chapters in this handbook. For instance, Chapter 13 alerts you to the fact that ethnicity can have its "roots" in other factors, such as religion or culture; and Chapter 5 warns that, "the study of economics cannot be divorced from the political context." Determining how such interrelationships function in the country under study puts a premium on reflection and breadth of thought, and the final section of each chapter is written to help you begin this process.

This leads to a third aspect of the analytical process supported by this handbook. Generally, your analyses will be undertaken in response to an identified issue, problem, or question. The analytical task may be broad or narrow -- for instance, "how does it work?" versus "does it need a new mainspring?" in the case of Swiss watches -- but it will call for explanation or prediction, as opposed to mere description. The issues and questions arising in your Civil Affairs and Psychological Operations assignments will be diverse, for example: "What type of civil affairs projects can make a difference in Ethiopia?" "How might current socio-political dynamics in Venezuela affect U.S. political-military operations, such as disaster relief, there?" "What propaganda themes will advance peacemaking/peacekeeping efforts in the Balkans?"

To answer such questions with confidence you must determine how each of the Pol-Mil factors might affect the particular issue or question being addressed. That effect is issue dependent, and its impact on your analysis can, and often does, vary from country to country and issue to issue. This then is really the heart your analysis -- assessing how each of these factors acts on the issue in question and then drawing the appropriate conclusions. In so doing, do not discount any of the factors *a priori*. You need to understand and consider all of them and then, if you conclude that several are not relevant to your conclusion, explain why.

---

[1] Apart from their role in developing a comprehensive assessment to the area, some of these concepts can also be used in a more discrete fashion For example, given a well developed democracy, the "median voter theorem" might be helpful in assessing the likelihood of country "x," perhaps Finland, adopting a particular policy, such as whether or not to join NATO.

In summary, use these sixteen factors as a framework for beginning analyses that address operational and planning issues in foreign environments. Determine how each is manifested in that area and how each influences the other there. Then assess those insights against the specific issue or question at hand. The result will be solidly grounded conclusions that you can use with confidence.

Table of Contents

Foreword

Introduction

Chapter 1 Research Methods

Chapter 2 History

Chapter 3 Natural Environment

Chapter 4 Regional Perspective

Chapter 5 Foreign Influence

Chapter 6 National Interests

Chapter 7 Ideology

Chapter 8 Political Systems

Chapter 9 Political Economy

Chapter 10 Role of the Military

Chapter 11 Leadership

Chapter 12 Elites

Chapter 13 The Cultural Environment

Chapter 14 Religion

Chapter 15 Ethnicity

Chapter 16 Technology

Chapter 17 Media

Chapter 1

Research Methods

I. Introduction:

This chapter includes the methods used to conduct social science research. It provides guidance in principle rather than instructions in detail. Therefore, it starts with an overview of how social science research uses ideas and facts to generate knowledge. Then, it moves to a brief description of the standards of scholarly research. This is followed by an examination of how theories and data are used in social science research. The chapter ends with sections on how to structure a research paper and how to attribute and document sources.

Important concepts are introduced and defined throughout the chapter. However, it will be useful to define the following key terms from the start[1]:

Method: the systematic application of reasoning to the analysis of data.

Analysis: "1. The breaking up of any whole into its parts so as to find out their nature, proportion, function, relationship etc." (*Webster's Deluxe Unabridged Dictionary*, 2d ed.).

Theory: A set of ideas that explain observed phenomena in terms of underlying relationships to other phenomena.

Data: Qualitative and quantitative observations of the world.

Empirical: Having to do with the analysis of data

II. Overview: Combining Ideas and Facts

The aim of scholarly research is to increase our knowledge about the world. But what is knowledge? Is it simply the sum total of factual information we have about the world? Astrologers have very detailed information about the movement of planets and stars but they ask questions and find answers that are very different from those of astronomers. This is largely because astrologers have a different understanding of how observable events (or phenomena) are related to each other than astronomers do. Given the same information, astronomers and astrologers will claim to know entirely different things about the world.

Therefore, one can define knowledge as a body of facts, and ideas that interpret and explain them. The importance of this definition is that it points to two approaches to gaining knowledge. Theoretical research focuses on ideas about how the world works and empirical research focuses on observing the world as it works. Though individual projects may be purely theoretical or empirical, social science research as a whole depends on the interaction of theoretical and empirical research to expand our knowledge of the world.

[1] With the exception of the definition of analysis, these definitions have been derived from common usage in social science. See Johnson and Joslyn (1995) for a more detailed discussion of these terms.

The methods of social science research emphasize the use of both theory and data (ideas and facts). Theories explain how two or more general classes of phenomena (e.g., income inequality and political violence) are related. In most empirical research, data is collected to test the generalizations that theories produce. Theories that survive the testing process (i.e., "hold water") are used to explain particular events or to predict the outcome of future events. Table 1-1 illustrates the role ideas and facts play throughout the research process.

Table 1-1: Interplay of Ideas and Facts

Ideas :		**Facts:**
		Observations suggest topic (or preliminary answer to question)
Other people's work suggests how to break topic down.		Further observation along with others' ideas refines understanding of topic.
Develop specific research goal.		
Look for and develop theoretical framework within which to consider facts.		
Use conceptual framework to generate new propositions about the world.	*AND/OR*	Collect and analyze data to test propositions about the world, OR Use theoretical framework to analyze the world.
Interpret results and draw conclusions		

III. Standards of Scholarly Research in International Relations (IR)

There are several substantive standards for research in social science in general, and IR in particular. Though they are often labeled and categorized in different ways, the following list captures the main criteria:

Interest: The research topic should be positive, significant, and general. A positive topic is non-normative and deals with the world as it is, not as it should be. A significant topic is not trivial and does not leave the reader asking "So what?" Research should also focus on events or classes of events that are likely to occur again and thus are general in nature.

Originality: Research should extend the existing body of knowledge. This can be done by adding new theories or data, by refining existing theories or data, and/or combining existing theories and data in new ways. It is incumbent on researchers to review the literature on their topic to ensure that they are not "reinventing the wheel".

Cumulation: Though it should be original, research should also build on existing theoretical and empirical research. Researchers are expected to use the information and ideas of previous researchers as a foundation for their research. In doing so, researchers must be candid and critical about what they take from others. That is researchers must properly attribute the

sources of their ideas and data to ensure there is no doubt which ideas are original and which are not. They must also scrutinize the ideas and cross-examine the information they use to ensure that the foundation of their research is solid.

Method: Research must have a discernible methodology that is appropriate, transparent, and persuasive. There are many different methodological approaches from which a researcher may chose. The choice of an appropriate methodology is often governed by the topic and the existing literature on the topic. Whatever methodology is chosen, it must be transparent to the reader how the research is conducted. That is, it must be apparent to the reader how each step of the research was conducted. This standard is that readers should be able to reproduce the research themselves (thus this standard is often described as reproducibility). Finally, the research must be persuasive in that it must support the conclusions of the researcher's analysis and there must have been the possibility that the research could have pointed to a different conclusion.

Results: Though the results may be qualified or ambiguous, research is not done until it comes to a conclusion. From the beginning of the research, it should be clear what the research is trying to explain, or what question it is seeking to answer. At the end of the research, the researcher should be straightforward about presenting the explanation or answer produced by the research.

IV. Using Theories

Theories explain observed events in terms of unobserved relationships to other phenomena. The events that theories explain are called dependent variables and the phenomena that are used to explain the dependent variable are called independent variables. Theories tell stories about how independent variables affect dependent variables. They also make predictions, called hypotheses, about what will happen to the dependent variable given different values of the independent variable.

Theories are very useful for analyzing particular events because they suggest likely cause and effect relationships. In so doing, they point out what data is important and what data is not. This filtering function simplifies the data collection task and prevents the researcher from being overwhelmed by data. Theories not only tell the researcher what data to collect but also what different the data mean. Thus, by providing a framework for interpreting the data, theories also simplify the analysis task.

One might object that, by driving the collection and interpretation of data, theories bias and limit the analysis. To a certain extent they do, but, as a practical matter, researchers must limit the data they collect and analyze. Whatever bias a theory may impart on the research, it is preferred to the bias that results from basing research on ad hoc explanations, or on the data that happen to be the most readily available. However, researchers must examine the "track record" of the theoretical perspective they select and be aware of the limitations it imposes on their analysis. For this reason, researchers usually employ more than one theoretical perspective when interpreting an event.

Finding Theories: Choosing a theoretical perspective or perspectives upon which to

base one's research is perhaps the most important part of the research. The selection and development of a conceptual framework of analysis is also the most intellectually challenging task a researcher faces. For this reason many students try to bypass this step and go straight to analyzing data. Unfortunately, in not making a choice, they have chosen to develop ad hoc explanations based on unsystematically collected data. This is an approach that is acceptable in journalism but not in social science.

Therefore, once a topic is assigned or selected, research must begin with a survey of the literature to identify the relevant theoretical perspectives. The Pol-Mil Factors Handbook presents theoretical perspectives on many different topics, and thus, it is a natural starting point. Students should also conduct a search of the scholarly literature on their specific topic to identify additional theoretical perspectives. Students should search academic journals, libraries and publishers for the latest scholarly articles and books on their topic. The emphasis here is on scholarly works because these will have more developed theoretical frameworks, as well as discussions of and references to the larger literature on the topic.

Using Theories: Once the various theoretical perspectives have been identified, the researcher must choose which one or ones to use. The researcher may choose to refine a theory, combine it with others, or develop a new theory. The choice is generally governed by the theory's record at producing results and its applicability to the exact question the researcher is interested in answering. Most importantly, the theory's dependent variable must be the same as that of the researcher. If the researcher is trying to predict how a war will end (the researcher's dependent variable), then theories that explain when wars start (the theories' dependent variable) are not applicable.

The goal is to create a conceptual framework that defines key concepts and specifies cause and effect relationships between them. Concepts are general characteristics or aspects of events under study. For instance one might describe events in Chechnya as a war, an ethnic conflict, a rebellion or a counterinsurgency. Each of these descriptions is a concept that needs to be explicitly defined before its relevance to the particular events can be examined. A good theory about the cause of ethnic conflicts will provide a clear definition of ethnic conflicts and well as of the causes. It can not be overemphasized that it must be clear what aspect of the event the researcher is trying to explain (the dependent variable), and what aspects of the event the researchers is using to explain it (the independent variables).

IV. Using Data

Once the conceptual framework has been established, the researcher is ready to engage the data. This part of the process is more concrete and systematic, but also more tedious and frustrating. The researcher must identify, find, evaluate, and analyze the data. Each of these steps is described below.

Identifying Data: The researcher must determine what data to collect to measure each of the key concepts in the conceptual framework. If the conceptual framework is well thought out, then it will be a fairly straightforward task to identify the ideal types of data. Of course, the ideal data are rarely available, but the researcher must start out with a good idea about what the best data would be in order to identify what the next best data are.

Finding Data: Given time and resource constraints, most student researchers use existing data, as opposed to conducting primary research to collect new data. Research libraries, such as UNC Chapel Hill's Davis Library, are some of the most valuable sources of data available. They either contain or have electronic access to an overwhelming supply of data. More importantly, they have a staff of reference librarians who are professionals at connecting researchers with information.

Unfortunately, students often attempt to collect all their information off the Internet. While the Internet is an invaluable research tool, the websites on it are a problematic source of information. Most high quality texts, articles and data are copyrighted, and are not available to the general public over the Internet. The best sources of information on the Internet usually require some kind of subscription or access fee.

Fortunately, libraries have started buying access to these services for their patrons. Many universities offer its full and part-time students remote access to a number of on-line subscriptions such as InfoSeek and EBSCO host. North Carolina Public Libraries offer cardholders access to a wide range of subscription services in a service called NC Live. A description of these services can be found at <http://www.nclive.org/>. UNC Chapel Hill cardholders have access to NC Live and a number of other services described on their website at <http://www.lib.unc.edu/>. NC Live and most of UNC Chapel Hill's services require the researcher to physically be in the library.

Evaluating Data: Researchers have a responsibility to critically evaluate the origin and quality of the information they use. This task has been greatly complicated by the explosion of information available on the Internet. The low cost and relative anonymity of web publishing allows not only for a diversity of ideas and viewpoints but also for a great deal of dubious or false information, and outright propaganda. Because web publications have typically not been through a review process, researchers must be much more critical of web publications than of traditional publications.

Generally, researchers must evaluate both the sources and content of their data. To evaluate the data's source, the researcher must identify the author of the data and how the author originally acquired the data. The researcher must also critically examine the reliability and objectivity of both the original author and the original author's data. Researchers are free to use data from biased or unreliable sources, as long as they acknowledge and describe the bias or unreliability, and qualify their analysis to account for the imperfections of the data.

When evaluating the content of sources, one of the biggest problems researchers face is sorting out propaganda from scholarship. Bodi (1995) lists the following indicators of propaganda and scholarship that students and researchers can use to evaluate both print and web publications:

Indicators of Scholarship:	Indicators of Propaganda:
Describes limits of data	Excessive claims of certainty
Presents accurate description of alternate views	Personal attacks or ridicule
Presents data that both does and does not Support favored views	Emotional appeals Distortion of data that doesn't support favored

Encourages debate, discussion, and criticism
Settles disputes with generally accepted Methods for analyzing data.
Looks for counter examples
Uses language in conventional ways
Updates information
Admits own ignorance
Attempts to discuss general laws and Principles
Finds fault and admits difficulties in own field
Relies on logic and critical thinking skills

view
Suppresses contradictory views
Suppresses contradictory facts
Appeals to popular prejudices
Relies on suggestion, innuendo
Devalues thought and critical appraisal
Transforms words to suit aims
Magnifies problems and minimizes problems with suggested remedies
Presents information and views out of context

Analyzing Data: Once the data has been evaluated in terms of itself, it must be analyzed in terms of the overall research question. If the data is qualitative in nature, then the researcher must subjectively appraise the data and use logic to derive conclusions. As stated before, the theoretical perspective adopted provides an invaluable starting point for logical arguments. A detailed discussion of how to construct logical arguments is beyond the scope of this chapter. However, useful discussion of using logic can be found at Purdue University's Online Writing Laboratory at http://owl.english.purdue.edu/Files/123.html .

Statistical methods are usually used to analyze quantitative methods. Again a detailed discussion of these methods is beyond the scope of this chapter. However, Johnson and Joslyn (1995) provide a thorough introduction to the range of statistical methods used in political science research. In addition, Middleton (1997) provides detailed instructions on using Microsoft Excel to conduct statistical analysis.

V. The Research Report:

The structure of the report, usually a paper, is a thing apart from the structure of the research. That is, the sequence of the paper does not follow the sequence of the research. While you can, and should, write large parts of the paper as you conduct the research, you must write the paper as a report of your results, not as narrative of your research. The main difference between the sequence of the research and the paper is that research will end up pointing to one fundamental conclusion while your paper must start and end with that conclusion.

Introduction: In terms of presentation, this section is the most important. It orients your reader to your question, methodology and subsequent conclusions. You want to lay out your paper for your reader by explaining what you're doing, and how you are doing it. It is essential that the writer and reader know where the paper is going from beginning to end. Generally, one should be able to read the first and last paragraphs of a paper (or the first and last pages of a thesis) and have it make sense. To that end, the introduction as a whole should answer the following questions:

What is the question, hypothesis or story you are telling? By the end of the first paragraph, the reader should know what your paper is about. You need to be very clear exactly what it is you are trying to explain or understand. In technical terms, what is your dependent variable?

What is the state of the art on this subject? Describe the literature as a whole paying particular attention to seminal works and the most recent works. If there is more than one school of thought on your subject, then describe the debate. Your purpose is to point out what has been done and what has been left undone. It may be that no one has looked at your particular problem or you think there is a shortcoming in their approach. Your review of the literature should lead into the answer to the next question.

What are you going to do to improve on the literature? Having pointed out the shortcomings of the literature, you must now show how you're going to - at least partially - correct them. Explain your methodology and how it improves on existing works. The reader should have a good idea of what it is you are going to do.

Where are you going from here? Your introduction should always end with a road map of the remaining paper or thesis. Explain the structure of your paper/thesis and the logic behind it.

Where will it end? You should always give a sense of what your conclusions will be. You are not trying to surprise your reader.

Methodology/Theory: It may be that your methodology or theory is particularly involved and requires a detailed explanation. If so you should briefly describe your methodology in the introduction and go into detail in a separate section.

Substantive Sections: Here you do the work. It is important that as you present information, you also analyze it. Never assume that a quote, a fact, a graph or figure speak for themselves. Always explain the significance of the data and the implications of the analysis for the overall point you are making. Don't wait until the paper's conclusion to point out the major points.

Conclusions: There should be nothing new in the conclusions. The reader should be convinced by now. If, when writing the conclusion, you see a new argument for or against your point, you need to go back and put that in the body. What you are doing here is summing up what you've found and suggesting broader implications of your findings.

Reference List: All papers require a reference list or bibliography. One should list only works that have been cited in the paper/thesis. There is a school of thought that advocates a "Reference List" of works cited and a "Bibliography" of a wider list of relevant works. However, if the work is so relevant, it should have been cited; or, if it isn't worth citing, it's not relevant enough to be listed. If there are interesting works on tangential subjects, it's better to comment on them in footnotes.

VI. Attribution and Documentation

The fundamental principle of academic integrity is simple. Ensure that there is no doubt about the origin of all the ideas and information in your work. Earnest adherence to this principle is far more important than adherence to any particular format. For this reason, the principles of attribution and documentation are discussed before going into details of format.

Attribution: It is a matter of academic integrity that scholars not take credit for the words or ideas of other scholars. At the same time, it is imperative for the cumulative growth of knowledge that scholars use the ideas and words of others scholars. Indeed, the value of a scholar's work is often measured by how often it is cited by others. Therefore, all scholars must learn to honestly use and properly attribute the ideas and words of others.

When you use someone's ideas or words, there are two things you must do. First, make it clear to what extent you are using them and, second, give the original author credit. The dual nature of the standard is most easily seen in the case of using another person's words. In such a case, the other person's words are separated from one's your own by quotes or double indentations, thus satisfying the clarity requirement. Then a citation is attached to it (as discussed below) to give appropriate credit.

When using someone's ideas, it is generally necessary, and preferable, to paraphrase and reinterpret the original author's words. Authors are expected to summarize, interpret and criticize the ideas of others, not to "cut and paste" their words. Therefore, lengthy direct quotations are discouraged. Instead authors are expected to write their narrative so that it is apparent to the reader where the other authors' ideas begin and end. Thus, though there are several specific formats for crediting authors, being clear about how you have used another's ideas is a very subjective matter which calls for good judgment on your part.

Documentation: As discussed before, research must be transparent and reproducible in order to be considered scientific. Therefore, it is important that all data presented as fact is from verifiable sources, and that sufficient information is provided to allow the reader verify those sources. This is not as much an issue of integrity as it is of competence. To this end, citations are used for data from documented sources and appendices for data from undocumented or inaccessible sources (e.g., results from a survey conducted by the author).

It must be added that documentation is not authoritative. That is to say that when you document a fact, you are not showing that it is correct. Rather you are showing that you did not make it up or misinterpret it to support your conclusion. Furthermore, ideas, as opposed to empirical observations, cannot be presented as fact. Therefore, if Henry Kissinger is quoted as saying that anti-war protests had no effect on policy in Vietnam, documenting the quote only allows someone to verify whether or not he said it. Documentation does not establish whether or not he was right. It is very important to avoid the temptation to prove by citation.

Styles of Attribution and Documentation: There are several formats, usually referred to as styles, for citing other people's work. Almost every professional association and journal will have its own particular style. The style presented below comes from the *Chicago Manual of Style* (1993; hereafter referred to as *CMS*) which contains extremely detailed guidance on writing and editing. While *CMS* is one of the most commonly used style manuals, it is far from alone in the field. *The MLA Style Manual* (Achtert, and Gibaldi 1985) is commonly used in the humanities, *Publication Manual of the American Psychological Association* (1994) is often used in social and behavioral sciences, and Turabian (1987) publishes a guide to writing papers, theses and dissertations which is very popular among students. While all of the styles presented in these manuals will satisfy the requirements of attribution and documentation, it is important that a writer chooses one and consistently uses it.

There are two basic styles of citation, the documentary-note system and author-date system (*CMS* 1993 15.2). The note system uses footnotes or endnotes to indicate the source of whatever is being documented. This system is popular in the humanities because it involves the least intrusion on the text. The author-date system uses in-text references, which consist of the author or authors' last name(s) and the year in which the work was published, and a reference lists with full bibliographic information. Since social scientists use citations more often for attribution than documentation, this system is favored in the social sciences because it gets the cited author's name into the text.[2] For this reason, and because the author-date system is so easy to use, I will concentrate on the use of this system.

As already mentioned, the author-date system has two components, the in-text reference and the reference list. In the next two sections, I explain how to list the full bibliographic information in the reference list and, then, how to use in-text references. For clarity, entries in the reference list will be referred to as references and in-text references will be referred to as citations. Therefore, citing an author's work will involve using a citation and a reference.

References: References provide the readers with the information they need to locate and acquire the works you cite. Therefore, it is important that the information given be accurate and complete. In the author-date system, references are associated with the citations made in the text. Therefore, given a citation, it must be easy for the readers to find that particular reference in the reference list. These then are the two standards for references, completeness of information and ease of use.

It is easier to meet both of these standards if you write complete references for works when you first get them and build your reference list before you write your paper. Attempting to put the reference in its final form alerts you up front to any possible questions about how the information should be listed. This is a question that is much easier to resolve when you have the book in hand and the time to consult a style manual. Also, if the reference list is written and in hand, it will be easier to correctly cite works as you write.

Books: Here is the basic format for a book reference and three examples showing how multiple authors are listed.

Author's Last Name, First Name Middle Initial. Date. *Title in Italics.* City of Publication: Publisher.

Bueno de Mesquita, Bruce. 1981. *War Trap*. New Haven, CT: Yale University Press.

Bueno de Mesquita, Bruce and David Lalman. 1992. *War and Reason*. New Haven, CT: Yale University Press.

Bueno de Mesquita, Bruce, David Newman, Alvin Rabushka. 1985. *Forecasting Political Events.* New Haven, CT: Yale University Press.

---

[2]This is not to say that only the author-date is used in social science. There is some social science journals (e.g., *International Organization)* that use the documentary-note system.

Journal Articles: Academic journals are usually published, paginated and shelved in yearly volumes. Therefore, it is usually sufficient to know the volume and page number of an article to find it. Accordingly, the volume and page numbers are the meat of the reference.

Author's Last Name, First Name Middle Initial. Date. "Title of Article." *Title of Journal.* Volume Number (Issue Number): Starting page – Final Page Number.

Grieco, Joseph M. 1988a. "Anarchy and the Limits of Cooperation." *International Organization*.42:485-508.

Chapter in a multi-author (edited) collection: A great many academic books are collections of works written by various authors. If you wish to refer to the entire volume, then the reference is done in the following manner:

Editors Last Name, First Name Middle Initial, ed. Date. *Title of Collection.* City of Publication: Publisher.

Midlarsky, Manus I, ed.. 1997. *Inequality, Democracy, and Economic Development.* New York: Cambridge University Press.

However, if you wish to refer to a chapter of the collection, then the chapter gets its own reference emphasizing the author of the chapter and not the editor of the collection. This is done even if the author of the chapter happens to also be the editor of the collection. This type of reference is done in the following manner:

Author of Chapter's Last Name, First Name Middle Initial. Date. "Title of Chapter." In *Title of Collection,* ed. Editor's First Name Middle Initial Last Name. City of Publication: Publisher.

Muller, Edward N. 1996. "Economic Determinants of Democracy." In *Inequality, Democracy, and Economic Development,* ed. Manus I. Midlarsky. New York: Cambridge University Press.

Midlarsky, Manus I. 1996. "Introduction." In *Inequality, Democracy, and Economic Development,* ed. Manus I. Midlarsky. New York: Cambridge University Press.

Theses or Dissertations: Universities keep copies of master's thesis and Ph.D. dissertations somewhere in their library systems. To reference one, it is sufficient to indicate the type of work and the university to which it belongs in the following manner:

Author's Last Name, First Name Middle Initial. Date. "Title." Ph.D. diss. (Or Masters Thesis.) Name of University.

Lynch, John M. 1998. "Algeria, Iran and Turkey: A Model of Secular Versus Religious Nationalism." Master's Thesis. Troy State University at Ft. Bragg.

Electronic Sources*:* The most important thing to remember when citing information

received from the web is that you are citing the content and not the site. Therefore, you need to include the information you would normally include in a citation and reference, plus the information about where and when it was retrieved from the web. Most importantly, as with all citation, you must cite the author not the work. This is both more difficult and more important on the Internet since authorship of websites is often obscured and obscured authorship is often a sign of questionable content.

As in other forms of citation, there are differing styles. However, the International Standards Organization's format is gaining widespread acceptance. Full description of this format can be found at http://www.nlc-bnc.ca/iso/tc46sc9/standard/690-2e.htm . An adapted form of the basic format is as follows:

Author. Date of Publication. Title of Content. Secondary Responsibility. [Type of Medium]. Place of Publication: Publisher. [Date of Citation]. Availability and access. Standard number.

Examples: Each of these example deviates from the basic format in some way based on the type of online document and the available information.

Bureau of Public Debt. 1999. "Historical Public Debt Outstanding – Annual 1950 - 1999." *The Public Debt Online* [online]. Washington: Department of the Treasury. Available on the WWW at <http://www.publicdebt.treas.gov/opd/opdhisto4.htm>.

CNNfn. 2000. "China-Taiwan WTO Link." February 15 [online][accessed on Feb. 16, 2000] Available on the WWW at <http://www.cnnfn.com/2000/02/15/asia/wires/taiwan_trade_wg/>.

Paul, Satya.1999. "Relative Deprivation, Envy and Economic Inequality: A Comment." *Kyklos.* [online]. 52 (3):441-449.[Accessed on Feb. 16, 2000] Available on EBSCOhost. AN: 2239560.

OECD. 2000. "OECD Policy Brief: Economic Survey of the Czech Republic, 2000." [online] Washington: OECD Public Affairs Division, Public Affairs and Communication Directorate. [Accessed Feb, 16, 2000] Available on the WWW at <http://www.oecd.org/publications/Pol_brief/economic_surveys/e-czech.pdf>.

Organizing the Reference List: The reference list must be organized so that cited works can easily be found. Since the citation includes the author's name and date of the work, the list is arranged alphabetically by the author's last names and chronologically by date. That is to say, where an author has more than one work listed, the works are listed chronologically. If an author has more than one work from a particular year, adding and a, b, c, etc. to the year distinguish the works. Here is an example of a short reference list.

Reference List

Bueno de Mesquita, Bruce. 1981. *War Trap*. New Haven, CT: Yale University Press.

Bueno de Mesquita, Bruce and David Lalman. 1992. *War and Reason*. New Haven, CT:

Yale University Press.

Bueno de Mesquita, Bruce, David Newman, Alvin Rabushka. 1985. *Forecasting Political Events.* New Haven, CT: Yale University Press.

Bueno de Mesquita, Bruce, David Newman, Alvin Rabushka. 1996. *Red Flag Over Hong Kong*. Chatham, NJ: Chatham House Publishers.

Grieco, Joseph M. 1988a. "Anarchy and the Limits of Cooperation." *International Organization*.42:485-508.

----- 1988b. "Realist Theory and the Problem of International Cooperation: Analysis with an Amended Prisoner's Dilemma." *Journal of Politics.* 40:600-624

----- 1990. *Cooperation Among Nations: Europe, America, and Non-Tariff Barriers to Trade.* Ithaca, NY: Cornell University Press.

Citations: As discussed above, citations are used to attribute ideas to their original author and to document sources of information. In the author-date system, the citation is provided through the use of an in-text reference. This reference takes the following basic form:

(Last Name of Author(s) Date of Publication)

Citations are quite easy to form if the reference list has already been written. Given the example reference list, if one wanted to cite Bruce Bueno de Mesquita's book The War Trap, one would simply write:

(Bueno de Mesquita 1981)

Notice that only the last name is used (albeit a long one) and no punctuation is used between the name and the date. However, punctuation is used if there is more than one author as in this citation for Red Flag Over Hong Kong:

(Bueno de Mesquita, Newman, and Rabushka 1996)

Notice here that all three authors' names are included, commas separate their names and the conjunction "and" are used. That is to say that their names are written as they would be in a sentence.

More than one work by an author can be cited at once. In such a case, commas are used to separate the dates. If one wanted to cite Grieco's three works on cooperation, the following citation would be used:

(Grieco 1988a, 1988b, 1990)

Works by several authors can also be cited in one in-text reference. When so doing semi-colons are used to separate the
works of different authors or sets of authors as the following examples show:

(Bueno de Mesquita 1981; Grieco 1988a, 1988b, 1990)

(Bueno de Mesquita 1981; Bueno de Mesquita and Lalman 1992)

If reference is being made to a particular part of a work, the page, chapter, section, or figure number should be given in the citation (note p or pp is not used) A comma is used to separate the date from the page or section number. The following examples illustrate this:

(Bueno de Mesquita 1981, 15) (Grieco 1990, 20-25 (Bueno de Mesquita 1981, fig. 3.2)
Using Citations in the Text: Citations may be put in the text in one of three ways. If no reference to the authors or text being cited is made in the text, then the citation is included where it makes the most sense to be and where it will do the least damage to the flow. For example:

It has been argued that nations will not cooperate if they are concerned about relative gains (Grieco 1988a, 1988b, 1990). Others (Powell 1991; Snidal 1991) argue that nations may cooperate in spite of relative gains concerns.

If the author is referred to in the text, then only the date is included in parentheses. For example:

Bueno de Mesquita (1981) presents an expected utility model of war initiation.

Finally, if the work is referred to in the text, then the whole citation is included in the text. In such a case the citation acts as a short title for the work. For example:

The analysis in Bueno de Mesquita, Newman, and Rabushka 1996 indicates that Chinese policy towards Hong Kong will be turbulent for the next decade.

References:

Bodi, Sonia. 1995. “Scholarship or Propaganda: How Can Librarians Help Undergraduates Tell The Difference?” [online] *Journal of Academic Librarianship.* 21: 21-26. [Accessed may 5, 1999] Available on EBSCOhost.

The Chicago Manual of Style, 2d Edition (CMS). 1993. Chicago: University of Chicago Press.

Johnson, Janet Buttolph and Richard A. Joslyn. 1995. *Political Science Research Methods. Third Edition.* Washington, DC: CQ Press.

Middleton, Michael R. 1997. *Data Analysis Using Microsoft Excel*. Belmont, CA: Duxbury Press.

Chapter 2

History

There is a relation between the hours of our life and the centuries of time. Ralph Waldo Emerson

The past does not repeat itself, but it rhymes. Mark Twain

I. Introduction and definitions

Emerson and Twain's perspectives on history are a useful starting point for understanding the role of history in analyzing political-military phenomena. Both ascribe value to a historical perspective while avoiding any tendency towards an absolute reverence for history as a sole means for understanding.

The purpose of this chapter is to discuss the role of history in: 1) understanding the past, 2) helping to illuminate the present, and 3) casting some light on the future. The study of history is not a panacea for understanding other cultures, but it is possible to gain some insight based on an exploration of the past. History is also useful in another vein. Understanding the prevailing *conceptions* of history among a people, when used in conjunction with the other pol-mil factors, can be a powerful aid in designing psychological operations campaigns and in the planning and execution of civil-military operations.

One significant benefit of the study of history for the political-military officer is that it can make us less ethnocentric. "Historical study leads to broader views, to escape from the parochialism of the present, to an understanding that there were once other standpoints as commanding as the tenets of today" (Vincent, 1996, p. 25). Shafer makes a similar argument; the study of history can liberate "us from our own narrow experience, our own time, our own society . . ."(1960, p. 156). Studying history helps us to *unlearn* the prevailing myths that we have both about our own culture and others.

History is defined as 1) the actual events of the past, and 2) the academic discipline that studies the character and significance of past events. Because we can never have absolute knowledge concerning the actual events of the past, we will focus on the second definition. But the definition by itself does not elucidate the essence of historical study. In addition to describing the past, historians also attempt to explain it.

The study of history includes the selection *and* interpretation of facts about the past. In the words of historian George Kent, "Facts have to be selected, arranged, and interpreted before they acquire meaning . . . the same facts, differently arranged and interpreted, can be used to arrive at different, even opposite conclusions" (Kent, p. 309). Since history is about interpretation done by individuals, there cannot be a definitive interpretation. For example, at the end of the 19th century, the history of the American Civil War written from the Northern perspective was a much different story than the history of the War from the Southern perspective.

If there can be no definitive interpretation, then we must look to the philosophy of history to further understand the value of the historical perspective.

II. Review of the literature

Why study history?

There exists a plethora of introspective material written by historians focusing on questions concerning the utility and method of historical work. The ancient historian Thucydides gave the following reason for studying history: "The accurate knowledge of what has happened will be useful, because, according to human probability, similar things will happen again." (As quoted in Jordan, 1960, p. 53) Like Emerson and Twain, Thucydides does not tend toward an absolute.

Throughout modern writings there is a recurring theme that the study of history is useful. But there is also a strong admonition against simply trying to apply historical analogies to current events. Lessons are never so clear cut. In the process of studying history we learn that there are no perfect historical analogies, only complexities and subtleties. We must be on guard against those who claim excessive fungibility. It is at least as relevant to ask: How are things different?

For Leff, (1969) the study of history is "the record of difference rather than of similarity" (p. 60). And from Leff's perspective, this is the proper role: "Something is historically important in the degree to which it makes a difference." However, Pratt's approach may be more complete. According to Pratt (1974), the historian must explore both continuity and discontinuity. The historian's "interest in continuity obliges him to pay attention to similarities and generalities. His interest in discontinuity leads him to seek the unique, the novel, and the particular" (p. 208). Change and continuity are not mutually exclusive.

Concerning the utility of history, Schlesinger (1966) makes the point: "history generally serves as a 'negative' model rather than a 'positive' model" (p. 317). History does not tell the things that we must do, rather it tells us the mistakes that we ought to avoid. Schlesinger also warns against those who look to history for superficial analogies: "The only antidote to a shallow knowledge of history is a deeper knowledge, the knowledge which produces not dogmatic certitude but diagnostic skill, not clairvoyance but insight" (p. 320). History can be an interpretive *guide*, allowing us to make judgments about what is possible or probable, particularly when studying the long-term effects of actions.

Jordan argues that the study of history may not be immediately useful to the task at hand; nonetheless, it is valuable as part of a general education. According to Jordan, the greatest purpose of studying history is to increase "depth and breadth of insight" (p. 52). A broad understanding of history helps in developing perspective. For the political-military officer, the study of the history of a particular people helps in a general understanding of those people. And a study of what they *perceive* to be their history is of at least equal value.

From Kammen's (1979) point of view, the purpose of studying history is: "To make us more cognizant of human differences and similarities, over time and through space; To enhance our awareness of the complexity of historical causation; To acknowledge more fully than we do the consequences of what is at stake when powerful people interpret history for partisan purposes" (p. 57). History is not merely a factual subject; rather it is an analytical one: "an attempt to discover the *significant* things that have happened, and *why* they happened, what *caused* them and what *they* caused in their turn" (Perkin, 1970, p. 70). But Perkin is traveling down a dangerous slope because the issue of causality is rarely clear-cut.

Is the study of history science?

Concurrent with the rise of the social sciences in the 20th century, historians have debated amongst themselves on the nature of the study of history. Historians look at what has happened and they strive to answer the question: why? Historians often try to isolate causes. But the cause and effect relationship is nebulous in the study of history. Much of the debate is in response to the influential historian Collingwood and his theory of historical knowledge which postulates that the discipline of history "should be regarded as scientific because the methods appropriate to it are as rigorous as those utilized in the natural sciences and lead to conclusions which are equally justified and defensible" (As summarized in Pompa, 1995, p. 168). This attempt to create immutable laws as a result of the study of history is also a reflection of what was once the fashionable Marxist trend to create all-encompassing theory out of past events.

Vincent argues that the study of history is by nature different than the natural sciences because history "is no longer there." All that the historian can study are the particular pieces of evidence that remain, and "That evidence is an infinitesimal part of the evidence which once existed" (Vincent, p. 2). It follows that the interpretation of events based on partial evidence is inherently limited.

> Science gives the same results in every place and time; history is incapable of such replication, for each historical event is unique . . . historical circumstances do not have knowable, predictable, and replicable causes and consequences, in a way that causes regularly beget consequences in science. (Vincent, p. 18, 46)

As Pompa adds: "the subject matter of history differs from that of the natural sciences because history is concerned with human activities and experiences" (p. 168 in Broucher et al). The number of variables, particularly human action, defies the attempt to isolate causes.

Although moving from observations of the available evidence to generalizations is risky, this is not to say that some degree of induction can not be applied to the study of history. As political-military officers we can look for relationships as long as we realize the limits and understand that the rhymes occurring in the centuries of time are not absolute laws.

Types of written history

One can identify several classifications of written history. First it is useful to make distinctions based on the purpose of the author. Though all authors have the bias of their own

history and opinions, there is clearly history that is written primarily for political purposes. Of this type, there is the official or state-sponsored history that is most often the servant of the ruling regime. This history is what is most likely to be found in state sponsored/mandated educational programs, which is not to suggest that all state-sponsored history is necessarily of this type, but the caution flag must be raised.

There is also the writing of history that supports political positions already formed. Butterfield (1951) argues that political leaders and statesmen use "history to ratify the prejudices they already had" (p. 227). By the same token, if you look for historical examples to support your preconceived point of view, you will find them.

It is also possible to classify based on what is covered. Much of written history falls into the category of political histories (to include diplomatic histories). This type of history focuses on the milestones and the events that seemingly "changed" history. But this type of history is not sufficient if it does not examine the context and the "system of values to which it belongs" (Leff, p. 62). To the extent that political history ignores a fuller social context, it risks missing important underlying factors.

Another category of history popular in the last century is economic histories. These studies often examine development or the lack thereof, the distribution of wealth, and socio-economic conditions and strive to make generalizations based on the economic systems in place. But historians of different bents can examine much the same evidence and arrive at very different conclusions.

Finally, there is what some historians call total history -- a history that focuses not only on politics but also includes social and cultural history. Butterfield was a strong advocate of this approach. In *The Whig Interpretation of History* he argues history should be the study of more than just kings and battles where the focus is only on politics. This type of total history will probably be the most relevant for the political-military officer.

Role of myth

No philosophical discussion of history can be complete without examining the role of myth. In the words of Vaughn (1985), "myth is more powerful than truth in guiding our actions; what we believe to have happened is more important than what did happen" (p. 10). Dunning echoes this sentiment: "whatever a given age or people believe to be true, *is* true for that age and that people" (as quoted in Kent, 1969, p. 310). This is not to suggest that the political-military analyst should only study myth, but it is important to understand the role and power of myth.

III. What/how to study?

As previously mentioned, historians, like so many others, do not agree. Two observers can look at the same events and draw very different conclusions and/or lessons. It is therefore prudent to be cognizant of sources of bias and proceed with caution.

There are many sources of bias, both intentional and unintentional. Related to the

previously mentioned bias of official history, is the possibility of a difference between what actually occurred and what is recorded. As Vincent points out, there is "bias in the creation of evidence, and a bias in the survival of evidence," (p. 51) and there is also a bias in what is accessible. By any name, much of what transpires in terms of both government and non-government action is "classified." Since the evidence is imperfect, so too may be the conclusions.

Because the study of history is the study of abridged history, we must be mindful of Butterfield's (1951) admonition:

> Abridged history gives men a greater appearance of sovereignty over events than they actually possess; and it tends to magnify the controlling power of governments over the next stage in the story . . . men and nations rely on the abridged history they have learned to give them their impression of their place in the sun, their purposeful intent, and their idea of what they can do with their destiny. They acquire an academic dream-impression of what statesman can do in the world, what governments achieve, what their national mission is, and what can be brought about by sheer self-assertion and will. (p. 226)

This is not presented to minimize the role of planned efforts and campaigns; it is only meant as a caution.

In selecting materials for study, there are two basic types of sources: primary and secondary. Shafer defines primary sources as: "manuscripts, published letters and memoirs of eyewitnesses, the public documents, the newspapers, the pamphlets, the books, and the material remains of the time about which we are writing" (p. 151, 152). Secondary sources are historical manuscripts derived from primary sources or from other secondary sources (which would more properly be called tertiary).

One of the greatest challenges in studying history is in selection of materials. The limits of time will often not permit us to study and focus on primary sources, so we usually must choose from the multitude of secondary sources. The key will be to use your knowledge about the discipline of history to aid in the selection of secondary sources. Then you must read those sources with a critical eye. Because of the omnipresence of bias, you should choose multiple and varied sources. It is particularly useful to read history from both the native perspective and the western perspective and then synthesize based on those sources. In making your choices, ask for assistance from others who have studied the area. In addition, you should consult annotated bibliographies. Trevelyan (1914) sums up the importance of reading diverse points of view: "The only way in which a reader can arrive at a valuable judgment on some historical period is to read several good histories . . . written from several different points of view, and to think about them for himself" (p. 198).

In addition to selection of materials, there are several issues to be aware of when studying history. For example, how far back should one look? There is no easy answer, but generally it must pass the relevancy test. That is, what events and periods seem to have an effect on current events and the current psyche?

The role of "facts" must also be considered. While facts in and of themselves are not

very useful, knowledge of facts and their context can help us arrive at insights. Knowing dates can be enlightening but only as part of the larger picture. For example, knowing that the American Civil War started in 1861 and that the Emancipation Proclamation was not issued until 1863 can shed some light on causal arguments. In addition, for the political-military officer, the knowledge of key dates in a region *and their importance* can also increase credibility with members of host nations.

When studying history (and the present) it is important to avoid the mistake of simply looking at political structures and arriving at conclusions based on those structures. Structures do not tell us how things may actually operate. For example, the rules of the U.S. Congress, the importance of agenda setting and control, the role of lobbyists, and the cost of election campaigns, may tell us more about the operations of Congress than a superficial look at structure.

The reading of historical documents is also not sufficient. If one were to merely read the contents of the Thirteenth, Fourteenth, and Fifteenth Amendments to the U.S. Constitution, one may well conclude that U.S. citizens were at last equal under the law. But if one continued with a study of court decisions, a social history, and an examination of poll taxes and literacy tests, then one would arrive at a very different conclusion (Zinn, 1970, p. 163).

IV. Questions to consider

What are the understandings about history that are prevalent? What are seen as the key events by the people?

What roles does the study of history perform in the society? What role does history play in the socialization of the young?

What are the historical analogies used by the current regime in support of policy? How does the regime use history to legitimize the current order?

What is the prevailing story associated with the birth of the state?

What are some of the prevailing historical myths?

What are the events and milestones (collective memory) that have shaped the current psyche? What is the perception about those events? What are the purported causes of selected significant events?

What are the important historical ideals? (e.g. the Declaration of Independence has certain ideals.)

Who are the important historical/legendary figures and what are their purported attributes?

What are the threads of continuity in the state's history?

What is the history of current political and social issues?
What are the significant variations in different sources?

V. Discussion of inter-relationships with selected other pol-mil factors

Given enough time, you could look at each of the other political military factors from a historical perspective. In fact, in many cases you will do this as a matter of course. In examining a political, social, or economic issue you generally can not understand the issue without looking at its history. For example, current monetary policy in Germany is probably affected by the German historical experience with inflation in the post WW I period.

Culture and history are inextricably intertwined. Shared historical experiences are one component of cultural tradition. According to Lerner (1982), history itself is a cultural tradition: "A shared body of ideas, values and experiences, which has a coherent shape, becomes a cultural tradition" and this "symbolic universe" can unite diverse groups (p. 106). And the method by which a culture captures and depicts its history sheds light on the way the culture comes to terms with its actual history.

As a political force, history can unite and divide. A common history can help to establish tradition, bind men together, and foster a sense of belonging:

> Nations, institutions, and social groups use it to inspire loyalty to themselves and to create a sense of shared community by the telling of stories about past struggles, victories and defeats, and the sacrifices made for the benefit of posterity. Heroes are held up for emulation and villains paraded as warnings (Nevins, 1938, 236).

People can be "bound together by reverence for the tale of their past" (Nevins, p. 241) or they can be separated by a history of ethnic disputes.

As previously mentioned, history is also intertwined with political systems and leadership. History "legitimates those holding power, by rooting its source in a distant past" (Lerner, p. 106). An historical perspective can show how political leaders use ideology to mobilize, legitimize, and retain power *and* it can show how those not in power use ideals in pursuit of power. The tendency for cultures to "make legends out of its leaders is a factor of immense historical importance" (Gallie, 1978, p. 80). To understand the qualities that are revered by a culture, look at its historical leaders. But when examining a historical figure, remember to relate the personage to the context in which they operated.

VI. Summary

That there is a relation between the past and the present, is not to suggest that they are twins. History does not provide universal laws. "History does serve some useful purposes, but it is not an infallible teacher . . ." (Stephens,1974, p. 98). Historical analogies have their uses in *thinking* about the present and future, but only if we accept the limits. Butterfield's admonition can be expanded to include the entire spectrum of military operations:

> "If men are to shape their minds too rigidly by a study of the last war, they are to some degree unfitting themselves for the conduct of the next one. If a nation decides conversely that it will set out with the particular purpose of avoiding the mistakes of the last war, it is still liable to be the slave of history and to be defeated by another nation that thinks of new things. Historical study, therefore, has sometimes had a deadening effect on military strategists; and it has often been a criticism of them that they were too prone to conduct the present war on the method of the previous one, forgetting how times had changed.
>
> It seems true, however, that many of the errors which spring from a little history are often corrected as people go on to study more and more history. If a man had a knowledge of many wars and of the whole history of the art of war, studying not merely the accounts of battles and campaigns, but relating the weapons of a given period to the conditions of the time, relating policies to circumstances, so that he came to have an insight into the deep causes of things, the hidden sources of the changes that take place -- if he allowed this knowledge not to lie heavily on his mind, not to be used in a narrow and literal spirit, but to sink into the walls of his brain so that it was turned into wisdom and experience -- then such a person would be able to acquire the right feeling for the texture of events, and would undoubtedly avoid becoming the mere slave of the past. I think he would be better able to face a New World, and to meet the surprises of unpredictable change with greater flexibility. A little history may make people mentally rigid. Only if we go on learning more and more of it -- go on 'unlearning it' -- will it correct its own deficiencies gradually and help us to reach the required elasticity of mind."

While the study of the past is often a necessary condition for understanding the present, and the possibilities of the future, it is never a sufficient one (Pratt).

References

Gallie, W.B. (1978). The uses and abuses of history. In Vaughn, Stephen. (Ed.). (1985). *The vital past: Writings on the Uses of History*. (pp. 78-88). Athens, Georgia: The University of Georgia Press.

Jordan, Philip. (1960). The usefulness of useless knowledge. In Vaughn, Stephen. (Ed.). (1985). *The vital past: Writings on the Uses of History*. (pp. 45-54). Athens, Georgia: The University of Georgia Press.

Leff, Gordon. (1969). The past and the new. In Vaughn, Stephen. (Ed.). (1985). *The vital past: Writings on the Uses of History*. (pp. 58-64). Athens, Georgia: The University of Georgia Press.

Perkin, Harold. (1970) The uses of history. In Vaughn, Stephen. (Ed.). (1985). *The vital past: Writings on the Uses of History*. (pp.68-71). Athens, Georgia: The University of Georgia Press.

Stephens, Lester. (1974). Lessons, analogies, and prediction. In Vaughn, Stephen. (Ed.). (1985). *The vital past: Writings on the Uses of History*. (pp. 323- 330). Athens, Georgia: The University of Georgia Press.

Vaughn, Stephen. (Ed.). (1985). *The vital past: Writings on the Uses of History*. Athens, Georgia: The University of Georgia Press.

Vincent, John. (1996). *An intelligent person's guide to history*. London: Duckworth.

Zinn, Howard. (1970) What is radical history? In Vaughn, Stephen. (Ed.). (1985). *The vital past: Writings on the Uses of History*. (pp. 158-169). Athens, Georgia: The University of Georgia Press.

Chapter 3

The Natural Environment

I. Introduction and definitions

The economic, political, social, cultural, and even military behavior and development of any society are influenced by that society's natural environment. The effects of the environment can be discerned--sometimes distinctly, sometimes subtly--in almost every aspect of a society, including the way it is organized and ruled; its trade patterns; its population growth, distribution, and migration; its eating habits and style of clothing; and its military formations. If a political-military analyst wants to do sound political-military analysis, his first step is to understand the environment of the region in which he is operating. Just as no one would attempt to launch an attack without first studying maps of the battle area--preferably with a good leader's reconnaissance on the ground as well--neither can they hope to analyze a country or culture without first knowing the environment in which it exists.

Natural Environment Defined

When discussing the natural environment, be concerned with the three-dimensional terrestrial space centered on the earth's surface within which all material things are contained.

When analyzing the natural environment, divide it into four spheres.

Atmosphere: The layer of gas around the earth. The condition of the atmosphere at any given time we call weather. The condition of the atmosphere over time we call climate. Climate, more than anything else in the environment, sets limits to what man can physically and economically do. For example, the debilitating heat and humidity of the tropics and the bitter cold of Siberia and northern Canada have hindered development in these regions. The cultural habits of many societies are linked directly to climate conditions. For example, the midday siesta-which is by no means limited to Central America--is a result of people's understandable desire to avoid work in the hottest part of the day. Other aspects of the atmosphere are of interest to us as well. For example, the thin air in the high altitudes of the Andes or Himalayas limits the amount of physical exertion that can be done in these regions. The quality of the atmosphere has also become an important concern lately as noted from issues arising from air pollution or depletion of the ozone layer by chlorofluorocarbons.

Lithosphere: The soil and rock crust of the earth and all that is beneath it. Landforms may facilitate or inhibit transportation and interaction among societies. The fertility of the soil or its ability to retain moisture can have a significant influence on societal development. Transplanted soils, such as the alluvium of the Nile River in Egypt or the loss of the Yellow River valley in North China, can be critical to the support of civilizations. Minerals, gems, oil, and liquefied natural gas have at one time or another had a great influence on societies around the world.

Hydrosphere: Water in liquid form, including rain. Water is key to human civilization and to plant and animal life. If water is scarce, people may have to move around to find it, leading to a nomadic lifestyle. If it is plentiful, a more sedentary lifestyle may be possible. Water can provide a means of irrigation, a source of power, or routes of transportation. For example, fully 70 percent of the land under cultivation in Pakistan is irrigated; much of the electricity in the United States is provided by hydroelectric plants; the extensive interdigitation of water with the land in the United States and Europe facilitated contact among societies, while the lack of extensive interdigitation in Africa has hindered interaction and exploration there. Average rainfall can be a significant influence as can the time of rainfall or even the quality of the rain. Finally, even if water is plentiful and the rain clean, water must be safe to drink. As with the atmosphere, pollution in the hydrosphere is a serious issue. There is an on-going debate in certain parts of the world today over who owns the rain and who is responsible if the rain is contaminated.

Biosphere: Living things on the earth. This includes everything from seaweed to sunflowers to sequoias and from microbes to muskrats to men. Three important aspects of the biosphere are human population, food, and disease. They are, of course, interrelated.

For people to exist, there must at least be a subsistence level of food and water. As with the hydrosphere, if food is scarce, a society may have to search for it and so become nomadic. If food is plentiful, societies may be sedentary, which may in turn allow for greater specialization and development within the society, since fewer people have to be involved in the quest for food. But, food must not only be plentiful, the diet it provides must also be balanced. There are several examples of people having plenty to eat who still suffer from malnutrition, such as the 19th century Irish whose diet consisted largely of potatoes. Finally, what is considered food in some societies may not be acceptable in others.

Disease may override all other factors in the biosphere. It can be transmitted by microbes, insects, animals, or men. It can inhibit development or even deplete a population. Many diseases are not killers, but can incapacitate or cripple their victims. Some diseases may not infect humans, but can decimate animals or plants, depleting the food supply. Finally, curing a disease or developing an immunity to it may increase the population beyond the capacity of the environment to adequately support it.

When disease is prevalent but localized to one segment of a population or one area, it is called epidemic. When it is spread over a large area throughout a population, it is called pandemic. When a disease is always present and has established an equilibrium among a population, it is called endemic.

Naturally, these four spheres do not exert influence independently. (In fact, they do not exert influence at all--environmental influence is passive.) Mountain ranges, deserts, grasslands, or waterways may facilitate or impede migration of species. Weather patterns are affected by bodies of water or landforms. The effects of rain can be beneficial or disastrous, depending on the location of rivers, wadis, valleys, and the type of soil on which the rain falls. To understand

a region's natural environment, don't look at just one sphere or one factor within a sphere (e.g., climate or resource distribution), look at it in total.

Geography Defined

It should be clear by now that political-military analysts study the natural environment to discern its interrelationship with human beings. Geologists, hydrologists, biologists, zoologists, meteorologists, and the like, study the environment as an end in itself. Political-military analysts, on the other hand, are interested in the field of study known as geography, which is the study of the relationships of various human phenomena and terrestrial space. (There is also a field known as physical geography that deals with non-human phenomena, but we have already discussed aspects of this when talking about the four environmental spheres.) Geography deals with the pattern of man's distribution over and his use of the earth, why he uses it differently in different places and times, and how this is related to man's economies, culture, political systems, etc. Geography is concerned whenever the concept of place or the question of where is involved.

When studying geography, the first thing to do is to distinguish between the concept of site or location and situation. Site/location is the actual ground on which a geographic phenomenon rests. This is important only insofar as it helps us understand the relationship between one area and the rest of the world and the effect of those relations, that is, that phenomenon's situation. It is not only important to know where things are, but also to know why they are there and how their location allows them to influence or be influenced by things elsewhere. This should not be difficult to understand. If the mission is to "take that hill," it is not because that hill is valuable in and of itself, but because controlling it is an advantage over the enemy. On a larger scale, knowing the number of miles of navigable waterways in a particular region *is less* important than knowing the patterns of distribution and interaction those waterways support. Situation, then, is relative. It is also changeable.

The growing concern among many nations over ownership of continental shelves is one example of how a geographical situation can change. Ordinarily, under international law, a continental shelf is considered to be the territory of the country from which it extends. The shelf normally does not extend for more than a few miles, but in some places it goes out considerably farther. Until relatively recently, even these longer extensions did not cause much trouble among countries. Now since technology has improved enough to allow the exploitation of the resources in the shelf, especially oil, countries are beginning to lay claim to territory they previously ignored. A similar occurrence is taking place with regard to small, often deserted atolls, such as the Spratley Islands in the South China Sea, which are claimed by no less than seven countries--all of whom hope to extract the oil believed to be in the vicinity.

II. Discussion of inter-relationships with selected other pol-mil factors

Six basic principles underlie the connection between human society and the environment.

Principle 1: Humans must form a workable connection with the environment. It does not have to be the optimal relationship, but it must at least allow the society to survive.

Principle 2: A human society and its environment form a system of interrelated elements, and change in one aspect can have significant ramifications throughout the system. Environmental change can occur two ways. First, **change may occur naturally** through such events as volcanic eruptions, floods, winds, or species proliferating or dying out without man's help. Second, change may be man induced. **People** have fundamentally remade the landscape in every area of the world that he has occupied in great numbers. He has dug canals, changed the course of rivers, built harbors, tunneled through mountains, cut down forests, planted new ones, depleted the soil or made it fertile, made deserts bloom, and turned verdant lands into deserts. The changes man creates in his environment react in turn on man and influence his settlement and activities. Man-induced change is not usually as sudden as natural change, but it is no less dramatic--or in some cases, no less catastrophic--for that.

Principle 3: A given environment can support several different types of societies.

Environmental conditions may provide opportunities and possibilities, but only human activity can make them reality.

The environment influences society, but does not determine it. Different people look for different things in similar environments and produce different results. Of the many things that are possible or which environmental conditions will allow, men will choose to do certain things because of a variety of factors that help shape their civilization, such as **political pressure**, **tradition, or cultural values**. Environmental conditions may tend to make one or a few choices more attractive or more successful than others, but choices may differ widely among different societies and at different times. This, of course, does not mean that the environment can be ignored in analysis, but that it should not be the only influential factor.

Principle 4: No environment is either favorable or unfavorable to all types of societies. A change in any element of **culture** may alter the significance of the natural surroundings. This is particularly true with regard to the impact of technology. Consider how the advent of air conditioning has influenced population distribution in places as disparate as Houston and Hong Kong. Even natural resources are resources only if we know how to use them for our purposes. The influence of the environment may become less important as technology increases, or things once taken for granted may become clear (e.g., clean air and water).

Principle 5: Just because a society is blessed with a rich environment does not mean that the society will prosper. **History** abounds with examples of societies that languished in the midst of plenty because of cultural constraints, inability to use the wealth at hand, or incompetent leadership. Similarly, a society in an austere environment short of resources may still be prosperous, such as Japan or the Asian newly industrialized countries.

Principle 6: The environment can affect human affairs in two ways: how man sees the environment and how it actually is. The first is actual or operational influence. Mountains and rivers may be impassable, soil sterile, or water scarce. The second way is perceived influence. Men may simply believe that they cannot cross mountains, grow crops, or find ample water. These beliefs will cause them to act in certain ways, whether the beliefs are true or not. **Military**

history alone is rife with examples of armies defeated by enemies who attacked over routes believed to be impassable.

The Concept of "Region"

One of the concepts used for analysis in geography is that of the "region." An area may be distinctive as a region because it coincides with the distribution of a particular type of climate, landform, or soil, or because it is characterized by a particular type of economic activity, land use, political system, culture, religion, etc. The first problem in regional analysis is to determine what gives the region its essential distinctive quality. Only then can we draw satisfactory regional lines.

The concept of "region" is a useful intellectual device for analysis, but we must remember that regional distinctions are products of our own minds, not complete descriptions of reality. In this sense, there are no "natural regions," only man-made or man-perceived classifications of regional differences. As such, regions can be single factor or multifactor. Regional differences are usually related in part to differences in the physical environment, but only in part. Differences are due as much to human society as to the physical environment.

Regions usually spread from a "regional core," also known as a "culture hearth." This is the hub or axis where our distinctive regional feature is most prominent. It may be a physical feature (e.g., a fertile plain, river, valley, or seacoast) or a cultural feature (e.g., center of political or military control, dominant trading center). Usually, this core is the first area to develop the dominant regional characteristic, which then spreads over the surrounding area as far as physical or cultural conditions will allow. The impact of a cultural characteristic may extend well beyond areas to which it is suited.

On the periphery of a region is the "transition zone" where the qualities that delineate one region significantly diminish and are replaced by another set of qualities belonging to another region.

Mental Maps

When an analyst looks at the world and studies his region, he has to be conscious of the tendency to see the world through his own "mental map." This mental map is the way he perceives the world and will rarely accurately reflect the world as it is. Part of this is due to his culture and to the use of ethnocentric maps in the education system. There are numerous examples of this type of distortion, such as placing the United States (or any other country) in the middle of a map, splitting Russia in half, or placing Alaska and Hawaii in the corner of a map off the coast of California, which belies the distances involved.

Another source of distortion in an analyst's mental map comes from his use of classifications as analytical tools. For example, the Philippines and India are both considered part of the "region" of Asia when in actuality, they have very little in common. Similarly, he tends to think of the Muslim world as being in the Middle East (another distortion of his mental map); when in reality, the most populous Muslim country is in Asia.

A third distortion may come from limited time on the ground in the region. This can be a case of a little knowledge being more dangerous than none at all. For example, a foreign traveler in China is generally limited to going from one city to another and may well come away with an impression of China as an urbanized country, although 80 percent of the population lives in the countryside. By the same token, an American soldier along the DMZ with the 2d Infantry Division in the Republic of Korea (ROK) will likely believe that the ROK is an underdeveloped country, unless he takes the time to visit Seoul and other parts of the country. Lastly, the longer people are away from a country, the less likely they are to see it accurately, both because their memories will begin to fade and because the country will have changed since they left.

Another way an analyst's mental map is formed depends on the areas and problems he is studying. It is natural for him to think that the area on which he is concentrating is the most important in the world and that the decision-makers are not paying near enough attention to it. Additionally, as he deals with situations and crises, certain countries assume greater importance in his perception of the world. Some distortion is natural and unavoidable, but be cognizant of their existence.

III. Some Analytical Questions to Consider

What are the consequences of economic development on the natural environment?

What effects has the natural environment had on the history of the country?

What effects has the natural environment had on culture?

What effects has the natural environment had on the country's economy?

What advantages and disadvantages stem from factors relating to the natural environment?

What effects has the natural environment had on foreign influence?

How has the effect of the natural environment changed over time?

How has the natural environment affected the country's military?

Can technology, science, and industry surmount all future natural resource problems?

IV. Conclusion

The political-military factor of natural environment interacts with several other factors. The natural environment may or may not be a limiting factor depending on its interplay with the other factors. A favorable natural environment may contribute to country's development, but it is not a sufficient condition.

V. Suggested reading

World Resources Institute. World Resources 1997-98. New York: Oxford University Press, 1998.

Gore, Al. Earth in the Balance: Ecology and the Human Spirit. Boston: Houghton Mifflin, 1992.

Young, Oran R., ed. Global Governance: Drawing Insights from the Environmental Experience. Cambridge, Mass.: MIT Press, 1997.

Struhsaker, Thomas R. Ecology of the African Rain Forest: Logging in Kibale and the Conflict Between Conservation and Exploitation. Gainesville: University Press of Florida, 1997

Jepma, C.J. Tropical Deforestation: A Socio-Economic Approach. London: Earthscan, 1995.

Relevant sites on the World Wide Web

1. http://www.ran.org/ran
2. http://www.wwf.org/action/lite/frame_climate.htm
3. http://ioc.unesco.org/iyo/
4. http://www.earthtimes.org/
5. http://www.worldwatch.org/

Chapter 4

Regional Perspectives

"A day will come when all nations on our continent will form a European brotherhood… A day will come when we shall see…the United States of America and the United States of Europe, face to face, reaching out for each other across the seas." -- Victor Hugo (1848)

I. Introduction

Regional perspectives are an important factor with which the political-military analyst must deal. Regional perspectives color the manner in which events are perceived, leading to reactions that may be quite unanticipated. The analyst must be able to identify and understand the general regional perspectives on a broad range of issues to judge their effect on future actions within the region. This is no simple task because of the complexity involved. International relations are not dyadic; every event affects secondary and tertiary actors through their individual perspectives and regional orientations. Explaining and predicting these effects is the job of the analyst.

Regional Perspectives and Where They Come From

Regional actors form their perspectives based on their perceptions of individual and collective interests on specific issues. These may be developed over a wide range of topics such as ideology, economic policy and developmental planning, military strategy, alliance relations, East-West and North-South conflicts, terrorism, and nuclear proliferation. Factors such as threat assessments, individual and collective capabilities, relative regional economic position, cultural traditions, religious orientation, political philosophy, and historical experience contribute to the forming of regional perspectives.

A region's perspective can often be determined by what its leaders say, what the states do, and by formation of organizations that reflect regional elements of unity. For example, the formation of the European Union, the Arab League, the Association of Southeast Asian Nations, the Organization of African Unity, and the Organization of American States were each motivated by a particular regional perception of threat (economic, political, or security). Each organization seeks to capitalize on a particular characteristic that can lead to greater regional or collective power and prestige through unity.

The Gulf Cooperation Council: An Example of Regional Perspective

The six Arabian Peninsula states (Kuwait, Saudi Arabia, Qatar, Bahrain, the United Arab Emirates, and Oman) of the Gulf Cooperation Council (GCC) share many things in common including geography, religion, monarchical political systems, oil interests, and security concerns. However, traditional rivalries among the states has prevented them from uniting for their common good, even though as individual actors they lack the power for credible deterrence. Iraqi threats on Kuwait in the late 1970's

and the fear of Iran's ultimate goals in the Persian Gulf fostered cooperation between these Persian Gulf states. In 1981, eight months after the Iran-Iraq war had begun, these states joined together in a union for partial economic and cultural integration. That union had evolved into one which now includes elementary joint defense agreements and closer coordination on foreign affairs. Through collective action, their coincident individual interests are stronger and continue to gain greater international importance. Through joint economic policies, they have reduced competitive and redundant development planning. Integrated defense planning has maximized the individual strengths of each member, producing a more credible deterrent to external aggression. The 1990 Iraqi invasion of Kuwait gave a significant boost to concrete measures in developing a credible deterrent.

Determining Regional Perspectives: Tools and Methods

How can the analyst determine what regional perspectives are? At the individual state level, trends in foreign policy, economic relations and policy positions consistently pursued by political, military and business leaders provide the basic answers. More answers can be deduced by charting actions and responses of regional actors following a crisis event. At the regional level, one source to examine is the agreements that establish regional organizations. These often contain specific statements, arrived at by group consensus, which outline those perspectives.

Of primary concern in determining regional perspectives is the regional assessment of a wide variety of threats. The United States viewed the former Soviet Union as the principal threat to American interests abroad. The USSR was considered the only nation that could credibly challenge the territorial integrity and survival of the United States. Additionally, it could challenge any of America's allies.

Most challenges to the United States were viewed as coming from issues related to the East-West conflict. For this reason, the United States shouldered the burden of maintaining a global perspective in foreign relations. Today, as the sole remaining "superpower" that far-reaching perspective has taken on new meaning yet to be defined.

Regional actors rarely enjoy such responsibility, perceiving a variety of more proximate threats to their survival ranging from internal instability to regional radicals and historical conflicts that constantly threaten to flare up and expand. For regional actors, these types of challenges appear to have a greater likelihood of causing change in the near term (1 to 2 years) or mid-term (3 to 7 years) than the broader external challenges. For obvious reasons, regional actors focus on these more immediate threats. This often leads to a virtual lack of concern for externally generated pressures.

The Conflict Between Global and Regional Perspectives

While the United States is concerned with regional issues as they relate to a global picture, regional actors do not often link regional and global events--their perspective is more limited. The result is often a misunderstanding, stemming from different

perspectives, over both the importance of events and responses that are appropriate to achieve desired results.

Often, even the desired results are different. For example, the United States had previously identified the Soviet Union as the major source of instability in the Persian Gulf, which threatened Western access to oil. To counter this threat, a decidedly military strategy was adopted.

Ideally, the stationing of American troops in the area would seemingly serve to protect US interests. From a regional perspective, however, the major causes of instability are Islamic fundamentalism, Iraqi ambitions, and the nonresolution of the Palestinian problem--all of which threaten the political stability of established regimes.

The strategy to resolve these sources of conflict is diplomacy. Stationing of American troops directly in the Persian Gulf may not achieve the expected results; in fact, it would possibly only exacerbate the problem by providing an additional focus for the opposition in its attempt to undermine existing rulers. Conflicting perspectives such as these make unified actions between the Persian Gulf States and the United States difficult, requiring the utmost in diplomacy with a nearby but "over-the-horizon" military presence.

II. Some Questions to Consider

What regional organizations does the host country belong to?

What regional treaties/compacts exist?

Are there obvious foreign policy trends?

What are the nation's responses to crises?

III. Summation

Regional perspectives focus on those issues that more immediately threaten local security and stability. The analyst must understand the roots of those perspectives, the depth of commitment to each issue both regionally and by the individual actors, and the areas of agreement and disagreement with the global perspectives of the United States. Such an understanding can serve as a basis for explaining regional behavior and predicting probable responses to a variety of possible actions.

REFERENCES

Magstadt, Thomas M. *Nations and Governments: Comparative Politics in Regional Perspective*. New York. Saint Martin's Press. 1998.

Chapter 5

Foreign Influence

"It can be harmful to come, without thought, under the sway of utterly new and strange doctrines."
-- Confucius (450 BC)

I. Introduction

History is riddled with examples of countries being influenced by forces that emanate from beyond their borders. These forces can shape culture, affect policy, change economies, threaten national security, or even topple governments. Recognizing and understanding the role foreign influence plays in the political-military environment of a country will assist the analyst in accurately assessing the overall situation of a country and making predictions about its future actions.

Foreign influence can be either direct or indirect. Direct influences are actions perpetrated by a foreign government or actor with the express purpose of influencing policy or actions of a specific state. Military actions or economic sanctions directed toward a country are examples of direct foreign influence. Direct foreign influences do not necessarily have to be government to government. Organizations such as the International Monetary Fund can also exert pressure on a country to effect change. Churches and religious leaders, such as the Pope or the late Ayatollah Khomeini, have also been known to target specific countries in an attempt to effect change.

Factors of foreign influence not under the direction of a specific outside agency can also affect the actions of the host country. These indirect foreign influences can come from a variety of sources. The adaptations a political system must make in response to these influences are not the goal of a specific agency but more a by-product of the change. Immigration that results in demographic change, expatriate foreign remittance to relatives, competition on international markets, technological advances, students educated in other countries and religious fundamentalism are a few examples of indirect influences that could affect a country and may or may not result in changes to that system.

There are numerous elements that may either encourage or discourage foreign influence in any given country, and it is beyond the scope of this short introduction to address them all. Therefore, four main elements will be identified in this chapter: geography, economics, cultural/ethnic factors, and history. The elements as they pertain to analysis within a particular country are covered elsewhere within political-military analysis. However, when discussing foreign influence, or the susceptibility of a nation to foreign influence these factors take on a slightly different light. Categorization of these elements is not of the greatest concern, but the identification of their presence and their possible impact upon a country is important.

Geography

Geography, both in terms of terrain features and actual location, does much to inhibit or encourage foreign influence. Obviously, a country with clearly defined borders that inhibit

transportation and communications will be less susceptible to foreign influence. The isolation of the Japanese islands, caused in great part by rough seas and difficult coastlines, made it for the most part immune from Chinese conquest despite its relative proximity to China. Compare this to Korea or northern Vietnam where the boundaries were not well defined and where Chinese influence played a major role in the development of their cultures. In Europe, the case of Poland and its open frontiers, is perhaps best known.

However, advances in communications and transportation have overcome many of the natural obstacles that for centuries protected and isolated countries. In the 19th century, technology enabled Admiral Perry to use his black ships to open the doors of Japan to the world after 200 years of self-imposed isolation. Or consider the more recent example of the Hunza region in northern Pakistan. For centuries Hunza has been a remote area isolated by distance and difficult terrain not just from neighboring countries but also from the central government. Recent advances in communications and transportation have made Hunza more accessible from the north, and thus more susceptible to Chinese influence. However, the distance between Hunza and Islamabad continues to isolate it from the rest of Pakistan. Features that at one time protected Hunza now aid the growing Chinese influence in the area.

Although terrain features of a country, such as rivers, mountains, or coastlines may make it more or less susceptible to foreign influence, the actual location of a country can do the same thing. For example, the Chinese see Korea as "lips to teeth," protecting the approaches to several major coastal cities; the Japanese have seen it as a "dagger" pointed to the heart of Japan; while to the United States, South Korea was not only a "bastion of freedom" facing the Communist threat, but was also the only US military foothold on the continent of Asia. .

However, a note of caution is necessary; location is not necessarily decisive. The analyst must consider how human will and technological advances can impact on elements of power. Returning to the Korean example, despite what has already been said about the peninsula, North Korea has forced a path of self-reliance with little influence from the former USSR, PRC, or any other outside force. Poland is another example of a country with an independent attitude, regardless of its geography. Located on the central European plain, with no easily defined geophysical borders, it has for centuries been an historical battleground between the Slavs and the Teutons. In spite of frequent incursions, the Poles have developed a determination to resist.

Economic Influence

The second element of foreign influence, economics, can, like geography, manifest itself in many ways. So long as countries are economically dependent or interdependent on others, influence will exist. There is no doubt that during the heyday of colonialism the influence of the European powers was felt heavily throughout the world. Economics was one of the driving forces behind the mercantilist expansion of the Western nations over the world. Economic activity took place at the direction and benefit of the colonial powers. The colonial relationship has left many economic legacies that exist to this day in terms of trading partners, items of trade, and economic institutions, as well as type and degree of development, legal and governmental systems, and elites.

Colonialism aside, the element of economics is a major consideration when determining the presence and extent of foreign influence. Countries that are economically dependent upon outside

sources of supply for critical items may let the source of supply influence their foreign policy. For example, Japan's heavy dependence on Middle East oil has caused Japan to refrain from taking a hard-line stand against Libya in response to terrorist activities.

Countries that depend on exports can be influenced by the policies of the countries they export to. The United States, for instance, uses the threat of increased protectionism toward foreign imports to pressure countries such as Japan, Korea, and Taiwan to drop trade barriers against US products. Also, countries with limited resources and whose economies are tied to the export of a single commodity may become dependent upon their export markets and leave themselves vulnerable for unbridled influence by foreign governments or multinational corporations. Other considerations include the existence of sanctions or trade embargoes.

It is also necessary to consider the regional organizations which may influence a country's economy. Being on the inside or the outside of organizations such as the North American Free Trade Agreement (NAFTA), the European Union (EU), Organization of Petroleum Exporting Countries (OPEC) or Asia-Pacific Economic Cooperation (APEC) can and does influence policy.

However, economic dependency on other countries doesn't always mean total subordination. Countries need not be subservient to suppliers or markets. Japan, Taiwan, and Singapore are examples of countries that were at one point totally dependent upon another country; all now more than hold their own on the international scene and, for the most part, chart their own destinies.

Cultural/Ethnic Influence

The third element, cultural and ethnic influence from foreign sources, is obvious in many regions around the world. Countries with large expatriate populations may be susceptible to formation of a "fifth column," directed and controlled by an outside source. Communist insurgencies in Malaysia, Indonesia, and Thailand were linked to the Chinese minorities living in those countries.

Where ethnic identities cross national boundaries, the ability of one country to influence another is also increased. Consider the case of Pakistan. Resurgent Islamic fundamentalism originating in Iran has found its way into Pakistan in part through the Baluchi ethnic minority, which occupies both sides of the border between Iran and Pakistan. In addition, on Pakistan's border with Afghanistan, ethnic Pathans, whose tribal lands cross the border, were used as a conduit for influence by the Soviets occupying Afghanistan. Soviet goods, money, and propaganda were used to alienate the Pathans from the Islamabad government, thereby loosening the Pakistani control of the tribal areas near the border.

Religion has the ability to be a conduit for foreign influence both through the adaptation made in a society to accommodate the religion over time and, therefore, direct influence of individual religious leaders, or through the evolution of religious movements seeking change. Traditions and doctrines of the Roman Catholic Church have influenced the Philippines in deep and lasting ways, making it unique in Southeast Asia and tying the Philippines to the West in a way different from other Asian nations.

Consider the influence of Islam in Southeast Asia. Although located thousands of miles from the Middle East, Malaysia and Indonesia have been affected by resurgent Islamic fundamentalism from the Middle East and have had to adapt to accommodate its influence.

History

The fourth and final element of foreign influence to be discussed is that of history. Countries with a history of relations with another country tend to continue to be influenced by that country. The historical animosities between China and Vietnam continue to influence the current situation in Indochina. The relationship between the United States and the Philippines, built upon since the turn of the century when the Philippines were a US possession, plays a considerable role in influencing both US and Philippine policies toward each other.

Knowing the elements of foreign influence will help the analyst understand the ways in which one country can be influenced by an outside force, but determining the nature and extent to which it affects a country is most important. Some additional indicators an analyst might examine are the types and numbers of treaty and alliance relationships a country has and the international organizations to which it belongs. The study should also include an examination of the nature and diversity of countries' interactions with the outside world. Some specific items to consider are joint military planning or joint training exercises, UN voting records, patterns of trade, foreign investment, aid relationships, technology sources, and overseas education. Consider also the influences of non-governmental organizations (NGOs) and private volunteer organizations (PVOs). These organizations involved in routine work or in disaster relief/humanitarian operations, can have far-reaching influences. Likewise, the blinding advances in Internet access and satellite technology can influence the way people eat, dress and how they view the rest of the world. The analyst should also consider the less obvious indicators such as tourism or cultural exchanges.

II. Some Questions To Consider

What are the direct and indirect influences?

Does geography affect foreign influence?

What economic influences are there?

Are there cultural or ethnic influences?

Do historical influences exist?

Are there NGOs and/or PVOs present?

What is the effect of technology (i.e. Internet, satellite media, cell communications)?

III. Summation:

As a factor of political-military analysis, foreign influence is directly related to several other factors. In actuality, it cannot be separated from factors such as history, religion, culture, geography, and economics, which serve as conduits for influence. Recognizing the susceptibility of a country to foreign influence and determining the type and degree of that influence within a specific country, allows a more accurate analysis to be formed.

REFERENCES

Crocker, Chester A. et al, *Herding Cats: Multiparty Mediation in a Complex World*. Washington, DC. United States Institute of Peace. 1999.

Risse-Kappen, Thomas. *Cooperation Among Democracies: The European Influence on US Foreign Policy*. Princeton, NJ Princeton University Press. 1995.

Strobel, Warren P. *Late-Breaking Foreign Policy: The News Media's Influence on Peace Operations*. Washington, DC. United States Institute of Peace. 1997.

Chapter 6

National Interests

"We have no eternal allies and we have no perpetual enemies. Our interests are eternal and perpetual, and those interests it is our duty to follow." -- Lord Palmerston (1848)

I. Introduction and definitions

The world has changed a great deal since Lord Palmerston made the above statement while serving as Great Britain's Prime Minister. What has not changed is the idea that nations will always attempt to conduct their foreign policy in a manner that best serves their own interests. This should be no surprise. While we may shake our heads and ask ourselves why France takes a particular stand on an issue or why the Palestinians make a controversial statement, once we look at the issues from *their* point of view, the actions may appear more reasonable.

The fact that actors--be they individuals, sub-state organizations, nations, or multinational corporations--seek to pursue their best interests is not in and of itself interesting or useful. In the international arena, self-interested behavior is the principal assumption upon which the policies of involved actors are based. Each actor will choose and pursue policies based on *their own* calculations of the national interests. It is critical then, to see another actor's national interests through that actors "eyes." To fail in this can lead to gross miscalculation of that actor's policies, actions and reactions.

The concept of national interest is overshadowed in its importance only by its difficulty of definition. Nearly as many different definitions exists as there are theorists who attempt to grapple with the subject. In fact, the difficulty is so great that many academics have rejected the concept completely rather than sink in the potential morass of differing ideas. Still others prefer to use the term "foreign policy objectives" in order to reflect the fluid nature of a nation's changing interests (Holsti p. 124).

Also, the use of any of these concepts *can be* dangerous. This danger stems primarily from the potential for the usurpation of national interests by a narrow constituency or the distortion of the selection process by the same (i.e. interest groups, mass media). If this occurs, the concept can be used to drive the governing powers to actions or policies that are not truly in the national interests, while nonetheless giving those interests as a justification for the policies.

Generally, "interests" or "objectives" are defined in the broadest of terms. This allows policy decisions to enjoy the widest appeal. It becomes much easier for policy makers to "wrap up their advocacy with the suggestion that their particular preferences are in the nation's best interests" (Spainer p.359). Wyllie offers a succinct definition: "…national interest is the basic term deployed by foreign policy-makers to describe the long term, core, collective objectives of the state…. In descending order of priority, the collective objectives are deemed to comprise the

security and survival of the state, economic prosperity, and the sustenance of the social and political values of the society of the state." (Wyllie p.3)

II. Review of the literature

Some look to the writing of Italian statesman Niccolo Machiavelli (1469-1527) for the beginnings of the concept of national interest. In his efforts to promote Italian unity, Machiavelli believed that while a state may have the loftiest of goals, unless that state, has the power to back those goals they are worthless. Many have attributed to Machiavelli the viewpoint: The end justifies the means – as long as the end is *moral* (Roskin p.5).

In his book, On War, Carl Von Clausewitz (1780-1831) writes of the notion that "all state behavior is motivated by its need to survive and prosper." Safeguarding its interests is the only reason a state should go to war. "Unlimited war, however, is foolish, for it serves no national interest" (Roskin p.5).

Roskin refers to the realism of our Founding Fathers as they administered and subsequently expanded the thirteen original states. He points to Washington's farewell address as an example of "shrewd appreciation of national interest: Europe has a set of primary interests which to us have no or a very remote relation. Hence she must be engaged in frequent controversies, the causes of which are essentially foreign to our concerns" (Roskin p.5).

German *émigré* and noted realist Hans Morgenthau (1904-1980) is frequently credited with bringing the concept of national interest into mainstream American thought. He defined interests in terms of power. His test was simple: "was the statesman acting to preserve and improve the state's power?" (Roskin p.7) He rallied support to oppose the Axis powers and later the Soviet Union not necessarily out of moral conviction but because he believed, " International politics, like all politics is a struggle for power" (Roskin p.6).

Political scientist Martha Finnemore, at George Washington University, asserts that most of what happens in the international relations arena today is not about states defending their national interests but about defining them (Finnemore p.ix). As states attempt to determine their place in the "new world order," it becomes apparent just how difficult it can be to pinpoint what their national interests are. The Cold War's East versus West bipolar world has given way to a multipolar world with redefined (often undefined), competing, changing interests.

A state's interests, after all, are what that state says they are today. Indeed, an excellent source to identify the interests of a nation is its local representative i.e. embassy, world headquarters, etc. Generally, the larger the state the more diverse its interests and the more opportunity there is to become involved in conflict. Smaller states with limited resources are less likely to have far-reaching goals. The formulation of specific interests is often influenced by domestic politics, perceptions, values, culture, and ideologies.

The National Interests of the United States - An Example

The DOD Reorganization Act of 1986 (the Goldwater-Nichols Act) requires the President to submit an annual national security strategy to Congress. The 1998 report, *A National Security Strategy for a New Century*, places US national interests into three categories:

> 1. ***vital interests*** – those of broad, overriding importance to the survival, safety and vitality of our nation. Among these are the physical security of our territory and that of our allies, the safety of our citizens, our economic well-being and the protection of our critical infrastructures. We will do what we must to defend these interests, including – when necessary – using our military might unilaterally and decisively.
>
> 2. ***important national interests*** – These interests do not affect our national survival, but they do affect our national well-being and the character of the world in which we live. In such cases, we will use our resources to advance these interests insofar as the costs and risks are commensurate with the interests at stake. Our efforts to halt the flow of refugees from Haiti and restore democracy in that state, our participation in NATO operations in Bosnia and our efforts to protect the global environment are relevant examples.
>
> 3. ***humanitarian and other interests*** – In some circumstances our nation may act because our values demand it. Examples include responding to natural and manmade disasters or violations of human rights, supporting democratization and civil control of the military, assisting humanitarian demining and promoting sustainable development. (pp.5,6)

Considering these broad categories, it is difficult to think of any undertaking that couldn't be "sold" as supporting our national interests. In the case of the United States then, factors such as domestic politics, political will, lobby efforts, military commitments, our value system and many others coalesce into a national policy at any given time.

III. Some Questions to consider

Where are the national interests articulated?

What are the state's professed national interests?

How does that state prioritize its interests?

How are the interests pursued? (militarily, economically, politically)

Who threatens these interests?

Can previous threats to national interests be identified; what was the response to the threat?

What role does regime preservation play in the articulation of national interests?

IV. Discussion of inter-relationships with selected other pol-mil factors

Just as with the other political-military factors outlined in this handbook, wherever appropriate, national interests must be also be analyzed as those interests relate to the other factors. The geography of a given *natural environment* can help determine interests; many claim that future wars in the Middle East will be over water, not oil. What effects do the devastation of the rainforests or over-fishing by huge factory ships have on American national interests? Should the continuing nightmare at Chernobyl concern us?

Political systems and economy are key factors to examine when determining how a state's interests are formulated. Domestic politics and the role of the *media* are components of this analysis. *Leadership, ideology and role of the military* are also important to the analysis of national interests. In the case of Turkey, for example, the secular legacy left by Kemal Ataturk is expected of that country's leaders today and is rigidly enforced by its military.

Your analysis of each factor and its relationship to the others is limited only by the time available. A complete analysis of national interests will include a look at how those interests relate to each of the political-military factors.

V. Summary

National interests can have an impact on the nation in question directly and indirectly. Hypothetically, if Western Europe is a vital interest of the United States, then the Persian Gulf oil fields and sea lines of communications between the Persian Gulf and Western Europe, which the Europeans consider vital to their interests, would also be a vital interest of the United States, albeit indirectly.

Understanding national interests is only the beginning in analyzing why a state acts the way it does. Examining who threatens those interests, and how, is also important. Knowing what a state's interests are can help put into context how that state views itself in the international arena (its worldview) and thus help predict how that state may respond in crises and non-crises.

References

A National Security Strategy for a New Century. Washngton, DC. The White House. 1998.

Finnemore, Martha. *National Interests in International Society*. New York. Cornell University Press. 1996.

Holsti, K. J. *International Politics A Framework for Analysis*. 4th ed. Englewood Cliffs, NJ. Prentice-Hall 1983.

Roskin, Michael G. "National Interest: From Abstraction to Strategy" in *Parameters*, Carlilse, PA. US Army War College. Winter 1994-95, Vol. 24, No. 4, pp.4-18.

Spainer, John. *Games Nations Play*. 8th ed. Washington, DC. Congressional Quarterly Press. 1993

Wyllie, James H. *European Security in the New Political Environment*. London. Addison-Wesley Longman. 1997.

Chapter 7

Ideology

I. Introduction and Definitions

How nations, societies, and peoples interact with one another is strongly influenced by the values they hold dear. These values provide a sense of right and wrong that contributes to the development of commonly accepted goals and interests. An essential element in any societal value system is its ideology. An ideology can serve to integrate communities, to advance the position of a particular group, and to strengthen the resolve of the people to act to change social, economic, and political systems.

> People with the same ideas about the world, our society, and its values band together. We are attracted by those with similar values and ideas, who like the same things we do, who have prejudices similar to ours, and who, in general, view the world in the same way we do. We talk of "like-minded" people, individuals who share certain beliefs and tend to congregate—in clubs, churches, political parties, movements, various associations, and so on. No matter how independent we claim to be, we all are influenced by ideas. We are sensitive to appeals made to us—to our honor, patriotism, family, religion, pocketbook, race, or class—and we can all be manipulated and aroused. We are creators and creatures of ideas, of ideologies, and through them, we manipulate others or are ourselves manipulated. (Macridis, 1996)

II. Review of Literature

Three sources were useful in the construction of this chapter. *Political Ideologies: Their Origins and Impact*, by Leon P. Baradat provides a comprehensive, chronological survey of the most important political ideologies within the context of significant social, economic, political, technological, historical, and contemporary events. It prepares readers to understand and relate the various political ideologies to the general political values of the left, the mainstream, and the right as they appear in contemporary political events and issues. The author assists the observer to see clearly how political theory applies to his own life.

Contemporary Political Ideologies: Movements & Regimes, Roy C. Macridis and Mark Hulliung, features lucid accounts of the political ideas that define the most important political controversies of our time. Professor Mark Hulliung has prepared a timely revision of the late Roy Macridis's leading text. Five chapters are new to this edition. This sixth edition offers more current analysis of fascism, nationalism, Marxism, anarchism, a historically informed view of multiculturalism and its impact around the world, and a case study of the student movements in the 1960's which shaped the politics of an entire generation now in power. Throughout the text they invite readers to enlarge their understanding of contemporary political controversies by comparing America to European countries.

Contemporary Political Ideologies: A Comparative Analysis, by Lyman Tower Sargent. This book introduces the dominant (and some of the minor) political ideologies of the modern world. Besides providing a comparative study of nationalism, democracy, feminism, Marxism, and Islam, Sargent also introduces readers to such ideologies as anarchism, liberation theology, environmentalism, fascism, and national socialism. The result is a thorough exploration of how political ideologies affect the way people think and governments act. Through his comparative approach, Sargent looks at each ideology from a variety of perspectives - presenting the arguments, positions, and counter-positions of each, including its roots in current political debates. The book emphasizes the link between recent world events and political ideologies by including updated coverage of the impact of nationalism, democracy, Islam, feminism, and the Green Movement.

Ideology Defined

There are as many definitions of ideology as there are ideologies and students of ideologies. How the concept is defined depends in large measure on what's being accomplished.

For analytical purposes, ideology is an emotion-laden, myth-saturated, action-oriented belief system accepted largely on faith as truth or fact by a group or people. It is composed of a set of attitudes toward the various institutions and processes of a society. By emotive symbols, it economically and efficiently spells out what is valued and what is not, what must be maintained and what must be changed. It provides believers with a particular picture of the world both as it is and as it should be. Additionally, some ideologies may have established rules or behavior that believers must follow to obtain and sustain this new picture of the world. In so doing, it organizes the tremendous complexity of the world into something fairly simple and understandable. This world-view is normally skewed, thus overemphasizing one or a few aspects of society while slighting or ignoring others. In contrast to philosophy, theory, and religion--which are concerned with knowledge and understanding or with personal, private matters--ideology incites people to and provides the basic framework for social and political action. In this sense, it is a "mobilized belief system." (Sargent, 1996, pp. 2-3; Macridis, 1996, p. 8.)

Maxwell Taylor, Chair of Applied Psychology at University College in the United Kingdom, has applied a behavioral approach to his definition of ideology.

> Ideology provides the linkage for people to unite under a common dimension and provides the framework for particular kinds of people to come together. Geographically or racially based ideology might be termed nationalism and uses, as its principal attribute of both membership and concern, reference to that geographical or racial grouping. Ideology might also link together, however, more conceptually defined groups; religious ideology, for example, addresses a very broad spectrum of people - class-based religious ideology would be one example of this. In this sense, therefore, ideology defines a group to which the member can belong. It might be an ill defined conceptual group, like the member of a class, or it might be a very particular physical group, like membership of a

church or club, that meets regularly and provides a focus for social activity. (Taylor, p. 89)

One of the most important issues to consider when it comes to analyzing an ideology is that the political-military officer must be able to distinguish between a philosophy and an ideology. Philosophies tend to be profound, personal, and encourage introspection. An ideology on the other hand is the tool from which a philosophical belief becomes realization. Five points to remember in defining and analyzing an ideology are: an ideology is a political term; it consists of a view of the present and the future; it is action-oriented; it is directed at the masses; and it is usually explained in simple terms so that it can be understood by all.

Major Themes Found in Ideologies

To analyze an ideology, look at its scope, its focus, and how it addresses several critical societal issues. The scope of ideological goals may be limited (e.g., women's rights, pro-life/pro-choice) or holistic (e.g., Marxism-Leninism, Confucianism). Similarly, ideologies may be social, economic, or religious in nature. However, regardless of scope, all ideologies will have a political component, since it is generally through the political system, or by its downfall, that ideological goals will be achieved. When speaking of ideology, you should speak of it in its political sense. Therefore, make your context known.

Next, determine the ideology's focus. Identify the crucial component that must be present or developed as a prerequisite for achieving the ultimate goal that the ideology establishes. For example, a religious-based ideology will stress man's relationship with his deity and will exhort adherents to mold society to meet the deity's desires. Similarly, fascism stresses the supremacy of the State; Marxism-Leninism-Maoism, society as a whole; Confucianism, the family; and democracy, the individual.

The focus and scope of an ideology will determine how it will address five major questions or themes.

First, is the role and the nature of the individual in a society. Is there such a thing as human nature? If so, is it good or bad? Should it be developed or restrained? Do people have natural, inalienable, "human" rights? Is there such a thing as a person outside the group (tribe, state, or party), or is man strictly a social being? Is the individual supreme or is the group?

The second theme is the nature of truth and how it can be discovered. Is truth unchanging? Can it be known to all or only to an elite to whom the rest of us must submit? Has the truth already been discovered? Is there more?

The third theme is the relationship between the individual and the group. Some social scientists have no concept of individuality and see an individual as part of the group. As a member of a group an individual is helpless without the protection and cohesiveness of the group. Other scientists believe that the group is made up of individuals and must submit to individual rule when it comes to property rights and security.

The fourth theme is political authority, which is related to the role of the individual and the nature of truth. An elitist will say that authority is important and that those who are privy to the truth must be obeyed. Those who accord supremacy to the individual and feel that all can find the truth will say that political authority must be limited so as to allow for full expression and participation by the individual.

Finally, the fifth theme relates to property rights versus personal rights. Which is more important, material and economic equality or legal and political equality? How does mankind resolve the inherent conflict between liberty (which allows for aggregation of property), and equality (which says all should get their fair share)? Is "equality of opportunity" sufficient and, if so, what exactly does it mean? Does property include such things as education, health, access to transportation and communication, unemployment benefits, etc.? Are freedoms negative or positive? Which freedoms are most important; e.g., freedom from hunger vis-a-vis freedom of religion?

Ideological Functions

Ideology may have several functions. First, it can legitimize or delegitimize a political regime. It can protect or restore a political system or change or destroy it. It can rationalize the status quo or challenge it. It may also justify the imposition of one political order on another deemed inferior, or can defend the right of a group to autonomy or self-determination in establishing its own order free of outside interference.

Ideology can enhance or weaken social stability. It can bind a community together or rend it apart based primarily on a model proposed by Roy Macridis.

Macridis has designed four criteria to help identify an ideology.

- **COHERENCE**. Look at the overall scope of the ideology, its internal logic and structure. How does it view the social, political, and economic systems in the society? Does it have clear goals and strategies? Does it have several goals or just one or two? What type of movement or party does it call for?

- **PERVASIVENESS**. How long has it been around? How has it changed over time? How does it differ among groups or among societies?

- **EXTENSIVENESS** of the ideology. How many people believe in it? Who are they? Does it cut across class, ethnic, and regional lines or is it limited?

- **INTENSITY** of the ideology, the degree and depth of its appeal. Does it call for rigid discipline among its adherents? What levels of commitment, loyalty, and determination are demanded? In many cases, a highly motivated, disciplined minority may be more powerful (or more threatening) than a large apathetic majority.

These criteria are fine as far as they go, but there are other considerations:

? First, a single ideology does not dominate an entire society. There are numerous ideological influences at work in all societies. Components of these ideologies (or within one ideology) may be inconsistent and in conflict with one another. To understand the ideological influences in a given society, be sure to look at all the ideologies at work in it.

? Second, because there is more than one ideology in any society, it follows that people in that society will be influenced by more than one ideology simultaneously. There are Confucian Marxists in China, Marxist Democrats in the United States, and Confucian Democrats in Japan, though none of these three ideologies seems logically compatible with the other two at first glance. As if this were not enough cause for confusion, keep in mind that people will not always act in accordance with the ideology they espouse. Ideology inclines people to act in a certain way; it does not dictate it.

? Finally, no single ideology is monolithic--no matter how coherent it may seem to be. There will always be factions and disagreement among believers as to the "true meaning of the word," which, if nothing else, will cause the thrust of the ideology to change over time.

The "Political Spectrum"

A convenient way to categorize ideologies or factions is to determine where the ideology falls on a political spectrum (Figure 1). It is this technique that is used in classifying a group or ideology as 'leftist" or "rightist." (These terms come from French royal political tradition where those members of the French court who generally supported the monarch sat to his right and those opposed sat to his left.) We can use the political spectrum technique to look at differences—

? Among ideologies in the abstract (e.g., Jeffersonian democracy versus communism).

? Within an ideology (e.g.. communism in the former Soviet Union, Albania, Italy, El Salvador, etc.).

? Among ideologies in a single society or country.

? Within one ideological party or group.

The political spectrum acts as a tool to determine the attitudes of the group or ideology about the desirability, direction, depth, speed, and method of change. Those people who fall toward the ends of the spectrum tend to advocate extensive, pervasive, rapid change through whatever means necessary, including violence. Similarly, those toward the middle of the spectrum promote moderate, incremental change through generally legal and/or nonviolent means.

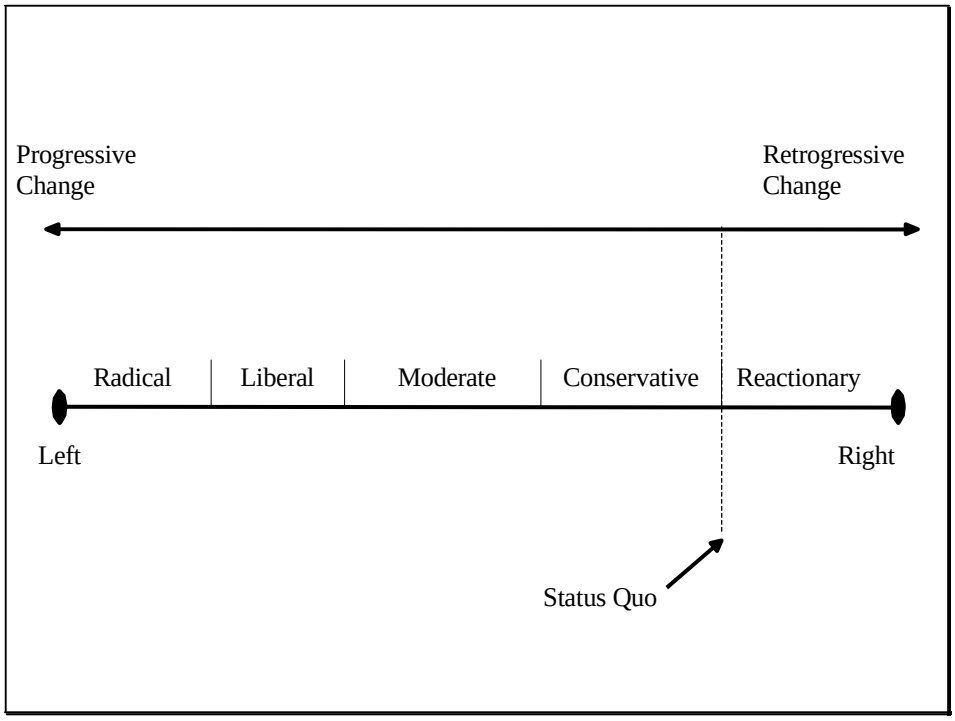


Figure 1

Moving from left to right across the spectrum, several familiar and generally misunderstood labels can be noted. Keep in mind that these labels are simply tools of analysis and are not intended either as pejorative or complimentary. Similarly, where an individual, group, or ideology falls along the spectrum will be determined by the context within which we are working. A liberal in our country may be a flaming radical in another, while a conservative in one party may be a reactionary in another. Furthermore, keep in mind that a person may hold liberal views on one issue and conservative views on another. Finally, where someone lies on the spectrum may change over time as society changes.

With these caveats, let us now define our labels.

- A radical is someone who is extremely dissatisfied with the social, political, and/or economic system. He favors revolutionary change, that is, change that is profound and fundamental. This does not mean that he advocates violence, though some radicals--those on the far left of the spectrum--do. Mohandas K. Gandhi and Martin Luther King are examples of nonviolent radicals.

- A liberal is someone who is generally satisfied with the basic structure of society, but sees substantial room for improvement. He tends to favor rapid, far-reaching change, usually instituted within the framework of the law.

- A moderate is essentially pleased with the system, but sees that some things can and should be changed. These changes are but minor adjustments accomplished by using existing procedures.

- A conservative is most content with the status quo. While his viewpoint is progressive (as opposed to retrogressive), he does not want a lot of change. He looks suspiciously on solutions that discard tried and true techniques for new and innovative procedures. A conservative values social, political, and economic order over change. This does not mean he is against change, only that he feels it should be done cautiously.

- A reactionary is someone who advocates retrogressive change as opposed to progressive change. He harkens back to a bygone era and wants to revive the "good old days." As with radicals, reactionaries are not necessarily violent, though those at the far right may well be so. For example, Confucianism is a reactionary ideology that views violence with distaste. On the other hand, several white supremacist movements in the United States hold an ideology that not only condones violence but also encourages it. To reiterate, people who fall at the extremes of both ends of the spectrum will call for deep, rapid, sometimes violent change, although the types of change and its objectives may differ.

- An additional term that does not appear on the political spectrum, but can fall at either end of the spectrum, is that of the fanatic. Contemporary use of this term describes an individual or group, whose behavior is excessive to the point of being considered abnormal, implying a focused and highly personalized interpretation of the world. In a political sense, it is behavior which is strongly influenced by and controlled by ideology, where the influence of ideology is such that it excludes or attenuates other social, political or personal forces that might be expected to control and influence behavior. (Taylor, 1991, p. x)

Three Broad Categories of Ideologies

In looking at the political spectrum the analyst can place ideologies into three broad categories:

- **Status quo** ideologies wish to keep and defend the current economic, social, and political order within a given society.

- **Radical** or **revolutionary** ideologies suggest major changes to the existing social, economic, and political order.

- **Reformist** ideologies fall between the status quo and radical or revolutionary ideologies.

It is important to understand that categorization of ideology is chronological. Communism in the Soviet Union was *revolutionary* in the beginning but once it established itself it sought to maintain the *status q*uo. One generalization to remember is that any ideological movement that challenges the *status quo* will more than likely use force to promulgate change in the social, economic, or political system.

III. Questions to Consider

Does the ideology answer the five major themes that an ideology must address? Look for the role and nature of the individual in the society, the nature of truth, the relationship between the individual and the group, the role of political authority, and property rights versus personal rights.

Does the ideology meet the functions and criteria that Macridis discusses? Determine if the ideology legitimizes or delegitimizes the political regime, does it protect or destroy the political system, does it suggest that one political regime is better than the other, will it enhance or weaken social stability. Determine if the ideology meets the four criteria of coherence, pervasiveness, extensiveness, and intensity.

Where on the political spectrum does the ideology fall? Determine where on the political spectrum the ideology falls and whether or not it deviates from its origination.

Does the identified country have more than one ideology? Complete domination by one ideology is virtually nonexistent and no ideology is monolithic.

Does the ideology propose violent or militant behavior? An example of this would be the Nihilist ideology, an ideology proposed in 19th century Russia advocating revolutionary reform and using terrorism and assassination. A more contempory violent ideology would be that of the millenarian ideology of Aum Shinrikyo in Japan.

IV. Conclusion

The process of identifying and analyzing an ideology can be a complex task. Only through further study and research can the political-military officer gain the knowledge needed to analyze an ideology of a given movement or nation. Ideology is a societal value and the failure to analyze its effect is on a given society is tantamount to failure. Wars have been fought, governments toppled, and great personal hardships endured all in the name of ideology. It is not only a societal value, but a significant social force as well.

References

Baradat, Leon P. Political Ideologies: Their Origins and Impact. 6th Edition. Englewood Cliffs, NJ: Prentice-Hall, Inc., 1996.

Macridis, Ray C. and Hulliung, Mark. Contemporary Political Ideologies: Movements and Regimes. 6th Edition. New York, NY: Addison-Wesley Publishing Co., 1996.

Sargent, Lyman Tower. Contemporary Political Ideologies: A Comparative Analysis. 10th Edition. Belmont, CA: Harcourt Brace & Co., 1996.

Taylor, Maxwell. The Fanatics: A Behavioral Approach to Political Violence. London, UK: Brassey's, 1991.

Chapter 8

Political Systems

I. Introduction and Definitions:

This chapter presents models for analyzing a country's political system. The review of the literature presents several common approaches to analyzing how a political system works. The next section describes several common governmental and electoral models, and discusses how the organization of the government affects a nation's political process. This is followed by a brief discussion of the dimensions of a nation's political climate. Finally, a model for predicting political outcomes is presented.

Many definitions of key terms will be offered throughout the chapter. However, it would be useful to start by defining some basic terms. The following definitions of key concepts are provided by Mayer, Burnett and Ogden (1996):

Political System: Those structures and processes that determine with accepted authority who gets how much of the things people value. The parts of the nation-state are part of the political system but so are structures and processes not part of the nations state**.**

Nation: A large group of people sharing a common sense of belonging, a common peoplehood. This may include a sense of community (defined below).

State: "The legal entity that exercises sovereign power over a given territory. The state may or may not coincide with the nation."

Community: "A set of individuals, usually a nation as defined above, who share, in addition to a sense of common peoplehood, a set of basic values."

Legitimacy: "Authority which is widely accepted as rightful. This acceptance is above and beyond whether there is of the performance of the system with regard to particular issues."

Sovereignty: "An essential property of a state that refers to the final or ultimate legitimate power to make and enforce rules for the society."

Political effectiveness: "The ability of a political system to resolve important issues to the satisfaction of the dominant parts of the population so as to minimize challenges to the system itself. Political systems maybe effective without necessarily being either democratic or just."

II. Review of the Literature:

Traditional Approach: The traditional approach to analyzing political systems was to dissect their formal governments. That is to say that the analysis focused on the state to exclusion of the nation. This approach was criticized for paying to much attention to legal procedures and governmental institutions and not enough attention informal processes and non-governmental groups (Chilcote, 1994). This shortcoming was especially relevant to developing nations as they had less developed formal institutions (i.e., political parties) and more varied governmental

structures. However, as the nations of the world have developed more formal political systems that are organized along similar lines, there is renewed interest in the traditional approach.

Structuralist Approach: Structuralists view politics, and indeed most human activity, as a struggle between different groups in the society. They see the society as a hierarchal structure of horizontal groups (e.g., classes, gender, religious groups, ethnic groups, etc.). Structuralists view the political, economic, and cultural systems as means for the group at the top to maintain its position. The state is thus simply a tool of the dominant social group and can only be analyzed in the context of the larger social structure and politics can only be understood as part of a larger social struggle.

There are various structuralist models but the Marxian model is the most common. A careful distinction must be made between a Marxian and Marxist approach. The Marxist approach is based on the political ideology (and dogma) of people who self-identified themselves as "Marxists" or "Marxist-Leninists". Generally this approach was based on the predictions of the future contained in *Das Kapital* and the political prescriptions offered in the *Communist Manifesto.* The Marxian approach is based on the manner in which Marx analyzed political systems as best exemplified in the less well-known *18th Brumaire*. Thus this approach is based on Marx's methodology not his conclusions. For instance this approach will see political issues as matters of class conflict, but will not assume that revolution is the only way these conflicts will be resolved.

The Marxian approach focuses on the socio-economic class structure of a nation. It analyzes the state in terms of the role it plays in advancing or protecting the interests of the dominant class. This approach also places great emphasis on the role of the state in economics and on the role of social institutions on supporting the status quo. Chilcote (1994) provides an overview of Marxian comparative analysis.

Economic Base:

Mode of Production- the forces and relations of production employed by a society at a given time. (e.g., feudalism, capitalism, socialism)

Forces of Production- the productive capacity generated by the physical capital, human capital and technology possessed by the society.

Relations of Production- the division of labor and property rights in the society or how production is organized in the society, particulary with regard to ownership of the means of production.

Means of Production- the physical capital, i.e., land, tools, buildings and machinery, that workers use to produce goods.

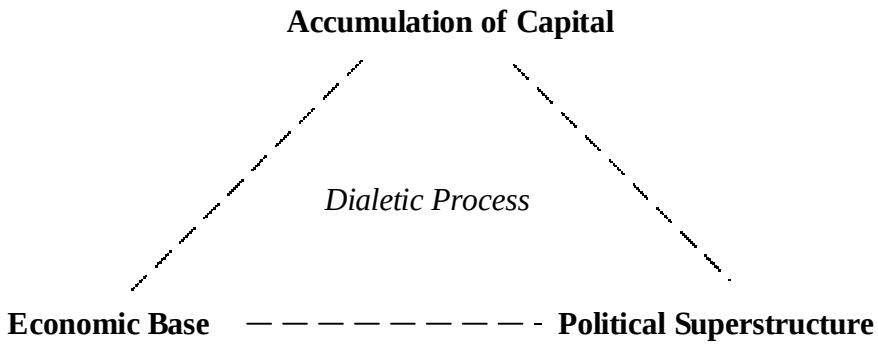
Political Superstructure:

State- the legal forms and instruments that maintain class rule

Class- large groups of people who are distinguished by their relationship to the means of production, and their role in the relations of production.

Ideology- legal, political, religious, and philosophical symbols which support class rule.

Figure 4-1: Chilcote's Marxian Model



Source: Adapted from Chilcote 1994, Figure 9.1

Class Analysis: Classes need to be identified by their role in the mode of production and thus each society may have a unique set of classes. Any class may be dominant at one point in history and then subordinate in another. Marx identified three classes in terms of their relationship to the means of production:

Workers(Owners of labor): People who do not own means of production, but have only their skills with which to make money. Their bargaining position vis-a-vis other classes depends on the abundance their skills relative to the demand for them.

Landowners (*Owners of Fixed Capital*): People who own land or more generally any physical means of production which is in finite supply. Membership in this class will be limited by the supply of land. The distribution or redistribution of fixed capital will be highly conflictual since it is by definition a zero sum situation. That is, for one person to gain land, someone else must lose it.

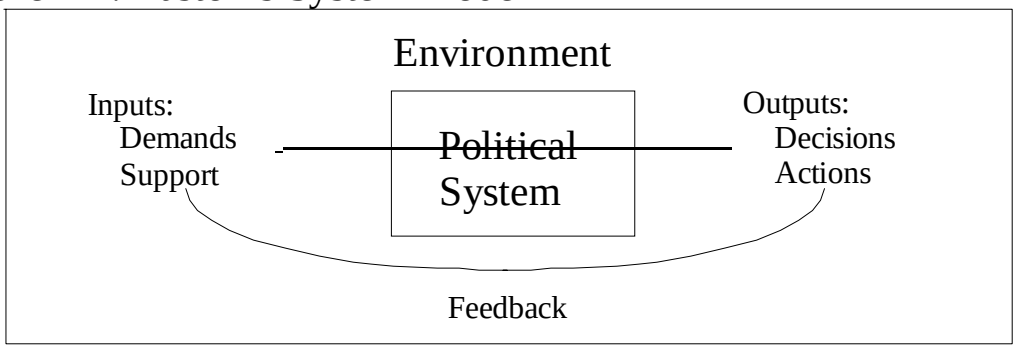
Capitalists (Owners of Reproducible Capital): People who own physical means of production that can reproduced such as machinery, buildings. The supply of this type of capital is not limited and the class may grow.

Dialectics: This is a theory of change based on conflict. The idea is that there is a state of the world (thesis) that generates opposition which is essentially support for negating the state of the world (antithesis). From this competition, some new state of the world emerges (synthesis).

Accumulation: The accumulation of capital or wealth is the ultimate outcome of economic activity. The size and distribution of the accumulation is highly dependent on both political and economic issues.

Functional or Systems Approach: Political systems can be analyzed and compared in terms of how they perform certain functions common to all systems. Easton (1953, 1965) modeled a political system in terms its inputs and outputs. He argued that a political system exists in an environment which places demands upon it and from which it draws support. From these inputs the system generates outputs in the form of decisions and actions. The environment absorbs these outputs and then generates feedback in the form of new demands and support. Figure 4-1 illustrates Easton's model.

Figure 4-2: Easton's System Model



Almond and Powell (1966) built on Easton's work by focusing on the functions and capabilities of the political system. Their structural-functional approach analyzes the political system in terms of how it performs certain function involved with absorbing inputs (input functions) and generating outputs (output functions). They define politics as activities associated with authoritatively controlling the behavior of a particular set of people within a particular geographic area through means that include the use of coercion. (Almond and Powell, 1996, 28)

Politics is not restricted to the state. Rather the state is part of a larger political system which Almond and Powell define as "...a set of institutions concerned with formulating and implementing collective goals of a society or of groups within it."(Almond and Powell, 1996, 28-29). This definition contains the following three critical concepts:

System: an object with moving parts that interacts with its environment
Structures: institutions set up to carry out specific activities
Functions: types of activity

To analyze a system, Almond and Powell use a structural functional approach. They define a generic political system in terms of the functions it must perform. Particular systems are analyzed by determining what structures perform each function. The functions are broken into three categories and are listed below.

Process Functions:
Interest Articulation: the expression of demands for policy to change or remain the same.
Interest Aggregation: the transformation of demands into policy alternatives
Policy Making: selecting between available policy alternatives
Rule Application: implementing a chosen policy

Rule Adjudication: resolving conflicts that arise from policy

System Functions:
Socialization: teaching values and norms to members of the society
Recruitment: the selection and inducement of individuals to fill specific roles in the political system.
Communication: the transmission of political information, issues and ideas.

Policy Functions:
Extraction: the collection of resources from the group or society.
Distribution: the use of resources for the benefit of members of the group or society.
Regulation: the enforcement of rules.
Symbols: the expression or affirmation of values held by the group.(not in A&P)

As defined, systems exist and interact with their environment. Since politics is a human behavior, the environment is largely understood to be the society in which the poltical system resides. One of the most relevant attributes of the society is its political culture which Almond and Powell define as the "... collective political attitudes, values, feelings, information and skills of the people in a society..." (Almond and Powell, 1996, 43). The following three aspects of the political culture are of primary importance in analyzing the political system:

System Propensities: acceptance of the system's values and organization
Process Propensities: attitudes towards participation (Participant, Subject, Parochial)
Policy Propensities: expectations of government's goals and methods.

Understanding these propensities among the people in the political system is critical to understanding the demands the society places on the political system and how it evaluates the system's performance.

III. Governmental Organization

Governmental Models:

Increasingly, civilian governments have become organized on similar lines. Almost all have a parliament, a chief executive and cabinet in charge of the bureaucracies, and a head of state who is the symbolic leader of the country. Governments differ primarily in how people are chosen to fill these roles and whether there is a separation between the parliament and the chief executive and cabinet, and between the chief executive and the head of state.

Pure Parliamentary (British) Model: In this model the chief executive (usually called the Prime Minister) and cabinet are selected by the majority party or a coalition of parties with a majority of seats in the parliament. The chief executive may or may not be the head of state. If there is a separate head of state, the office is largely ceremonial. In many European, the royal family acts as head of state. Ireland elects a President who has virtually no political power. In many commonwealth nations, the Queen (King) of England is the titular head of state and the British Governor General performs many of the day to day functions of head of state.

In the pure parliamentary model, the ruling party's power is not limited by governmental check and balances but by electoral and party checks. In such systems, if the government fails to win an important vote (i.e., a "vote of confidence") in the parliament, then the government is dissolved and new elections are called. Thus, the government is restrained by the opposition party and by its own rank and file membership. Otherwise, it has complete control over the state. For this reason, this model is usually chosen by nations with a sense of community such that they don't fear giving the "other" parties or groups unfettered control of the state.

Mixed Parliamentary (French) Model: Here, the prime minister and cabinet are selected from parliament but a president is elected separately. Generally, the prime minister functions as the chief executive and is in charge of most of the bureaucracies. The ministers of each bureaucracy are chosen from the parliament and continue to serve as members of parliament. The president functions as head of state and has control of the foreign ministry and military. In such systems, the president very often has some influence on parliament (i.e., he or she may be able to dissolve the parliament and call for new elections). A president in such a system may have considerable power to rule directly. He or she may be able to bypass parliament by calling for a referendum on a particular issue. Some presidents have the authority to declare an "emergency" and rule by decree for limited periods of time (usually subject to parliamentary approval after the fact).

In this system, the ruling party has control of both the parliament and bureaucracy, but may or may not have control of the presidency. Thus, the government may be divided with a president from one party, and a prime minister and cabinet from another. In such a case, the division may act as a brake on rapid policy change. However, if there is no majority party in parliament and there is difficulty forming a coalition government, the president may act as a stabilizing influence and source of policy guidance. For this reason, this model has often chosen by nations with a more divided sense of community such that political turmoil was expected.

Pure Presidential (U.S.) Model: Here the chief executive is directly elected and is, generally, the head of state. The bureaucracies are completely separated from the parliament. The president selects ministers (secretaries) to run the bureaucracies and, while serving, those ministers are not members of parliament (congress). Though presidents in this system have control over executing policy, they have far less formal power than prime ministers in either parliamentary system, and far less discretionary power than presidents in the mixed parliamentary system. However, presidents in the pure presidential model are far more independent of their political parties than are prime ministers. After all, prime ministers owe their office not to the voters, but to the other members of parliament from their party.

Electoral Models:

There two essential components to an electoral system. The first is the selection of candidates from which voters will choose, and the second is the selection of the officeholder from the pool of candidates. All the methods of selection can be characterized by the relative influence of masses versus elites.

Selection of Candidates: One of the most universal functions of political parties is the selection of candidates for office. In most systems, political parties are allowed to choose candidates by their own internal process. The mass of party members may or may not have a role

in selecting the candidate. Petitions and primary elections are the most common means of mass participation in the selection of candidates. More often, the task of selecting candidates is given to the party leadership or governing structure.

Selection of Officeholders: Though electoral systems vary considerably, there are three predominant models in use around the world.

Single Member Districts: In this system, each officeholder represents a geographic region and is selected on an individual basis. Voters in that district pick one candidate, by name, to hold office. In such cases the individual officeholders are beholden to their district's electorate for their jobs.

Single member district systems can be divided into plurality or "first past the post" systems, and majority or "run-off" systems. In plurality systems, the candidate who gets the most votes, whether or not its a majority of votes, wins. This system is used to elect member of Congress in the US and members of parliament in Britain. This system will generally favor the rise of two predominant political parties over smaller parties. Also the parties in this system will tend to converge towards the center of the political spectrum. As a result there will be less difference between policies of different parties, and more emphasis of personalities than in other systems.

In the majority system, a candidate must receive a majority of the votes cast to win. If no candidate wins a majority, then a run off election between the two lead candidates is held. This system is used in some state governments in the US and to elect the president in France. In this system, small parties can be influential by preventing a candidate from larger parties from winning a majority and then demanding concession in exchange for its support in the run off.

Proportional Representation: In this system, multiple are to be selected (i.e., the members of parliament) and the electorate votes for a party not for a candidate. The offices are then distributed among the parties in proportion to the votes they receive. That is, if a party receives 55% of the votes cast in the nation, it will receive 55% of the seats. The party then selects individuals to fill those seats (or offices). Thus, officeholders do not represent specific regions and they owe their job more to the party than the electorate.

This system favors the rise of more parties than the single member district system. This is because a party that party receives 10% of the nationwide vote in a single member district system (especially a plurality based one) will probably never win a seat in the parliament. However, in a proportional representation system, it will receive 10% of the seats. Because geographic distribution of this 10% is irrelevant, party lines will be drawn more along ideological, socio-economic or religious divisions, as opposed to geographic divisions of the electorate. Furthermore, since officeholders are not selected by name, party policy issues are more important to the voters than are the individual officeholder's views, character, or seniority. This also leads to greater cohesion and discipline within each the party. It also leads to a greater difference in policy position between parties.

List Systems: In these systems, the electorate chooses multiple officeholders by name from a list of candidates. Parties may determine what candidates are on list, but the voters choose which candidates hold office. Therefore, unlike the proportional representation system,

officeholders are beholden to both the voters and the party. Also, because voters choose officeholders by name, the individual characteristics of the candidate are more relevant in this system. However, unlike the single member district system, in this system, voters may split their vote among two or more parties. Thus third parties, especially those with charismatic candidates, are more likely to rise in this system. However, if the districts are not national, these parties need not be national in their appeal and thus there may be a scattering of "independent" candidates throughout the system. This system is commonly used to elect town or city councils in the US and in China.

IV. Political Climate

The political climate refers to the relationship between the citizens and the government, more specifically, to the degree which each influences the other. Thus, the climate is characterized by the nation's existing level of democracy and civil liberty. Democracy may be defined as the ability of the citizens to influence government composition and behavior. Liberty may be defined as the inability of the government to interfere in the personal lives of its citizens.

Legitimacy:

Legitimacy is often referred to as the acceptance of a system's, usually the state's, right to make authoritative decisions (Mayer, Burnett, and Ogden 1996). Thus legitimacy is a matter of perception on the part of individuals and can be measured in terms of its *universality* (i.e. what percentage of the group accepts the system's right to make decisions for them). However, an individual may accept a political system's authority over one issue but not another. Therefore, legitimacy must also be measured in terms of its *scope* (i.e., the set of issues over which members of the group accept the system's authority). For instance an individual may accept the government's authority to collect taxes, conscript for the military, and to convict murders while not accepting its right to determine whom they may marry, what religion they practice or what they wear. Of course, legitimacy is not limited to the state. Individuals might accept the right of their family to make decisions over certain issues (e.g., whom they marry) and of their employer to make decisions over others (e.g., what they wear).

Strictly speaking, legitimacy is a normative concept based on the population's judgements of what it is right and wrong for the state, or any other political system, to decide. That is to say that legitimacy is the range of issues over which the people think the state should decide, not the issues over which it actually decides. Therefore when looking to measure legitimacy, one must look at people's attitudes towards the government (and/or actions which reflect that attitude) rather than at the government's actions or inactions. To understand the source of a government's legitimacy, one must consider the factors which would weigh on an individual's judgement, i.e., ideology, religion, culture, the government's political effectiveness, and the presence and perceived effectiveness of available alternative political systems.

Liberty:

Liberty is the individual's actual freedom from governmental influence. Very often it is defined in terms of the issues which an individual is free to chose for himself, i.e., what religion to practice, what job to have, what clothes to wear, when to get up in the morning, what to think, whether or not to wear a seat belt, etc. At one extreme there is anarchy where individuals are free

to decide all issues for themselves. At the other extreme is totalitarianism, where individuals are not allowed to decide anything for themselves. These theoretical extremes do not exist in reality but have been examined in literature in William Golding's *Lord of the Flies* and George Orwell's *1984*. In between these extremes, nations have various ranges of issues over which the individual is free to choose and this range is the nation's liberality.

Unfortunately, liberality is not a linear function between two extremes. In the west women are free to drive cars but not to drive or ride in them without a seat belt; while in some countries women may not drive cars but are free to not wear seat belts when riding in them. Determining which of these countries is more liberal depends on which of these issues one thinks is more important. From a western point of view, the comparison is ridiculous, but from another culture's point view, it may be very apt. Thus, measuring liberty in a meaningful way depends upon the normative point of view of the person doing the measuring. This does not mean that one can't measure liberty, but that the measure will not be objective or universally accepted.

Democracy:

At its roots, democracy means the involvement of the mass public in government. Given the interpretation of political systems as processes, scholars have typically defined democracy in procedural terms. Schmitter and Karl (1996) offer the following definition:

> *Modern political democracy is a system of governance in which rulers are held accountable for their actions in the public realm by citizens, acting indirectly through the competition and cooperation of their elected representatives*. (p. 50; italics in original)

There are several key aspects of this definition. First, it places an emphasis on rulers being accountable as opposed to being selected by the citizenry. Second, it requires that the accountability be in the public realm so that the accounting is acknowledged and visible. Third, it requires that the accountability be to the citizens at large where citizens are understood to be most of the adult population. Fourth, it allows that rulers will be indirectly, and thus imperfectly, accountable through a competitive political process.

V. Predicting Political Outcomes: The Median Voter Model

Most models of political systems seek to explain or describe the systems origins, structure and/or function. Few, however, seek to predict the outcome of the system's decision making apparatus. Thus, these models are good at explaining how a decision is made but not at predicting what decision will be made. However, there are models that forecast political decisions in most types of political system. The most widely used of these is the Median Voter Model. The model is based on the following proposition:

Median Voter Theorem: When voting by simple majority over a single issue, if the policy alternatives can be ordered from left to right and voters are placed on this spectrum according to the location of their ideal policy, then the policy of the median or middle voter will be chosen

Bueno de Mesquita (1984, 1996; Bueno de Mesquita, Newman and Rabushka, 1985) has

used this theorem to create a model for forecasting political outcomes. Though it is a “voting” model it has been applied to non-democratic as well as democratic decision making bodies. There are four steps in using the model as listed below. To use th model

Identify all Stakeholders: A stake holder is defined as any group with an interest in the decision. The premise here is that any group that stands to lose or gain from a decision may try to influence that decision. The model takes a broad view of the political system in that stakeholders do not need to be part of the formal political system. They just have to be effected by the outcome. Bueno de Mesquita (1984) uses this model to predict the policy of Iran after Khomeini’s death (Khomeini was still alive at the time). Bueno de Mesquita asked a group of area experts to identify the stakeholders on several issues. The experts identified the groups listed in table 4-1 (note: relative influence is explained later).

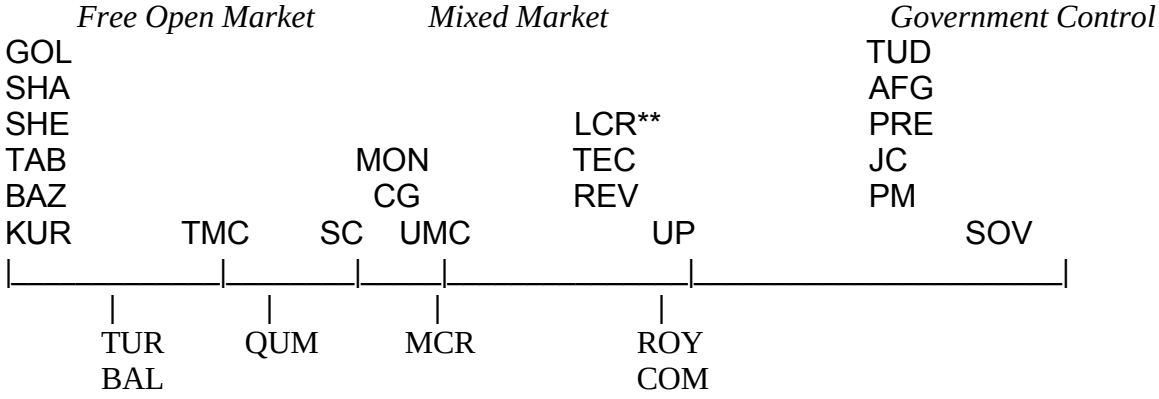
Table 4-1: Stakeholders in 1984 Iran

Group	Relative Influence	Group	Relative Influence
Afghan Refugees (AFG)	0.5	President Khamenei (PRE)	10.7
Tudeh Party (TUD)	0.6	Prime Minister Musavi - Khamenei (PM)	9.0
Kurds (KUR)	2.3	Tehran Militant Clerics (TMC)	3.4
Turkoman (TUR)	0.3	Qum Clerics (QUM)	4.5
Baluchis (BAL)	0.6	Supreme Court (SC)	4.5
Royalists (Roy)	0.2	Aaytollah Montezari (MON)	0.1
Bazaaris (BAZ)	5.6	Revolutionary Guards (REV)	12.4
Middle Class Rural Peasants (MCR)	0.9	Committees/Cabinet (COM)	11.8
Lower Class Rural Peasants (LCR)	4.5	Council of Guardians (CG)	9.0
Urban Middle Class (UMC)	1.1	Ayatollah Golpayegani (GOL)	0.6
Urban Poor (UP)	4.5	Ayatollah Shariat Madari (SHA)	0.6
Technocrats (TEC)	0.6	Ayatollah Sherazi (SHE)	0
Junior Clerics - Rafsanjani (JC)	11.3	Ayatollah Tabot Tabai (TAB)	0
		Soviet Union (SOV)	0.6

Source: Bueno de Mesquita 1984 231

Identify each stakeholder's Position: Each stakeholder's ideal policy on each issue under consideration must be identified. The stakeholders are then placed on a policy spectrum (i.e., a line) according to their position. With regard to the government's role in the economy, Iranian stakeholders were organized in the following way:

Figure 4-3: Economic Policy Spectrum in 1984 Iran



Cumulative Distribution of Influence:

9.1 10.0 13.4 17.9 22.4 32.6 33.5 55.5* 67.5 100.2

Source: Bueno de Mesquita 1984 234

Determine each stakeholder's Influence: The next step is to determine each stakeholder's influence over the decision making process relative to the others. When predicting the outcome of democratic decision making process, the percentage of votes each group controls is usually a good measure. For other processes, an estimate is made about how much influence each group has relative to that of the others. Bueno de Mesquita (1984) aggregated the subjective estimates of his panel of area experts to determine the relative influence of each group as listed in table 4-1. The numbers represent the percentage of influence possessed by each group.

The information about influence is used to "weight" each group according to it's influence. Starting from the one side of the policy spectrum in figure 4-3, each group's influence is added up to produce the cumulative distribution listed below the line in figure 4-3. The group or groups whose ideal policy is at the point where the distribution is equal to 50% is the median party. In this case, the position is shared by the Lower Class Rural (LCR), Technocrats (TEC), Revolutionary Guards (REV), and Urban Poor (UP). The model predicts that their favorite policy (a mixed economy with fairly heavy state involvement) will be implemented.

Determine each stakeholder's Salience: A stakeholder's salience is the degree to which a particular policy issue is important to the group. Each group's salience is considered to determine how much effort they will expend to achieve their ideal outcome on a particular issue. In the example of 1984 Iran, the urban poor (UP) and lower class rural (LCR) were estimated to have a much higher salience for the economic issue than the revolutionary guards (REV) and technocrats (TEC)(Bueno de Mesquita 1984). Therefore, one could predict that the urban poor and lower class rural would be more active in pursuing their economic goals (i.e., might form a coalition) with perhaps only tacit support from the technocrats and revolutionary guards.

There are several important points to take from this model. First, control over policy is as much a matter of position as power. Groups with seemingly little political power may determine the outcome by virtue of the position they hold vis a vis the other groups. Groups with a large share of the political resources may be ineffectual because their policies are too extreme. Second,

the median is a relative position based on the positions and power of all the groups. Thus the median position is not necessarily a centrist position. If a group, or set of groups, on one end of the country's political spectrum held 50% or more of the political resources, then they would be the median voter. Third, because groups hold different positions on different policies, the median group changes with each issue. However, there are usually one or two issues that dominate the political system, and the position of groups on these issues determines what coalitions are formed.

References:

Bueno de Mesquita. 1984. “Forecasting Policy Decisions: An Expected Utility Approach to Post-Khomeini Iran.” *PS.* Spring 1984. 226-236.

Bueno de Mesquita, Bruce, David New man, and Alvin Rabushka. 1985. *Forecasting Political Events: The Future of Hong Kong.* New Haven, CT: Yale University Press

---- 1996. *Red Flag Over Hong Kong.* Chatham, NJ: Chatham House Publishers, Inc.

Chilcote, Ronald H. 1994. *Theories of Comparative Politics: The Search for a Paradigm Reconsidered.* Boulder, CO: Westview Press.

Easton, David 1953. *The Political System*. Chicago: University of Chicago Press.

---- 1965. *A Framework For Political Analysis*. Chicago: University of Chicago Press.

Gastil, Raymond D. 1991. “The Comparative Survey of Freedom: Experiences and Suggestions.” in *On Measuring Democracy: Its Consequences and Concomitants,* ed. Alex Inkeles. New Brunswick, NJ: Transaction Publishers.

Mayer, Lawrence C., John H. Burnett, Suzanne Ogden. 1996. *Comparative Politics*. Upper Saddle River, NJ: Prentice Hall.

Ryan, Joseph E. 1996 . “The Comparative Survey of Freedom--1993-1994 Survey Methodology.” *Freedom in the World: The Annual Survey of Political and Civil Liberties 1993-1994.* [http://sedac.ciesin.org/pidb/freedom/FH-methodology.html] July 9. 1998.

Schmitter, Phillipe C., and Terry Lynn Karl. 1996. “What Democracy Is ...And Is Not.” in *The Global Resurgence of Democracy,* 2d ed., eds. Larry Diamond and Marc F. Plattner. Baltimore: The Johns Hopkins University Press.

Chapter 9

POLITICAL ECONOMY

I. Introduction and definitions

Political economy is often defined as a study of the relationship between politics and economics. J. Stuart Mill's followers describe political economy as a deductive science, drawn from assumption; while the school of David Ricardo considers it an inductive science, built upon elementary facts. A third school of political economy to which belong August Comte and Daniel Webster, argues that Political Economy is only an assemblage of truths; therefore, not a science because of its lack of law or principal. The simple premise of recognizing the reciprocity between economics and politics leads us to ask the following question: what is political economy?

"On the one hand, politics largely determines the framework of economic activity and channels it in directions intended to serve the interests of dominant groups; the exercise of power in all its form is a major determinant of the nature of an economic system. On the other hand, the economic process itself tends to redistribute power and wealth; it transforms the power relationships amongst groups. This in turn leads to a transformation of the political system, thereby giving rise to a new structure of economic relationships. Thus, the dynamics of international relations in the modern world is largely a function of the reciprocal interaction between economics and politics." (Gilpin, 1975, pp. 21-22).

In studying political economy, the following concepts defined by Johnson (1996) are important:

Aggregate demand

"Also more accurately referred to as *aggregate expenditure*, this is one of the key concepts introduced by John Maynard Keynes that still today is at the heart of most macroeconomic theories about the determination of the overall level of employment (and thus the level of national income produced) in a country's economy during a given year…Thus Keynes invented most of the basic ideas of what is today the macroeconomists' conventional system of national income accounting when he formulated his famous aggregate demand identity:

$$\boldsymbol{Y = C + I + G + (X - M)}$$

Which simply means that a single country's aggregate demand for national product (*Y*) is always equal to the total demands of its households for Consumer goods and services (*C*), plus the total demands of its firms for Investment goods (*I*), plus the total demands of its various Government agencies for goods and services (*G*), plus the net demands of foreign consumers, firms and governments for the country's goods and services (exports minus imports)."

Comparative advantage

"The ability of one economic actor (an individual, a household, a firm, a country, etc.) To produce some particular good or service at a lower opportunity cost than other economic actors can. That is, the economic actor with a comparative advantage can produce the particular good or service by giving up less value in other goods or services that he could otherwise produce with his labor and resources than the other economic actors would have to give up in producing that same good or service. "

Fiscal policy

"That part of government policy which is concerned with raising revenue through taxation and with deciding on the amounts and purposes of government spending."

Monetary policy

"That part of the government's economic policy which tries to control the size of the total stock of money (and other highly liquid financial assets that are close substitutes for money) available in the national economy in order to achieve policy objectives…*Monetary policy is said to be "easy," "loose," or "expansionary" when the quantity of money in circulation is being rapidly increased and short-term interest rates are thus being pushed down. Monetary policy is said to be "tight" or "contractionary" when the quantity of money available is being reduced (or else allowed to grow only at a slower rate than in the recent past) and short-term interest rates are thus being pushed to higher levels*."

Relative Deprivation

Tedd R. Gurr developed this concept in his book titled: "Why Men Rebel." He uses a conceptual model to explain internal rebellion, particularly political violence in a form of insurgency. The theory is developed through two basic concepts: the perception of deprivation and the relative nature of the deprivation. Relative deprivation refers to a difference or gap between what people believe they have a right to receive (expectations) and what they actually receive (achievements). Gurr analyzes different scenarios that the divergences between expectations and achievements create (Gurr 1970).

Politicians rise and fall according to their successful management of economic matters. No clearer example of the dependency of a politician's fortune on economics exists than President Ronald Reagan's poignant question to Americans in the 1980 presidential debate: "Are you better off now than you were four years ago?" The answer to that question helped carry him into office despite the public's concern with other issues of the Republican political platform. Events elsewhere in the world have, likewise, shown how domestic economic failures have contributed, in either a negative or positive manner, to the fortunes of national leaders. Examples include the fall of Ferdinand Marcos in the Philippines in 1986, the success of the Solidarity movement achieving political power in Poland in 1989, the fall of Nicholae Ceaucescu of Romania and Erich Honecker of East Germany in 1989, and the elections to the presidency of Sam Nujoma of Namibia, Carlos Menem in Argentina, and Alberto Fujimori of Peru all in 1990. Most recently, the downfall of President Suharto of Indonesia and Prime Minister Hashimoto of Japan are excellent examples of mismanagement in economic matters. Currently, the stagnation of the economy is having significant effects upon the Russian political system.

II. Review of the Literature

Several books were used for the construction of this chapter. *International Political Economy: The Struggle for Power & Wealth*, by David Skidmore and Thomas Lairson, is a general textbook on International Political Economy intended for use either as a main text or as a supplement. The authors explain the basic concepts, theory, history and policy of international

economics. They include data and significant information on topics such as globalization, hunger, population and sustainable development, and methods for measuring development. Included also are economic liberalization country studies on China, India, and Brazil. Discussions on regional economic blocks, the Uruguay Round, and the World Trade Organization are also covered. Skidmore and Lairson also conduct an analysis of investment flows to developing countries and an examination of the 1994-95 Mexican peso crisis. Lastly, they conduct a comparison of post-communist systems in Russia, China, and Vietnam.

The Politics of International Economic Relations, by Joan Edelman Spero describes Western, North-South, and East-West economic systems. The two basic themes of Spero's book are the influence of politics on international economic relations and the political management of international economic relations in the years since World War II.

Economics by Martin Bronfenbrenner, Werner Sichel, and Wayland Gardner is an excellent, detailed textbook concerning well-established and controversial topics in economics. The authors go into discussion on such topics as microeconomics, macroeconomics, comparative economic systems, and international economics.

The definition of political economy includes both domestic and international dimensions. On the national level, public policies deal with issues such as road construction, housing, hospitals, and public education, federal budget, inflation, taxes, unemployment, and the environment. Politicians rise and fall according to their successful management of economic matters. How, then does political economy evolve nationally? And what policies do states put in place to deal with the complex issues of international trade and finance?

III. National political economy and its inter-relationship with other pol-mil factors

Domestically, political economy is the economic analysis of public policy issues and the making of policies for addressing these issues. Economics, the process of the authoritative allocation of society's values and its resources, pervades domestic politics since almost every political decision has an economic consequence.

A regime's political legitimacy, that is how well it is recognized by the public as the authorized bearer of national power and responsibility, is derived from various **religious**, **historical, cultural, ideological,** and economic sources. For example, the constitutional monarchy of King Hassan II of Morocco derives its legitimacy form the King's claim to the descent from the line of the Prophet Muhammad, his Alaouite dynasty's historical claim as the sole rulers of Morocco since 1649, and the monarchy's role in protecting Arab culture against Western influences and in negotiating independence from French colonialism. Perhaps of even greater significance is the King's ability to maintain strong military forces and his success at making the Moroccan economy one of the strongest in North Africa without the benefits of oil. Since a government's primary function is the maintenance of the national well being, its legitimacy depends heavily on its ability to provide economically for its citizens in terms of equity (income distribution), efficiency (economic regulation), and stability (economic growth and development). Thus, when a government loses the popular support of its population in these areas, it must either respond to retain its authority or eventually fall, whether it is a democratic or

authoritarian regime. The failure of the Communist Party in Czechoslovakia to sustain itself in national elections in 1990 is an example of the consequences of the loss of legitimacy. Similarly, the student demonstrations and massacre in China's Tiananmen Square in June 1989 profile an example of a government's harsh response to popular dissatisfaction and disillusionment. The level of popular dissatisfaction will determine a government's ability to loosen political and economic restraints for fear of losing its power to opposition groups. In the United States, the success of the Clinton administration to win election to a second term was due in part to the American public's impression of a strong robust economy.

> "Economic strength is the basis on which a nation satisfies the needs of its people for goods and services, and also on which it is able to build its organized military capabilities, manufacture arms, supply manpower, and provide the logistic and technical support needed by modern armies, navies and air forces. Through investment and trade, nations help to enrich one another, and standards of living depend not only on the efficiency of national economic activity but also on access to resources and markets through international commerce." (Pay S. Cline, World Power Trends and US Foreign Policy for the 1980's.)

Inherent in the preservation of the national well being is the capacity of a government to defend itself and to secure its interests abroad. The price to pay for security is high; **military** forces must be paid, equipment purchased, and wars fought. No government can devote its entire resources to security. Even in wartime, it must ensure food, clothing, and shelter to its population. Thus, the issue of guns versus butter surfaces as a political dilemma for most nations. Politicians must balance military expenditures with other expenditures for the national well being. The state must address issues such as how much of the nation's budget should be allocated to social security, agricultural support, education, development or improvements in infrastructure, and strategic and conventional weapon systems. In democracies, these perennial questions mold public debate; in authoritarian regimes the same issues shape policies -- but behind closed doors with little or no public redress for unpopular decisions. Until recently, the United States, Eastern and Western Europe were willing to devote large portions of their national budgets to defense. That situation has changed and defense cuts are appearing in the budgets of most of these countries. Some states such as Vietnam, China, North and South Korea, El Salvador, Israel, and Iraq, to name a few, still devote significant portions of their budgets to the military.

The guns-versus-butter dilemma affects military strategy in two ways: capabilities and strategy formulation. For instance, the American strategies of "deterrence" and "massive retaliation" evolved in American foreign policy in response to several different factors after World War II. First, the United States was reluctant to invest in a large military force to oppose Stalin's aggressive foreign policies. In this post World War II era, the American public was also heavily investing in the reconstruction of Europe and Japan, while the American economy continued struggling to throw off the vestiges of the depression, find jobs for returning troops, and convert wartime industries to peacetime industries. Nuclear weapons were cheaper than conventional military forces and carried a more significant and, therefore, effective threat of total destruction. The decision to pursue a nuclear deterrence strategy based on massive retaliation allowed for both "guns" and "butter" in the American economy.

On the other hand, the high cost of sufficient conventional forces to meet the Soviet threat compelled the United States in the 1950's to adopt a new strategy. "Massive retaliation" depended upon nuclear weapons to counter overwhelming Soviet conventional forces. While "Flexible response" has superseded it, costs still dictate ultimate reliance on nuclear weapons for conventional deterrence.

National interest determination frequently relates directly to the size and capability of a nation's budget. A country can only pursue those interests for which it has sufficient resources. In 1983, President Ronald Reagan decided that it was in the national interest of the United States to develop the Strategic Defense Initiative (SDI or "Star Wars."). In another example, Libya, in support of its stated national interests, has for years provided financial and other resources to various political extremist groups from the Irish Republican Army to the West German Red Army Faction to various dissident Palestinian groups based in Damascus. With the fall in the price of oil beginning in 1986, Libya has seen the bounties of high oil prices disappear. Colonel Qaddafi, Libya's leader, has been forced to cut back on his support of such international groups. Linked to Libya's national interests have been those of West European governments, especially France and Italy. Their decision to pursue diplomatic relations and ease economic restrictions imposed on Libya in 1986 after the bombing of a discotheque in West Berlin, reflect their economic interests in Libya.

Observations such as the aforementioned reinforce the intuitive recognition of the need for a solid understanding of a country's economic system to predict with any validity its actions and policies; therefore, the analyst must evaluate the political constraints and imperatives induced by economic conditions. This study commences with an assessment of the three economic functions of government: equity (income distribution), efficiency (economic regulation), and stability (economic growth). Sustained deficiencies in these areas mandate governmental actions to retain regime legitimacy.

In most Organization for Economic Cooperation and Development (OECD) countries, income distribution can be readily measured from published statistics. Median and model incomes and poverty-level figures provide a basis of measurement. In the absence of a significant middle-class, wide variance in income or wealth may lead to popular dissatisfaction that could foster governmental change or even revolt.

In non-OECD countries, the necessary statistics are often either unavailable or unreliable. For instance, in the former Soviet Union, President Gorbachev's salary was 900 rubles a month, much less than the 2,000 rubles a month a Soviet marshal earned. Yet, special discount stores--open only to the highest party officials--readily furnished expensive goods at lower prices, which the general public could not obtain at premium prices. In these situations, the analyst must rely upon nonstatistical measurements such as rationing, black market practices, and queues to describe the differences in living standards.

Government also assumes the responsibility of managing the supply of goods and services by regulation to assure the economy meets the needs of the populace. In a free or mixed market economy, a fundamental governmental task is to guarantee competition by controlling monopolies. In command economies where competition is minimal, this function includes

provisions for adequate production inputs. But efficient management of the economy also entails control of corollary production factors: spillover effects (pollution, unsafe drugs and foods, strip mining), public goods (public health services, highways, and law and order), and taxation. For instance, Zaire's (which is now the Democratic Republic of Congo) lack of adequate transportation systems impeded the flow of agricultural products and induced a return to subsistence agriculture after decolonization.

Finally, the government seeks to stabilize the economy to eliminate the peaks and troughs of the business cycle. Sustained economic growth results from an effective macroeconomic policy that consists of high output, high employment, price level stability, and sustainable balance of payments. While the Gross National Product (GNP) is the basic measurement of an economy, macroeconomic policy is gauged respectively by productivity, the unemployment rate, the inflation rate, and net exports. Lack of improvement in these four areas may pose the greatest threat to a government. Radical change or consistent failure in these areas indicates problems that governments cannot ignore without significant adverse consequences.

IV. International political economy and its inter-relationship with other pol-mil factors

Internationally, political economy is the interplay of economic and political factors in international relations and foreign policy. It may involve trade issues, monetary policy, or debt relief and economic restructuring. It has manifested itself through calls for a New International Economic Order (NIEO), a set of demands by the Third World to alter the existing international economic system to improve its economic conditions, and Dependency Theory, a neo-Marxist explanation for the continued impoverishment of the poor countries of the world. The Bretton-Woods International Monetary Order, the General Agreement on Tariffs and Trade (GATT), the International Monetary Fund (IMF), the World Bank, the World Trade Organization (WTO), and various Development Banks and international aid agencies are all responses to international economic problems within their political context. On a more regional basis, the effects of the direct relationship between politics and economics appeared in the European Union, the Magrebi Union of North Africa, the Gulf Cooperation Council, the Latin American Free Trade Association, the Central American Common Market, the Association of Southeast Asian Nations, the Asian Development Bank, and the North American Free Trade Agreement.

The examination of a state’s economy and international trade patterns can reveal vulnerabilities to **external influences**. Other states can use these weaknesses to achieve their own objectives. Economic sanctions offer a negative inducement. The Soviet grain and OPEC oil embargoes overtly illustrate this point, but often the tacit threat works more effectively. Although United States dependence on critical minerals from South Africa tempered American criticism of the Afrikaner regime, sanctions were imposed against South Africa.

The most difficult and perhaps the most rewarding political objective of international economics lies in the creation of economic ties of such a strong nature that countries mutually benefit from the relationships. Historical examples of this include: the European Coal and Steel Community; the context of the General Agreement on Trade and Tariffs (GATT); the Bretton Woods Accord; the Maghrebi Union of North Africa; the Asia Pacific Economic Caucus (APEC); and the North American Free Trade Agreement (NAFTA).

To determine economic dimensions of vital **national interests** and **international influence**, the analyst needs a framework to define existing relationships. Import-export balances, exchange rates, and current account deficits depict a country's general position in the international system. The peaks, troughs, and rapid changes of these economic indicators suggest external penetration and potential vulnerabilities, and indicate problems that could cause policy shifts.

As no event occurs in isolation from its predecessors, national economic systems do not operate in seclusion from the world around them. Most modern industrialized economies depend on imports to furnish raw materials and on exports to pay for them. No industrial economy can function without energy, yet few states have sufficient resources within their borders. Thus, the 1973 oil crisis offers a poignant example of the economic factor in the determination of vital national interests. The oil embargo prompted radical measures in Europe and the United States. Europe's continued dependence on foreign oil supplies led President Carter in 1979 to declare the Persian Gulf a vital national interest to dispel any delusions the Soviets might have had, following their invasion of Afghanistan, of continuing south to attain a warm water port. Similarly, Nasser's nationalization of the Suez Canal threatened British and French trade routes upon which their industrial development depended. His action intensified other grievances against him and precipitated the 1956 Anglo-French invasion of Egypt to recapture the Canal. The Gulf War was a result of a coalition of nations determined to repel Saddam Hussein’s invasion of Kuwait and the security of the rich oil deposits in the region.

A more accurate analysis surfaces through an examination of a country's self-sufficiency in four elements of economic power: energy, critical nonfuel minerals, industrial capacity, and food production. The need for energy permeates economies and, while oil constitutes the primary source, hydroelectric power, nuclear reactors, and old-fashioned coal enhance self-sufficiency and modernization. Scarce nonfuel minerals -- for example, iron ore, copper, bauxite, chromate, and uranium -- are critical to modern technology and, therefore, military hardware production. Three products most effectively indicate industrial capacity: steel (basic industry), aluminum (light industry), and concrete (building materials). These products, in turn, describe the country's capability to produce military equipment and necessary goods. People must eat, so food production also determines economic power. It can best be measured by net import-export of three basic foods: wheat, coarse grains, and rice.

The preceding factors depict gross vulnerabilities to external influence. They must be refined by examination of patterns of trade. If a country depends on a single country or region for any of the critical ingredients, a stranglehold could be established. If no alternative sources exist, then the source could be a vital interest. Similarly, trade routes by which products and raw materials are shipped become vital interests; e.g., the Panama Canal, and the Straits of Malacca and Gibraltar. In any case, any dependence on foreign sources for any of the economic factors of national power becomes a possibility for external influence by either denial or assistance.

While economics or any other single political-military analytical factor cannot tell the whole story, its pervasive impact on domestic politics, foreign policy, defense policy, and diplomacy dictates its prominent place in the analyst's repertoire of tools. Decisions always incur costs, and in today's intricate international system, they often have both an economic

impetus and an economic impact. As such, foreign policy can neither be understood nor predicted without consideration of the economic dimension.

V. Questions to consider

There are several basic questions the analyst must address when analyzing a nation's political economy:

1. In its bilateral or multilateral relations with other states, does the country use economic rewards or punishments; how effective are these techniques?

2. How dependent is the nation's economy on the outside world?

3. What kind of economy has the government established?

4. What are the social and political consequences of the decision to either shift or not to shift the economy?

5. Where does the nation's economy fall within the International Political Economy?

6. How do international law and regulations affect the nation's political economy?

7. Is the nation adopting protectionist practices? If so, why does it set barriers to foreign trade?

VI. Summary

Despite recent setbacks in Russia, Asia, and Brazil, the American economy appears vibrant thanks to its sound and effective economic policies. Faster economic growth supported by less government regulations and lower marginal tax rates on economic gains. A century ago, Karl Marx, the father of socialism, and John Maynard Keynes, the father of modern capitalistic economics, distinguished themselves by becoming two of the first economists to recognize the economic basis of political change. Although socialism and communism have since been discredited, their followers have not forgotten that relationship. Until recent times, capitalist scholars, politicians, and analysts have tended to separate economics from politics. Dramatic events of recent times have reminded them of the economic dimension to domestic and international political events. For the political-military analyst, the study of economics can not be divorced from the political context.

References

Caporaso, James A. and David P. Levine. Theories of Political Economy. New York: Cambridge University Press, 1992.

Brofenbrenner, Martin and Sichel, Werner and Gardner, Wayland. *Economics*. Boston, MA: Houghton Mifflin Company, 1987.

Lairson, Thomas and Skidmore, David. *International Political Economy: The Struggle for Power and Wealth.* New York, N.Y.: Holt, Rinehart and Winston, Inc., 1993.

Spero, Joan. *The Politics of International Economic Relations.* New York, N.Y.: St. Martin's Press, 1990.

Jones, Walter S. *The Logic of International Relations.* (pp.225-259). New York, N.Y.: HarperCollins Publishers Inc., 1991.

Kegley, Charles W, and Eugene R. Wittkopt. *World Politics: Trend and Transformation.* (Pp. 207-215). New York, N.Y: Worth Publishers, 1999.

Gurr, Ted R. *Why Men Rebel.* Princeton, N.J.: Princeton University Press, 1970.

Relevant sites on the World Wide Web:

1. http://www.auburn.edu/academic/liberal_art/pol_sci/U120/U120.html
2. http://g8.cuonline.edu
3. http//www.oecd.org/
4. http://www.wto.org
5. http:www.usitc.gov/tr/tr.htm

Chapter 10

Role of the Military

I. Introduction

This chapter introduces the military as an aspect of national power, a political actor, an economic force, and a key national institution. It outlines factors the analyst may use to explain and predict military behavior within a country. Focusing on the regional analysis mission of the PSYOP/Civil Affairs Officer, this chapter concentrates on societal roles and the relationship of the military to the political system. It leaves aspects such as tactics, order of battle and combat readiness to the military intelligence community.

II. Definitions

Military

For political-military analysis, the word "military" describes those armed forces identified by a government as its military. If a country considers its police forces to be part of the military, you should so treat them.

Types of Militaries

Because foreign militaries differ, the analyst operationalizes the definition by describing, contrasting and comparing their organization, makeup, roles, missions, and practices.

- Regular forces. Look at interservice and intraservice solidarity or rivalry; cliques or factions based on class, ethnicity, language, regional ties, or socioeconomic class and patronage ties.
- Defense establishment. This includes civilian leadership and bureaucrats.
- Militia/reserves/national guard.
- Paramilitary forces. A border patrol would be an example of a paramilitary force.
- Police or other security forces.
- Private armies/warlord armies. Private armies are those outside the regular military force structure; however, they are recognized as legitimate in the society. Warlord armies are those that are extralegal or illegal. Both armies generally hold personal loyalty to their leaders above loyalty to the government.
- Regular forces, paramilitary units, security forces, and private/warlord armies may contain mercenary units as well as indigenous soldiers.

"Non-Political" Roles of the Military

Militaries play a role in the society in which they exist and influence its development and function. Some of the roles that the military can play (other than defense) are --

Economic

Consumer

The military consumes significant resources, including funds, material, land, technology, and manpower. Defense costs a lot and may be a nation's single greatest expenditure. Military consumption creates jobs and can have a significant economic impact, at least on a regional basis.

Producer

Some militaries, such as in Burma, China, and Brazil, produce goods and services for the general public as well as for their own consumption. Most others at least assist in the areas of transportation, communications, disaster relief, and other public works projects. A lot of military production and technology is dual-use and provides benefits and spin-off products for the rest of society; e.g., cars, trucks, jeeps, electronics, and medical advancements.

Social Leveler

The military in many countries provides a path of social mobility for disadvantaged groups. In some countries, the upper classes disdain military service, so the middle and lower classes serve instead. The military also provides educational and training opportunities, ranging from basic literacy and other skills to advanced degree programs. This training often carries over into civilian life once the soldier has been discharged, providing a pool of both skilled labor and trained, experienced managers. Many countries go even farther and provide preferential treatment for former servicemen in civilian education and training programs. Whereas the military may provide an avenue of advancement for lower classes or minority groups, this can also lead to class conflict within the military or between the military and the ruling class. Similarly, in many countries participation in the military by certain groups is restricted.

Nation Building

When the military is the best-organized, strongest, most capable force in a country (and normally has a number of technical and problem-solving skills), it may be the entity best able to conduct sustained collective public activity. This may involve the exploration or settlement of border regions or other frontiers, such as during the 19th Century in the American West, in China, and in the United States and former Soviet space programs. It can include civic action projects such as building schools, hospitals, sanitation facilities, or resettlement villages. It can provide infrastructure such as bridges and roads, wells, canals, and irrigation systems. It can provide medical services, education and training for the general public as well as for soldiers.

The military can also provide citizenship training and some sense of national identity among the people, both through the training and indoctrination of recruits and through programs designed to inculcate the public with national values. Finally, the military can contribute to nation building by providing security and protection for the people and infrastructure from invasion or insurgency. This allows the government to establish legitimacy and the society to develop with stability.

Source of Force

The state is usually the sole legitimate source of force, and the military the primary medium to use it. The expertise of the military profession is the "management of violence," and this expertise can extend or restrict the control of a government.

Foreign Influence

The military can influence foreign countries positively and negatively. As a tool of foreign policy it provides influence along a spectrum ranging from exchange visits to foreign military training to advisors to shows of force and outright belligerent action. Territorial defense, its most universally accepted role, dissuades or repels invasions.

Political Roles of the Military

The non-political roles of the military have significant political implications. Moreover, since the military is a powerful, well-organized and well-disciplined institution, it is a political force just by existing. Although there may be clearly differentiated areas of responsibility between the civilian authorities and the military, the expertise and knowledge vested in the military also make it a significant political factor. The analyst determines how and to what degree. For example, what are the legal and historic parameters for military involvement in politics? What are the channels for military decision making, expression, and dissent?

In many developing countries, the armed forces have major political roles beyond what we in the United States consider appropriate for own forces.

Military involvement in politics varies from simple influence to direct military control of the political process.

Influence

The military is always one of several government agencies contending for power, position, and resources. Although there may be well-defined areas of responsibility between civilian and military authorities, the military may try to expand its own numbers, acquire larger revenues, and enhance or perpetuate its own position in the system. Either individual soldiers in key positions or the military as a whole can do this.

Active Participation

In some systems, the military plays a central rather than peripheral role in the political process. There are still clearly defined areas of responsibility among branches of the government, but the military may have certain veto authority and administrative duties. Soldiers may even occupy certain cabinet positions. The military may also put certain limits on the political process by delineating who it will or will not accept as a government leader.

Military Control with Partners

In this case the military is clearly in charge of the political system, but it has co-opted civilian technicians and bureaucrats. This type of government typifies "military regimes."

Praetorianism

In a praetorian state the military dominates politics. Perlmutter defines praetorianism as "A political process (as well as a type of government and type of civil-military relations) that favors the development of the military as the core group of the ruling class." A praetorian state is one in which "the military intervenes with and tends to dominate the executive."

Non-intervention

The military's refusal to act may render a government impotent, thus bringing it down. An example of this is the withdrawal of active military support for the Marcos regime in the Philippines in February 1986, leading to the accession of power by Corazon Aquino.)

Military Intervention in Politics

Definition

This section describes military interventions that are not part of the current accepted or legal system. These interventions forcibly substitute the military's policies and/or leaders for those of the civilian government.

Sub-coups

Displacement
The military intervenes directly by removing or otherwise neutralizing politicians, officials, bureaucrats, elites, or groups in an illegal, extralegal, or unconstitutional manner. They may also replace such parties with military members.

Pressure, Blackmail, and Threat
The military intervenes indirectly by forcing the government to act according to the military's agenda.

Intervention by Invitation or Default

The military may gain influence or political power under conditions not of its own making. Civilian authorities may ask the military to step in if the civilians feel incapable of governing, as in Burma in the late 1950's. The military may also be the only institution to survive domestic social and political turmoil, gaining political power by default. An example of this is the large number of government positions held by soldiers in China at the end of the Cultural Revolution in 1976 after several political leaders had been killed, imprisoned, or banished.

Characterization of an Intervention by the Military

Reason for the Intervention

Usually the military characterizes an overt intervention as necessary. Relying on a broad interpretation of national defense, the military moves to protect the country from the threat of weak, corrupt, and incompetent politicians, or to resolve a crisis. Even if the reasons for intervention are less noble (e.g., class, regional, ethnic, corporate, or individual self-interest), the military will cloak or justify its actions in the rhetoric of patriotism, national interests and security.

Planned Duration of the Intervention

The military usually asserts that an intervention is temporary, and promises to restore normal government when the conditions prompting the interventions are gone. However, sometimes the military is reluctant to relinquish power and return to the barracks.

Military Coups (*coups d'etat*)

Definition

A military coup is a forcible takeover of the legal government by the military.

Actors

With exceptions, field grade officers of the national army usually plan and lead intervention or *coups d'etat*. Since senior officers are normally part of the ruling elite and have a stake in the status quo, coup leaders may see them as part of the situation-giving rise to the coup. A senior officer or a junta of senior officers may end up in power, but field grade officers normally instigate interventions. Company grade officers, NCOs, or the rank and file usually do not have the expertise or the span of control necessary to plan and implement a coup. Similarly, police and militia forces normally do not have the national command structure, organization, and orientation necessary to intervene.

Results

Once the military has taken power, it has four basic options. It can either return or retain power, or it can expand or restrict political participation. If the military intervenes because of specific policy grievances, it may restore civilian rule once those grievances have been corrected. Intervention prompted by a breakdown or distrust of the political system as a whole, however, usually leads to the establishment of a praetorian state. Once the military takes power, only rarely does it succeed in building more effective democratic political institutions.

Instead, military rulers are often "civilianized" and political parties and electoral systems bent to meet the desires and needs of the military regime.

Despite the military's assertions that the intervention is temporary, military rule is generally of long duration. More important, once the military has intervened, it is likely to intervene again, assuming it gives back power in the first place.

Similarly, if the military does intervene, it is usually unable to govern a complex society on its own and must, therefore, co-opt the civilian structure, if for no other reason than to establish its own legitimacy. Since it is hard to govern indefinitely by brute force, and since militaries are not usually adept at handling the subtleties and complexities of running all aspects of a country, cooperation with certain civilians is essential. Those civilians are usually willing to cooperate once they realize that their own prerogatives are not threatened by the military regime. This leads to "military control with partners."

Indicators for Intervention

The only states that seem relatively safe from military intervention are well-established Communist totalitarian states and well-established liberal democracies. Even these states are not immune, as the French experience in Algeria in the early 1960's attests. The following indicators apply to most military interventions.

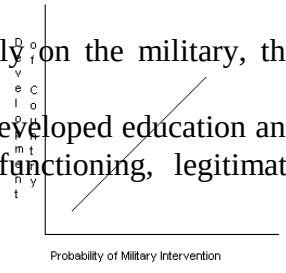
Indicators in the Military

- Heritage of Intervention. Regardless of their legal mission and role, militaries do not ignore their historical role. By far the most consistent predictor of a military coup is a previous coup. Moreover, the more coups have occurred, the more likely is a subsequent coup.
- Delineation of Responsibilities. The more clearly defined are the areas of responsibility between the military and the civilian authorities, the less likely is intervention. This clear delineation also facilitates civilian control of the military.
- Civilian supremacy as a totally accepted rule. This grossly inhibits intervention. See *Civilian Control of the Military*, below.
- Readiness. The fear that politicization will destroy the military's ability to fight reduces the probability that they will intervene.
- Fear of Failure. The military may fear that losing the intervention will bring about the end of the military. This deters intervention.
- External and Internal Mission. Risk of intervention is also reduced the more the military is oriented on defense against an external threat. Conversely, the use of the military to quell civil unrest increases the possibility of intervention. If the government uses the military against political opponents, especially against the advice of the officer corps, intervention is even more likely. Furthermore, the more involved the military is in internal issues, the more political it becomes. Finally, militaries which are active in civic action operations are less likely to intervene. It is therefore important to distinguish clearly between the international and domestic duties of the military, police and/or militia.

- Guardians of the Nation. The explicit or implicit mission of soldiers to be the saviors or guardians of nation or the constitution stimulates intervention when either is in danger. (Note that the constitution may prohibit intervention.) Note that this distinguishes between a mission to serve and protect the nation from a mission to serve and protect the government. Furthermore, when the military identifies itself as embodying national interest, it feels entitled to intervene.
- Ulterior Motives. The military may use the nobler motives of national interest and patriotism to disguise protection of a sector (the rich), a class (elites), the military itself, or for motives of pure careerism.
- Divisions in the military. Certain factions in the military may be at odds with other factions. In many coups, these factions separate themselves and pursue their agenda through intervention. On the other hand, such disagreement or factionalism may inhibit the military's ability to intervene.
- Geography. Military units scattered throughout the country or deployed overseas are less able to intervene than if they are concentrated in the national capital.
- Specialization and division of labor. The more technical the military is, the more complex and well-defined missions and responsibilities are within it, and the less chance there is of intervention. Ground forces are more likely to intervene than naval and air forces because the army is usually the largest but the least complex of the uniformed services in a country. In many cases it is deployed in large numbers in the vicinity of the capital, often as a "palace guard."
- Political awareness of the officer corps. Generally, the more politically sophisticated the military in general, and the officer corps in particular, the more likely is an intervention.
- Consciousness of kind. Militaries with extreme senses of being distinct, special, and elite, are more emotionally capable of intervening.
- Sense of power. To the extent that militaries see themselves as overwhelmingly powerful, they may be disposed to intervene.
- Grievances. A military that believes itself already the victim (or under the threat) of some societal or government wrong is more willing to seek redress against the offending system.
- Defeat in war. A defeated military, especially if it feels the government had somehow let it down, is more likely to intervene.
- Officer recruitment patterns. Officers of the same social strata of the governing elite are less likely to initiate or participate in interventions.

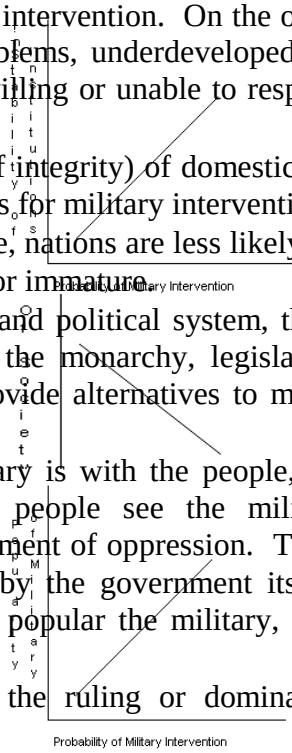
Indicators in the Situation

- Domestic Circumstances. In all cases there is a plausible national "reason" for a military intervention. Overt crisis, latent crisis, or a power vacuum all provoke the military to intervention. If they are not the real cause, they may be the putative cause.
- History. Countries with one coup have a far higher probability of a coup than countries with no coups in their history. Countries with more coups are more susceptible. The more recent the coup, the more probable the next.
- Civilian dependence on the military. Where society relies heavily on the military, the military has more opportunity for successful intervention.
- Development of the Country. As a rule, a high literacy rate, well-developed education and communication systems, urbanization and a well established, functioning, legitimate



political system in the country, all tend to inhibit military intervention. On the other hand, agrarian societies with serious economic and social problems, underdeveloped education and communication networks, and a political system unwilling or unable to respond to the needs of the nation face a higher risk of intervention.

- Stability of the Country. Perceived disintegration (loss of integrity) of domestic, political, economic, and social institutions is one of the main reasons for military intervention.
- Political Culture. Where political culture is high or mature, nations are less likely to accept intervention than in nations where political culture is low or immature.
- Complexity of Society. The more complex the society and political system, the less the chance of intervention. Other foci of power, such as the monarchy, legislature, labor unions, the bureaucracy, and opposition factions can provide alternatives to military rule and, therefore, inhibit intervention.
- Popularity of the Military. The more popular the military is with the people, the more likely the chance for intervention, especially if the people see the military as a counterbalance to the government rather than as its instrument of oppression. The military may even be asked by the people, and in some cases by the government itself if it is threatened with popular revolt, to take over. The more popular the military, the greater their perception of their actions being accepted.
- Ethnic and Class Cleavage. If these conflicts attack the ruling or dominant group, likelihood of military intervention rises.



Civilian Control of the Military

Importance

Civilian control of the military is a characteristic that typifies nations free from military intervention. Whether it exerts a causal, inhibiting effect is academic. However, many of the factors, characteristics and circumstances that accompany or facilitate civilian control of the military relate closely to factors that do inhibit intervention.

Constitutional Constraints

Nations constrain the military by placing a civilian commander in charge of the armed forces or by explicitly subordinating the military to a civilian governmental organ. They can vest power in the civilian legislature to raise and maintain armies and navies, to conduct investigations, to declare wars or states of emergency, and to pass or approve budgets. Almost all countries have constitutions or laws that specify civilian control, but constitutional restraint requires the willing acquiescence of the military.

Ascription

This is where the military identifies closely with the political system and the ruling class. This can be done by integrating the military with social forces or by keeping it separate from them. The integration occurs in three ways:

- Class congruity. The military, especially the officer corps, can come from the same social class as the ruling elite. This has been true especially of West European armies. Even in

colonial armies, the officer corps has had ties to the homeland and generally did not even intermarry with the natives.

- Nation-in-arms. The country requires universal military training and service. This guarantees security by total participation of the polity. There is a small professional military core. The army comprises citizens who become soldiers in time of crisis; however, these soldiers do not permanently set aside their civilian roles. Government civic education is tied to military training and defense. The civilian militia may act as a counter to the threat of a coup by the professional army. Civilian-educated officers often serve a similar purpose. This system is used in Switzerland, Israel, and to a degree in postwar United States.
- Party control. Placing the military under control of the "party" integrates it with social forces. Communist countries use this means.

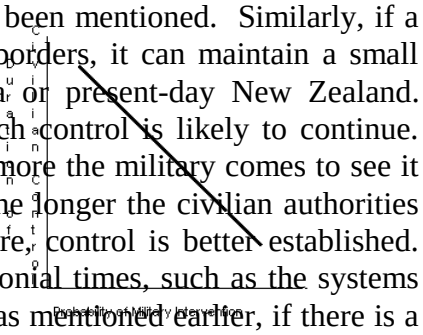
Separating the military from society. Drawing the military from certain areas or groups and stationing them in places other than their home regions or in remote borders and frontiers accomplishes this. This was common among colonial armies, who not only set large numbers of soldiers' abroad but also recruited locals from what they called the "martial races," such as the Gurkhas or the Sikhs. Many countries, including the former Soviet Union, China, and 19th Century America, have practiced stationing troops along borderlands or in frontier regions.

Army of the Ruling Party

Many Communist countries use this means to enhance civilian control. Communist revolutionary armies politicize the masses as part of their overall strategy. Revolutionary guerrilla warfare is as much political as it is military. Once in power, the party continues to use its parallel apparatus of the commissariat to control the military. Many countries also give preferential treatment to soldiers applying for party membership, causing soldiers to identify with the goals and well being of the party and, therefore, the state. In a Communist political system, party hegemony is linked to military power. The military is the linchpin of the party-state relationship.

Geography and History

The benefits of stationing forces in remote areas have already been mentioned. Similarly, if a country is relatively isolated or has no serious threat on its borders, it can maintain a small army, which is easier to control, such as in early America or present-day New Zealand. Additionally, if a nation has a history of civilian control, such control is likely to continue. Civilian control is self-perpetuating. The longer it exists, the more the military comes to see it as proper, and military intervention as unnatural. Similarly, the longer the civilian authorities govern, the more experience and expertise they gain; therefore, control is better established. This can even be true of armies who trace their history to colonial times, such as the systems extant in India, Malaysia, and Singapore. By the same token, as mentioned earlier, if there is a history of intervention, then intervention is likely to recur.



Clearly Defined Spheres of Responsibility

This factor is perhaps the most important.

- Military. The wider the sphere considered appropriate for military involvement, the greater the chances for intervention in politics. The more well defined and restricted the military sphere of responsibility, the less the probability of intervention. However, a corollary to this is that the military should have relative autonomy within its own areas.
- Civilian. Civilian interference in military affairs is just as unpalatable, and in some cases just as risky as military interference in civilian affairs. The best protection against military intervention may be legitimate, widely supported, effective political institutions on one hand, and a voluntary restraint on behalf of the military and civilian authorities alike not to use the military for domestic security on the other.

III. Analytical Questions

The answers to the following questions relate directly to the principles stated above.

- What is/are/constitute the military forces of this country? Who says?
- What is/are their organization(s)? Makeup? Roles? Missions? Practices?
- Are there inter/intra-service rivalries? Cliques? Factions? Why? How? Who?
- What is the nature of the defense establishment?
- How significant is the military economically? In what ways? Producer? Consumer?
- Are military responsibilities delineated clearly? Does practice follow the delineation?
- Does the military serve and protect the nation or the government?
- What internal (domestic) roles does the military have? What have they done?
- What external roles does the military have? What have they done?
- What is their capability to defend? Attack? State of training? Equipment? Maintenance?
- Who are the soldiers? Officers? Where do they come from? How are they educated?
- What is their economic and social status? Are there restrictions? Preferences?
- How is the military organized politically? By unit? By year group? By branch?
- Are any military leaders part of the elite? Do they go on to become elites?
- What are the legal limitations on the military? Are they clearly defined? Clearly obeyed?
- Is it subordinate to civilian authority? How? How much? How long?
- Is the military apolitical or political? In what ways? How much? Which part?
- Is it cohesive? Are there opposed factions?
- Is it geographically dispersed? Are there units near the capital? The border?
- Does anything threaten the military? Budget? Limitation of influence?
- Is this a military regime? Military control with partners? A praetorian society?
- Have there been coups? How? When? Why? Who did it? The surrounding circumstances? How many? How recently?
- Does the public think the coup(s) was (were) a good thing?
- How long did the military stay in power? How did they relinquish power?
- How does the military handle its weaknesses at governing?
- Is the country well developed? Is literacy high? Are the people informed? Are there social and economic problems?
- Is there a crisis? Is the government solving the problems?
- How long has the government been democratic (if at all)?

- Is there popular support for the military?

IV. Inter-relationships with other Pol-Mil Factors

- History: The primary predictor of military intervention in a country is prior interventions and their nearness in time. Likewise, all military behavior is as predictable (or unpredictable) as any other human endeavor, using history as the basis.
- Natural Environment: In many countries, nation building requires the military to tame the environment. Conversely, the environmental truths of countries often define the role and makeup of the military. Coastline determines the size of the navy. The number of boundary nations determines ground forces. The extent of the hinterlands affects the capabilities and the use of the air force. The military's success or failure in natural disasters may affect its prestige, legitimacy, acceptance, and overall influence.
- Cultural Environment: Culture determines the makeup and acceptance of the military, as well as its roles.
- Political Systems: Political systems determine the legal basis for the military and the politicization of its members. The robustness of political systems determines the probability of military intervention.
- Political Economy: Militaries consume and produce. They enforce customs rules, protect national waters and lands for enterprise.
- Ideology: Militaries constitute guarantors of ideology as it becomes policy. Military culture often reflects national ideology, especially as it relates to patriotism.
- Religion: In some cultures, militaries are comprised of soldiers of one religion. In some cultures, religions prohibit or discourage military service.
- Foreign Influence: The military might constitute a national resource to exert influence on other countries, or resist influence from other countries. Some militaries are linked to other states through shared military histories or current operations and cooperation.
- Leadership: Many nations recruit leaders from the military, and in praetorian societies and military regimes, the military are the national leaders.
- Regional Perspectives: The strength of a nation's military, especially compared to the militaries of other nations, affects its outlook in international affairs -- how it forms alliances, and how it pursues solutions to problems.
- National Interests: As reliable, competent and obedient bureaucracies, nations view their militaries as mechanisms to pursue their interests.
- Ethnicity: Many militaries draw enlisted and officers from certain ethnic segments of society.
- Elites: As in leadership, the military may contribute its leaders to the elites, or may form the main elite structure for the nation.

V. Conclusion

The military plays an important role in virtually every nation, serving as both cause and effect. Determining the nature of that role, and its relationship to other analytical factors, may enable you to better explain and predict important events, recommend appropriate policy, and generate sound courses of action.

References {Annotated}

Finer, S.E. The Man on Horseback: The Role of the Military in Politics. The Man on Horseback: The Role of the Military in Politics. 2d Ed. Baltimore, MD: Penguin
Books, 1965, 1972. {Provides a well documented and supported model of when, why, and how militaries intervene. Discusses how motive, mood and circumstances affect military intervention, and describes military regimes. Finer's discussion of military professionalism as a factor was also a source, but not under that title, because of the contradictory use of the term.}

Janowitz, Morris. Military Institutions and Coercion in the Developing Nations. Chicago and London: The University of Chicago Press, 1977. {Janowitz uses comparative analysis to establish categories, patterns, relationships, and indicators that describe and explain political-military relationships.}

Perlmutter, Amos. The Military and Politics in Modern Times: On Professionals, Praetorians, and Revolutionary Soldiers. New Haven and London: Yale University Press, 1977, 1978. {This book describes military professionalism and corporatism, and describes the traits of the soldier. It establishes categories across the gamut of political-military relationships, and then maps these categories across geography and history. The book specifically addresses the following geographical cases: Prussia-Germany, France, Japan, USSR, Africa, the Arab states, Latin America, China, and Israel.}

Permutter, Amos, and Valerie Plave Bennett, eds. The Political Influence of the Military: A Comparative Reader. New Haven and London: Yale University Press, 1980. {This is a great collection of writings on military in politics. It contains several articles about professionalism in the military. The conflicting views on professionalism justify its omission here as a separate factor. Also, the book has articles on praetorian regimes by region, and the history of praetorian societies.}

Welch, Claude E. Jr., ed. Civilian Control or the Military: Theory and Cases from Developing Countries. Albany, NY: State University of New York Press, 1976. {Welch places nine case studies between two of his own articles on the subject. His first article describes the attractiveness of civilian control, and provides a model to analyze the extent of civilian or military control of government. His last article prescribes methods to attain or enhance civilian control of the military. The case studies cover India, Malaysia, the Philippines, China, Japan, Finland, Mexico, Lebanon, and Chile.}

With Arthur K. Smith. Military Role and Rule: Perspectives on Civil-Military Relations. North Scituate, MA: Duxbury Press, 1974. {This work constitutes a solid primer on analysis through case studies of military intervention and military rule. The first section of the book posits principles of intervention. The second section provides case studies from Thailand, Nigeria, Peru, Egypt, and France. The last section analyzes these case studies to validate the principles proposed in the first section.}

Chapter 11

Leadership

I. Introduction

Even though we personify countries when we say things like "Russia announced today that . . ." or "Egypt today took action to . . .," usually some leader caused or influenced the action. Accordingly, explaining and predicting the leader's actions help to explain and predict the country's actions.

II. Definitions

Leadership occurs when, in a context of competition and conflict, people with motives, purposes and resources mobilize other people in order to realize goals independently or mutually held by both leaders and followers. (Burns, passim.) Leadership may be legal, illegal, or extralegal.

Leaders exercise power and authority.

Power is the ability to mobilize or immobilize people to produce intended results for particular purposes. The exercise of power may be legal, illegal, or extralegal. It relates to the purpose or goal of the power-wielder only. National leaders obviously have power (as do robbers, rapists, priests, parents, oligarchs and Army officers). Brute force is one form of power, but not the only one.

Authority is the legitimate exercise of power. When people recognize the right of a person or group to wield power over them, even to the point of using force, then that person or group has authority. Authority may be acquired through special training, conferred by virtue or one's position, or both. Army officers, teachers, and policemen all have authority, even though many of them may not be leaders per se. Again, concern for effects is largely one-way.

Relationship of Leadership, Power, and Authority. Leadership transcends power and authority because it incorporates the goals and aspirations of the subordinate as well as the leader.

The expected response from the led conditions the behavior of the leader. The leader may be able to mobilize others for his own purpose, but more often he is "merely adept at identifying himself with the conditioned will of the crowd and identifying for the crowd its own purposes." (Galbraith, pp. 44-45.)

The leader articulates, defines, or creates goals and objectives for the followers. He may do this by making their goals his, his goals theirs, or both. He may arouse latent attitudes and desires or give rise to new ones. He can establish an identity for the crowd, showing its members what they have in common; e.g., Mao and the Chinese peasant. In

so doing, the leader can change an amorphous mass of people into a powerful political force.

Effective leadership tends to appeal to higher, more general and comprehensive values that will embody the more fundamental, mundane needs of the follower.

Types of Leadership

James MacGregor Burns distinguishes between two types of leadership.

Transactional leadership. The leaders and followers exchange something for something; e.g., jobs or lower taxes for political support, cooperation and obedience for promotion. The exchange may be on a political, economic, or psychological level. This is the kind of leadership the vast majority of leaders exercise. It is also the kind of leadership most of us exercise as Army officers.

Transformational leadership. The transformational leader looks for potential motives and attempts to engage the full power of the follower, satisfying the follower's higher needs, and raising him to a higher level of motivation and morality.

This leader acts as a moral agent. He may be "inspirational." Again, this leadership is symbiotic, and considers the needs of the follower.

While transformational leadership is rare, it is what most military officers like to believe they are exercising. (Burns only uses "transformational leader" for those who take their followers to a higher moral plane. Other scholars feel that this is too restrictive. To them, all the leader has to do to be "transformational" is to transform his followers, for good or ill.)

Although a transformational leader must also engage in transactional leadership, someone who is adept at one may not be at the other. A good transactional leader may be better able to hold his position through good management practices than a transformational leader who rises by sheer force of personality--only to get mud on his toga once in office.

Culture and Leadership

Social and cultural contexts help explain leadership. Culture plays a role in shaping the needs, values, and personalities of leaders and followers alike. What, in each culture, confers the mantle of leadership?

To accomplish his goals, the leader must direct the behavior of others. How he does this will vary greatly among societies. Cultural norms create expectations and judgments regarding the appropriate behavior of leaders and followers. These norms may be mystical or religious, practical or technical.

Since these norms differ, Pye points out that political leaders don't travel well across cultural lines. There is no such thing as the leader for all people in all societies at all times.

(Leaders in one culture can be effective or have significant influence in another society. However, he probably will not achieve leadership status outside his own culture; e.g., Gandhi. Leaders may also come to power in spite of cultural obstacles; e.g., Indira Gandhi of India, Bhutto of Pakistan, and Sirimavo Bandaranaike of Sri Lanka.)

The culture helps determine the centers and sources of leadership in the society. These may include interest groups, government bureaucracy, military, media, political parties, trade unions, universities, or religious organizations. Some will support the current ruling authorities and some will be in opposition. Some will be legal or nongovernmental, others will be illegal or extralegal.

Within and among these centers an analyst can discern the mode of distribution, or the formal numerical distribution of leadership roles; the mode of mobilization, or the means available to leaders for carrying out their roles; and the means of allocation, or the types of leadership opportunities that exist, the purposes and methods of training new leaders, and how individuals and groups gain access to leadership positions. (Rosen in Kellerman, pp. 39-42.)

How a leader becomes a leader.

There are at least six ways that people can assume positions of leadership. They may also occur in combinations.

- Inheritance. This is common historically, especially in societies where the upper classes were specially trained for leadership as part of *noblesse oblige*. Where this phenomenon is found today, ascription and achievement usually go hand-in-hand. Someone may gain initial access to leadership positions by right of birth, but must undergo special training and prove themselves worthy of leadership. Leaders in societies as diverse as Britain, Japan, and North Korea still assume leadership positions through inheritance.

- Force or threat of force (military coup or rebellion).

- Ideological appeal (Gandhi).

- Foreign support and assistance.

Starting one's own organization. This normally occurs when the needs of the leader and those who follow him are not being met through existing organizations. People who achieve significant positions of leadership in a society via this mechanism usually do so in times of crisis.

- Institutional selection. This is the most common today. Positions and duties of leadership are formalized by one's predecessors and by regulations and codes. The leader comes up through the institution, holding lower offices in successively more responsible positions. At the upper echelons, leadership within the institution can translate into national leadership. This does not necessarily mean that the process is democratic. Communist parties and the military are two examples of organizations that have undemocratic institutional leadership selection processes.

Aspects of Leadership

Leadership can be better understood if looked at as a system where the leader, in conjunction with the follower, mobilizes resources and means to accomplish goals for particular purpose within an environment of conflict. The following model reveals several aspects of leadership.

o Leadership is purposeful. Naturally, the purpose must meet the needs of the leader and followers alike once it is achieved.

o Leadership is goal oriented. Leaders point a direction and tell how objectives are to be accomplished.

o Leadership is causative. Leaders affect social relations and political institutions, if only to maintain them. The leader tries to bring about change. Good leaders bring about intended rather than unintended change.

o Leadership is dissenting.

Leaders overcome obstacles in the environment to accomplish goals. Without obstacles, his followers could accomplish their goals on their own. Obstacles include opposition groups, laws, scarce resources, and cultural constraints.

Conflict also exists between leader and follower. Followers have goals and agendas which may not fit snugly with those of the leader. Few will agree with their leaders on all issues. Leaders must reconcile divergent groups and resolve conflicts among their various constituencies. This is especially true in political parties.

Conflicts may also arise between party bureaucrats who want to serve party interests, and government officials who are party members but who feel a responsibility to serve the needs of a larger constituency.

o Leadership is social.

In the symbiotic relationship between the follower and the leader, the leader fulfills some need for the follower, who then consents to follow. Two or more followers constitute a group. Individuals join groups to add their voice to others with similar ambitions, gaining access to a wider audience. Through the group the individual

converts personal effort into social action. Leaders, then, must not only meet individual needs but also group needs.

Leadership does not have to be governmental, but it is institutional; e.g., Lech Walesa or Desmond Tutu. However, it is not enough for a leader to meet the needs and wants of large numbers of followers. The leader must also be aware that in doing so he reorganizes the needs and goals of the followers, creating new wants and needs in the process. He must then be prepared to help formulate those new demands as well and to meet them. This is done through an organization.

Organization in Leadership

Organization is the most important source of power for leaders in modern society. Usually, that person whom we call a "strong" leader not only has a dominant personality and other personal "leader" traits, but also a strong group or coalition of groups behind him. Similarly, a "weak leader" is generally one whose supporters are few or poorly united. Obviously, personality may be closely related. A leader with a strong personality will draw large numbers of people to him, which may allow him to garner more influence if he can incorporate them into his organization.

Subordinate leaders are a significant part of an organization. Each leader deals with subordinate leaders who have needs, goals, and resources of their own. Second and third echelon leaders are a significant part of the leadership system. A change in subordinate leadership may signal a change in policy. It may also be a source of unintended change because of the way the new subordinate implements policy. Moreover, the type of subordinates he has can provide some insight into the type of person the leader is. First-rate leaders surround themselves with first rate subordinates, while second-rate leaders surround themselves with third-rate subordinates.

The ostensible leader may not really be in charge of an organization. Government decisions are usually collective. One particular leader may get the credit or the blame, such as in the "Bush administration," the "Thatcher government," or the "Mubarak regime," but politics is by and large a team sport. This collective nature of governmental leadership can make it difficult to distinguish just who the most important leaders really are.

"Headship" is not necessarily leadership. There are several heads of state who are merely figureheads, while the head of government actually runs the country. Similarly, economic and social status do not necessarily equate to political leadership; e.g., Malaysian Chinese or Buddhist monks in Southeast Asia. The real leader may not be the person nominally in charge, but the one who gets things done; e.g., Deng Xiao-ping in China. Determine where the real power lies. Only some ministries and committees in government or other positions in society are most important (for example, the Senate Armed Services Committee or the House Ways and Means Committee in the U.S. Congress, the Military Affairs Commission in China, or the Catholic Church in the Philippines). The same is true for opposition groups. In most environments, the

opposition has power and can exercise leadership. Even leaders who may currently be out of favor can exert influence or play roles in the future. Deng Xiao-ping was purged twice before he last came to power in China. Ayatollah Khomeini was in exile for years before he came to power in Iran.

Personal Characteristics of the Leader

o Maintaining power. No matter how effective he may be, no leader is omnipotent. Accordingly, his first order of business is to maintain and/or enhance his position. Because of the friction between leaders and followers, there will always be a system of checks and balances, both formal and informal. As a result, the leader will believe that he has insufficient power to accomplish his objectives and so needs to acquire more. If the checks and balances are weak, the leader can abuse the power he obtains. This is what occurs in authoritarian leadership systems.

o Feet of Clay. As a human being, the leader responds to human personal and psychological pressures. Some of these influences weigh more heavily on the leader. They might be sex (Gandhi), family (MacArthur), class, religion, age, money, health, or the spouse. The leader may be people oriented or structure/process oriented. He has an ideology, a world view, a background and a personal history. He has personal goals. He may be consistent or erratic. Someone may influence him, like Suharto's soothsayer. This type of information resides in biographical dossiers maintained at embassies and various intelligence organizations, biographies and autobiographies, and certain journals or newsletters like Defense and Foreign Affairs Weekly or Current Leaders. Retroactive psychoanalysis of past leaders may reveal a lot about leadership in the culture in which the subject lived.

III. Analytical Questions The answers to the following questions relate directly to the principles stated above.

o Who is the true leader of this organization?
o Does this organization exercise real power or influence? How?
o What factions support the organization?
o Who are its members?
o Is it strong? Well supported? Widely supported? By whom?
o What motivates this leader (money, sex, recognition, power, ideology)?
o How did the leader come to power? Is he charismatic?
o How do leaders come to power in this organization? In this culture? Does he have those traits?
o Did he come to power via normal channels or did he circumvent them?
o What are this leader's strengths? Weaknesses? Desires?
o What strong lessons has he learned through success? Failure? Difficulty?
o In which environment does he thrive?
o Is he an "organization man" or a maverick?
o Does he fit the traditional mold, e.g., right family, right school, or is he an upstart?
o To whom is he beholden? What are their goals?

- o Who are his confidants?
- o Is his focus on international affairs, domestic politics, economic and social issues, or defense?
- o Are his management approach and leadership style autocratic, democratic, or laissez faire?
- o Does he share power or hoard it? With whom does he share?
- o Does he make decisions with input from others?
- o Do others actually participate in the decision-making process, or does the leader make the decision and then seek or demand support for it?
- o What type of people does he surround himself with?
- o Is he reluctant or too quick to make decisions?
- o What threatens his position? His organization? His goals? His organization's goals?
- o Who are his subordinates? Which can be leaders?
- o Is there succession? How does it work?
- o What friction is there between the leader and the led?
- o Has the organization changed personnel recently? Why? Who caused it?

IV. Inter-relationships with other Pol-Mil Factors

o History: Patterns of the characteristics of past leaders repeat themselves within a region and a country. Charismatic leaders harken back to other successful leaders, and play on their similarities and differences.

o Cultural Environment: Culture determines the accepted characteristics and sources of leaders.

o Political Systems: Political systems determine the legal basis for governmental organizations, and establish the conditions for nongovernmental and opposing organizations.

o Political Economy: Economic problems create the openings for leaders. Economic successes help them maintain power.

o Ideology: Leaders identify themselves with ideologies, and may derive their power and followership with this identity.

o Religion: In some cultures, the true leaders are religious leaders. In some cultures, religious leaders exert greater influence than the political structure suggests. In other cultures, leaders must recognize and comply with religious strictures to maintain legitimacy.

o Foreign Influence: More than elites, leaders serve as the principle agents between governments, and are often the conduits or definers of international agreements and negotiations.

o Regional Perspectives: A source of legitimacy for leaders is the quality of their adherence to regional perspectives, and how their agendas and policies reflect commonly held views.

o National Interests: Political leaders articulate and openly pursue national interests.

o Ethnicity: Ethnic groups may choose leaders to represent them. Leaders may be chosen or not on the basis of their own ethnicity.

o Elites: Although a person can be an elite and a leader, elites differ from leaders in that they always represent the top of some class, while leaders need not. Furthermore, leaders must have followers, while elites need not. Finally, both leaders and elites exert real power and influence.

V. Conclusion

Because they exert real power and influence, leaders are often the immediate cause of important circumstances. Accordingly, political-military analysts must understand the leaders in a region. Explaining and predicting leader behavior will help to explain and predict national behavior.

Chapter 12

Elites

1. Introduction

Analysts study elites because they occupy the most influential positions or roles in the governing institutions of a community, or exert influence on those institutions. They are incumbents, leaders, rules and decision-makers. Watching them provides insight into the core values of a community because those core values determine what constitutes the best, what characteristics or activities are influential, and what constitutes real power. Watching them also helps establish cause and effect relationships, since power and influence define elites.

11. Definitions

- **Elites**. For the purpose of political-military analysis, elites are defined as people who:
    - **Are the best of their class.** This class can be any categorization of people, activity, or sphere of social life. Those at the top are the elite. Within their category, other members look up to them, defer to them, and often follow them. The members of the class determine who is best and how "best" is measured.
    - **Exercise power and influence.** The elites that we study are only those who exercise real power or influence. This part of the definition simply relieves you from studying excellent people who do no significantly affect the situation. Some elites have more weights than others because they exert more influence.
- **Strategic Elites.** The ruling elite, top influentials, or the power elite are other terms to describe those elites who exert their influence on society as a whole, rather than on a segment. These leading individuals or groups maintain and develop the society and its culture (patterns of beliefs and values, shared means of communication, and major social institutions) are the strategic elites. No single stratum exercises all key social functions. Accordingly, the functions and the associated elites are specialized.
- **Segmental Elites.** Elites who exert their influence on a major subdomain of society.

Types of Elites

- **Ruling Caste.** One stratum does the most important social tasks, obtains its personnel through biological reproduction, and is set apart by religion, kinship, language, residence, economic standing, occupational activities, and prestige. Religious ritual is the main force that supports the position of this ruling stratum.
- **Aristocracy.** A single stratum monopolizes the exercise of the key social functions. The stratum consists of families bound by blood, wealth, and a special style of life and supported by income from landed property.
- **Ruling class.** A single social stratum is associated with various key social functions, and recruits its members into its various segments based on wealth and property rather than of blood or religion. Historically, ruling classes have held economic rather than political power, but their influence tends to extend to all important segments and activities of society. Although various differentiated and specialized sectors may be distinguished, they are bound together by a common culture and by interaction across segmental boundaries.

Functions of Strategic Elites.

Elites focus attention, coordinate activities, and keep things working. They help a country manage problems, change, growth and crisis. Elites symbolize and perpetuate the unity of a culture by emphasizing common purposes and interests. They coordinate and harmonize diversity. They minimize factions and resolve group conflicts. They try to protect their group from external danger. These functions can be grouped as:

- Goal attaimnent, the setting and realization of collective goals. These are the current political elite;
- Adaptation, the use and development of effective means of achieving these goals. These are economic, military, diplomatic, and scientific elites;
- Integration, the maintenance of appropriate moral consensus and social cohesion within the system. These elites exercise moral authority, such as priests, philosophers, educators, and first families;
- Pattern maintenance and tension management, the morals of the system's units individuals, groups and organizations. The elites that keep the society knit together emotionally and psychologically, are such celebrities as outstanding artists, writers, theater and film stars, and top figures in sports and recreation.

Quantity and variety of elites.

- In less complex societies elites are few in number and comprehensive in their powers. In societies at very simple levels of development, one elite may perform all four-system functions.
- More advanced industrial societies will tend toward several elites whose functional specialization accompanies a growing moral and organizational autonomy among them. As populations grow, occupations become differentiated, moralities vary, bureaucracies increase, and societal leadership moves from aristocracy or ruling class to leadership based on strategic elites. A large, industrialized country, with many occupational, regional, and ethnic differences, a society with levels of power, work, prestige, wealth, and lifestyle will probably not vest leadership in a single hereditary or traditional group, or in a single ruler. Instead, these elites will probably be specialized and varied.

Elite Goals

Elites seek to:

- Preserve the ideals and practices of their societies and sub-domains.
- Maintain their status as elites. This is the most predictive characteristic of an elite.

Recruitment

Elite replacement, or recruitment, is the process of attracting and selecting suitable candidates. Recruitment occurs in two basic ways: on the basis of biological (or social) inheritance and on the basis of personal talents and achievements. One of these tends to prevail. Understanding how and why elites are recruited suggests general social tendencies toward expansion or toward consolidation. Expanding societies or subdomains recruit more on the basis of personal achievement. Consolidating groups tend to recruit based on inheritance of status. The style of recruitment reflects profoundly on social mobility, individual incentive, and discontent among social strata. Styles of recruitment affect both the composition of the elites and their outlook.

In more modem industrial societies, recruitment and selection pattern accompany differentiation and autonomy among the elites. Recruitment based on social inheritance is giving way to recruitment based on individual achievement. Recruitment may also be based on ancestry, education, experience, and training. The public elects some elites, others are appointed by predecessors or superiors. Some are born to their positions. Some elite positions are temporary, others for life.

Sources of recruitment. Some elites can be found in training or in preparation. Military academies, prestigious prep schools or universities, key postings, cathedrals and seminaries, key fraternities or clubs, and elite branches of military service are all fishbowls to spot and study prospective elites.

Rewards. This is recruitment from the viewpoint of the elite candidate. Rewards for becoming an elite may be esteem, money, power, acceptance, or merely the ability to live up to expectations. Understanding the rewards that accompany elite recruitment reveals motivation, and accordingly, sources of leverage and manipulation.

Watching Elites.

Examining the varying skills, styles, and backgrounds of elites reveals truths about the complex system they represent. The activities of these elites will in many ways reflect the desires of the heterogeneous populace they represent.

Finding Elites.

The analyst identifies elites through research. Excellent sources are:

- US Intelligence agencies (CIA, DIA). Call the desk officer for the country, and ask.
- The US International Information Program formerly USIA). Call the desk officers in Washington and in country, and ask.
- FBIS. Review the names of key parties to major events.
- Embassies, attaches, and mil-groups. All of these have up-to-the-minute information on local elites.

III. Analytical Questions.

- How does or will a circumstance or policy affect the elites?
- How do they exert pressure, influence, or power? What kind of influence? When and why do they do it?
- What are the rewards for this type of elite? Are the rewards threatened?
- Who are the elites in this society? What segments do they represent? What categories are there?
- What functions do they perform?
- What functions does the segment perform? Who does it represent? How are they recruited? From where? Are there limitations?
- Where do the elites come from? Is there a pattern?
- What is there about this elite that reflects societal patterns or trends? (If this elite is also a leader, see the questions in "Leadership".)

IV. Inter-Relationships with Other Political - Military Factors.

- History: Elites represent the historical movement from aristocracy and oligarchy to pluralistic ideologies. Often major historical events defined what are now the traditional elites.
- Natural environment: Sources of elites may be tied to environmental realities, as in the landed agricultural elite of Argentina, or the oil sheiks of the Middle East.
- Political systems: By definition, elites hold key political positions, and the nature of the checks and balances associated with those systems limit or define the associated power and influence.
- Political economy: Traditionally, wealth is a major identifier of elites. People who control wealth, such as major industrialists, form an important segment of elites in capitalistic societies.
- Role of the military: The military presents a source of elites in most countries.
- Ideology: Some societal segments or subdomains are defined by ideology. The paragons of each ideology become elites, and are strategic elites if the holders of that ideology exert power and influence.
- Religion: Like the military, organized religion is a societal segment or subdomain that is a source of elites.
- Foreign influence: From a reverse perspective, elites may be the targets of foreign influence. The Pope influenced the religious elites of Latin America by promoting "liberation theology", which enabled political activism by the Catholic clergy.
- Leadership: (see "Leadership" chapter)
- Regional Perspectives: As the representatives of various societal segments or subdomains, elites are the repository of a culture's point of view.
- National interests: Elites manifest themselves by exerting influence and power to define national interests in their favor, or to resist national policy that is not in their favor.
- Ethnicity: Ethnicity can be both a recruitment prerequisite and disqualification. Each ethnic group will have elites, and if the group is influential enough, these elites will be strategic elites.

V. Conclusion

Political-Military analysts study elites because they exert power and influence. This helps to explain and predict, and to establish cause and effect relationships. When we ask, "Who gets helped or hurt?" to find a cause or predict an effect, we look first to the elites.

Chapter 13

The Cultural Environment

I. Introduction

The analyst uses culture as an important factor to explain and predict behavior. This chapter distinguishes culture from other factors and introduces the analytical aspects of culture. The chapter does not address the use of culture in your interactions in other countries.

II. Culture and Society Defined

For our purposes, culture is learned and shared attitudes, values, and ways of behaving in a society. Culture includes customs, folkways, manners, mannerisms, etiquette, behaviors, body language, gestures, celebrations, milestones, dress, outlooks, perceptions, and thought patterns. It is embodied in history, art, myths, legends and heroes. It addresses appropriate responses to situations. It determines the circumstances and quality of apology, retribution, reward, punishment, equity, commiseration, disdain, shame, guilt, congratulations and pride. It selects and applies social sanction and reward. It expresses itself in superstitions, outlooks, perspectives, conventional knowledge and points of view. It encompasses the sense of time, individuality, possessions, sharing, self-worth and group-worth. It establishes the social hierarchy, defining roles by sex, age, position, religion, wealth, family and profession. In essence, culture defines what is and is not okay, accepted, and normal.

Culture also includes what you may call "Big 'C' Culture." This culture includes the fine arts, theater, famous artists, films, music, dance, and literature.

Culture relates to society. Society refers to those regularized mutual patterns of behavior among a specific group of people who share a geographical area and culture. Attitudes, values, and patterns of behavior characterize a society. These patterns of behavior demonstrate social organization; i.e., reciprocal rights, duties, and expectations between individuals in the group. Society and culture are interdependent concepts. One cannot exist apart from the other. However, they are not the same. Society refers to people and their social organization, while culture refers to their learned and shared way of life.

Because of differences in environment and historical experience, members of different human societies exhibit widely different patterns of behavior. Since social behavior is based upon commonly held ideas or notions of what is the correct response to a given stimulus, the most basic differences between peoples in different societies lie in the realm of ideas.

Culturally defined groups share a sense of common identity among members. This common identity works at different levels. It might be characteristic of a subgroup of society--a club, profession, or descent group. At its broadest level, it might include a collectivity called an “ethnic group."

Groups, Norms, and Values

Groups. Since we define culture as learned and shared behavior it is clearly a group phenomenon. Accordingly, an understanding of group structure and process illuminates culture. All societies are comprised of a number of groups that may be related to each other in various ways. Political-military analysis requires that the analyst correctly identifies important groups in a society and correctly assesses patterns of behavior (culture) characteristic of each group.

Primary and Secondary Groups. Behaviorally, a primary group refers to groups that are small, intimate, and informal. The family is an excellent example of a primary group. In Africa, a lineage segment (of closely related kinfolk) in a local area would be another good example. Secondary groups, on the other hand, are utilitarian, formal, and impersonal. School classes, student bodies, labor unions, and PTAs are examples of secondary groups. In America, a religious denomination would normally be a secondary group. In Senegal, an Islamic religious brotherhood might well be a primary group. A person's primary group associations are usually more important to him, and will more likely affect his behavior than his secondary group associations.

Folkways, mores, and laws profoundly influence how one society will interact with another. They can have a significant effect on interstate relations. For example, a Judeo-Christian ethic--a Western model of appropriate behavior--results in certain expectations by Americans that others share our concern for individual human rights, whether or not the foreign cultures share the same ethic. A political-military analyst is expected to be able to assess the influence of folkways and mores on the formulation of national policies.

Acculturation (Acquiring Cultural Competence)

Society's purpose is to make each member a fully responsible and functional individual within the whole. Accordingly, it does whatever is necessary to aid any one of its members to learn proper and appropriate behavior for any given social setting or situation. The individual, in becoming culturally competent, subordinates his dreams and expectations to the shared rules and requirements (norms and values), not only for the larger society but also for every specific demand within the life as a whole. The intent of society is responsible participation. Most members of the society eventually absorb the ideas and are appropriately "acculturated."

Obviously, a native-born adult member of a foreign society has a natural advantage over the analyst who is trying to acquire 30 years' cultural competence in two or three years. However, outside observers are often more insightful than insiders because of a lack of an agenda or embedded prejudices.

Social Controls

Society imposes cultural competence through social controls. A society's regular and expected patterns of behavior are called norms, and society expects its members to live by them. These norms are embodied in folkways, mores, and laws. As you might expect, not everyone in a given society always follows the norms. It follows that all societies have mechanisms for

social control. These mechanisms operate at different levels.

The lowest level of mechanism for social control is "folkways," which are the manners and customs of a culture. They catalog the "normal" way to do things. Although these are taken very seriously, law does not enforce them, and failure to follow them is not considered an act of immorality. Folkways usually refer to behavior-like manners, dress, greetings, and other such activities. The observance of folkways makes for smooth interactions in society. Rewards for compliance include acceptance, inclusion, and esteem. Ridicule, avoidance, negative comments, and similar mechanisms usually enforce them negatively.

"Mores" are more powerful social controls. These might include sexual and marriage rules and other requirements of virtuous conduct. Mores are social rules and regulations of a moral nature. Their observance furthers membership, inclusion, regard and esteem. Various sanctions enforce them, although again, scorn, ridicule, isolation and exclusion are the primary mechanisms. Society permits its members to withhold from a transgressor any discretionary good thing.

The highest level of social control is that of laws. Laws are rules and regulations that are enforced by the state. The state may legitimately use force to assure compliance. Laws usually grow out of folkways and mores.

Culture, Change, and Predicting Behavior

Ideas, models, norms, values, and behavior are always changing. Usually, the changes occur so slowly that most members of a society easily accept them. However, a variety of factors can accelerate change to the point that local models, ideas, and social organization cannot adequately cope. This is frequently the result of changes in the natural environment (drought, epidemic disease) or changes in economic conditions associated with national development.

Conditions of accelerated change often provoke regional tension, instability, and strife. The political-military analyst anticipates such circumstances and predicts the outcomes. This involves explaining and predicting how individuals in specific groups will act in response to social change. It requires an understanding of the key themes, models, and patterns of behavior in that cultural context. At the same time it necessitates a good historical perspective--an ability to recognize tendencies and patterns in similar circumstances in the past. Finally, it requires that the analyst clearly understand the range of viable economic and political options available to the group under study. Often, the analytical techniques provided by the disciplines of economics, political culture, and political science can apply.

Of course, to perform this role competently, the analyst must not only understand the processes of cultural adaptation to change but also the dynamics of change in specific natural environments and natural economies.

Language

To the extent that thought and language are interdependent, language is key to understanding

culture. No culture can be completely understood without understanding the language. Languages will be rich in words about what is culturally important, and poor in words that have little cultural significance. However, knowing the language in no way indicates mastery of the culture.

Ethnocentrism and Cultural Relativism

Ethnocentrism and cultural relativism are opposed approaches to understanding and explaining behavior in foreign-cultural contexts.

Ethnocentrism is the practice of interpreting and evaluating behavior and objects by reference to the standards of one's own culture rather than by those of the culture to which they belong. It results from the acculturation of the analyst that has internalized his own culture's norms. This internalization generates the notion that his culture's norms are superior to all others.

An ethnocentrist carries the notion to the point of defining an action as right or wrong by the standards of his own culture. Other ways of doing things make sense or do not make sense only in this light. Ethnocentrism allows a person to be satisfied and complete within the context of his own culture. However, it embodies, engenders and communicates an attitude of superiority of one's own ideas over all others. Consequently, ethnocentrism may decrease the analyst's ability to understand, explain or accurately predict behavior in other cultures. In extreme cases, it can lead to xenophobia. The Shiite fanatics of Iran provide a classic example.

Cultural relativism is the practice of interpreting and evaluating with reference to the normative and value standards of the culture to which the behavior belongs. It views the world and explains behavior in terms of the relevant culture (the culture under analysis). In this approach, behavior is appropriate or inappropriate. It makes sense and follows patterns, based upon the norms and values of that culture. The relativist carefully avoids judging others based only on his own cultural prism.

For the analyst, cultural relativism provides access to the other person's point of view and perspective. This, in turn, provides insight, competent explanation of otherwise opaque and strange happenings, and a powerful ability to predict human action and reaction.

Although a powerful analytical tool, cultural relativism should not serve as an article of faith. Extreme cultural relativism is actually derogatory of the culture being analyzed in that it assumes the absence of universal natural laws or human traits. All people bleed when cut; all cultures prohibit stealing, murder, rape, etc. Indeed, ethnocentrism provides the analyst with familiar cultural examples to compare and contrast. It tells him how different or how the same is the culture he analyzes. Finally, it provides him with a lexicon which people of his own culture can understand when he reports his findings.

Going native. This unflattering phrase describes behavior, not analysis. The person who adapts his behavior to that of a foreign culture gains a lot in his ability to accomplish missions, avoid problems and find out information. However, some people interpret these gains as signals that they can scrap their own core values in favor of the ones under analysis. At this point, they have gone native, and are of no further use to their country.

Categories, Stereotypes and Labels

Political-military analysis selects those cultural factors (categories) that particularly influence political and military behavior in a given region, and determines their likely influence on the situation at hand. It considers local groups, local social organization, key cultural themes and values, and historically sanctioned modes of adaptation to social change. Finally, it expresses these relations with precise, carefully defined terms that clearly illustrate social dynamics.

Often, one must categorize groups of people, e.g., traditional, secular, Western, Islamic, etc. However, these labels are often very arbitrary and misleading -- they may or may not conform to the way the people themselves define their social universe. Terms in popular English usage, which Americans frequently apply to foreigners with little empirical justification, further complicate identification of social groupings. For instance, we often describe Islamic residents of the Middle East and North Africa as Arabs, even when they are of other than Arab ethnic origin. Ethnic distinctions among Africans are popularly ascribed to "tribalism," even though the actual African distinctions are often more analogous to European "nationalities" or even to economically defined social classes. While the competent analyst is obliged to use labels, he must use labels with great care, avoiding imprecision and stereotyping.

- The labels that are of most interest to political -military analysts are cultural distinctions; that is, they are distinctions based upon commonalties in ideas and behavior among certain populations. Within this very broad category are a number of subcategories. These, too, are labels that require careful use.
- Distinctions among language, cultural values, and sociopolitical cohesion also provide insight. For example, what analytical category does the word Jewish suggest? Is it a religious, racial, national, cultural, or linguistic term? Who is a Jew? It is such a complicated issue that the definition has never been officially defined in Israel. Obviously at times the term Jew has been used in all categories. For instance the term “anti-Semitism” generally refers to anti-Jewish prejudices. However, the word Semitic refers to a language family to which both Hebrew and Arabic belong. Therefore, technically speaking anti-Semitism refers to Arabs as Jews.
- Do not confuse patterns in human physical features with patterns in human behavior. Human distinctions based on differences in outward <u>physical appearances (phenotype)</u> might not correspond to differences in cultural norms and values. An example would be Americans of Asian descent who exhibit very <u>few</u> behavioral traits unique to the Asian society of their ancestors. Although some human populations do exhibit a higher incidence of unique physical or genetic traits within themselves, the analyst must avoid stereotyping groups by phenotype.

Analysts must be very careful in the use of labels. If a term that is primarily a linguistic category might not imply the corresponding social or political correlation. Not all-native speakers of English are ethnically English nor are they all subjects of the English sovereign. If the term (Hausa, Swahili, or Somali) designates a general ethnic group, a corresponding political cohesion does not necessarily apply. For example, neither foreign nor domestic scholars agree on the meaning of 'Arab'. Is it a linguistic group, a race, a culture, or simply a political term?

The word 'Arab' conjures up very different perceptions by different people in the Middle East. Must all Arabs be Muslims? Some Muslims would adamantly affirm that they are synonymous. Christian Arabic speakers of Jordan, Iraq, or Palestine would vociferously deny that. Are all people of an Arab nation Arabic? The Maronite Christians of Lebanon have died by the thousands to assert their distinct cultural identity. So it goes, and every Arab summit convened will be ripped asunder by the same unanswered question: "Who/what is an Arab?"

A clear distinction should be drawn between terms that primarily describe shared cultural identity, such as "society" or "ethnic group" or "nation," and terms that have primary reference to a governing political structure, such as "state." A political-military analyst must be able to discern the difference and understand the ramifications of this distinction for a specific region.

In many areas of the world, primary cultural identities do not correspond to state boundaries. The contradictions between the culturally specified identities of local populations on the one hand, and the identity of a recently created state on the other, force national decision-makers to devote considerable attention to nation building. By definition, this involves efforts to undermine peoples' loyalty to other institutions. India and Nigeria are good examples. Occasionally, these attempts threaten regional stability or great power interests.

Many states of Western European design are typically formal, secular, and territorial in nature. Other states contain societies with various systems of government that may or may not interface well with the national political structures. In times of transition and stress, societies often display tendencies to reacquire and redefine social or political behavior hallowed by tradition that supposedly characterized a better, earlier age. When this is combined with religious revitalization, the results can be revolutionary. The Mahdiya in the Sudan in the 1880's and the Ayatollah Khomeini's revolution in Iran are good examples of this. The political-military analyst should be able to anticipate such events by noting the historically sanctioned behavior exhibited by a society undergoing great stress.

The competent analyst must be able to sort factors and apply labels that assist in understanding social organization and behavior. He or she must know when certain factors and labels are important and when they are not. Good political-military analysis requires an incisive elaboration of the ideas behind collective behavior. To achieve this, great precision in the use of categorical labels is of paramount importance.

The following table, created by Dr. Gary Weaver on pages 75 and 76 of his book Culture, Communication and Conflict, lists many of the terms, factors, categories and labels that sociologists and anthropologists use to analyze cultures. Further study will illuminate what these terms measure, and how those measurements aid in analysis.

CHARACTERISTIC CULTURE	
Abstractive	Associative
Gesellschaft	*Gemeinschaft*
Society	Community
Urban	Rural

Apollonian	Dionysian
Heterogeneous	Homogeneous
SOCIAL STRUCTURE	
Individualistic	Collective
Small or nuclear family	Extended Family
Overt social rules	Implicit social rules
Loose in-group/out-group distinction	Rigid in-group/out-group distinction
Achieved or earned status	Ascribed status
Flexible roles	Rigid roles
Loosely integrated	Highly integrated
Class	Caste
Social and physical mobility	Little social or physical mobility
Low power distance	High power distance
PHILOSOPHIC OUTLOOK	
Mastery or control over nature	Harmony with or subjugation to nature
Melodramatic/escapist	Tragic/realistic
Humane/inhuman	Human/inhumane
Objective	Subjective
Quantitative	Qualitative
Alloplastic	Autoplastic
Mind/body dichotomy	Union of mind and body
PSYCHOLOGICAL ORIENTATION	
Psychology of abundance	Psychology of scarcity
Schizoid or fragmented	Comprehensive or holistic
Need for achievement	Need for affiliation
Abstractive and logical	Anthropomorphic & complexive
Masculine	Feminine
Direct responsibility	Indirect responsibility
Great use of extensions	Little use of extensions
Extension transference	No extension transference
Steep pleasure gradient	Flat pleasure gradient
Weak uncertainty avoidance	Strong uncertainty avoidance
Guilt-internal	Shame-external
THOUGHT PATTERNS	
Analytic	Relational
Theoretical learning and knowledge	Experiential or kinesthetic learning and knowledge
Dichotomous/divisions	Holistic/joining together
Linear-separations	Nonlinear-comprehensive
Abstractions/prose	Imagery/poetry
BASIC VALUES	
Doing	Being

Change/action	Stability/harmony
What/content	How/style
Individualism	Belongingness
Independence	Interdependence/dependence
Self-reliance	Reliance upon others
PERCEPTION	
Mind/body dichotomy	Mind and body are one
Monochronic time/action	Polychronic time/action
Linear or segmented time	Nonlinear or comprehensive time
Future orientation	Past or present orientation
Space/objects separated	Continuity of space/objects
Subject-object	Subject-subject
Nonsensual and non-senseful	Sensual and senseful
INTERACTION	
Low-context	High-context
Competition	Cooperation
Verbal emphasis	Nonverbal and verbal
Written or electronic	Face-to-face
Impersonal	Personal
Schizoid/fragmented relationships	Holistic/interdependent relationships
Monological	Dialogical
Practical/aloof	Nonpurposive/involved
Easy to break action chains	Difficult to break action chains
Systematic	Spontaneous

Imperatives for Cultural Analysis. Use the following to direct your use of culture as an analytical factor:

- Be a cultural relativist, but not an extreme one. Adjust your point of view, understand the other person's position, and empathize. "Table" your own point of view for the purpose of explanation and prediction, but never abandon it. Do not 'go native' in thought or deed.
- When you find yourself thinking: "These people are (dirty, stupid, lazy, immoral, evil, etc.)," you are probably being ethnocentric.
- Most people in a culture behave appropriately. Inappropriate behavior happens less often in all cultures. Hence, if most everyone behaves in a certain way, it is appropriate to the culture. This provides predictability to reactions. Most people react appropriately.
- All differences between one culture and another culture are positions on a continuum, without a fixed scale. That is, you can say Germans value family more or less than Spaniards, but you must resort to examples to demonstrate how much more or less.
- Cultural generalizations, although sound and valid, suffer from the same defects as all generalizations: you particularize them at risk. You might use your knowledge of machismo to predict a Mexican election, but you may not assume any particular Mexican man is macho.
- Cultural generalizations are often snapshots in situation, time and place. You can expect that

many cultural truths change over time, that they vary between urban and rural situations, and that they may erode with the advent of global mass media, industrialization and other forms of development.

III. Interrelationships with Other Political-Military Factors:

- History. History explains culture as it follows the evolution of society over time. History explains the ways in which a population has adapted to the combination of its natural environment and other forces over time. History catalogs the external and internal influences and events that condition a society, and records the reactions. History provides the examples of how culture predicted and explained past events.
- Natural environment. Societal adaptation always includes accommodations or exploitations of the natural environment.
- Culture and Religion. Religion and culture overlap, especially where religion is dominant. Religion often exerts social control, prescribes and proscribes behaviors, and embodies perspective and outlook. Religion may form societal groups or establish a social hierarchy. These and other functions of religion are also functions of culture and society.
- Ethnicity. Again, ethnicity and culture overlap. In some cases, ethnicity and culture are nearly identical.
- The role of the military. Attitudes about and within militaries are cultural. Militaries form very cohesive secondary groups with exceedingly clear social controls, norms, and behaviors. Acculturation is so thorough and universal in military organizations, that soldiers are predictable over a larger span of behaviors than almost any other secondary group.
- Mass media. Mass media serves to dilute culture. Soap operas, commercials, movies, and international news all provide examples of people acting successfully in different ways. The portrayed people may accept or receive rewards for behaviors, which are locally unacceptable. They may receive sanctions for doing things, which are locally acceptable.

Sources of region-specific cultural information.

- Brigham Young University publishes a Culturgram for every country in the world. These are extremely rich and concentrated sources of cultural information.
- Travel guides available in most bookstores will have introductions, capsules, or whole chapters of cultural information.
- Tourist bureaus and chambers of commerce of many countries publish cultural hints (usually flattering), often on websites.
- U.S. embassies will direct you to a culturally savvy office in the country team of most countries. Often this will be USIA, which manages a cultural interchange.
- Foreign embassies in the United States will publish or direct you to cultural information about their country.
- Language texts and dictionaries provide great insight into what is important in a culture, especially if the text distinguishes usage from country to country.
- Foreign books, magazines, newspapers, films radio and television programs provide familiarity with almost all components of the culture under study.
- Language immersion programs normally include a substantial cultural component.

IV. Analytical Questions.

- What are the modal personality traits of the people of the area you are studying?
- How does language act as a mirror of the society? Is language a cohesive or divisive element? Does language coincide with class and/or racial divisions?
- How are the roles of men and women defined in this culture? Is there a major difference between the *hoi polloi* and the elite? To what extent does this affect your study of the culture or more importantly, operating within it?
- What are the basic values of this society? How do they translate into a worldview?
- What are the major environmental determinants affecting the shaping of culture in this society?
- What is the impact of the prevalent cultural attributes on the political system and popular view of government?
- What is the prevalent view of the individual, vis-à-vis the family and state?
- What are the significant sub-cultures within the area you are studying?
- In Weaver's chart (above), where does this culture fit on each of the scales? Which of these have operational importance in explaining and predicting?

Recommended Further Reading

Edward T. Hall. *The Silent Language* (New York: Anchor Press), 1973
Edward T. Hall. *Beyond Culture*. (New York: Anchor Press), 1976.
Edward T. Hall. *The Hidden Dimension.* (New York: Anchor Press), 1969
Nicholas Dima. *Cross Cultural Communication* (Washington DC: Institute for the Study of Man). 1990.
Hans Binnendijk. *National Negotiating Styles* (Washington DC; Foreign Service Institute, US Dept. of State), 1987
Gary Weaver, ed. *Culture, Communication and Conflict: Readings in Intercultural Relations.* 2nd ed. New York: Simon and Schuster) 1998.

Chapter 14

Religion

I. Introduction and Definitions

Religion is one of the most important and pervasive phenomena in the human experience. Even someone who does not himself subscribe to any particular religious belief cannot help but be struck by the influence religion has had on societies and cultures around the world and over time. It has permeated the collective psyche of mankind. It has inspired much of the world's finest art, literature, dance, drama, music, and architecture. We use religious occurrences to mark time, such as A.D., B.C., A.H. Religion has influenced the types of political systems under which we are governed, the economic systems in which we trade, and the social systems in which we live. There is no example in history of a culture without religion, and all governments and states that have tried to eliminate religion have failed. People have endured the most horrible of pogroms and oppression and have made great sacrifices to cling to their religious beliefs. Even in societies normally held to be secular or "non-religious," e.g., Western democracies or Confucian China, religion has been and remains a basic and powerful social force. Across time, space, and cultures, the search for gods is a constant theme in the community of man.

Do not argue the rightness or wrongness of religion or promulgate a particular religious belief. Instead, define what religion is, the role it plays in various societies, and how it is studied. From there, try to figure out what effect a particular religious belief has on the political, social, economic, and cultural fabric of the society in which the religious order exists. Remember that political-military analysts are not theologians.

Religion Defined

Religion develops from man's feeling that because there is so much in this world that is beyond his control, he himself is not the final answer and, therefore, there must be something greater than he. Once he accepts this concept, he will try to modify his behavior to coincide with what he perceives as the edicts of that greater power. Religion, then, is both the inner experience an individual has when he senses a supernatural force and the ways in which he tries to bring his own personal and social life into harmony with that force.

Since religious practice always involves some sort of community, the term “religion” is commonly used to refer to an organization of people who subscribe to similar beliefs and practices. There is a difference in focus when referring to religion, on one hand, and a religion, on the other.

Common Traits

There are several religions in the world today that differ dramatically from one another and which among them have thousands of sects. However, all religions have at least three traits in common. These traits are a belief in a force superior to man, a code of conduct, and the

concept of transcendence.

The first trait, already alluded to, is belief in a force superior to man. This may be a god, a pantheon of gods, or an impersonal, abstract force. Most Western religions have personal gods, which are individual beings. Some Eastern religions instead believe in a creative principle or force.

The second common trait is a code of conduct, which will assist the believer in harmonizing his life with the divine will. This code is often the foundation of a society's moral and ethical systems, such as the Ten Commandments of the Judeo-Christian tradition or the Eightfold Path of Buddhism. (Morality is a way of living based on precepts believed to be true. Ethics is a way of explaining, defending, or construing moral action.)

The third trait common to religions is the concept of transcendence--that we can somehow escape this world. Every religion will have transcendence as its ultimate spiritual goal, whether by following moral rules as a path to an other-worldly paradise, by practicing forms of physical or mental discipline to escape the endless cycle of desire and suffering in the world through enlightenment, or by devoutly appeasing the gods through prayer and ritual.

Eleven Components of Religion

A comparison of two or more religions can be made by looking at several different aspects. The first aspect is the numerological belief; e.g., the types of supreme power the religion reveres. Is it based on an impersonal Absolute, on personal monotheism, or on polytheism?

Second is the historical aspect. Who, if anyone, is the founder of the religion? Is he real or mythical? Where and when was he born? What was his life like? When and under what conditions did he found the religion? Did he claim to be of supernatural origin or to have a special relationship with the deity? How did he die and when? How did the religion spread and develop over time?

Third is the revelatory aspect. Is the religion based on a revelation to the worshipers from the deity (such as in Christianity, Judaism, or Islam), or is it based on self-discovery (such as in Hinduism, Buddhism, or Taoism)?

The fourth aspect is the cosmology of the religion. How and why was the world created? Is it real or illusory? Is it eternal? If not, how and when will it end? Has it ended before, only to be re-created? Are there several dimensions of it?

The fifth aspect consists of the anthropological beliefs. How does the religion view man and human nature? What is man? How did he come to be? Why? What is the value and purpose of life? Do only humans have souls or is all life valued equally? Is man immortal? Will he live again? Must he?

Views toward proselytzation and excommunication comprise the sixth aspect. Is the religion a missionary religion? How does one qualify for membership in the religion? Is there anyone who can be forbidden membership? What means can be used to obtain a conversion?

Under what conditions can a member be expelled? Once expelled, can he be readmitted? If so, under what conditions?

Sociological precepts comprise the seventh aspect. What types of earthly social order does the religion call for? Are all believers equal before the Divinity? Who is not equal, on earth or in heaven, and why? What types of roles do people play in both the religious and secular communities? How is religion used to determine who plays what role? What types of interpersonal relationships are called for? What types of segregation or integration are established and on what basis? Who are the leaders? Who are the followers? Why?

The eighth aspect deals with the soteriology (the study of salvation) of the religion and addresses the concept of transcendence. Is the spiritual goal of the religion salvation or liberation? Have they already been chosen, or does everyone still have a chance to gain enough merit to achieve the goal? How is such merit gained? How is the goal achieved? Is it possible to know that one has achieved it prior to death? If we achieve it, what happens then? What happens if we do not achieve it?

The ninth aspect is the sacramental component and deals with that which the religion holds as sacred. This has several aspects.

o Sacred space and time. What are the sacred places of a religion? Why are they sacred? What is the proper conduct within them? What are the sacred times--usually celebrated as holidays--for the religion? Why are they considered holy? What is the proper form of celebration? Sacred events usually occur in sacred places and times. Sacred places are those locations where one goes to worship. They may include shrines, temples, and churches as well as rivers, mountains, and promontories. The places and dates of the founder's birth and death are normally held to be holy, as are the place and date of the founding of the religion. Even those religions that lack this type of historical grounding will often see the place where the believers dwell as the Holy Land and will have religious festivals and holidays to mark certain occasions.

o Sacred words and writings. This category can be broken down into at least three subdivisions. First are the scriptures. Is there a Holy Book or Books? Is it held to be the word of God? Is its author known? Was there only one author or many? Is there only one acceptable scriptural language or may any language be used? The second subdivision is sacred stories. These may be in the scriptures or may be secondary works. They may be based on fact or be legends, myths, or fables, but are generally allegorical. They are a profound aspect of any religion if for no other reason than to tell us how people see themselves in relation to their god. For example, Shintoism says the Japanese islands are godly creations and their inhabitants are descended from gods; the Judeo-Christian tradition holds that man was created in God's image, but fell from grace in the Garden of Eden; Hinduism says that the four social castes sprang from parts of Brahma’s body--the lower the body part, the lower the caste. The third subdivision of sacred words is the moral code contained in scripture and stories. It may be laid out explicitly or merely implied.

o Sacred people. These may be historical, legendary, or contemporary. They can be divine, such as the Dalai Lama or the Japanese emperor; semidivine, such as Christian saints;

mortals with a special connection with the gods, such as a shaman or a witch doctor; or simply mortals with special training, such as priests, preachers, monks, or imams. Part of studying sacred people is to determine if the religion has a clergy. If so, who are they? How are they selected and trained for their profession? Are they venerated? Can anyone join the clergy or are certain categories of people (e.g., women) excluded? What is the clergy's relationship with the population at large?

o Sacred symbols. All religion is symbolic in that it is an outward manifestation of an inner experience. If man could not symbolize, there could be no religion. Symbols may be verbal, such as invocations like "Praise the Lord," "Amen," or "In the name of Allah, the merciful and compassionate." They may be actions, such as bowing the head and placing our palms together to pray or making the sign of the cross. Symbols may also be physical, such as the Kaaba, Buddhist and Hindu statues, or the Crucifix. Some sacred places or writings are also sacred symbols. For example, Christians swear on the Bible, while Muslims face Mecca while praying.

The tenth aspect of religion we can study is its ritual and rules of worship. Ritual is one of the most important aspects of religion. There are rituals for every aspect of life from birth to marriage to funerals. There are rituals for daily prayer; for celebrating holy times and for worshipping in holy places; for asking the gods for a good crop during the planting season and for thanking them when the crop is harvested; for choosing sites for houses, shrines, and graves and protecting those sites from evil once they are chosen. Even if we worship privately, we tend to so with socially acceptable rituals. When studying these rituals try to determine what they mean and why. What is the tradition behind them? Who can perform the ritual? Where and when? Who can observe or participate in it? Who is expressly forbidden from observing or participating? Why? Do believers worship as congregations? Must they? How does the believer prepare himself for ritual or worship? How does the ritual for congregational worship differ from the ritual for individual worship? Is the purpose of ritual and worship to gain favors from the gods or to avoid their wrath?

The final aspect of religion is the difference between the Little Tradition and the Great Tradition. There is no religion today that is practiced purely as espoused by its founder or indeed as espoused by its current believers. In religion, as with culture in general, we must distinguish between what is said and what is done, what is preached as the ideal and what is really practiced. With religion, however, this concept becomes more complex. Robert Redfield said that there are two ways of expressing religious motifs. One is what he called the Great Tradition. This is intellectual, literate, scholarly, elitist, orthodox, and it has a long-term perspective oriented on history. The other means of religious expression Redfield called the "Little Tradition." This is illiterate or non-literate, oriented on the present or on cosmic time. It is the religion of the common man and is transmitted by family and community rather than through formal training. The Little Tradition is the religion of myths, festivals, local shrines and temples, and local gods and spirits. The Great Tradition is the religion of scholarship; debate; beautiful cathedrals and churches; and omnipotent, omniscient, omnipresent deities. The Great Tradition is the religion of the priest, whose responsibility lies in maintaining the whole social and religious order for the long-term welfare of the believers. The Little Tradition is the religion of the shaman, who deals with the exigencies of daily life and the immediate and temporal

welfare of his clients. For the political-military analyst, the Little Tradition may often be more important, because it has a greater influence among the common folk. The practices of the Little Tradition and its shaman may allow for a channel of communication or manipulation.

Five Levels at Which Religions Operate

The religion one espouses is usually an accident of birth. To be sure, there are normally provisions in the religion for conversion, but most people who subscribe to a particular religion today are not converts. They are members of a particular religion because their parents were. In fact, in many societies, one does not "join" a religion per se, since religion cannot be separated from the totality of life; e.g., Hindu India or Islamic Arabia. For most people, religion is an integral part of their day-to-day existence, not just something they do two hours one day a week between brunch at the officers' club and mowing the lawn.

Religion can operate on at least five levels in a society. These are individual, social, economic, military, and political. Since societies are made up of individuals, we include the individual level as our first. Religion meets man's basic psychological need to come to terms with the world around him. As one wag has said, "religion lets us explain the inexplicable, ponder the imponderable, and 'unscrew the inscrutable." It provides comfort and guidelines man can find nowhere else.

o Religion gives man a sense of self. Some even define religion as that which allows man to come to terms with his real self. As such, it gives one a sense of belonging and maybe even well being. It helps answer questions like who am I? Where did I come from? Why am I here? What happens when I die? How and why was the world created? What am I to this world? Religion often helps us feel that no matter how insignificant or inconsequential we may be to our fellow men, we are important at least to our god. He/she cares for us, even if no one else does.

o Those who come to grips with their true selves often feel that they can now see the world more clearly, that they have reached a higher state of consciousness. This can be a deeply personal religious experience, usually described as achieving a state of inward joy, or serenity and inner peace. Some may feel as if they have been enlightened or have "seen the light." Many feel as if they have actually been "born again," leaving behind their old life to begin a new one in service to their god. To many people, this is the most important aspect of religion.

o Religion also helps people establish personal moral codes. For many, "good' and "bad" and "moral" and "immoral" are relative and arbitrary; therefore, they are meaningless, without the sanction of a divine will behind them. These codes may address behavior as mundane as proper clothing and eating habits or as serious as sexual relations and the sanctity of life. Religious codes help people make tough choices that might not otherwise be made. With a religious code, choices and options are prescribed by a Higher Authority.

o The final facet of the psychological level is its power to encourage acceptance of one's role in life while, paradoxically, giving hope for something better at another place and/or time.

Religion helps the common man go through hell. He accepts his fate because it is ordained by karma and dharma, because of kismet or God's will, or because there is a better world waiting for the meek on the other side. Religion can also inspire hope. Men beseech their gods for protection, help, wealth, and health. Through religion, personal concerns are met with religious truths. Religion may well have risen out of man's realization that in this world we are ultimately all alone. Religion helps us prepare emotionally and intellectually to bear with those aspects of human existence that are beyond our control. There are some that posit that the purpose of religion is not so much morals as it is morale. As Will Durant has poignantly pointed out, "As long as there is poverty there will be gods." But never be mislead into believing that religious fervor is a function of an economic environment. Many of the post-modernists would have you believe that a poverty-free society would discard religious beliefs. This has time and again been proven to be more of an ideological wish than reality. For instance the wealth of the Kuwaiti citizen has not diminished an increasing movement toward a more strictly interpreted Islam.

The second level at which religion operates is social. Religion always finds expression in some sort of community. In fact, for a belief system to be considered a religion, it must have at least two adherents. They may be considered heretics, but at least it is accepted that they have a religion. If only one person holds a belief system, he is merely considered mad. Religion operates on the social level in several ways.

o One social function of religion is that it provides a definition of the community. Just as religion always is grounded in a community, so do communities define themselves at least in part by reference to religion. This may in fact be the central concept of the community's collective identity, such as in pre-World War II Japan or modern-day Israel and Pakistan. The religion may also stipulate that certain non-believers be accorded conditional membership in the community, such as Islamic perceptions of Jews and Christians as "People of the Book." Finally, religion also helps identify “them” Vs “us.” Non-believers are then classified as "infidels," "pagans,” "heathens,” or "heretics" or as simply the uninformed.

o Another social function is to establish a normative standard for social organization and conduct. These standards normally regulate social relationships and may address everything from sex, marriage, and male-female relations in general to filial piety, teacher-student relations, and relationships at the work place.

o The third social function of religion is social legitimization. It can be used to justify a social system or to support its overthrow. Members of the society may be encouraged to accept their lot in life because God has willed it so. Those who are better off in the society enjoy their status and wealth because they are the chosen of God. Similarly, if the social system is at odds with a religion, the religion can be used by its believers to incite rebellion.

o The fourth social function is social mobilization. Religion can serve as the focus or impetus for social action. Many charitable organizations are religious-based, and some religions call for believers to care for the less fortunate. For instance within Christianity the Protestant movement put emphasis on personal salvation through faith while Catholicism has

emphasized good works as being in tandem with faith. Similarly, a community's religious center may also serve as the social center. Many social activities are oriented on religious events, times, and places. Religious leaders often serve as social leaders and are in some cases more effective in this realm than political figures.

o The final social function is scholarship. Religion has historically been one of the main vehicles used to promote literacy. People learn to read in many parts of the world by studying scriptures. A basic textbook in many Islamic countries is the Qu'ran. Monks and other religious leaders often double as teachers. Universities and other institutions of higher learning have been established in the name of most major religions. Similarly, missionaries of several denominations have established schools around the world. Many of these schools have had a significant impact on the education systems of the countries in which they were established, even if efforts to proselytize were not especially successful. Religion, as interpreted by more devout clergy, however, may also retard scholastic, or more properly, scientific progress, by proscribing the study of certain subjects or by dictating how facts may be interpreted, understood, or presented. This is generally very rare and more of an ideological mantra than a reality.

The third level at which religion operates is economics. Religion generally encourages certain types of economic practices while prohibiting others. Economic topics religion can address include the distribution of wealth, welfare responsibilities, taxation, banking practices, economic development, investment, use of material resources, acceptable occupations or vocations, and economic relations with other countries. For instance within Islam usury or interest loans are forbidden. The American Catholic bishops regularly issue tracts on economic justice.

The fourth level at which religion operates is the military. Is military service compatible with religious beliefs? Under what conditions? Who serves? Who is prohibited from serving and why? Who fights and who only serves in supporting roles? With whom do we fight, why, with what, when, and under what conditions? Is special merit gained by fighting? How is the enemy to be treated if captured or defeated? What can we expect from the enemy if we are captured or conquered?

The fifth level at which religion operates is politics. There are several aspects to this.

o Religion may promote or oppose certain types of legislation, such as those regarding birth control or abortion, divorce, taxation, or child care. On the other hand, the government may be compelled to pass laws that circumscribe religious practices regarded as unhealthy or pernicious by the society as a whole, such as polygamy.

o Religion can be used to promote national integrity among a country's peoples. Countries as diverse as Israel, Pakistan, and Burma have appealed to religion as a way to overcome ethnic or other divisions among the citizenry. On the other hand, religiously pluralistic societies such as Malaysia and India have had to overcome religious differences in their struggle for national unity. Some countries, like the United States, have even stressed tolerance of religious differences as a means of encouraging national integration.

o Religious organization or principles can be used as the focus for political mobilization. Even secular leaders of parties may appeal to religious values as an attempt to gain support from the polity for their positions on issues considered secular by some.

o Religion can also be used to justify support of opposition to political regimes or political programs. This is common in Islamic countries.

o Religion can influence the political system through its influence on individual leaders. The religious belief of political leaders can have a significant impact on the efficacy of a government or on its policies. The deep religious convictions of America's President Carter or, Iran's Ayatollah Khomeini are cases in point.

o Religious influence on government need not be limited to a few leaders here and there. In some countries, especially those with political systems that are specifically religious-based, political representations may be determined by religious affiliation. A certain number of seats in the legislature or certain numbers or types of government jobs may be reserved for particular religious groups. The Iranian majlis, (parliament) for instance, has seats reserved for Christians, etc.

o The final political area upon which religion may impact is foreign policy. Nations may band together over certain issues in a display of religious solidarity or may side against another nation for religious reasons. Examples are non-Arabic Islamic nations who side against Israel on many issues to show their support for their Islamic brethren, or the U.S.-Israel relationship, which is based at least in part on the Judeo-Christian connection. The Organization of Muslim Countries (OIC) is one such example.

Aspects That Exhibit Political Influence

Of the five levels of influence a religion may have in a society, the political-military analyst is, of course, most interested in the political level. Donald E. Smith has identified five aspects that can be studied to determine how much political influence a religion may exert. Naturally, none of the five dictate a given level of political involvement. They merely indicate whether or not such a proclivity exists.

The first aspect is how the religion views history. Religion will help determine how history is remembered, interpreted, and used. If history is seen as unreal, the believers will be unconcerned with political power. If history is seen as crucial, then believers will be more prone to seek political power as a means to influence the course of history. Islam is an example of a religion deeply imbedded in history to the extent that history before the advent of the Prophet Muhammed is called the era of Jahaliya- the era of ignorance.

The second aspect is tolerance of other religions. Generally, the more tolerant a religion is of other religious beliefs and practices, the less politically active it will be. On the other hand, intolerant religions encourage garnering political power as a means to suppress what are seen as heretics or apostates. More frequently demagogues use religion and its presumed uniqueness to demonize other groups out of political expediency. Islam is unfortunately used by political

demagogues as a vehicle in this context.

The third aspect is ecclesiastical organization. The better organized a religion is, the better suited it is to political action, at least in general. However Sunni Islam is an exception to this in that they have no structured clerical hierarchy but on a grassroots level exert considerable power.

The fourth aspect is the way the religion views Church-State relations. If there is a clear distinction between ecclesiastic and political roles, the less politically influential the religion will be. If no such distinction is made, the odds of political involvement increase.

The final aspect is social regulation. The more a religion stipulates regulation of social life, the greater the areas of potential conflict between religion and other aspects of the society. The believers may then seek political power to resolve such disputes in their favor. Conversely, the less regulation called for by the religion, the fewer points of conflicts there will be, and there will not be as great an incentive to seek political influence.

Caveats for the Study of Religions

Shamanism and animism are still very much alive today, especially in the civil affairs/psychological operations arena in developing countries. The political-military analyst may find that this considerably complicates his attempts to study the religions of his regions.

Distinguish between communalism and religion. It can be bewildering to see adherents of religions that preach tolerance and love, killing one another in the name of their religions. This does not necessarily mean that they do not believe in their religion, just that other concerns take precedence. In this case "love thy brother" may be construed to mean "kill thy non-brother."

When studying a religion, attempt whenever possible to distinguish between major sects and denominations. Learn what it is that makes them different. In some cases, the differences may be so great as to make them all but separate religions.

Religion is an integral part of a culture, but it is only a part. There are many different aspects of life and culture that will distinguish people from one another, no matter how close their religious beliefs. A Japanese Christian is still Japanese, and a Javanese Muslim is still a Javanese. Their affiliation with Christians and Muslims in the United States or the Middle East, while important, are not nearly as significant as the differences among them.

Religions may change over time, although the irony is that in trying to maintain "relevancy" they may secularize themselves out of existence by attempting to fit within the current zeitgeist. A myriad of social, political, economic, and intellectual forces are constantly buffeting religious concepts. Religious teachings and practices must confront these but carefully as to avoid becoming a therapeutic "feel good" exercise. The constant drumbeat to modernize the belief system usually results in it becoming irrelevant as the deep rooted need for spirituality

leads people to more traditional belief systems.

Religions have a fundamental paradox in that the basic legitimating idea--the spiritual goal--is unattainable in this life. One must die to get to heaven or achieve Nirvana. This has not proven to be a handicap, as shown by the influence religion has retained even today. It may in fact be one of the reasons religion has remained a powerful force. If the goal were in this life, once it was achieved, there would no longer be any reason to continue adhering to the religion.

The worst thing political-military analysts can do is put religion in a purely secular context. Adherents believe what they do on faith. For them, their belief is true and not open to dispute. Similarly, miracles are quite real for believers. What to us may seem commonplace, coincidental, or just plain phony--such as faith healing, speaking in tongues, or water stains that look like a religious figure--can be major religious experiences for someone who believes. It is counterproductive, to try to dispel these believers or to convert them. Besides, the mission of a political-military analyst is not to gain converts or correct what he may see as misperception--it is to understand the religion and use that understanding to accomplish the mission. The political-military officer should also be aware of the danger of allowing his assessments to be influenced by an attraction to the powerful appeal of a number of traditional non-western religions.

II. Interrelationships With Other Political-Military Factors

As we Americans are imbued in most cases with the idea of the separation of Church and State, we have difficulty understanding those many cultures in which separation of religion from government or any other sphere of human activity is unthinkable. Within Islam, for instance, the persuasiveness of the religion has a profound influence on every aspect of the sixteen factors. For instance there is a whole field of study on Islamic economics. The Qu'ranic and Hadith prescribes very particular ways of conducting business and the use of wealth, advocating social justice and governing other aspects of economics. Within Christianity the concept of social justice is particularly emphasized subject. The "just war " concept is a facet of Christian theology, which was widely discussed during the 1991 Gulf war. The view of Islam toward "jihad" and the interrelationship of the military and use of force in the "house of peace, house of war" concept must be understood by those assigned to the Middle East. The interrelationships between political systems, ideology, and religion must also be recognized. The interplay between ideology and religion is often so intense as to make them appear inseparable. For instance the "Islamists" have basically abducted the religion of Islam and transformed it into an ideology with a "heaven on earth" millenarianism to obtain power, and institute a political system of their own preference.

III. Questions To Be Considered

1. What is communalism? Discuss in the context of the country under study.
2. Discuss how a religion exhibits political influence as structured in the Smith outline, i.e., aspects that exhibit political influence in your area of evaluation.
3. How does religion intersect with political ideology and political systems? How powerful (or weak) is it in the nation under study.
4. How does religion of the region affect the conduct of warfare - if any?

5. To what extent is the religion or religions of the country a unifying or divisive element in society?
6. Is the religion compatible with technology and modern science? Is it all encompassing or a general guide?
7. Define the national impact of history on religion and religion on history.
8. What are the general trends in the country, i.e., a move toward secularization or a revival of religious fervor?
9. What is the relationship between the leadership and secular leadership?
10. What influence do religious leaders have over the populace in matters of state?

IV. Conclusion

Religion is a complex and fascinating topic. As stated earlier, even someone who does not believe in a particular religion must respect it as a major social force. William and Ariel Durant put it eloquently when they wrote--

"Even the skeptical historian develops a humble respect for religion, since he sees it functioning, and seemingly indispensable, in every land and age. To the unhappy, the suffering, the bereaved, the old, it has brought supernatural comforts valued by millions of souls as more precious than any natural aid. It has helped parents and teachers to discipline the young. It has conferred meaning and dignity upon the lowliest existence, and through its sacraments has made for stability by transforming human convenants into solemn relationships with God. It has kept the poor (said Napoleon) from murdering the rich. For since the natural inequality of men dooms many of us to poverty or defeat, some supernatural hope may be the sole alternative to despair. Destroy that hope, and class war is intensified. Heaven and utopia are buckets in a well: when one goes down the other goes up; when religion declines communism grows".

Recommended Further Readings

Crim, Keith ed. *Abington Dictionary of Living Religions*. (Nashville TN: Abington Press), 1981

Smith, Huston *The World's Religions*. (San Francisco: Harper), 1991

Schoeps, Hans Joachim. *The Religions of Mankind.* (New York: Doubleday), 1966.

Keller, Werner. *The Bible Of History.2nd edition.* (New York: Bantam books), 1988.

Limburg, James. *Judaism: An Introduction for Christians*. (Minneapolis: Augsburg Publishing), 1987.

Esposito, John L. *Islam the Straight Path*. (New York: Oxford University Press) 1988.

Klostermaier, Klaus K. *A Survey of Hinduism*. (Albany: State University of New York). 1989

Corless, Roger J. *The Vision of Buddism.* (New York: Paragon House), 1989.

Chapter 15

Ethnicity

I. Introduction and Definitions

Ethnicity is an historical process that develops from society and culture. Often it is a complicated and emotional classification of people and their perspective of where they fit in the nation-state. The modern nation-state is based on citizenship; implying a degree of allegiance and exclusivity from other nations or people. However, within the nation-state there are those groups of people who may not belong to the politically dominant groups and hold distinct cultural and/or social differences. They are labeled "ethnic" groups and at times, “minorities," whose differences are often granted recognition in all aspects except political self-determination. At times these ethnic groups will aspire to become their own nation-state and then ethnicity produces the rise of conflicts or wars aimed at self-determination or liberation.

As Manning Nash writes (*The Cauldron of Ethnicity in the Modern World),* “Ethnicity... is clearly related to politics, to class, to economics, and to culture and ethos.” He goes on to say that ethnicity has a deep personal component either as an embattled minority or as a member of a majority struggling to maintain control. All too often the post-modernist writers try to cram every conflict into a convenient category of race, class, or gender. While related to those factors ethnicity goes well beyond them to the core identity of individuals. While many observers of the Middle East tied the bloody civil conflict in Lebanon to class and political struggle, the crux of the conflict was the powerful catalyst of ethnic (religiously based) hatreds exacerbated by economic and political power disparity.

Ethnicity Defined

Most individuals would define ethnicity based on race, skin color, language, or nationality. This outward manifestation, however, is only a first step in defining ethnic differences. One must examine beyond the surface of an individual or group and recognize that perception defines their ethnicity. This perception is based on primordial ties--ties that initially define who a person is, what he is like, and how others are different. Thus, we can define ethnicity as "a self-perceived group of people who hold in common a set of traditions not shared by others."

These traditions may be based on language, religion, history, or other ties considered the 'building blocks' of ethnicity. These building blocks remain unchanged over time and are not subject to politics or economics:

o Body - biological components relating to blood, genes, flesh. This relates more to racial divisions.

o Language - communication that contains meanings and elements unique from other languages. An example here would be the division between French Canadians and the rest of Canada.

o Shared history - struggles, fate, a common purpose. An implication that personal and group fate are one in the same. This would apply most emphatically to the Arab feeling of unity

beyond religion, or nation, buttressed by a common (more or less) language.

o Religion - beliefs and practices that relate a group to some religious group different from the majority. There are many examples of this of which the southern Sudanese, Muslims of Mindanao, Christians of East Timor, the Copts of Egypt are but a few examples
.

o Nationality - a desire for the symbolic and, at times, political means of an independent people. Traditionally this has defined Americans although some would now question this in light of the daily bombardment of divisive points of view, and the highly politicized environment of hyphenated America in which we live. It is ironic that as we urge other nations to grow beyond Tribalism, we seem to be reverting to it. John LeCarre in his book *Our Game* has a character saying "While we are pulling down economic borders these ethnic crazies are putting up national borders."

Using these building blocks, an ethnic group develops a perception of themselves and where they fit in the nation-state. If the nation-state is a pluralistic society, pecking orders based on politics, race, region, religion, or language may develop. A combination of these pecking orders has produced some great empires--Greek, Roman, Chinese, and British, as examples. Those groups who did not assimilate and/or retained visible manifestations of their ethnicity, maintained a perception that they were distinct from the dominant group, an example being the Jews of Palestine.

Ethnic distinctions may be determined by eight referents: physical characteristics, name, nationality or national origin, language, religion, tribal affiliation, history, and cultural aspects such as clothes, eating habits, houses, and so on. Any of these components may be changed and a new ethnicity assumed. Individuals may adapt to changes quickly but group changes require more time, usually more than one generation if a different ethnicity is to take hold.

Individuals may display their ethnicity with varying degrees so that their ethnicity becomes latent, minimized or active. Different situations may require different displays of ethnicity depending on geographical location, emphasis by a political leader, or perhaps arrival of immigrants. In other words, depending on the context, individuals may choose to play down or play up their ethnic identity. They may even go so far as to challenge their national identity, regardless of the context. A Breton will probably declare himself a Breton first and a Frenchman second, whereas a Parisian will remain first and foremost, a Frenchman. Ethnic identity may not be static either. For instance an Egyptian may identify himself as an Egyptian one day and an Arab the next. It largely depends upon the context of the situation and with whom he may be speaking.

Why doesn't the Breton call himself a Frenchman or the Parisian call himself a European? Modernization appears to have pushed in the opposite direction of sociologists' predictions of a united, technologically bound universe. Instead of merging, societies search for smaller, more intimate ties against the alienation that modernization produces. Ethnicity then serves as a counterweight to that alienation. This is a particularly important concept to remember as we preach the "global village." While the European Economic union seems to be pulling Europe together, one only need to observe the world soccer competition to understand that the

nativist pull is far more powerful-at least in a certain time frame - than any economic cooperation.

As individuals seek these smaller ties, they may lean toward stratification and segregation. Stratification deals with access to political, economic, or social privileges. Segregation deals with physical separation of people. In stratification, individuals hope to break the barriers that curtail their economic benefits (such as unemployment), their political influence (lack of legitimate representation), or their social acceptance (an unfavorable background). In segregation, individuals may be subject to microsegregation (separate facilities), mesosegregation (ghettos), or macrosegregation (confinement to reserves or homelands). In analyzing these forms of segregation and stratification, the analyst needs to determine whether they are intentional or unintentional, formal or informal, or even official policy. The currents presently (2000) moving through the American Black community are examples of this dichotomy. One group seeks the more traditional goal of integration into the overall tapestry of American life, while a more recently organized group seeks to reinstitute segregation, in terms of university living arrangements, black colleges, unions, churches etc.

Today, some form of conflict is normal in a pluralistic society. One cannot examine the politically successful groups of a country without analyzing their influence over conflict. The political elite can no longer ignore those who may have been absorbed politically since minor groups may be the next majority. Thus, we might assume that the more ethnic groups that are visible in a country, the greater the chance for conflict. This conflict may occur in various political, economic, or social spheres and at various intensities. In order to minimize the potential for ethnic conflict, political elite's may employ several methods--

o An ideological commitment to minimize ethnicity, as we used to do in the United States, until recently when, as stated above, the renewed emphasis on ethnicity by minorities has reintroduced a new sort of segregation desired by the minority in contradistinction to the earlier segregation imposed by the majority.

o A nonethnic basis for consensus, such as religion, meaning the same sect. Being Muslim or Christian is not enough. One must be the "right kind" of Muslim or Christian. (Shia-sunni split in Lebanon, the Catholic - Protestant conflict in Ireland, the Orthodox - secular Jewish antagonism in Israel.)

o Creating a sense of belonging whereby the survival of the nation takes precedence over the individual or sectarian identity. The reluctance of French Canadians to go it alone must be based at least partially on the fear of being swallowed up economically and culturally by the United States.

Understanding ethnicity provides insight on the political, economic, and social structure of a foreign environment. Ethnicity will play a bigger role in the potential for conflict as countries become less homogenous. In a 1988 study by Walker Connor, of 168 surveyed countries, fewer than 25 percent were considered homogenous societies. The presence of ethnic groups vying for pieces of the political and economic pie can be a decisive element for examining the success of the political elite. The military analysts will probably find few areas of the world where ethnicity and the potential conflict it brings does not affect the power base of ruling elite's. The analyst is charged with understanding the extent of influence that a given

ethnic group may have and its potential to affect the political, economic, and social make-up of the region he studies.

The study of low intensity conflict (LIC), operations other than war (OOTW), counter insurgency (COIN), Small Wars, or whatever these political-military conflicts are called when you are reading this, must increasingly entail a greater understanding of ethnic warfare. Much of our Vietnam strategy in dealing with insurgency- what little there was- was focused on revolutionary warfare. This requires a much different strategy than ethnic warfare. For instance revolutionary warfare emphasizes the importance of wealth distribution, better government, land ownership, civic action etc. While all of these have a place in ethnic warfare, all the civic action in the world, or most efficient government, will not solve the problem of Palestine. There is little doubt that the Arabs of the West Bank are better off economically, socially, and in terms of personal freedom, than most Arabs in the surrounding Arab nations, but this has in no way diminished their ultimate desire to obtain independence from Israeli rule. So it is in Yugoslavia, the former Soviet Union, Sudan, Cyprus, the Kurdish regions and a myriad of other places in the world.

II. Interrelationships With Other Political-Military Factors

Since ethnicity is based upon religion, or language, or history, or culture and is often maintained or exacerbated by environmental, political, ideological, or economic factors, these must be analyzed in conjunction with ethnicity. For instance socio-economic factors are very important in assessing the volatility of an ethnic environment. When examining an ethnic group within a nation, generally analysts see socio-economic vertical stratification of a sect or ethnic group as a stabilizing factor while horizontal status as a destabilizer. For instance when an ethnic community is represented at all levels of the socio-economic ladder, there is little likelihood of violent conflict but when one socio-economic group occupies the lower end of the socio-economic spectrum, the potential for violence is high. This was the case with the Shia in Lebanon. Looked down upon by both Christian and Sunni Muslim communities, and virtually powerless at the national level, a rapidly growing Shia community swarming into the cities were ripe for rebellion. "Justice comes from the barrel of the gun." This became their slogan - borrowed from the Palestinians in their 1970's war against the Israelis (who had borrowed it from Mao).

The existence of the growing ethnic problem in every area of the world has particular interest for the political-military officer such as the SOF officer. The depth and detail of knowledge will be a much greater requirement in an ethnic conflict. For instance launching a PSYOP campaign, or a civic action project based on an assumption that the Kurds are a monolithic group with common aspirations will be a fatal mistake. And so it is throughout most of the world. Ethnicity is particularly important in the composition of the military. For instance in the United States the Army is composed of almost one-third Black or Hispanic soldiers (as of June 1998). Almost half of the total force originates from the South. Does this have an impact on our goal of an apolitical force? The Lebanese army splintered into three separate factions at the beginning of the civil war in 1976, supporting their confessional factions rather than the nation. The non-Arab or Shia soldiers of Saddam Hussein's army had little stomach for the war in the Gulf. The bottom line is this. Most nations in the world are multi-

ethnic and ethnicity as a force has put stress on the nation state as a viable concept. Can a nation survive and prosper in an environment of divided loyalties, segregated communities, and barely - concealed mutual antagonisms?

III. Questions To Be Considered

1. Define ethnicity. Identify the various ethnic groups in the nation under study. How strong are their loyalties to the central government? What is the central government's attitude toward minorities?

2. Is ethnicity a danger to nation state and why? If not why? Could it be exploited?

3. What is the ethnic composition of the military? The officer corps? The soldiers? What is the distribution of ethnic groups throughout the various arms and branches?

4. Does the socio-economic structure break down along ethnic lines? How? Any potential for conflict?

5. Do the ethnic minorities have a neighboring nation of the same minority with an irredentist history?

6. How unified, in terms of culture, language, religion, etc., are the minorities? Are they concentrated in certain geographical areas? Are they dominant in certain occupations? Are these occupations critical to the functioning of the country?

7. In philosophical terms can the nation under study integrate ethnic minority issues within a majoritarian democracy? Will there be some power sharing by the minority?

8. In terms of psychological operations themes, how general can these themes be, i.e., is there one-size fits all appeal or must the appeals be pencil thin in focus? In other words does the national populace respond to the same stimulus or symbols?

9. Does your own ethnic background predispose you to an affinity to one side or the other? Is there a tendency to assign devils and saints to opposing sides in an ethnic conflict, particularly among the media?

Recommended Further Readings

Ericksen, Thomas Hylland. *Ethnicity and Nationalism; Anthropological Perspectives.* (Boulder: Pluto Press),1993.

Montville, Joseph V. ed. *Conflict and Peacemaking in Multiethnic Societies.* (Lexington Ma. Lexington Books), 1989.

Nash, Manning. *The Cauldron of Ethnicity in the Modern World.* (Chicago: University of Chicago Press), 1989.

De Atkine, Norvell. "Communal Strife: The Insurgency of the Future," *Special Warfare* vol.5 no. 2 (October , 1993), pp.49-51.

Gary Weaver,ed. Culture, Communication and Conflict. Readings in Cross-cultural Relations. 2nd ed. (Needham Heights, Ma. Simon and Schuster),1998.

The periodical: *Nationalism and Ethnic Politics*, especially since 1996. Publisher Frank Cass, London, UK.

Chapter 16

Technology and Political Military Analysis

I. Introduction

This section on technology is a new addition to the POL MIL Handbook so several parts are still in draft and some issues remain to be explored. This will happen, in part, by developing questions and observations about technology during the long seminars and in the Media Technology course. The first question to be addressed here is why this Handbook should include a "new" section on technology? In other words, what is new about technology that makes it important in political military analysis?

II. The Definition of Technology

To begin with, we need to remember that technology means the application of knowledge to create solutions. This means that we need to think of technology as a concept rather than as a specific invention like a CD player or a computer or a hammer (and sickle). How we use such tools to solve problems is what matters here and this is where Twenty First Century technologies differ significantly from the tools of the previous centuries. In the past, technology has referred generally to the devices and machines that multiply the strength and abilities of men to make and move things. Whether we consider personal automobiles and power tools or giant cranes and planes, these devices generally serve as manpower multipliers. They are also designed and operated in terms of Newtonian Mechanics characterized by linear cause and effect relationships such as the watch works described in the introduction to this Handbook. With such technology, accuracy depends on precise parts working in unison and transaction speeds are constrained by the force of gravity.

By contrast, Twenty First Century technologies achieve precision through micro-circuitry operating at light speed. Former General Perry Smith describes it in terms of his digital watch:

> I wear a digital watch that tells time in various formats and has three alarms, a stopwatch, and the storage capacity for twenty telephone numbers. For a time I had a faulty watchband and I dropped the watch on the ground at least ten times while I was jogging, yet the watch has never broken. I have had to replace the battery only twice in five years. This watch is certainly much more complex than the old wind-up watch that told time but did nothing else. In comparative terms, the watch I wear today is the least expensive watch I have ever had, and yet it is the first watch I have owned that has never had to be fixed or cleaned. It is a much more sophisticated watch but it's also much, much more reliable" (Smith, p. 146)

Precision, reliability and uncertainty are key aspects of the new technology.

Characteristics of Twenty First Century Technology

In general, there are four distinct aspects of new technologies that we need to understand in order to use the concept of technology as a productive frame of reference for political military analysis. These include the shift from analog to digital systems, the multi user functionality of space based platforms, the speed and volume of digitized transactions, and their non-linear complex nature.

The shift from analog to digital systems can be "seen" quite literally by comparing the faces of the two watches described above. The digital watch represents the compression of data about the physical world into "bits" at the smallest atomic level which is then stored, combined and reconfigured on microchips at light speed. As, explained in user-friendly detail by Nicholas Negroponte in **Being Digital**, this process involves reconfiguring information about the physical world into digitized grids that are then encoded and decoded through digitized computations. The effect is "virtual" reproduction of physical phenomena through information processing.

A second significant aspect of this technology relates to the fact that such information processing systems, or devices, can be interlinked by transmitting light signals across space. This allows for the expansion of digitized processing through the non wired, as well as hard wired channels and facilitates information sharing and programming. The unique new aspect here is the increasingly large set of earth orbital transmission and relay satellites servicing businesses, government, militaries, and private users alike. As a result, both information products and services have become readily available to commercial users around the world so long as they have the decoding devices (i.e. cell phones, modems, computer terminals, etc.). The effect of this technology on cultures, finance markets, militaries, polities and ecological environments cannot be understated and is described as "globalization" by Thomas Friedman in his book **The Lexus and the Olive Tree**. This process has created a globally linked system in which digital computation devices constitute the infrastructure and space based platforms constitute the superstructure of the Twenty First Century.

A third aspect of new technology has already been mentioned above and will be developed during the program. This refers to the compression and transmission of data at light speeds based on the use of silicon chips. This not only allows for global "real time" communication but also for the development of technology designed to address aspects of human behavior never before understood. This includes the kind of biogenetic research that relates to cloning, human performance enhancement, disease immortality (cancer and AIDS), and artificial life. This has led not only to medical breakthroughs but also to a shift from user-based interfaces to agent-based interfaces with computers. In other words, Twentieth Century computers are built around button pushing and power point paradigms, whereas twenty-first century computers and devices will be built around the use of voice and face recognition and sensory signaling.

More important, both from a research and national security standpoint, this aspect of new technology introduces an era in which digitized information can be designed to

permutate and self replicate. This means that technology can "create" knowledge beyond computational solutions, facilitate artificial life and "invent" other technology. The related processes have important implications in all aspects of scientific research and have been shown applicable to phenomena as diverse as bee colonies and commodity prices. From a national security point of view, it ushers in the age of warfare through "smart" weapons and an array of new threats such as information viruses.

The fourth dimension of "newness" about this technology comes from the fact that research on the physics of light has generated important and paradoxical theories about how the world works. In a sense, these theories have asked: is light a particle or a wave? And the empirical answer is: yes. Traditional physics theories require that the answer be one or the other (either a wave or a particle) but "complexity" theories show that it can behave like both. In other words, we must accept paradoxical answers and uncertainties about physical relationships in order to create new technologies. This means we live in a world of multi-causality (and some times a-causality, i.e. no cause) where simple linear constructs fail to model human behavior effectively. Indeed, they may even lead to self- deception about how the world works.

Consequently, leaders in political military affairs, business, medicine, and all major professions have begun to change their views of the world according to new paradigms of action. This shows up in research on *national security* such as Thomas Czerwinski's Coping **with the Bounds, Speculations on Non linearity in Military Affairs**; on *leadership*, as in Margaret Wheatley's **Leadership and the New Science:** in *business*, as with Peter Senge's **The Fifth Discipline**, and in many emerging studies that will reshape the way we think and act.

In short, multi agent and multi causal models represent a needed paradigm shift in the analysis of political military affairs and International Relations.

Requirements of the New Paradigm

Where action on the ground is concerned, CA and PSYOP officers need to understand these concepts, because they have important doctrinal implications related to the expectations of policy makers regarding high tech solutions. This is especially important with regard to Operations Other Than War where the role of new technology in such operations emerges as a "qualitatively different problem from command and control in peace operations…" This requires new thinking in order to use the new technologies effectively. In other words, "…we are moving from a Newtonian and Cartesian paradigm of viewing the world as a clockwork universe, inherently mechanical, predictable, rational and reductionist, to viewing the world as flowing, adapting, nonlinear and holistic. (OOTW, p1) This view guides current and forthcoming military analysis such as the Strategic Assessment 2000 published by the National Defense University.

Based on this paradigm shift, "…new tools have been developed due to the increased synergy between the computer and our own minds, the ability to compute what

models, or descriptions of nature, we had conceived, but had, heretofore, only approximated." (OOTW, p2) Some of these new tools are described below, but the essential point here is that they are useful to the extent that they interface with users and doctrine that embody new operational concepts. This includes successful management on the ground of technology based on phenomena such as neural networks, cellular automata and genetic algorithms.

While we need not know the technical scientific definitions or theoretical aspects of these phenomena, the point here is that they refer to different ways of getting things done in the operational environment. In particular, they affect our views of "control" and uncertainty regarding political military outcomes. Ironically, the prospect of pinpoint precision and total networking of operational personnel can trigger an overload of information yielding an uncertainty over priorities, protocols and traditional command and control issues.

As the 1998 Marine Corps study on Maneuver Warfare concludes:

> Just a few years ago, we could not accept living with uncertainty on the battlefield. The prevailing view was that if we were able to collect and process enough information, with the right models and equations then we could prosecute war better. However, what [we know from] complexity theory … is that we cannot overcome or "control" uncertainty through the collection and processing of information. In fact, we may be fooling ourselves in thinking that we could have any control at all. (Hoffman and Horne, 1998, p7)

Thus, the technological challenge for the CA PSYOP officer is to develop a political military interface that accurately matches outcome expectations with appropriate technologies.

Technology and Operations Other Than War (OOTW)

The current technology revolution has introduced important new tools in many fields including medicine, telecommunications, microelectronics, and military operations. As a recent study by the National Defense University has noted "many technologies are being developed for many purposes, but these technical 'solutions' often appear out of step with operational priorites."35. Consequently, technology effectiveness depends heavily on "educating operators about what is available and feasible...[and to do so in a way that] bridges the present gaps between technology, policy and operations"(OOTW, p. 35)

For example, several generic technologies "appear to have wide application across representative OOTW" in just this manner. The data in Figure 1 juxtaposes generic technologies with possible missions. "In the military context, most of the technologies require integral C2, or are themselves a C2 application." (OOTW, pp. 39-41)

Figure 1. OOTW Missions and Generic Technologies

OOTW Technologies Missions	Information Disinformation	Information Sharing	Information Handling	Day/Night All Weather	Signatures	Training and Simulation	Sensors Platforms		Non-Lethal Weapons
Counter-Insurgency	+	+	+	+	+	+	+	+	+
Counter-Terror	+	+	+	+	+	+	+	+	+
Peace Enforcement	+	+	+	+	+	+	+	+	+
Peace Operations	+	+	+	+	+	+	+	+	+
Counter Drug	+	+	+	+	+	+	+	+	+
Civil Operations	+	+	+	+		+		+	+
Non-Combat Evacuation	+	+	+	+		+		+	+
Disaster Relief	+	+	+	+		+	+	+	+

Thus, C2 requirements, not just technical feasibility determine potential mission effectiveness. These same OOTW mission areas can be juxtaposed to technology applications that support each mission as shown in Figure 2 (below) to demonstrate "near-universal application across many mission areas." (OOTW, p. 41)

Figure 2. OOTW Missions and Technologies

OOTW Technologies Missions	Counter Insurgency	Counter-Terror	Peace Enforcement	Peace Operations	Counter Drug	Civil Operations	Non-Combat Evacuation	Disaster Relief
Demining	+	+	+	+				
PSYOPS	+	+	+	+	+	+	+	
Sniffers	+	+	+	+	+			+
Computers	+	+	+	+	+	+	+	+
Mechanical Disablers	+	+	+	+	+			
See Through Walls	+	+	+	+	+			
Acoustics	+	+	+	+	+			
PSYWAR	+	+			+			
Lasers	+	+	+	+	+			
Terrorist Atk Warning	+	+	+	+	+			
Radio Frequency	+	+	+	+	+	+	+	+
Counter Sniper/Mortar	+	+	+	+				
Body Armor	+	+	+	+	+			
AP/AM	+	+	+	+	+			
Anti Sam	+	+	+	+				
Auto Translation	+	+	+	+	+	+	+	+
Crowd Control	+	+	+	+		+	+	+
Location Recovery	+	+	+	+	+	+	+	+

Specific OOTW technologies currently under development include demining equipment, non-lethal weapons and several specific devices listed below:

Soldier 911, PRC-112/GPS Tracking and Warning system –
Preprogrammed border location and situational alert transmitting.

Livermore Labs
"Lifeguard" Anti Sniper IR System –Infrared sensing system to track sniper bullet trajectories and return fire automatically

-***People/Vehicle/Metal Sensors*** - For use in Border Patrol to distinguish people from metal background objects

Hovering UAVs – "local area satellites" that can be fitted with sensors to provide "near real time" data

MHD (Magneto Hydro Dynamics) - designed for actions such as "disabling equipment and stopping vehicles "with electromagnetic power impulses"

High Power, Low Frequency Sound Systems – Acoustic NLW that can cause intestinal distress and disorientation

High Intensity Lights/Laser Weapons – designed to "flash-blind" people and disrupt or disable optical and infrared targeting system

Stink Bombs – A negative olfactory experience

Micro Sensor Networks – Designed to create randomly scattered fields deployable from a wide range of delivery systems

Taken together, the research, development and fielding of such technologies introduces new issues in doctrine, training, and rules of engagement and new uncertainty in political military affairs.

Technology in Regional Theatres

High technology has transformed the way we do business in all key areas of life and this has penetrated every major region of the world. Just log on to the Internet for an example: http://www.arab.net/gid/welcome.html. This is the web site of the Jordanian state intelligence service. And consider the political demand of a Chinese politician in a "dirt poor" northern Chinese village: "We need more trees, also fiber-optic cable so everyone can have a telephone." (Friedman, p. 60) Fiber optics in rural China where schoolhouses have dirt floors? What does this tell us?

In short, any given region of the world will exhibit a mix of technologies unique to that area so we need to analyze how high tech resources interface with low-tech environments.

So, what are the operational considerations? A hallmark of the new technology paradigm is the opportunity, indeed the necessity to approach the world as a mix of dynamic systems and to adapt to diverse environments with a mix of high and low tech solutions. This means that we must adopt "non linear [models] and methods that will help better represent the real world." We need new questions that generate field applicability of political military analysis.

As an observational exercise, for example, we can ask which technologies elites and masses in a given environment use to process and exchange information. How does this compare to the information technology we use? What can we expect counterparts to know and not know about us as a result? And, how can we exploit what the counterpart does not know about us?

From an operational standpoint, additional questions related to mixed technology environments can shed light on how to interpret various aspects of the political military environment. For example, can low tech environments characterized by manual labor and handicraft economies "modernize" rapidly to attain high payoff productivity? Why (or, why not)? What is the relationship between technology and prospects for sustained development? Along these same lines, what role does culture play in technological and economic development. Do cottage industries and traditional village cultures signify intellectual and political inferiority because of high tech poverty or, are all people essentially equal in capability given the same technology? We may find valuable results by simply asking how local people and their elites solve problems in terms of available technology.

Asking and answering these kinds of questions can help the political military officer use the sixteen factors of analysis a "heuristic" device to create a "crude picture of the whole" operational environment, with technology as a pivotal dimension. In this manner, the "inherently nonlinear nature of the military C2 system" and the dynamics of mixed technology environments can offer new tactical and strategic opportunities.

This means that observing how people communicate, conduct business and go about their daily lives can tell us not only about technology but also reveal behavioral "codes" by which people collectively confront challenges, cope with disaster, relate to authority and sustain their identities.

III. Conclusion

As a new addition to the pol mil framework, this discussion of technology is still in draft so it remains for the reader to identify and research additional technology issues related to political military affairs. In particular, it is important to reckon with the multi-dimensional aspect of the technology concept because not all pol mil environments are high tech. Indeed, technology must be viewed in terms that go beyond just a simple spectrum of low to high tech assets that populate any given environment in order to arrive at an effective plan of action. We must therefore ask where each nation(s) of a target environment experiences advantages and disadvantages. And, in doing so, we will have another part of the puzzle that this book seeks to piece together. By assessing the technological dimension of the environment we can create more accurate explanations about how nations and their societies "form, function and fail." (Pentland, 1994)

Works Cited:

Thomas L. Friedman. **The Lexus and the Olive Tree. Understanding Globalization**. New York: Farrar, Strauss, 1999.

F.G. Hoffman and Gary Horne (eds.) **Maneuver Warfare Science 1998**. Washington, DC: Department of the Navy, 1998.

Institute for Strategic Studies. **Strategic Assessment 2000**. Washington, DC: National Defense University Press, 2000.

Nicholas Negroponte. **Being Digital**. New York: Knopf, 1995.

Operations Other Than War: The Technological Dimension. Washington, D.C.: National Defense University, 1995, 1997.

Pat A. Pentland. **Center of Gravity Analysis and Chaos Theory.** Readings Vol. IV, Center of Gravity Analysis. School of Advanced Airpower Studies, 1994.

Peter Senge. **The Fifth Discipline. The Art and Practice of the Learning Organization**. New York: Doubleday, 1990.

Perry M. Smith**. How CNN Fought the War. A View From the Inside**. New York: Birch Lane Press, 1991.

Margaret Wheatley. **Leadership and the New Science**. San Francisco: Barrett-Kohler, 1999.

Resources:

David S. Alberts and Thomas Czerwinski. **Complexity, Global Politics, and National Security**. Washington, DC: National Defense University Press, 1997. Essential discussions by high level leadership.

Patrick Cronin (ed.) **2015: Power and Progress**. Washington, DC: National Defense University Press, 1998. Analytical assessments of regional issues, including environment, coalitions, technology and information warfare.

Chaos and Complexity for Social Scientists: An Annotated Bibliography of Useful Books and Articles. http://www.hehd.clemson.edu/complex/annotBib.htm

Thomas Czerwinski. **Nonlinearity and Military Affairs: A Working Bibliography**. Washington, DC: Information Resources Management College, July, 1999.

Andrew Ilachinski. **Complex Systems Theory Related URL Links on the World-Wide-Web: HTML Listing**. Alexandria, VA: Center for Naval Analyses, 1996. This is a twenty five-page listing of web sites.

National Defense University Library. **The New Sciences: A Bibliography**. Washington, DC: National Defense University Press, 1997 .

Chapter 17

Media

I. Introduction

While we generally accept that the role of the mass media is a critical political-military factor, it is difficult to know precisely what the influence is. In analyzing the role of the media, one of the most pervasive questions may be the hardest to answer. What is the power, influence, and effects of various media? The short answer is: causal relationships are difficult to as certain because of the confounding effects of multiple variables.

Dutton defines media as a "critical *cultural institution* in which ideas and meanings are created and circulated within the society (Dutton, 10)." Mass media is a relative term; it refers to media that reach a large number of people.

Analyzing media can be approached from the standpoint of the basic elements of communications theory: sender, medium, message, and receiver. In looking at the media from these elements we will also highlight the tenets of the major theoretical perspectives. Be wary of theories that try to explain the media by focusing on only one aspect of the communication process.

II. Analyzing the Senders

A common question posed is: who "controls" the media? Who determines what messages to transmit? Is it the government, commercial sources, journalists, editors, the public (by what they will tune in to), or some combination of the above?

The propaganda and Marxist models focus on the senders and their messages. These theories focus on what *media does to people.* In these models, the media is an agent of social control, subservient to the dominant forces (elite) in the economic and political environment. Media is seen as a shaper of culture. In the words of Dutton, "The interests of the ruling group (be it a ruling class, patriarchy, etc.) are maintained through the media reproducing a dominant ideology, a set of beliefs and ideas which represent those interests as natural (Dutton, 5)." Ownership of the media is regarded as a key component in the domination of one class over another. From the Marxist perspective, the concentration of ownership and high entry costs prohibit contending viewpoints from being heard.

In the economic model, the mass media is viewed as industry. The mass media caters to market segments. The owners or senders seek to maximize audiences, rather than control or change audiences. In this model, what is produced is determined by demand. Profitability is the overarching goal. From this perspective, the prevailing views espoused in the media will be those in consonance or harmony with the prevailing cultural norms and values.

In the pluralist and free press models, no single sector of senders is omnipotent. There is a distribution of power in society; many competing interests have access to the media. While mass media tend to reinforce central values, the mass media also reflect culture. Changes in culture are reflected in changes in media. Even within sectors, no group is a monolith. For example, within government, there are differences between what the various actors have to say, The evidence of the utility of this model is indicated by the degree of diversity in a country's media.

In the functionalist model, the focus is on determining the roles and functions that media serve in a society. What role does the media play in socialization? Is the function of media entertainment, informational, ritual, or some combination (for example, "infotainment")?

In analyzing senders in a country, examine who owns mass media systems. But also realize that there may be a difference between who owns media and who finances media. For example, corporations own much of the media in the West, but media is primarily financed by advertisers (and indirectly, the audience). Also look at the role of conglomerates. Is ownership highly concentrated and what are the implications of this concentration? Who has access to media production?

How does the government influence media? Is there overt control by the government? Or does the government have an impact in other ways? How important is the government as a source of information? Even when the media is not explicitly controlled by the government, what role does the media play in disseminating government viewpoints? Is the news primarily generated by government press releases and news events or does investigative reporting play the major role? What influence does the government have in determining how issues are framed?

What is public policy, law, or regulation with regard to the media? Are there license fees, accreditation procedures, or legal restrictions on what can be propagated? Is there overt censorship? What happens to those who produce "illegal" media? Imprisonment? Are there subtle or indirect forms of censorship? Is there a government ministry of information (or culture) which has an impact on what is produced? For example:

> Every [Arab] government but Qatar has an information ministry whose Essential task is to mobilize the media - and through them, the public at large -in support of government policies. Information ministries monitor reporters' activities and whereabouts and help to shape (and sometimes wholly shape) the news agenda - both that which they produce for domestic consumption, and that which they allow to be broadcast overseas (Alterman, 1998, p.49).

How does the government control or influence media emanating from external sources? Are there restrictions on foreign ownership? Are there rules that favor certain producers? For example, in Saudi Arabia, in addition to overt rules, *al-Sharq al-Aswat (The Middle East)* is the only international newspaper that is printed in Saudi Arabia. This means it is the first international paper available each day. The paper is generally very supportive of the Saudi regime (Alterman, 1998).

Is the media in the country in transition from being state-dominated to a more pluralist model? And what are the implications? In states where media have been dominated by political propaganda, there are indications that people react differently to new media, particularly advertisements. This has been true in Russia, where the population is unforgiving of anything resembling propaganda or distortion (Davidson, 1992). Overall in Russia, advertisements have tended to remain heavily factual rather than persuasive (Mueller, 1996). Based on survey research of Russians after being exposed to Western TV commercials in 1990, a member of the J. Walter Thompson agency described the Russians as ambivalent about advertising:

> Emotionally, commercials are capable of evoking two opposing kinds of responses. On the one hand, they give a quality catharsis - an escape from daily hardship into fantasy and dreams. On the other hand they are capable of causing deep resentment and a wish to

> distance oneself because the imagery is too painful and absurdly removed from current reality. (As quoted in Davidson, 1992. p.48)

Brzezinski (1993) makes a similar point in his discussion of global communications and their effect on increasing awareness of inequalities.

What effect has technology had on the sender? Does technology make it more difficult for governments to control what people receive? Although some may predict that the Internet will reduce the ability of the state to control the flow of information; the opposite may be true. Those states with a propensity to try and control information will probably attempt to continue that propensity. Electronic searches may make it easier. It depends on encoding and routing. And the government may still have a gatekeeper function. For example, Bahrain, the UAE, and Saudi Arabia all have firewalls that control access into and out of the country (Alterman, 1998). While new mediums may hamper traditional censorship, the effect is not preordained.

III. Analyzing the Medium

Examine what media are commonly used. A good reference book, such as World *Radio & TV Handbook 1999, is* a useful starting point for radio and TV. Other reference books are available for other media. Also determine the relative importance and role of the various types of media. Is society oral, print-based, electronic or some combination depending on the sector? For most of the world, oral modes of communication continue to be an important means by which societal values are transmitted and acculturation takes place. Media can be classified into three broad categories:

a. Visual

- Newspapers
- Books
- Posters
- Internet (can also be audio-visual)
- Magazines
- Leaflets/pamphlets
- Direct Mail
- Billboards

b. Aural

- Telephone
- Radio
- Audio Recordings

c. Audio-visual

- TV (broadcast, cable, satellite)
- Internet
- Rallies/public speeches/conventions
- Schools (esp. compulsory public ed)
- Word of Mouth
- Audio-visual recordings
- Film
- Plays/live drama
- Church
- Loud speakers

Also examine what effect the medium has. Marshall McLuhan answers this question in the often quoted "the medium is the message," where is the focus is on technology and production.

What effect has technology had on mediums? According to Altschull the press in some countries "has been losing its character as an instrument of substantive information One result of technology is the constant news cycle. There is a premium on having something new. Those with the hottest news can capture audience and therefore advertising dollars. Previously, the news cycle was twice a day: the morning paper and the evening news. In the twice a day cycle there was more time for reflection, analysis, and confirmation. What role does live coverage have? We

see a compelling television image and we believe. But do images mask reality? The image may not be indicative of a greater reality.

And technology may not be the decisive factor. In the Iranian revolution, cassette tapes were critical in broadcasting the revolutionary message. Although there were more sophisticated technologies present, they were not readily accessible to the revolutionary movement.

Also determine if language poses a barrier to use of new technologies? For example, only a few search engines can search Arabic text (Alterman, 1998).

IV. Analyzing the Masses

In analyzing the media in a country, look at the form and content of the media products that are produced. What is mediated? Read the news available in the Foreign Broadcast Information Service (FBIS). Analyze advertisements. What symbols and themes are used by advertisers of products that are successful in a country? Even if you don't understand the language, watch film or TV. Try to answer the following questions:

- What are the dominant styles and formats found in the media?
- How are the visual arts used?
- How is music used?
- What symbols are used?
- What are the themes?
- Who is the messenger?
- Who are the opinion makers?
- What are the patterns?
- What is the regularity and how much repetition is used?
- How much variance is there?
- Do all of the major providers basically provide similar material in similar formats?
- What is the length?
- What is the role of sports in the media?
- What is the role of the news?
- What is considered newsworthy, and what is the content of the news?
- Who judges what is important?
- In prosperous and stable times, how interested are people in political news?
- Is news primarily information or entertainment?
- Is it analysis, commentary or opinion about the news?
- How prevalent are statements by public officials in the news?
- What is conspicuously absent from the media?

When analyzing the media in a country, look at a wide cross-section of media products. Doing so can provide a window into the culture.

V. Analyzing the Receivers

While the propaganda model focuses on the sender and the message, Elihu Katz poses the question in terms of what media does to people, but *what people do with the media.* Katz's basic argument is: the media must be analyzed within the context of social, cultural, and political institutions. The focus is on the reception and consumption of the message. In his 1977 book (co-authored with Wedell), *Broadcasting in the Third World: Promise and Performance*, Katz analyzes the introduction of broadcasting institutions into developing countries. Drawing on

original research in eleven countries, he concludes that there is a significant difference between expectations and actual effects across countries. The intended message may be very different than the audience's reading.

Katz's cross-cultural study *The Export of Meaning: Cross-Cultural Readings of Dallas* further indicates that viewers interpret according to their cultural prism. In other words, media that emanate from foreign sources interact with indigenous factors. The result in one country may be very different than in another. Do not assume you know what the effect will be. There are many factors which influence acceptance of a message, including the value system of the receiver, credibility given to the source, and repetition.

When assessing the impact of mass media on audiences, examine the characteristics of media that has a wide audience. From a purely behavioral standpoint, what are the patterns of reception? What is the dispersion/concentration of media and of audiences? Are there diverse products for a diverse audience?

What is the effect of technology on the receiver? As Alterman reports, "Only about 10 to 15 percent of all Arabs have regular access to satellite television, a smaller number reads the international Arabic press, and a smaller number still is proficient with the internet (p.3)." Although technology may provide access to new sources of information, to what degree do people use those sources? And what percent of the audience can afford access?

VI. Inter-relationships and Some Analytical Questions

Cultural Environment

- What role does media play in transmitting culture within the society?
- What role does media play in creating/sustaining a national identity?
- To what degree does the media serve as an agent of change?
- What is the form and content of prevalent media?
- What explicit meanings are in this content?
- What implicit meanings are in this content?
- To what degree does content reinforce the status quo?
- How are subcultures reflected in the media?
- Are new products or genres easily accepted, or are products that differ too much from the mainstream rejected?
- Does transnational media contribute to distorted perceptions about other cultures?
- To the extent that Western media has significantly penetrated the culture, how has it affected the culture?

History

- Do shared media experiences become history?
- Does the portrayal of history in mass media become the prevailing understanding of history?

Elites

- What differences are there in media consumption patterns of elites and others?
- What is the role of opinion leaders who interpret events?

Foreign Influence

- What is the degree of foreign media penetration?
- Is foreign ownership permitted; are there restrictions?
- What is the effect of transnational media?
- Does it highlight relative deprivation?

Political System

- What are the parameters of political debate within the media? (While debate may be acceptable, there may be area that are out of bounds and therefore not tolerated by governments or accepted by the general populace.)
- What is the degree of press freedom?
- What topics are taboo?
- Is it permissible to criticize the head of government?
- Is there an alignment between media and political parties or particular interest groups?
- How does access affect what is produced?
- Are those journalists who present issues in a light most favorable to the regime rewarded with better access to officials?
- How dominant is the state in the shaping of the media?

National Interests

- Has the country entered into any interstate agreements concerning the flow of media
- What effect has media had on the power and influence of non-state actors?

Political Economy

- Who owns mass media systems?
- Who finances media?
- What is the relationship between the state, the economy, and the media?
- What is the economic impact of the media?

Role of the Military

- How is military service portrayed in the media?
  For example, the perceptions created by the movie *Saving Private Ryan* are much different than the view of military service portrayed in Top Gun.

Religion

- What impact has the media had on traditional religious values?
  For example, Sinclair (1987) argues that the advertising prevalent in Western media has the cultural effect of legitimizing consumption and de-emphasizing religious dogma. Advertising appeals to desire, pleasure, and achieving satisfaction through consumption. The effect may serve to undermine some religious conditioning which focuses on rewards in an afterlife rather than earthly rewards. In a culture that constantly and pervasively emphasizes consumption,

individual gratification is no longer taboo. Brzezinski (1993) makes a similar point in his discussion of "permissive cornucopia".

VII. Summary

There is no single framework for analyzing and understanding the media. The relevance of different theological perspectives change by country. The role, importance, and functions of the media also change from society to society. You must examine media in the *context* of the other political-military factors. Economics, politics, culture, and the media are inextricably intertwined. Media can be an independent variable, acting as an agent of change, and media can also be the dependent variable, changing in response to other factors.

Selected References

Alterman, Jon. *New Media, New Politics? From Satellite Television to the Internet in the Arab World. The Washington Institute for Near East Policy, 1998.*

Dutton, Brian. *The Media.* New York: Longman, 1986.

Herman Edward S. and Chomsky, Noam. *Manufacturing Consent: The Political Economy of the Mass Media.* Pantheon, 1988.

Katz, Elihu and Wedell, E. *Broadcasting in the Third World: Promise and Performance.* Cambridge: Harvard University Press, 1977.

Keohane, Robert and Nye, Joseph. "States and the Information Revolution," *Foreign Affairs,* September/October 1998.

This Page Is Intentionally Left Blank

The Fairchild Papers

The Role of Rhetorical Theory in Military Intelligence Analysis

A Soldier's Guide to Rhetorical Theory

Gary H. Mills
Major, USAF

AIR UNIVERSITY LIBRARY

The Role of Rhetorical Theory in Military Intelligence Analysis

A Soldier's Guide to Rhetorical Theory

GARY H. MILLS
Major, USAF

Fairchild Paper

Air University Press
Maxwell Air Force Base, Alabama 36112-6615

August 2003

Air University Library Cataloging Data

Mills, Gary H., 1967–
The role of rhetorical theory in military intelligence analysis : a soldier's guide to rhetorical theory / Gary H. Mills.
p. : ill. ; cm. — (Fairchild paper, ISSN 1528-2325)
Includes bibliographical references and index.
ISBN 1-58566-121-X

1. Foucault, Michel. 2. Military intelligence. 3. Rhetoric. 4. Discourse analysis. 5. Intelligence officers. I. Title. II. Series.

358.3432—dc21

Disclaimer

Opinions, conclusions, and recommendations expressed or implied within are solely those of the author and do not necessarily represent the views of Air University, the United States Air Force, the Department of Defense, or any other US government agency. Cleared for public release: distribution unlimited.

This Fairchild Paper and others in the series are available electronically at the AU Press Web site http://aupress.maxwell.af.mil and the Air University Research Web site http://research.maxwell.af.mil.

Dedicated to
Muir S. Fairchild (1894–1950), the first commander of
Air University and the university's conceptual father.
General Fairchild was part visionary, part keen taskmaster,
and "Air Force to the core." His legacy is one of confidence
about the future of the Air Force and the central
role of Air University in that future.

Contents

Chapter		*Page*
	DISCLAIMER	*ii*
	DEDICATION	*iii*
	FOREWORD	*ix*
	ABOUT THE AUTHOR	*xi*
	PREFACE	*xiii*
	ACKNOWLEDGMENTS	*xv*
	ABSTRACT	*xvii*
1	INTRODUCTION	1
	Notes	4
2	LET'S GET RHETORICAL	5
	Notes	10
3	INTELLIGENCE PROCESS	11
	Notes	19
4	[WHAT THE] FOUCAULT?	21
	Notes	26
5	POWER PLUG	27
	Notes	37
6	DISCONTINUITY FEVER	39
	Notes	46
7	IN THE TRENCHES	47
	Notes	54
8	CONCLUSION	55
	Notes	57
	BIBLIOGRAPHY	59
	INDEX	63

Illustrations

Figure *Page*

1 Military Briefing Origins 8

2 Intelligence Organizations (Agencies) 12

3 Intelligence Cycle 12

4 Spectrum of Thought 25

5 The Panopticon's Point of View 29

6 Power and Knowledge Flow 32

7 Discourse Hierarchies 33

8 Discourse Tactical Considerations 34

9 Power Analysis 40

10 Influence of Deception Warning Signs on Analysis 43

11 Communication Triangle 48

12 Communication Analysis 49

13 Enhanced Communication Triangle 50

Photographs

National Reconnaissance Office Corona Satellite 13

SA-2 Missile Site 14

U-2 and the Predator 15

Formal and Tactical Intelligence Briefings 18

Iraqi Aircraft Shelter 19

C-130s and Troops 28

Photographs *Page*

E-3 Sentry and E-8 Joint Surveillance, Target Attack Radar System 30

Refugees of the Conflict in Kosovo 41

Uncertainties of Conflict: Crews Train in Chemical Warfare Ensembles 42

F-16 Vipers 47

US Embassy Damaged by Terrorists in Tanzania 56

Table

1 Intelligence Sources 16

Foreword

The Role of Rhetorical Theory in Military Intelligence Analysis: A Soldier's Guide to Rhetorical Theory by Maj Gary H. Mills is another in an Air University Press series of substantive essays considered too short for publication as monographs but too lengthy to be journal articles. The purpose of *The Role of Rhetorical Theory in Military Intelligence Analysis* is to share Major Mills's rhetorical understanding with young officers attending initial intelligence training. Throughout he infuses key elements from the rhetorical discourse community into the discourse community that deals with training in military intelligence. Major Mills notes that his target audience is the military intelligence community. However, Air University Press is pleased to include this study as one of its Fairchild Papers because many aspects of *The Role of Rhetorical Theory in Military Intelligence Analysis* can enhance the rhetorical analysis of traditional university students and instructors.

Shirley Brooks Laseter

Dr. Shirley B. Laseter
Director
Air University Library & Press

About the Author

Maj Gary H. Mills, USAF, is currently serving as a senior analyst at Supreme Headquarters Allied Powers Europe. Prior to his current assignment, he was an assistant professor of English in the Department of English and Fine Arts at the United States Air Force Academy (USAFA), Colorado Springs, Colorado. Additionally, Major Mills was design director of *War, Literature and the Arts: An International Journal of the Humanities* and *Andre Dubus: Tributes* (Xavier Review Press, 2001). He holds a Master of Arts in technical and expository writing. Major Mills was commissioned through USAFA in 1990.

Preface

Nimitz's concept of intelligence was dynamic: Facts were high-grade ore to be sifted carefully, the pure metal of knowledge extracted and forged into a weapon to defeat the enemy.

—Gordon W. Prange
Miracle at Midway

I completed training for USAF intelligence-applications officers more than a dozen years ago. Since then I have used and adapted the USAF's practical discourse and analytical skills in a wide range of situations around the world. However, I never fully grasped the rhetorical framework behind these critical modes of communication until I was exposed to discourse theory at the University of Arkansas at Little Rock. As a result of my studies, I have learned how the rich backdrop of theory adds to the daily application of intelligence analysis.

Fortunately, as a result of my rhetorical education, I have a greater understanding of the critical theory behind each briefing, presentation, and mission-planning product. More importantly, theory focuses a penetrating analytical view on the power coursing through threat systems and hostile countries. Clearly, Air Force intelligence specialists will benefit from a detailed look at the ways an understanding of rhetorical theory enhances intelligence analysis. My purpose is to share my widened rhetorical understanding with young officers attending initial intelligence training. Throughout this study, I infuse key elements from the rhetorical discourse community into the discourse community that deals with training in military intelligence. As a result of this union, a powerful discourse paradigm shift places military intelligence specialists in a unique rhetorical position—one that will turn rhetorical theory into a powerful force multiplier.

My target audience is the military intelligence community; however, many aspects of this study can enhance the rhetorical analysis of traditional university students and instructors. The same targeted and tailored analytical approach used with threat systems applies equally well with almost any subject placed under the rhetorical "crosshairs." While adapting this

study to nonmilitary analysis, the reader should feel free to replace the intelligence cycle—discussed later—with processes specific to his or her discourse community. Additionally, the unit-level issues—addressed in the chapter titled "In the Trenches"—are applicable to a wide range of nonmilitary organizations and discourse groups.

Michel Foucault's rhetorical lens allows a detailed view of power and discontinuity in a widening range of situations and organizations. Rhetorical theory's application, in the enhancement of intelligence analysis, highlights its powerful, universal utility; with equally powerful utility, other rhetorical masters are also addressed. Readers should open themselves to the dynamic utility of rhetorical theory and remember that it is a power tool that continues to shape discourse and perceptions. For many, theory is an ephemeral element in the course of day-to-day activities; and in 1994, according to Ferdinand Saussure, "the very ones who use it daily are [often] ignorant of it." Fortunately, for those who can see and wield it, theory serves as a force enhancement and a catalyst for powerful paradigm shifts. In 1995 Walter J. Ong noted in his book *Orality and Literacy: The Technologizing of the Word* that rhetorical theory will continue to surround and shape our human identity. Through a strong rhetorical understanding, we bridge the gap between theory and application, resulting in the enhancement of our daily operations and analytical growth.

Acknowledgments

I thank the following professors for their outstanding support and guidance: Brig Gen (USAF, retired) Jack Shuttleworth, PhD, permanent professor and department head, Department of English and Fine Arts, USAFA, Colorado Springs, Colorado; Dr. Charles Anderson, Dr. Julia Ferganchick, Dr. Michael Kleine, Dr. Barry Maid, Dr. Roger Munger, and Dr. Richard Raymond, all from the Department of Rhetoric and Writing at the University of Arkansas at Little Rock. They excelled as academic authorities and, most importantly, professional mentors. I also recognize Naval Doctrine Publication 2, *Naval Intelligence,* which served as a key inspiration for my selection of some of the epigraphs for each chapter. Additionally, the Central Intelligence Agency's *A Compendium of Analytic Tradecraft Notes* bridged a daunting gap between theory and application, thus helping to open the way for rhetorical theory in the intelligence career field.

Abstract

As an unconventional analytical source, Michel Foucault contributes new power perspectives to intelligence analysis; and he gives a nontraditional look at a growing, evolving threat environment. As highlighted in *The Foucault Reader,* Foucault's analytical edge confronts these threats "by refusing to separate off knowledge from power." "His strategy has been to focus his work, both political and intellectual, on what he sees as the greatest threat—that strange, somewhat unlikely, mixing of the social science and social practices developed around subjectivity." Foucault's theories address the human behind the satellite images and database numbers: the result generates a powerful perspective on threat countries, systems, and situations.

His power influences resonate in every human system and organization. Specifically, he addresses the flow of power through organizational hierarchies. Through Foucault's rhetorical vision, one can look at an organization as a power being with a rhetorical circulatory structure supporting its existence. Power (discourse and knowledge) flows through the entire organization. Now, as a power-influenced (human-conceptualized) entity, organizations have spatial, temporal, and social compartmentalizations. These compartmentalizations require a physical means (conduits) of sharing information in order to allow power to flow. Additionally, Foucault addresses—in the 1982 book titled *The Archaeology of Knowledge and the Discourse on Language*—how the power shifts, ruptures, and discontinuities in the conduits can take on many forms when overlaid against the wide range of global norms. Most importantly, based on theory's powerful utility, the seeds of analysis must be planted as early as possible. Rhetorical theory is the key to enhanced analytical growth—an outgrowth that serves as a powerful military-intelligence force multiplier.

Chapter 1

Introduction

> *Knowledge is for me that which must function as a protection of individual existence and as a comprehension of the exterior world. I think that's it. Knowledge is a means of surviving by understanding.*
>
> —Michel Foucault

As intelligence specialists, the exterior world—more than 260 countries, geographic regions, and their associated political and military challenges—will test your ability to organize, process, and analyze vast amounts of information.[1] You have joined a skilled community responsible for the tireless analysis of potential and active threats against the United States. Fleet Adm Ernest King, USN, retired, effectively voiced the demanding requirements and standards for the modern intelligence specialist: "Institute rigorous, continuous examination of enemy capabilities and potentialities, thereby getting the utmost value of information of the enemy and enabling our forces to be used with the greatest effectiveness. It is particularly important to comprehend the enemy point of view in all aspects."[2]

Comprehension of the threat point of view requires a rhetorical vision that can be focused only through a fundamental understanding of how communication (verbal, textual, symbolic, and electronic) influences the intelligence cycle and, ultimately, joint combat operations.[3] Simply put, rhetorical theory (the exploration of communication and its impact, influence, and relationships in all forms) is in action all around us; it applies to every aspect of human existence. The role of theory in intelligence analysis is even more pronounced. Theory is a force multiplier; it is a natural, often overlooked, military enhancement.

An operationally tailored application of rhetorical theory can make the intelligence community—more importantly, your day-to-day work—even more effective. Typically, years of train-

ing and operational experience are needed to groom an outstanding analyst. Through a tailored instruction of rhetorical theory, new intelligence specialists just joining the career field can develop and mature at faster rates.

Well-worn steps and checklists are deeply ingrained in the military mind-set; however, the rich tapestry of rhetorical theory is unfortunately lost in the application of intelligence analysis at the level of a typical small unit. Dr. Charles Anderson, graduate-program director of the University of Arkansas at Little Rock's Department of Rhetoric and Writing, believes that we all know what to do come Monday morning, but theory helps us understand why. At unit level, theory takes a backseat to operations tempo, additional duties, and challenging requirements to meet a growing range of duties with fewer personnel. Typically, as a mission-oriented community, we tend to shun concepts and theories that do not appear to directly support the war fighters (soldiers, sailors, and airmen) in the completion of a broadening array of duties ranging from direct, conventional combat to peacekeeping operations. Theory is a powerful and integral part of current and future military conflicts. However, a look at a few unconventional rhetoricians is in order to focus the power of theory.

Sherman Kent, former Central Intelligence Agency (CIA) senior analyst and author, highlights the changing role of theory in intelligence analysis: "Intelligence today is not merely a profession, but like most professions it has taken on the aspects of a discipline: it has developed a recognized methodology; it has developed a vocabulary; it has developed a body of theory and doctrine; it has elaborate and refined techniques. It now has a large professional following. What it lacks is a literature. From my point of view, this is a matter of greatest importance. As long as this discipline lacks a literature, its method, its vocabulary, its body of doctrine, and even its fundamental theory run the risk of never reaching full maturity."[4]

Kent's call for a refined and tailored intelligence discourse makes the need for a solid comprehension of rhetorical theory even more critical. Additionally, he provides a superb example of rhetorical theory in action:

> The literature I have in mind will, among other things, be an elevated debate. For example, I see a Major "X" write an essay on the theory of indicators and print it and have it circulated. I see a Mr. "B" brood over this essay and write a review of it. I see a Commander "C" reading both the preceding documents and reviewing them both. I then see a revitalized discussion among the people of the indicator business. I hope that they now, more than ever before, discuss indicators within the terms of a common conceptual frame and in a common vocabulary. From the debate in the literature and from the oral discussion, I see another man [or woman] coming forward to produce an original synthesis of all that has gone before. His [her] summary findings will be a kind of intellectual platform upon which the new debate can start. His [her] platform will be a thing of orderly and functional construction and it will stand above the bushes and trees that once obscured the view. It will be solid enough to have much more built upon it and durable enough so that no one need get back in the bushes and earth to examine its foundations.[5]

Rhetorical theory can work exactly, and as easily, as Kent advertises in many settings with impressive results. Unfortunately, many analysts view this process as an administrative speed bump instead of an intellectual catalyst. Additionally, Kent's analytical foundation is only partially constructed if you fail to bring the right tools to the work site. With luck this guide will serve as a useful tool kit.

Application of targeted theory takes on many forms. For example, the CIA calls its process an "analytic tradecraft"—a process based on creative use of all source information and in-house best practices, in order to support "individual intelligence consumer's concerns."[6] Former deputy director for intelligence John Gannon—currently chairman of the National Intelligence Council—clearly recognizes both strengths and challenges of discourse. The growing "revolution in information technologies has improved our access to sources and our ability to quickly deliver intelligence."[7] Conversely, the rapid flow of information "has also made our [intelligence community's] work more challenging as we are bombarded with information of varying quality, relevance, and depth."[8]

All too often stereotyped and disregarded as pure academia, rhetorical theory is at the very core of military analytical development. Additionally, the same theory forms the basis of what many military intelligence specialists all too easily chalk up to mere experience. Through an operationally tailored analysis of Michel Foucault, this study will uncover a rhetorical framework

supporting the military analysis process: a rhetorical template designed to bridge the application gap between strict checklist discipline and power analysis, resulting in the highest quality of intelligence analysis.

Notes

1. Central Intelligence Agency, *The World Factbook* (Washington, D.C.: Brassey's, 1998), n.p., on-line, Internet, 10 June 1999, available from http://www.cia.gov/cia/publications/factbook/country.html.
2. Naval Doctrine Publication (NDP) 2, *Naval Intelligence*, 1994, n.p., on-line, Internet, 11 July 2003, available from http://www.nwdc.navy.mil/Library/Documents/NDPs/ndp2/ndp20001.htm.
3. Lydia A. Fillingham, *Foucault for Beginners* (New York: Writers and Readers Publishing, 1993), 100.
4. Sherman Kent, "The Need for an Intelligence Literature," *Studies in Intelligence*, spring 1955, 3, on-line, Internet, 2 February 1999, available from http://www.odci.gov/csi/books/shermankent/2need.html.
5. Ibid.
6. John Gannon, "Foreword," in Jack Davis, *A Compendium of Analytic Tradecraft Notes*, ed. F. Douglas Whitehouse (Washington, D.C.: Government Printing Office, 1997), v.
7. Ibid.
8. Ibid.

Chapter 2

Let's Get Rhetorical

> *The DI (Directorate of Intelligence) will need greater interaction with outside experts to meet the broad and complex analytic challenges it faces. It must position itself to compete in a new information age in which consumers increasingly will have ready access to alternative sources of high-quality data and expertise.*
>
> —*Analysis: Strategic Plan*
> Central Intelligence Agency
> Directorate of Intelligence

As an integral part of the military's new information age, you need to be aware of alternative sources available to enhance your communication and analytical skills. Recently retitled as intelligence operators, intelligence personnel must apply every available tool in order to support worldwide warfighter operations. As highlighted by the CIA Directorate of Intelligence, your effective use of "outside experts will yield useful information and insight, along with constructive challenges to [your] working assumptions, that can only sharpen [your] analysis."[1] In this study, Foucault's discourse theories serve as the primary rhetorical workshop. As a result, there is a need to define the wide and essential scope of rhetorical theory, including a brief look at its history. The word *rhetoric* brings to mind many different meanings: "The practice of oratory [discourse or speech]; the study of strategies of effective oratory; the use of language, written or spoken [or electronic], to inform or persuade; the study of the persuasive effects of language; the study of the relation between language and knowledge; the classification and use of tropes and figures; and, of course, the use of empty promises and half-truths as a form of propaganda."[2] Intelligence officers interface with most of these overlapping meanings.[3] You even study many influences and forms of propaganda. However, most importantly, you must understand that "rhetoric is an action" and that it affects communication and analytical perspectives.[4] "In

one sense, rhetoric is an action human beings perform, and in a second sense, it is a perspective humans take. As an action, rhetoric involves humans' use of symbols for the purpose of communicating with one another. As a perspective humans take, rhetoric involves focusing on symbolic [and analytic] processes."[5] With some luck, this study will effectively communicate the strength of rhetoric's influence on intelligence—ultimately changing and shaping your perspective on analysis.

As service-trained communicators, you use written, spoken, and electronic discourse on a daily basis. Unfortunately, aside from military briefing style and training in audience awareness (for aircrews, command staffs, threat working groups, etc.), military technical schooling provides very little instruction in rhetorical theory. Your job is to organize, analyze, and share information; yet, ironically, you get very little training in the formal discipline critical to the core of your military profession—a fifth-century B.C. discipline that was initially established to settle conflicting property claims.[6]

"A revolution on Syracuse, a Greek colony on the island of Sicily, in about 465 B.C." brought about the end of a dictator's reign and ushered in a democratic system of government.[7] As a result of this change, Corax of Syracuse saw the need to equip citizens with skills to settle their property disputes since "they could not hire attorneys to speak on their behalf as we can today."[8] "Corax realized the need for systematic instruction in the art of speaking in the law courts and wrote a treatise called the 'Art of Rhetoric.' Although no copies of this work survive, we know from later writers that the notion of probability was central to his rhetorical system. He believed that a speaker must argue from general probabilities or establish probable conclusions when matters of fact cannot be established with absolute certainty."[9]

It is intriguing to consider that the standard "Probable Course of Action" portion of our crisis and situation briefings shares a formal genesis that extends as far back as Corax's *Art of Rhetoric*. Origins of this often elusive and mystic discipline are based on a very pragmatic and simple need to clarify and establish truth.

Development of rhetorical theory has changed dramatically over the years. "The historical development of rhetoric [is] divided into conventional chronological periods: the Classical (from the birth of rhetoric in ancient Greece to about 400 [A.D.]), the Medieval (to about 1400), the Renaissance (to the early seventeenth century), the Enlightenment (from the seventeenth to the end of the nineteenth century, a bit longer than in conventional usage), and the twentieth century."[10] Years can easily be spent studying each period of rhetorical development. This study includes these rhetorical divisions to underscore the fact that, much like the military, rhetorical theory is always changing and establishing new communication paradigms.

Intimately tied to origins of the formal art of rhetoric, the classical preparation of a speech or briefing—a principal medium used to share intelligence information—is particularly important. "Aristotle devoted a large portion of his *Rhetoric* to invention, or the finding of materials and modes of proof to use in presenting those materials to an audience."[11] Aristotle's canons (rules or laws) resulted in the first "pragmatic processes of presentation."[12] The rhetorical process of preparing a speech or briefing is divided into five stages: "(1) invention, search for persuasive ways to present information and formulate arguments; (2) arrangement, organization of the part of a speech to ensure that all means of persuasion are present and properly disposed; (3) style, use of correct, appropriate, and striking language throughout the speech; (4) memory, use of mnemonics and practice; and (5) delivery, presenting the speech with effective gestures and vocal modulation."[13] These five canons remain the cornerstone of the study of rhetorical organization, and key elements of this organization are in all effective intelligence briefings (fig. 1).[14] Additionally, it is important to note, under the arrangement stage, that "Aristotle says that all speeches have four parts: the introduction, the statement of the issue, the argument, and the conclusion."[15]

As an essential element in modern intelligence briefings, "classical emphasis on logos [logical appeals used to persuade during the invention step] is presented as if in recognition that human beings respond most strongly to rational appeals."[16] Aristotle codified two additional forms of persuasion: ethos (character and

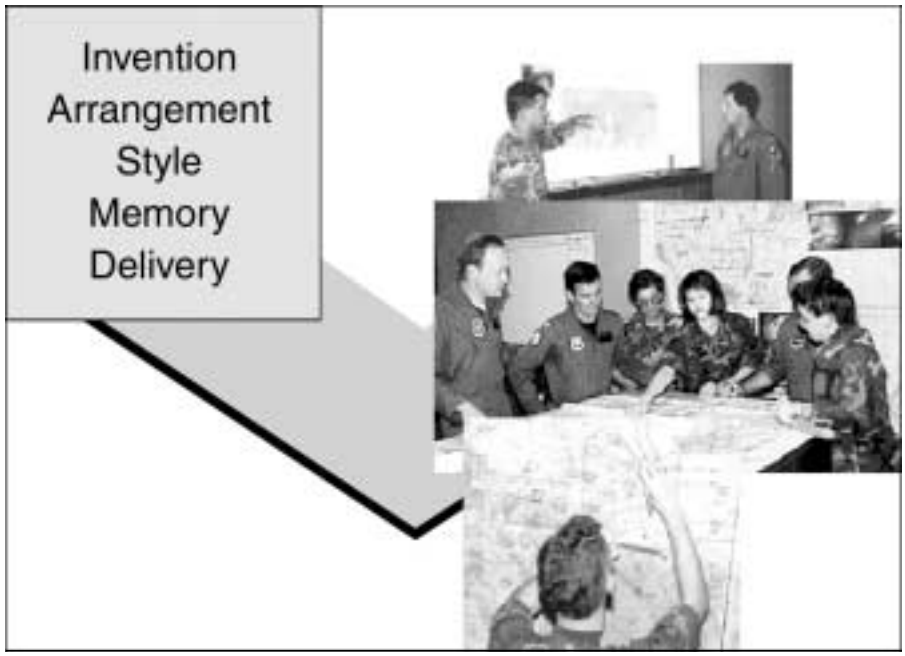


Figure 1. Military Briefing Origins

credibility) and pathos (the production of a certain attitude or emotion in the audience).[17] Obviously, you need to focus on logos and ethos—a logical analysis shored by credible sources (and a credible, ethical presenter) will serve you well. Methods you select to shape an audience's perception greatly influence your credibility. "As a rule, then, the consumer's confidence in the analyst's estimative judgment comes only after he or she has established credentials for expert command over all source information."[18] Importantly, you must respect pathos as a very powerful form of persuasion; however, please try to avoid emotional appeals—a sure way to crash and burn during a mission or current intelligence briefing.

Underlying the military's technical paradigm shifts, from linear formations to joint warfare and from muskets to precision weapons, exists an even more impressive rhetorical transition that continues to gather strength. Rhetorical theory is as alive today as it was during the days of its two key architects, Corax and Aristotle. Rhetorical theory is not as murky a

subject as some may have initially envisioned. You are already using, adapting, and improving on the rhetorical blueprints of the greats. "But there is more to say about the marriage of war [the profession of arms or military analysis] and knowledge."[19] Aristotle, a critical analytical cornerstone, raised an issue of analytical proficiency that should balance your growth as an analyst and officer.[20] He details the levels of knowledge required for true proficiency:

> Every systematic science, the humblest and the noblest alike, seems to admit of two distinct kinds of proficiency; one of which may be properly called scientific knowledge of the subject, while the other is a kind of educational acquaintance with it. For an educated man [or woman] should be able to form a fair offhand judgment as to the goodness or badness of the method used by a professor [or commander, allied or enemy] in his [or her] exposition [or leadership/tactics]. To be educated is in fact to be able to do this; and even the man [or woman] of universal education we deem to be such in virtue of his having this ability. It will, however, of course, be understood that we only ascribe universal education to one who in his [or her] own individual person is thus critical in all or nearly all branches of knowledge, and not to one who has a like ability merely in some special subject. For it is possible for a man [or woman] to have his [or her] competence in some one branch of knowledge without having it in all.[21]

You must avoid becoming strictly competent in only one branch of knowledge. Be "able to tell the difference between sense and nonsense, as we might say using modern terms, about the field [of intelligence]."[22] You must also be critical of a wide range of disciplines and be "able to distinguish between sense and nonsense even when [we are] not . . . specialist[s] in any one area of knowledge."[23]

Rhetorical theory is one of many disciplines at the heart of Aristotle's universal education—an education you will need in order to excel as an analyst.[24] Thanks to rhetorical theory, you can apply discourse-power theory to better understand how power flows influence real-world threat systems. Additionally, even without specific technical specialization, you can apply this rhetorical template to any system, resulting in a honed, critical perspective: a viewpoint filtered from the nonsense and focused on threat systems and potential crisis situations.[25]

Critical analysis is the trademark of the intelligence career field; however, it is impossible to accomplish without rhetorical theory. Interestingly, the topic of this project has been dis-

cussed with many of my friends in the intelligence community, and I have received a wide range of winces and head tilts in response to rhetorical theory. Ironically, rhetorical theory is at the root of my colleagues' most basic skills of organization and discourse: tasks they accomplish daily with little to no understanding of theory's rich history and framework. It is easy to live in theory denial; however, if you open yourself to an element of universal education, you will enhance the theory you are already using—and potentially take into combat.

Notes

1. Central Intelligence Agency, *Analysis: Directorate of Intelligence in the 21st Century* (Washington, D.C.: Government Printing Office [GPO], 1996), 20.
2. Patricia Bizzell and Bruce Herzberg, eds., *The Rhetorical Tradition: Readings from Classical Times to the Present* (Boston: Bedford Books, 1990), 1.
3. Ibid.
4. Sonja K. Foss, Karen A. Foss, and Robert Trapp, *Contemporary Perspectives on Rhetoric,* 2d ed. (Prospects Heights, Ill.: Waveland Press, 1991), 14.
5. Ibid., 14.
6. Ibid., 1.
7. Ibid.
8. Ibid., 2.
9. Ibid.
10. Bizzell and Herzberg, 1.
11. Foss, Foss, and Trapp, 4.
12. Ibid.
13. Bizzell and Herzberg, 3–4.
14. Ibid., 4.
15. Ibid., 5.
16. Ibid., 4.
17. Ibid.
18. John Gannon, "Foreword," in Jack Davis, *A Compendium of Analytic Tradecraft Notes,* ed. F. Douglas Whitehouse (Washington, D.C.: GPO, 1997), 17.
19. Charles van Doren, *A History of Knowledge: Past, Present, and Future* (New York: Ballantine Books, 1991), 286.
20. Ibid., 135.
21. Ibid.
22. Ibid., 135–36.
23. Ibid., 136.
24. Ibid., 135.
25. Ibid., 136.

Chapter 3

Intelligence Process

The success of any crisis deployment hinges on the existence of a reliable command and control system and of a flexible, reliable system for gathering, analyzing, and disseminating strategic and tactical intelligence.

—Gen H. Norman Schwarzkopf
United States Army
Operation Desert Storm, 1991

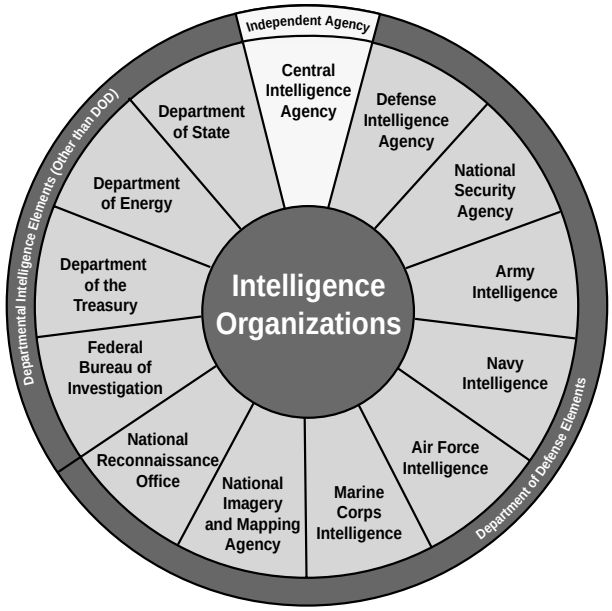
Before pressing forward with Foucault's rhetorical theories, I will review basic military intelligence pedagogy to highlight the key process that serves as a rhetorical road map. According to Joint Publication (JP) 2-01, *Joint Intelligence Support to Military Operations*, the intelligence cycle is the "process by which information is converted into intelligence and made available to users."[1]

As evidenced by the joint (Army, Navy, Air Force, and Marines) document on the subject, the cycle is well ingrained into each military service. It forms a fundamental bond among 13 national-level and service-level intelligence agencies (fig. 2).[2]

Planning and Direction Phase

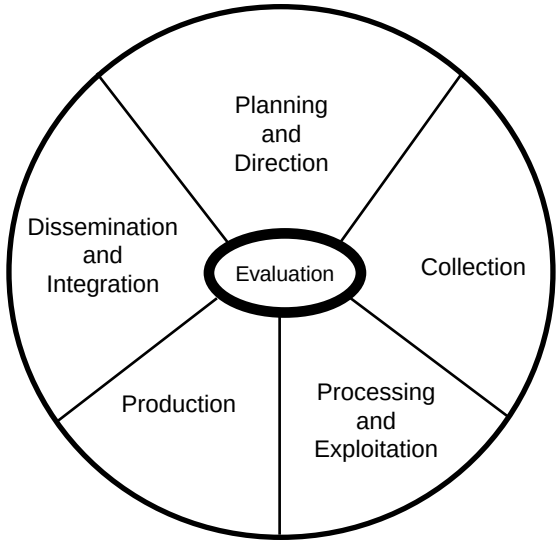
The intelligence cycle begins with the planning and direction phase (fig. 3), in which commanders and intelligence analysts "identify and prioritize information requirements."[3] Key elements of information are identified, and a plan is then developed to satisfy as many user requirements as possible. "Early discovery of any requirements that cannot be satisfied through organic (internal to the unit or service), theater, or national intelligence collection resources will highlight potential intelligence gaps."[4]

Before continuing, I must highlight a critical distinction between information and intelligence: "Information is data that have been collected but not further developed through analysis, interpretation, or correlation with other data and intelligence. The application of analysis transforms information into intelligence."[5] A particular style or method of transforming information



Source: Central Intelligence Agency, *Agencies of the US Intelligence Community (USIC): 1998*, n.p., on-line, Internet, 10 June 1999, available from http://www.cia.gov/ichome.htm.

Figure 2. Intelligence Organizations (Agencies)



Source: Adapted from Naval Doctrine Publication 2, *Naval Intelligence*, 1994, 24.

Figure 3. Intelligence Cycle

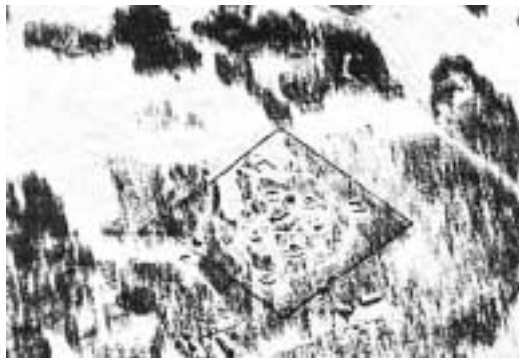
into intelligence is also at the core of rhetorical theory. You join the ranks of the great rhetoricians every time you take a piece of data, such as an image, troop positions, and so on, and process it through your experiences or knowledge of past or similar events. The widening range of information mediums presents additional rhetorical challenges to experience throughout the course of your career. Unfortunately, military events have proven that many of you will be "thrown into the mix" with a relatively limited experience base soon after graduation from intelligence school.

Collection Phase

Since 1960 the quality and quantity of artifacts made available to intelligence analysts have dramatically increased due to many technical advancements associated with the collection phase of the intelligence cycle. Collection of intelligence data has a firm, often infamous, footing in world history. Maj Gen Oleg Kalugin, the KGB's first chief directorate, now retired, highlights that "spying (politically toned as collecting) has been with the human race from time immemorial; it has often been called 'the second oldest profession' and was used by ruling elites as a major tool to protect their power from real or imaginary threats and rivals, both domestic and external."[6] General Kalugin intimately understands how "intelligence-gathering was transformed by satellites, lasers, computers, and other gadgetry capable of ferreting out secrets from every corner of the globe."[7] Specifically, an example of one of the most sophisticated collection organizations was publicly unveiled in 1992 with declassification of the National Reconnaissance Office (NRO).[8] NRO also revealed a revolution in data collection that began with the 1960 launch of the Corona reconnaissance satellite (photo below).[9]

National Reconnaissance Office Corona Satellite

Examples of the early artifact evolution include more than 800,000 Corona satellite images (one example is provided in the photograph below) that were declassified in 1995.[10] NRO "enable[s] U.S. global information superiority, during peace through war."[11] A quick look through NRO's archives clarifies the concerns of former CIA deputy director Gannon about the increasing flow of information. Obviously, since the launch of Corona, subsequent collection platforms have increased the number, type, and quality of intelligence artifacts.



Former Soviet SA-2 (surface-to-air) missile site, Corona, shown here in 1969.

In addition to spaceborne satellites, there are air-breathing (operating within Earth's atmosphere) collectors spanning from reconnaissance aircraft (photos shown on next page) all the way to original air-breathing collectors—humans. "Rulers and military leaders have always needed to know the strengths, weaknesses, and intentions of their enemies. Consequently, the trade of spying [intelligence collection and analysis] is as old as civilization itself. Around 500 B.C., ancient Chinese strategist Sun Tzu wrote about the importance of intelligence and espionage networks in his classic book *The Art of War*. The Bible [also] contains more than a hundred references to spies and intelligence-gathering."[12] Importantly, through collection and analysis, rhetorical theory has been there to put the key pieces together.

Left:* U-2. *Above:* The Predator unmanned aerial vehicle flies Navy reconnaissance close to the carrier USS *Carl Vinson.

Processing and Exploitation Phase

In addition to the collection of information, the processing and exploitation phase takes information and converts it into "forms suitable for analysis and production."[13] Processing information includes "translating foreign languages, developing film from tactical reconnaissance aircraft, generating hard (paper) or soft (electronic) images provided by electro-optical or infrared sensors, and converting raw electronic intelligence data into a standard message format suitable for automated handling."[14] Suitable analytical forms are often intimately tied to systems collecting the data, as evidenced by the Corona satellite images. The exploitation phase is a rich discourse mechanism for rhetorical research.

Production Phase

The production phase turns planned, collected, and processed information into "finished intelligence."[15] "Intelligence production is the integration, analysis, evaluation, and interpretation of information from all available sources into tailored, usable intelligence. A key principle in production is the fusion of information from various sources to form a complete and accurate product. Fusion is essential for an effective intelligence production

process that accurately reflects and supports the commander's prioritized essential elements of information (EEI)."[16] The human element is not only key to the transformation of information into intelligence but it also shapes your analytical techniques.

Additionally, the fusion from multiple sources demands an understanding of both operational and rhetorical benefits of each intelligence source (table 1).

Table 1

Intelligence Sources

IMINT*	Imagery Intelligence
PHOTINT	Photographic Intelligence
SIGINT*	Signals Intelligence
COMINT	Communications Intelligence
ELINT	Electronic Intelligence
FISINT	Foreign Instrumentation Signals Intelligence
TELINT	Telemetry Intelligence
RADINT	Radar Intelligence
HUMINT*	Human Intelligence
MASINT*	Measurement and Signature Intelligence
ACINT	Acoustical Intelligence
OPTINT	Optical Intelligence
ELECTRO-OPTICAL	Electro-optical Intelligence
IRINT	Infrared Intelligence
LASINT	Laser Intelligence
NUCINT	Nuclear Intelligence
RINT	Unintentional Radiation Intelligence
OSINT*	Open Source Intelligence
TECHINT*	Technical Intelligence
CI*	Counterintelligence

*Primary Sources

Source: Naval Doctrine Publication 2, *Naval Intelligence*, 1994, 22.

Along with accelerated political and military events, advances in technology have accelerated the need for a heightened rhetorical understanding. Unfortunately, at the unit level (your primary training grounds), analysis is subtly pushed to the sideline in favor of information management. Technology provides a wide array of artifacts (imagery, electronic signals, databases, and so on), and inexperienced personnel often mistake these artifacts as analyzed intelligence. Rhetoricians

Russell S. Tomlin, L. Forrest, M. M. Pu, and M. Kim highlight the analytical implications of these artifacts: "This artifact, in essence, contains the meaning intended by the speaker [or the reporting-collection platform]. It is conducted to the listener [or analyst] in either spoken [or visual] or written form. The text [or image, data, etc.] is then unpacked and its meaning extracted from the text artifact by the listener [or analyst]."[17]

Within this process, analysts must extract meaning from data and images. The collecting system (camera, electronic spectrum receiver, and so on) may not accurately or adequately frame meaning or significance with the artifact. An analyst's difficult task is further complicated by the nature of the artifact. Without an associated, precise meaning, "the source, sometimes the only source [of information]," requires the analyst to engage "actively in constructing [his or] her own conceptual representation of the matters [or situation] at hand."[18]

Analysis is often confused as a product instead of a key (critical) rhetorical process. Conflict between artifact (product) and process will continue to complicate intelligence analysis. However, rhetorical theory is integral to the packing and unpacking of meaning behind modern artifacts.[19] Specifically, theory enhances the ability to visualize a battle space or situation when the artifacts fail to contribute to analytical "knowledge integration."[20] Rhetoricians have focused on challenges that thwart effective artifact analysis; the problem is twofold. The first hurdle deals with an analyst's ability to integrate information (knowledge integration) into a "coherent representation," resulting in construction of "concepts and events virtually identical" to the actual situation.[21] Deception and misinformation can significantly degrade your ability to develop a comprehensive understanding of a system or event. Equally debilitating, the second obstacle deals with management and control of the ever-increasing information flow (information management) in a "dynamic, real-time interaction."[22] Knowledge integration and information management continue to stress and stretch military analysts' capabilities. Unfortunately, the distinction between intelligence integration and information analysis is often blurred. "Knowledge integration (analysis) requires effective information management, but effective information management

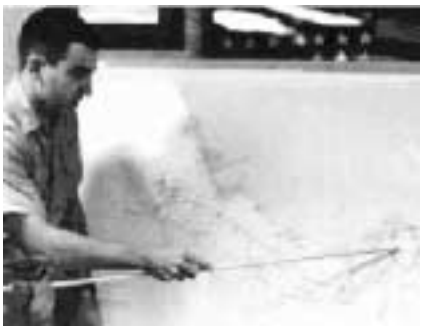
is not enough to account for knowledge integration."[23] With the growing number and diversity of artifacts, the intelligence community's focus on effective integration must remain paramount.

Dissemination and Integration Phase

During the dissemination and integration phase of the intelligence cycle, intelligence is provided directly to the user in a format that is "readily understood."[24] Answers to the commander's EEI are satisfied in a "timely manner without overloading the user and minimizing the load on communications capabilities."[25]

> Getting the product to the user is the last step in the intelligence cycle; but, because the cycle is dynamic, the process does not end with dissemination. First, intelligence personnel must ensure that the product is actually used. This is a particular obligation of intelligence personnel who are members of operational staffs. They are in the best position to demonstrate the value of intelligence products to commanders and other staff members. Second, intelligence personnel must see to it that dissemination is refined by gathering feedback from the commander or other users [aircrews] to ensure that intelligence requirements have been satisfied and the finished intelligence products are usable.[26]

Intelligence within this phase is "pushed" and "pulled" (as seen in photographs below) as analysis flows through intricate communication networks from command echelons down to individual flights, companies, and naval elements.[27]



Left to right: **Formal intelligence briefings "push" information to users, but tactical intelligence briefings "pull" it from them.**

The intelligence cycle is a proven tool to effectively fulfill many of the commander's objectives, as shown in the next photograph. An operationally focused instruction in rhetorical theory can

Aircraft scored a direct hit on a reinforced Iraqi aircraft shelter.

strengthen this process. Specifically, rhetorical theory can help ensure that analysis efforts and resources are tasked against threat pivot points. Seeds of analysis must be planted as early as possible through a focused interest in theory. Rhetorical theory is key to enhanced analytical growth. We will look to Michel Foucault, the master rhetorical gardener, for guidance before this author spreads more fertilizer.

Notes

1. Joint Publication (JP) 2-01, *Joint Intelligence Support to Military Operations*, 1996, II-2.
2. Central Intelligence Agency, *Agencies of the US Intelligence Community (USIC): 1998*, n.p., on-line, Internet, 10 June 1999, available from http://www.cia.gov/ichome.htm.
3. Naval Doctrine Publication (NDP) 2, *Naval Intelligence*, 1994, 24.
4. Ibid., 25.
5. JP 2-01, II-2.
6. Quoted in H. Keith Melton, *The Ultimate Spy Book* (New York: DK Publishing, 1996), 7.
7. Ibid.
8. National Reconnaissance Office, *Who We Are*, n.p., on-line, Internet, 20 March 1999, available from http://www.nro.odci.gov/background.html.

9. Ibid.
10. Ibid.
11. Ibid.
12. Melton, 18.
13. JP 2-01, ix.
14. NDP 2, 26.
15. JP 2-01, ix.
16. NDP 2, 26.
17. Russell S. Tomlin et al., "Discourse Semantics," in *Discourse as Structure and Process*, ed. Teun van Dijk (London: Sage, 1997), 64.
18. Ibid.
19. Ibid.
20. Ibid., 65.
21. Ibid.
22. Ibid.
23. Ibid.
24. JP 2-01, x.
25. Ibid.
26. NDP 2, 26.
27. JP 2-01, x.

Chapter 4

[What the] Foucault?

I think we should have the modesty to say to ourselves that, on the one hand, the time we live in is not the unique or fundamental or irruptive point in history where everything is completed and begun again. We must also have the modesty to say, on the other hand, that even without this solemnity—the time we live in is very interesting.

—Michel Foucault
Power/Knowledge: Selected Interviews and Other Writings

Paul-Michel Foucault—a prominent philosopher, historian, and rhetorician—was born in Poitiers, France, in 1926.[1] School was an exciting aspect of Foucault's life from a young age, and he excelled rapidly through the French school system.[2] While in his teens, Foucault experienced the toils of war as his town fell under control of German occupation forces during World War II.[3] "In his Jesuit school, Paul-Michel wasn't exactly a war hero [then again, he was only in his teens], but he did help other kids steal wood from the Nazis to heat the school."[4] During the German occupation, he experienced his "intellectual, sexual, and political coming of age" under an oppressive power shift that resulted in the "disappearance, flight and arrest of teachers, town's people, and relatives in the horizon of Nazi authority."[5]

Even after the rigors of a trying childhood, Foucault progressed intellectually and academically after the war. "Foucault went from school to school, doing extremely well on his exams, until he had reached the summit: he scored fourth among all the students in the country competing for entry to the Ecole Normale Supérieure in Paris—the most exclusive and intellectually intense college-level school in France."[6] His driven study of philosophy, psychology, and psychopathology fostered his drive to chart the "independent systems" that shape discourse and society.[7]

Foucault never served in the military; however, his firsthand occupation experience and painstaking study of history,

human behavior, and—most importantly—power, made him a social and intellectual tactician of the highest order. The breadth of his studies covers many expansive and elusive aspects of society.

> Foucault's early studies concerned the history of mental illness and society's response to it. Society's use of the concept of madness in the 17th century is the subject of his *Folie et Déraison: Histoire de la folie à l' âge classique* (1961; *Madness and Civilization).* In his book *Surveiller et punir: Naissance de la prison* (1975; *Discipline and Punish: The Birth of the Prison),* he examined the origins of the modern penal system. In these and other books, Foucault put forth the thesis that institutions such as asylums, hospitals, and prisons are society's devices for exclusion and that by surveying social attitudes in relation to these institutions, one can examine the development and uses of power.[8]

Foucault's other pivotal works include *The Order of Things: An Archaeology of Human Sciences* (1966), *The Archaeology of Knowledge* (1969), and *History of Sexuality* (three volumes, 1976–1984).[9]

His works are sometimes difficult to read, and he can test the mettle of even the best students of rhetorical theory. Furthermore, these books do not take up much shelf space in the military community's libraries. However, do not let this discourage you from seeking rhetorical sources to help you think and operate outside of the box. Foucault's work in this study is transplanted into the realm of military analysis, far from his original target audience. However, contemporary author and rhetorician Sonja K. Foss highlights the utility of Foucault's rhetorical theory: "In the area of rhetorical scholarship, Foucault's originality lies not in the introduction of totally new concepts for use in rhetorical theory but in how his notions may be used by others to stretch existing conceptualizations or may be applied to new domains."[10] Foucault would frown upon this "institutional" use of his power analysis. He once stated that "the goal of my work during the last twenty years has not been to analyze the phenomena [*sic*] of power, nor to elaborate the foundations of such an analysis. My objective, instead, has been to create a history of the different modes by which, in our culture, human beings are made subjects."[11] Fortunately, Foucault's analysis of the cultural modes and norms results in a striking power blueprint: a social projection that is bolstered by his refusal "to separate off knowledge from power."[12] Most importantly, even as a very reluctant,

unintentional military tactician, Foucault understood the critical, pivotal elements and practices of society: his most general aim was to "discover the point at which these practices [social, political, economic, legal, philosophical, and scientific traditions] became coherent reflective techniques with definite goals, the point at which a particular discourse emerged from these techniques and came to be seen as true, the point at which they are linked with the obligation of searching from the truth and telling the truth."[13] His detailed studies of mankind reveal critical discourse linkages—such connections are discussed in greater detail later in this paper.

Interestingly, he superbly catalyzes the domain of tactical analysis. Specifically, elements of his military applicability are highlighted during an interview conducted by Alessandro Fontana and Pasquale Pasquino. Foucault was asked the following question concerning the military model of power: "You have said about power as an object of research that one has to invert [Carl von] Clausewitz's formula so as to arrive at the idea that politics is the continuation of war by other means. Does the military model seem to you, on the basis of your most recent researches, to be the best one for describing power; is war here simply a metaphorical model, or is it the literal, regular, everyday mode of operation of power?"[14] Foucault frames his power response to the above question and generates even more compelling questions:

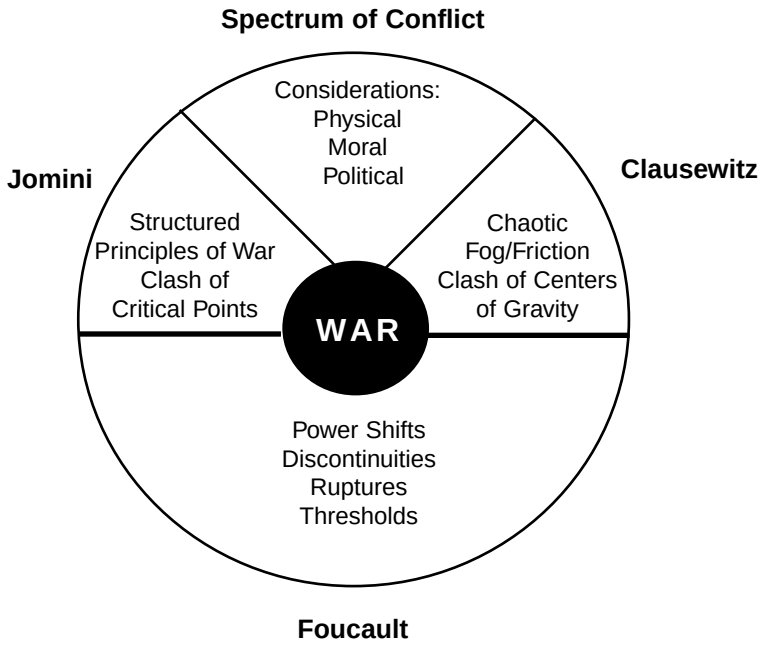
> As soon as one endeavors to detach power with its techniques and procedures from the form of law within which it has been theoretically confined up until now, one is driven to ask this basic question: Isn't power simply a form of warlike domination? Shouldn't one therefore conceive all problems of power in terms of relations of war? Isn't power a sort of generalized war which assumes at particular moments the forms of peace and the state? Peace would then be a form of war, and the state a means of waging it. A whole range of problems emerges here. Who wages war against whom? Is it between two classes, or more? Is it a war of all against all? What is the role of the army and military institutions in this civil society where permanent war is waged? What is the relevance of concepts of tactics and strategy for analyzing structures and political processes? What is the essence and mode of transformation of power relations? All these questions need to be explored. In any case it's astonishing to see how easily and self-evidently people talk of warlike relations of power or class struggle without ever making it clear whether some form of war is meant, and if so what form.[15]

Foucault's understanding of power relations serves as a primary analytical platform. More power specifics are discussed later.

Ever since you were young cadets or officer candidates, an understanding of Clausewitzian principles on the spectrum of conflict formed the basis of your understanding of combat. From structured, gentlemanly conflict under Gen Baron Antoine Henri de Jomini's warfare theory to chaotic conflicts described by Clausewitz, warfare is a historically prevalent element of human life.[16] Clausewitz's concepts of fog and friction were readily seen in the conflict in Kosovo. The fog (uncertainty) of combat is highlighted by smart weapons missing targets, US soldiers being captured, and stealth aircraft (F-117s) being inexplicably uncloaked (mangled debris) by Serbian television.[17] Similarly, the friction (countless minor complications) of supporting large combat formations with weapons, fuels, maintenance, personnel (aircrews and ground-support technicians), and accurate intelligence also complicates modern conflicts.[18]

At this point you may be asking, "What the Foucault?" Well, underpinning the entire spectrum of conflict is a complex, ever-shifting flow of power, ruptures, and discontinuity.[19] "One can never be absolutely positive that all enemy capabilities [power pivot points and decisive points] are associated with evaluating enemy intentions . . . intelligence preparation of the battlefield can reduce vulnerability to enemy actions by describing enemy courses of action so that they can be countered, forestalled, or exploited."[20] Power, as briefly discussed above, is often veiled: its absence is as poignant as its presence. As intelligence officers, your task is to chart the power plays on the political fronts and battlefields (fig. 4).

Foucault highlights many avenues for the analytical development of power. Conflicts share integral power relations resulting in valuable "concepts of tactics and strategy for analyzing structures and political processes."[21] Most importantly, Foucault asks, "What is the essence and mode of transformation of power relations?"[22] In order to help answer at least a portion of this critical question, I use Foucault's understanding of power flows and discontinuity. The effective preparation of the battle space for the prevention or prosecution of conflict



Source: Squadron Officer School, "4100-L-1," lecture, Class 97-D, Maxwell AFB, Ala., 1997.

Figure 4. Spectrum of Thought

begins with an understanding of these "warlike relations of power."[23]

All too often you focus on the physical platforms of the profession of arms (aircraft, computers, ships, tanks, etc.); however, it is the human element that allows the entire process to succeed. By the end of this discussion, I hope you have an appreciation of how rhetoricians such as Foucault can help you better understand the elusive human element of conflict—and the analysis of human struggles. As intelligence officers, you are also instructors, mentors, and subject-matter experts on a wide range of operational and tactical issues. Along these lines, you have an obligation to remain current in many forms of intellectual literacy. Marcus Cicero (106 to 43 B.C.), a famous Roman statesman, lawyer, and scholar, is remembered as one of history's greatest orators.[24] Cicero clearly highlighted his commitment to the arts: "No one should be numbered with the orators who is not accomplished in all those arts that befit the

well-bred; for though we do not actually parade these in our discourse, it is nonetheless made clear to demonstration whether we are strangers to them or have learned to know them."[25] You simply, much like your rhetorical forefathers, need to remain open-minded to the best available concepts in all fields. Unfortunately, discourse theory spends little time in the spotlight. However, as the primary communicators (orators as Cicero put it) of the military, you need to understand the underlying concepts of your trade.

Notes

1. Lydia A. Fillingham, *Foucault for Beginners* (New York: Writers and Readers Publishing, 1993), 19.
2. Ibid.
3. Ibid.
4. Ibid.
5. Ronald C. Tobey, *Foucault, Michel,* n.p., on-line, Internet, 11 March 1998, available from http://www.kaiwan.com/~lucknow/horus/guide/cm108.html.
6. Fillingham, 20.
7. Michel Foucault, *The Archaeology of Knowledge and the Discourse on Language* (New York: Pantheon Books, 1984), 12.
8. *Encyclopedia Britannica,* CD-ROM, 1999 ed., s.v. "Michel Foucault."
9. Ibid.
10. Sonja K. Foss, Karen A. Foss, and Robert Trapp, *Contemporary Perspectives on Rhetoric,* 2d ed. (Prospect Heights, Ill.: Waveland Press, 1991), 232.
11. Quoted in Michel Foucault, *The Foucault Reader,* ed. Paul Rabinow (New York: Pantheon Books, 1984), 7.
12. Ibid.
13. Ibid.
14. Ibid., 64–65.
15. Ibid., 65.
16. "Leadership: Combat Leadership," lecture, Squadron Officer School, Maxwell AFB, Ala., 1994.
17. Ibid.
18. Ibid.
19. Foucault, *The Archaeology of Knowledge and the Discourse on Language,* 9.
20. "Leadership," 15.
21. Foucault, *The Foucault Reader,* 65.
22. Ibid.
23. Ibid.
24. *Encyclopedia Britannica,* CD-ROM, 1999 ed., s.v. "Marcus Cicero."
25. Quoted in Erika Lindemann, *A Rhetoric for Writing Teachers,* 3d ed. (Oxford: Oxford University Press, 1995), 43–44.

Chapter 5

Power Plug

Here I believe one's point of reference should not be to the great model of language (langue) and signs, but to that of war and battle. The history which bears and determines us had the form of a war rather than that of a language: relations of power, not relations of meaning.

—Michel Foucault
Power/Knowledge: Selected Interviews and Other Writings

During spring 1999, I watched as 22 aircraft laden with airborne infantry and equipment from the 3d Battalion, 504th Parachute Infantry Regiment surged forward to form an impressive line of gray and camouflaged aircraft feeding onto the runway at Pope Air Force Base (AFB), North Carolina (see photos, next page). Each C-130 turned out of its parking location onto taxiways with near-drill-team precision. I reflected on the four previous 16-hour days involved in planning and preparation of the formation, including route analysis, many modifications, and then the scramble to provide each crew with mission-ready products. The mission was now under way. Concept and formation briefings were long since over. The final mission presentation, the joint mission briefing, was met with approving head nods and closing remarks from an Army brigadier general and an Air Force colonel. While standing at the edge of the legendary Green Ramp, the loading area for airborne troops and equipment, I was overwhelmed by the roar of 88 propellers cutting through the air. Although this was just an exercise, I could not help considering the physical and rhetorical ramifications of the event.

Later that evening, after all the aircraft were aloft, I returned to the mission-planning area to observe a second rhetorical event. An Army officer, one of the evaluators of the loading process, was honing his power-analysis skills and reading Robert Kaplan's *Balkan Ghosts: A Journey through History*. Considering the conflict in Kosovo, the officer's effort to explore a

Left: **C-130s parked on the ramp at Pope AFB, North Carolina.** ***Right:*** **Airborne troops getting ready to board.**

critical element of rhetorical analysis (history) was impressive—specifically, the officer's drive to bridge a daunting, expansive gap between a volatile region's history and the potential application of the power, like the force now airborne. Obviously, the two power events vary greatly in magnitude; yet, they share a common rhetorical thread—a tailored analysis of your own and the threat's power infrastructure.

Since you are intelligence specialists, understanding the power in both your and the adversary's capabilities and systems is extremely critical. Sun Tzu clearly understood the value of this critical examination of adversary and self: "So it is said that if you know others and know yourself, you will not be imperiled in a hundred battles; if you do not know others but know yourself, you win one and lose one; if you do not know others and do not know yourself, you will be imperiled in every single battle."[1] Knowing yourself and others, as Sun Tzu puts it, requires a detailed understanding of the physical (weapon systems, ranges, guidance types, etc.) and rhetorical (origin, history of use or misuse, supporting institutions, and infrastructure) power coursing through every aspect of intelligence analysis.

It is difficult to use power effectively unless it is studied and observed from an appropriate vantage point. For Foucault, the vantage point starts at the "panopticon."[2] Foucault adapts Jeremy Bentham's concept (physical plan) for the panopticon in order to give each power event its proper perspective.[3] "The panopticon consists of a large courtyard, with a tower in the center, surrounded by a series of buildings divided into levels

and cells. In each cell there are two windows: one brings in light and the other faces the tower, where large observatory windows allow for the surveillance of the cells. The cells become 'small theatres, in which each actor is alone, perfectly individualized and constantly visible.'"[4] Bentham's panopticon represents an actual architectural mechanism for observing and controlling a subject from a central position.[5] Although not exactingly adapted by Foucault, the panopticon is crucial to his power analysis.[6] Foucault uses the observation point in his search for power mechanisms and architectures. Figure 5 illustrates a potential hierarchical flow of power or discourse through two typical organizations. The pyramid on the left—shown in each of these panoptic illustrations—represents a sample US organization while the structure on the right represents a look at an adversary's power connections. The centrally placed observation tower, or panopticon, represents Foucault's power-observation position. The transparent cubes of the pyramid represent the panoptic cells with windows we

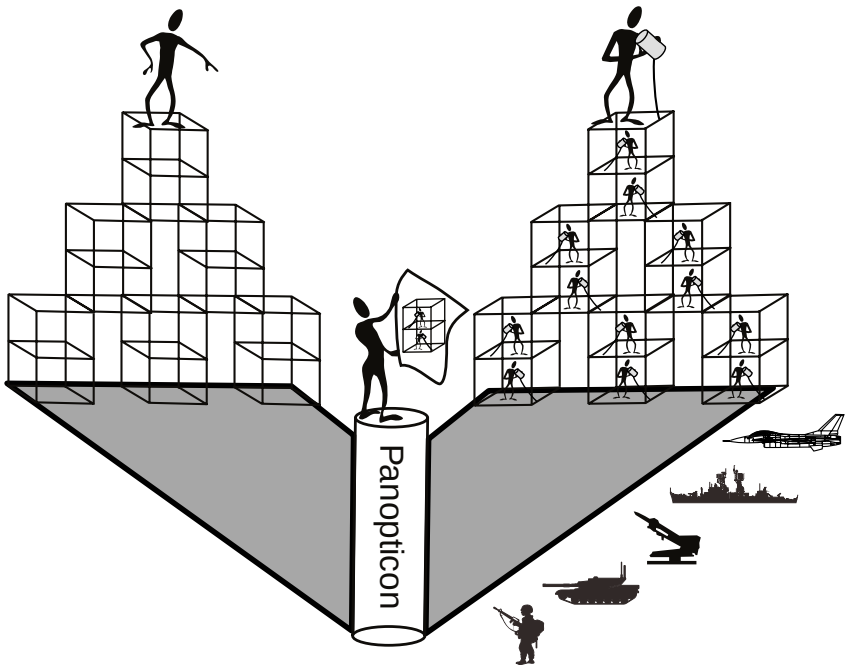


Figure 5. The Panopticon's Point of View

look through with the help of many intelligence sources.[7] Spread before the panopticons are Foucault's "institutions, economic and social processes, behavioral patterns, systems of norms, types of classification, [and] modes of characterization."[8] "The panopticon offers a particularly vivid instance of how political technologies of the body function. It is a 'generalizable model of functioning; a way of defining power relations in terms of the everyday life of men. . . . [I]t is the diagram of a mechanism of power reduced to its ideal form. . . . It is in fact a figure of political technology that may and must be detached from any specific use.'"[9]

Analysts can identify the same power infrastructures in everything ranging from an integrated air defense system to the training doctrine behind an individual soldier in the field. There are many operational panopticons in the military. Airborne command, control, and surveillance systems (see photos below) take their place as the high-tech, mobile observation points. These modern advancements embody many of the essential elements of Bentham's original concept. Military installations, field camps, and airborne formations depend heavily on the ability to observe and analyze a battle space or conflict. "Thus, through spatial ordering, the panopticon brings together power, control of the body, control of groups and knowledge."[10] The power analysis "perch" is well defined

Left: **The E-3 Sentry is an airborne warning and control system (AWACS) aircraft that provides all-weather surveillance, command, control, and communications needed by commanders of US and NATO air defense forces.** ***Right:*** **The E-8 joint surveillance, target attack radar system (JSTARS) is an airborne platform equipped with a long-range, air-to-ground surveillance system designed to locate, classify, and track ground targets in all weather conditions. Its capabilities make JSTARS effective for dealing with any contingency, whether actual or impending military aggression, international treaty verification, or border violation.**

and well organized; however, it too is subject to its own level of control. “As the final step in architectural and technological perfection, the panopticon includes a system of observing and controlling the controllers. Those who occupy the central position in the panopticon are themselves thoroughly enmeshed in a localization and ordering of their own behavior.”[11]

US military services, especially their service infrastructure, are built around many of the same “system[s] of observing and controlling the controllers.”[12] From controlling who has information access through panoptic background investigations to centralized control of access mediums—message traffic, encrypted Internet Web sites, and compartmented programs—intelligence agencies carry many of the same watermarks of Bentham’s original panopticon blueprint.

Importantly, the system of checks and controls adds to an organization’s “economy of power.”[13] “That is to say, procedures which allowed [and still allow] the effects of power to circulate in a manner at once continuous, uninterrupted, adapted, and ‘individualized’ throughout the entire social body.”[14] A clear understanding of an organization’s circulatory system will lead to the heart of its key strengths and weaknesses. Physical and social procedures surrounding the flow of power serve as key power conduits that you must take a look at through Foucault’s rhetorical lens.[15]

Foucault’s analysis techniques not only match the intelligence architecture but they also work as a “focusing lens” for the organization’s power flow. Additionally, Foucault’s analytical lens works equally well to magnify the often-hidden power conduits in an adversary’s structure. A detailed understanding of power conduits and the restrictions placed upon them is needed to apply Foucault’s analytical tools.

From the combatant commander down to the soldier in the field, a conceptually simple yet powerfully complex power architecture exists. Each power level in the architecture acts as a power plug in a “network of relationships that are systematically interconnected” in a series of standard and potential connections (fig. 6).[16] Our routine conduits constitute what is seen as standard operating procedures; furthermore, these connections end up in baseline field orders, air tasking orders,

and special instructions to energize US power architecture with discourse power. Intelligence officers can excel as "power boosters" and/or "surge protectors" in order to maintain an optimal balance in the flow of "juice."

> In this task of adjustment, discipline had to solve a number of problems for which the old economy of power was not sufficiently equipped. . . . It must neutralize the effects of counterpower that spring from them and which form a resistance to the power that wishes to dominate it: agitations, revolts, spontaneous organizations, coalitions—anything that may establish horizontal conjunctions. Hence the fact that the disciplines use procedures of partitioning and verticality; that they introduce, between the different elements at the same level, as solid separations as possible; that they define compact hierarchical networks; in short, that they oppose to the intrinsic, adverse force of multiplicity the technique of the continuous, individualizing pyramid.[17]

As you partition your view of yourselves and others, an objective view of critical-power choke, pooling, and stop points gains strength and clarity.

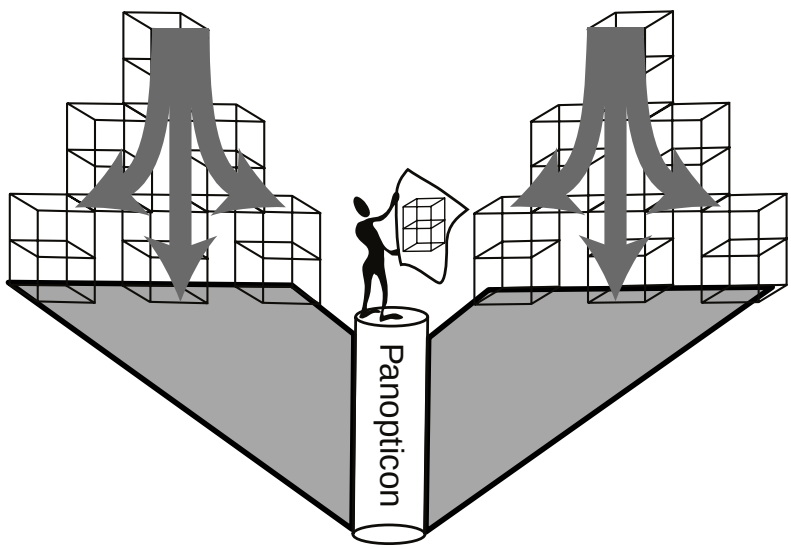


Figure 6. Power and Knowledge Flow

Power, pyramids, and vertical partitions were covered. Just in case you are wondering—no, you do not need to splice an electrical engineering degree with a course in Egyptology. Just keep in mind that observation and control of power depends on a complex group of relations—interactions that depend heavily on

communication.[18] For Foucault, "discourse is a form of social action" built on networks of archives, social practices, and institutions (fig. 7).[19] "[Foucault] demonstrates the microphysics of power that resides in the knowledge that is disseminated in discourse and embodied in laws, regulations, tests, and in the very architecture of hospitals, schools, and prisons, showing the ways that seemingly diverse discourses come together in formations that affect social practices and social controls."[20]

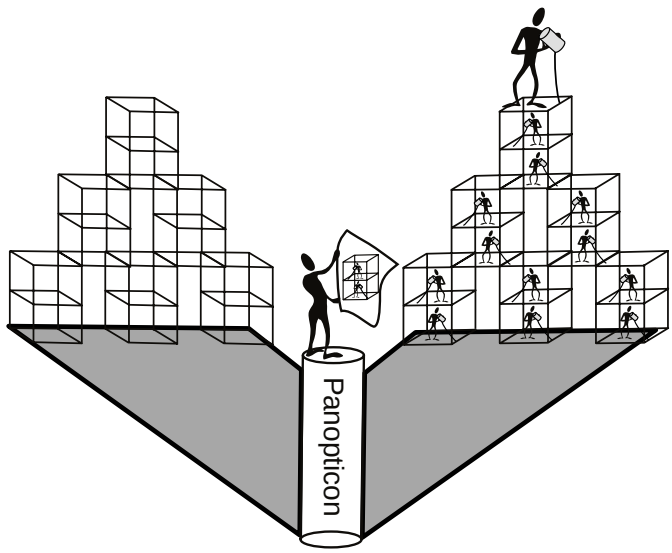


Figure 7. Discourse Hierarchies

If you can understand both your own and the adversary's discourse formation, you can better identify pivot points to reinforce, degrade, or attack. Appropriate action can be initiated if you can highlight the tactics of power that fulfill Foucault's three criteria for "the ordering [structuring] of human [power] multiplicities."[21] These social pivot points serve as critical elements in power analysis. Key discourse pivot points (fig. 8) and target areas will exercise power economically (a significant reduction of hierarchical effort, social resistance, and physical/monetary expense). They will take power to its maximum intensity and range; they will link power and economy through amplifying mediums (visual, electronic, tactile, etc.) and organizations (educational,

military, industrial, etc.) in order to add clarity and strength.[22] If you can understand these areas, you will fully realize your own capabilities. These points are also known as centers of gravity and decisive points. Additionally, these pivot points will help you comprehend the enemy point of view.

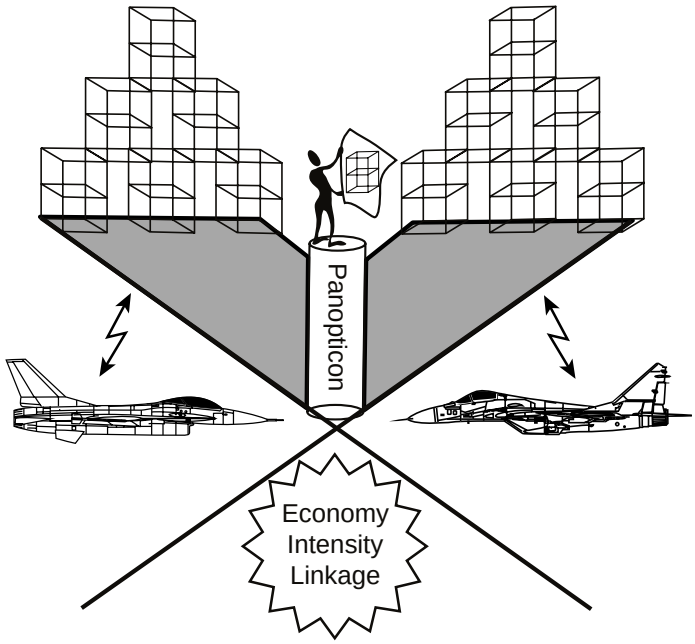


Figure 8. Discourse Tactical Considerations

The fighters in figure 8 represent just one element of a country's military capability. Additionally, they embody every aspect of Foucault's three criteria. For example, the aircraft on the left represents a US plane, and the one on the right represents a hostile force's air capability. The corresponding countries' power structures are directly responsible for employment of their aircraft. Power flow starts at the top of the discourse hierarchies and proceeds down a complex system of conduits (shaped by social and physical procedures, tactics, and strategies) with each aircraft representing the military manifestation of the power flow. Inside each aircraft, there are several additional sets of power conduits. Each aircraft's physical power (speed, range, weapons, etc.) and each pilot's capability repre-

sent another critical set of conduits. The aircraft's physical power is readily seen; however, the pilot's training (aircraft systems and procedures), threat knowledge (systems and tactics), and access to information via (a secure and reliable) connection to the main conduit (with the panoptic view of the battle space) are rarely acknowledged. Overall strength of an allied or hostile power flow is directly tied to the economy, intensity, and linkage of the flow.

Operation Allied Force (Kosovo conflict), the air campaign against Serbian forces, is an example of economy, intensity, and linkage in action. NATO successfully engaged Serbian military infrastructure through an effective use of its own economy, intensity, and linkage. According to *DOD News Briefing* (July 1999), NATO's economy was demonstrated through destruction of 110 Serbian tanks, 210 armored fighting vehicles, and 449 pieces of artillery and mortars, with loss of only two aircraft (pilots rescued unharmed) during 78 days of flight operations. The monetary economy or expense of the operation was considerable. However, the ultimate economy was realized through preservation of NATO and civilian lives throughout the operation. According to Secretary of Defense William S. Cohen, "of the 23,000 bombs and missiles used, only 20 went astray causing collateral damage."[23] Equally, intensity of the weapons employed by NATO aircraft was very evident, as highlighted by the number and variety of targets disabled or destroyed. Additionally, unrestricted range and employment of NATO aircraft highlight the intensity of their employment. Finally, linkage of the employment was underscored by use of multinational command and control systems, aircraft, and personnel in attainment of a common objective. The airpower portion represents only one component during one phase of the conflict in Kosovo. Operation Joint Guardian, the follow-on operation, involved employment of NATO peacekeeping forces (ground troops) in Kosovo.

During the Persian Gulf War, intelligence analysts effectively identified Iraqi pivot points as they determined critical targets against which coalition forces would apply physical power. According to the *Gulf War Air Power Survey*, vol. 1, *Planning and Command and Control,* experienced intelligence analysts were

able to chart the flow of power through the Iraqi military architecture.

> American intelligence recognized the highly centralized nature of the Iraqi military and political systems. And this leadership resided in the person of Saddam Hussein. The CIA, DIA, and State Department devoted a great deal of effort [to] examining him and concluded that he would remain in power for the foreseeable future despite the presence of numerous, ineffective, and demoralized opposition groups. . . . Saddam and the Ba'ath Party maintained their power through a pervasive, effective, and harsh intelligence and security apparatus that periodically infiltrated and decimated internal opposition groups. Thus, both CENTCOM [Central Command—responsible for the Iraqi area of operation] and CENTAF [Central Command Air Forces] staffs targeted leadership before the crisis erupted, but only the military portion of this foundation supported the Baghdad regime. The inclusion of additional political targets into air campaigning occurred only after the United States was committed to Operation Desert Shield.[24]

The Iraqi power structure's economy, intensity, and linkage were effectively identified.

Unfortunately, a misapplication or misunderstanding of our own pivot points can create unwanted entropy that can wreck an operation. Effective discourse fuses power and knowledge critical to any successful military operation.[25] Again, drawing from Operation Desert Storm, a delayed amplification of our own pivot points resulted in an initially poor rhetorical economy of power that was successfully overcome via our superior physical force.[26]

> As in past conflicts, intelligence enabled the planning for Desert Shield and Desert Storm—it did not formulate it. In the case of defensive planning for USCINCCENT [US combatant commander of Central Command] OPLAN [operations plan] 1002–90, intelligence analysts were caught in the post–Cold War transition from Soviet–European emphasis to smaller, but more numerous regional threats. As a result of the region's relatively low priority before Desert Storm, their information on Iraq was less than comprehensive and woefully out of date. Even when those analysts who were watching the Arabian Peninsula detected early signs that Baghdad might be preparing for military operations, they were unable at first to capture the attention of senior policy makers who, up until the summer of 1990, had been advised that Iraq had been exhausted by its war with Iran and would limit its bellicosity to the diplomatic arena.[27]

Fortunately, thanks to Foucault's power analysis, the ability to chart this power flow will help you to operate more effectively during any future conflict—at any echelon (from higher headquarters down to the unit level). Specifically, use of the

military's panopticons can help map the power conduits in each level of an organization—conduits shaped by the organization's social hierarchies, physical structures, procedures, tactics, and strategies. Additionally, an understanding of how Foucault's elements of economy, intensity, and linkage dramatically affect the flow of power or discourse through the conduit structure of any organization, system, or situation will prove helpful.

Obviously, our intelligence capabilities do not allow a complete, unhindered view of an adversary's discourse infrastructures. Moreover, we cannot address discourse mechanisms of real-world threat systems; doing so would move this discussion into a classified realm. Discourse and power flows can be encrypted, hidden, duplicated, and circumvented by many high- and very low-technology means. From satellite communications to hand signals, discourse power flows can branch, ebb, and pool in many ways. However, if you can understand how to isolate, block, or manipulate the discourse flow of any weapon system, you have effectively removed it as a threat. As more is learned about megatons, Mach numbers, cyclic fire rates, and ranges of a wide array of weapon systems, it is very important to consider the power plug for each system; it will undoubtedly highlight the most pivotal characteristics to avoid or exploit.

Notes

1. Sun Tzu, *The Art of War* (Boston: Shambhala Publications, 1988), 82.
2. Michel Foucault, *The Foucault Reader*, ed. Paul Rabinow (New York: Pantheon Books, 1984), 18.
3. Ibid.
4. Ibid., 19.
5. Ibid.
6. Ibid., 20.
7. Ibid., 19.
8. Michel Foucault, *The Archaeology of Knowledge and the Discourse on Language* (New York: Pantheon Books, 1982), 45.
9. Foucault, *The Foucault Reader,* 18.
10. Ibid., 19.
11. Ibid.
12. Ibid.
13. Ibid., 61.
14. Ibid.
15. Ibid.

16. Sonja K. Foss, Karen A. Foss, and Robert Trapp, *Contemporary Perspectives on Rhetoric,* 2d ed. (Prospect Heights, Ill.: Waveland Press, 1993), 224.
17. Foucault, *The Foucault Reader*, 208–9.
18. Foucault, *The Archaeology of Knowledge and the Discourse on Language,* 45.
19. Patricia Bizzell and Bruce Herzberg, eds., *The Rhetorical Tradition: Readings from Classical Times to the Present* (Boston: Bedford Books, 1990), 1128.
20. Ibid.
21. Foucault, *The Foucault Reader,* 207.
22. Ibid.
23. Linda Kozaryn, *Cohen, Shelton Say NATO's Patience, Precision Paid Off,* n.p., on-line, Internet, 5 July 1999, available from http://www.defenselink.mil/news/Jun1999/n06111-99906113.html.
24. Eliot A. Cohen, ed., *Gulf War Air Power Survey*, "Planning," in vol. 1, pt. 1, *Planning and Command and Control* (Washington, D.C.: Government Printing Office, 1993), 206–7.
25. Bizzell and Herzberg, 1128.
26. Foucault, *The Foucault Reader,* 61.
27. Cohen, 191.

Chapter 6

Discontinuity Fever

The test of a first-rate intelligence is the ability to hold two opposed ideas in the mind at the same time, and still retain the ability to function.

—F. Scott Fitzgerald
The Crack-Up

Foucault raises a key question in reference to the flow of power and knowledge: "What is the essence and mode of transformation of power relations?"[1] This discussion has shown how the panopticon can help identify critical pivot points in the power relations of a given architecture. However, in order to fully evaluate power surges, you must examine the flow with a power analysis focused on complex shifts, ruptures, and discontinuities underlying the power structure (fig. 9).[2] The base-line requirement is to "differentiate the networks and levels to which they [power events] belong" and to use power analysis to "reconstitute [detect, characterize, and evaluate] the [discourse] line along which they are connected and engender one another."[3] Foucault clearly understands the strengths and difficult consequences of power analysis: "The notion of discontinuity is a paradoxical one: because it is both an instrument and an object of research; because it divides up the field of which it is the effect; because it enables the historian [tactician] to individualize different domains but can be established only by comparing those domains."[4] A "powerful and flexible grid of interpretation with which to approach relations of knowledge and power" forms the architecture of the organization.[5] You monitor "longer-range continuities in cultural [power] practices" that form Foucaultian norms in order to highlight trip-wire events.[6] Unfortunately, even norms expand and contract to set new and sometimes dangerous tensions on trip-wire power events.

Power shifts, ruptures, and discontinuities can take on many forms when overlaid against a wide range of norms across the globe. For example, the death in 1994 of North Korean leader Kim Il Sung created a relatively small ripple in the power flow

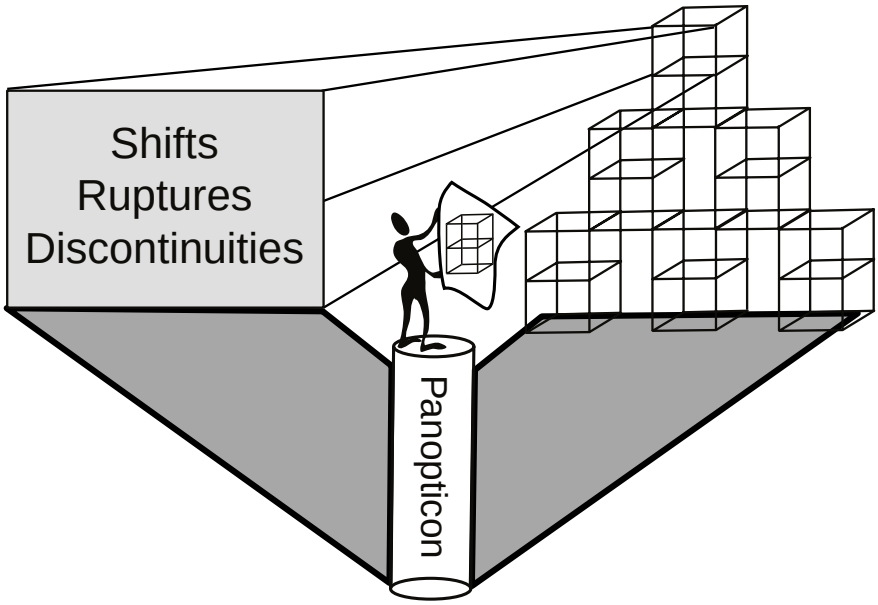


Figure 9. Power Analysis

when compared to deaths of other leaders in other regions. Conversely, the death of Marshal Tito (1892–1980)—anti-Nazi resistance hero from 1941 to 1945 who served as "godfather of all Yugoslavs" after the war—created not only a power shift but a power rupture (creation of new power nodes) with innumerable discontinuities.[7] There are many positive and negative aspects to these power mutations.[8] Obviously, Tito's cohesion of volatile Balkans came at a high price—specifically, his secret police and island prisons.[9] Power ruptures and discontinuities continue to surge throughout the former Yugoslavia—as witnessed in Bosnia and Kosovo (photo, next page). Also, Iraq experienced a dramatic power shift in 2003. The regime change there opened many ruptures and discontinuities as this once repressed country gradually moves toward democracy. Observe the new power nodes that are established, modified, and removed as Iraq is returned to the control of its people. Importantly, consider how these changes can be viewed and analyzed with the help of a rhetorical lens.

Refugees of the Conflict in Kosovo

Other countries (the former Soviet Union, Iran, Cuba, etc.) have faced significant bends in power flow over the years. David Brownstone and Irene Franck's *Timelines of War: A Chronology of Warfare from 100,000 BC to the Present* exhaustively lists recurring (some ongoing from their very origins) issues behind the world's conflicts. The need and the importance of effective intelligence analysis are in no danger of decreasing. James F. Dunnigan and Austin Bay comment on the analysis of global strife: "Wars don't just happen. Organized violence, like the weather, is never a complete surprise. There are signs and long-term trends. You cannot predict exactly what the weather will be at noon tomorrow. You can, however, analyze past and ongoing conflicts and use the results to project the major trends shaping similar current and future events."[10] Shifts, ruptures, and discontinuities (trip-wire events) often precede many signs and long-term trends. You must carefully examine a battle space and help determine a wide array of trip-wire events. Assets, ranging from local (organic) to national level, can be tasked through the intelligence cycle in order to observe these events.

Unfortunately, according to Enoch Powell, even with trip wires, conflicts will remain a permanent part of our history. "The various techniques through which power is enacted are acceptable to us only because most of the power is hidden. The effectiveness of power increases as its visibility decreases.

This disciplinary, normalizing power is far more subtle and pervasive than the easily identifiable, spectacular, repressible, and potentially violent types of power, so we acquiesce readily in ways we would not to more overt forms."[11] As a result of this hidden potential, trip wires can in no way be redirected from the power infrastructure into an isolated checklist. Uncertainties of knowledge (photo below) continue to exist even during our age of high technology.[12]

Uncertainties of Conflict: Crews Train in Chemical Warfare Ensembles

Directly tied to uncertainty is the possibility of deception. The CIA's *A Compendium of Analytic Tradecraft Notes* highlights several key warning signs associated with deception.[13] An understanding of a target country's capabilities, opportunities, and motives helps to scale "the likelihood that a country or organization is engaged in an attempt to distort the analyst's perceptions."[14] "Knowledge of which secrets an adversary most seeks to protect adds a distinctive perspective to the analysts' understanding of the country's military, political, and economic priorities."[15] Additional warning signs highlight the "anomalies in the information available to the analyst."[16] Suspicious gaps in collection, suspicious confirmations, and contradictions to carefully researched patterns represent discontinuities underscored as key warning signs (fig. 10).[17]

Suspicious gaps in collection are generated when "conclusions and judgments received through one collection channel are not supported to the extent expected from the take of other collection systems."[18] Although certain patterns of behavior are subject to rapid change, analysts "should examine criti-

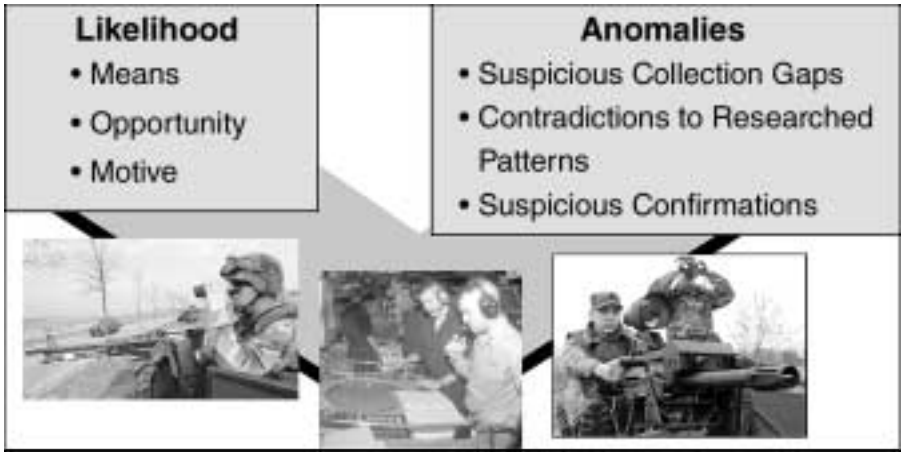


Figure 10. Influence of Deception Warning Signs on Analysis

cally information that signals an inexplicable change, for example, in an adversary's priorities and practices" resulting in contradictions to carefully researched patterns.[19] As a final warning sign to a deception operation, suspicious confirmations result "when a new stream of information from clandestine sources or technical collection seems to reinforce the rationale for or against a U.S. policy initiative."[20] "In these circumstances, receiving the same 'story' from more than one DO [director of operations, or other source] does not in itself speak to the authenticity of the information."[21]

In an attempt to understand power flows and uncertainty or deception, you must remember that analysis is a process— analytical steps steeped in rhetorical theory. Power and discontinuity analysis represent two effective ways to analyze a foe's actions or capabilities. However, prior to initiating any analysis, you need to understand that power (its conduits and flows) influences everyone. Consequently, Foucault's power influences can be found in every human organization and system. Now, you can look at an organization as a power being with a rhetorical circulatory structure supporting its existence. Power (Foucault's discourse and knowledge) flows through the entire organization. As a power-influenced (human conceptualized) entity, an organization has "spatial, temporal, and social compartmentalizations,"[22] which must have a physical means of sharing in-

formation in order to allow power to flow. If you understand the power movement, you can understand the entire organization.

The simplest example of an organization is two people occupying their individual compartmentalizations just a few feet away. You can observe them communicate (visually, verbally, or physically) and can watch what actions take place.[23] The conduits they use are shaped by "social processes, behavioral patterns, systems of norms, types of classification, [and] modes of characterization."[24] Through the proper vantage point (panopticon), you can learn more about how conduits are socially and physically shaped. You can then understand how and when power moves from compartment to compartment. The conduit—along with its content—may take the form of a simple verbal message from one person to another, or it could take on the form of an encoded satellite communication link from headquarters to the cockpit of an aircraft many miles away. Once each actual (suspected or possible) conduit is identified, you can associate actions and events with each type of power flow and conduit. Additionally, critical pivot points—as defined by the Foucaultian elements of economy, intensity, and linkage—can be isolated, attacked, or avoided. If you plot and highlight the conduit's pivot points, you can effectively map the power flow of any organization.

Power shifts, ruptures, and discontinuities in conduits can take on many forms when overlaid against a wide range of global norms. You must be aware that conduits can rapidly change, fail, and fall from expected norms. According to Foucault, "the problem is no longer one of tradition, of tracing a line, but one of division, of limits; it is no longer one of lasting foundations, but one of transformations that serve as new foundations, the rebuilding of foundations."[25] Importantly, many of these power transformations occur naturally. However, you must understand that deception can effectively hide or disguise transformations. Deception can affect your analysis of an organization: a standard consideration for CIA and military analysts. The CIA's *Tradecraft Notes* underscores a need to consider the possible use of deception from the beginning of your observation of an organization, system, or situation.

If uncertainty remains, you continue to focus on the threat power flow, but now you repeat the intelligence process with a different rhetorical perspective/lens.[26] The views of rhetorical theorists such as Kenneth Burke, I. A. Richards, and Walter Ong can also serve as superb perspectives for intelligence analysis. Power flow is one of an unlimited number of rhetorical tools. Historians and tacticians represent "the diversity of sources and thought that both enrich and complicate" analysis.[27] Hopefully, this (Foucaultian) rhetorical sampler illustrates at least one way theory can enrich your analytical perspective.

Unfortunately, all too often you underestimate the power flow and conduit capacity of an organization. You tend to gravitate towards a simple (inadequate) analysis of a threat country's capabilities. According to Eliot A. Cohen and John Gooch, an inadequate analysis—a setback the Israelis faced during the 1973 Yom Kippur War—results from "the products of a failure to think through the many dimensions of a changing strategic challenge."[28]

> Moreover, the IDF [Israel Defense Forces] underestimated the import of substantial improvements in the quality of Arab (and above all, Egyptian) training and coordination since 1967. Because of intensive Soviet advice and, more important, their own efforts, the Egyptian and Syrian armed forces had improved considerably since that war, at virtually every level. To be sure, the IDF had also made tremendous strides in this period, and hence many IDF officers then and since have argued that the relative gap remained the same or had even opened slightly in Israel's favor. The Israeli conception of relative advantage, however, oversimplified the changing relationship between the two sides.[29]

Equally devastating, you also tend to overestimate the power flow and conduit capability of our own military forces. A clear path to understanding our unintentional self-deceptions starts with a step towards understanding our (individual) power strengths and limitations, resulting in an effective "comparative assessment of doctrine and effectiveness"—a penetrating view providing a clear "net assessment" of any situation.[30]

Each one of us serves as a positive or negative pivot point in our organization's power flow. Take the time to learn more about yourself and the other power players in your unit. Learn from those who can successfully analyze the key pivot points and trip wires. Additionally, while in the trenches, document your successes and pass the best analytical processes throughout your

unit and the intelligence community, thereby establishing a powerful conduit for the "rebuilding of [rhetorical] foundations."[31]

Notes

1. Quoted in Michel Foucault, *The Foucault Reader,* ed. Paul Rabinow (New York: Pantheon Books, 1984), 65.
2. Michel Foucault, *The Archaeology of Knowledge and the Discourse on Language* (New York: Pantheon Books, 1982), 5.
3. Foucault, *The Foucault Reader,* 56.
4. Foucault, *The Archaeology of Knowledge and the Discourse on Language,* 9.
5. Ibid.
6. Ibid.
7. James F. Dunnigan and Austin Bay, *A Quick and Dirty Guide to War: Briefings on Present and Potential Wars,* 3d ed. (New York: William Morrow and Co., 1996), 204.
8. Foucault, *The Archaeology of Knowledge and the Discourse on Language,* 12.
9. Dunnigan and Bay, 205.
10. Ibid., xv.
11. Sonja K. Foss, Karen A. Foss, and Robert Trapp, *Contemporary Perspectives on Rhetoric,* 2d ed. (Prospect Heights, Ill.: Waveland Press, 1991), 225.
12. Charles van Doren, *A History of Knowledge: Past, Present, and Future* (New York: Ballentine Books, 1991), 338.
13. John Gannon, "Foreword," in Jack Davis, *A Compendium of Analytic Tradecraft Notes,* ed. F. Douglas Whitehouse (Washington, D.C.: Government Printing Office, 1997), 42.
14. Ibid.
15. Ibid., 43.
16. Ibid.
17. Ibid.
18. Ibid.
19. Ibid.
20. Ibid.
21. Ibid.
22. Foucault, *The Foucault Reader,* 10.
23. Foss, Foss, and Trapp, 14.
24. Foucault, *The Archaeology of Knowledge and the Discourse on Language,* 45.
25. Ibid., 5.
26. Foss, Foss, and Trapp, 12.
27. Ferdinand de Saussure, "Nature of the Linguistic Sign," in *Professing the New Rhetorics: A Sourcebook,* ed. Theresa Enos and Stuart Brown (Boston: Blair Press, 1994), 5.
28. Eliot A. Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War* (New York: Vintage Books, 1991), 130.
29. Ibid., 129–30.
30. Ibid., 129.
31. Foucault, *The Archaeology of Knowledge and the Discourse on Language,* 5.

Chapter 7

In the Trenches

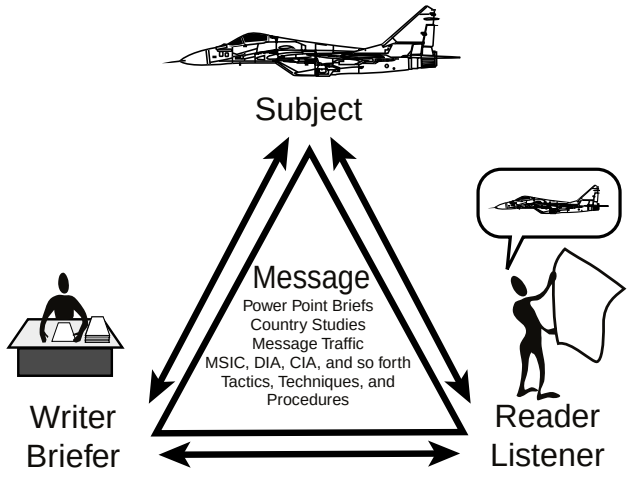
> *But war is not a true adventure. It is a mere ersatz [imitation]. Where ties are established, where problems are set, where creation is stimulated—there you have adventure.*
>
> —Antoine de Saint-Exupéry
> *Flight to Arras*

Real adventure begins at your first assignment when you interact with your primary customers (commanders, crews, and support personnel). The schoolhouse world quickly disappears in a flurry of daily demands. Within your office, you will experience influences of internal Foucaultian power surges from "innumerable points."[1] Some challenges to face include manpower reductions, equipment shortages, and many deployments, as well as a wide array of additional duties. High demand for intelligence support continues to increase as shown in the following photo. Simply put—you will be expected to do more with less. Fortunately, your understanding of rhetorical theory can help.

The F-16—referred to as the Viper by its pilots—is one of many systems you will be expected to support.

From force protection to follow-on test and evaluation of new aircraft and tactics, intelligence support is deeply seeded in daily military operations. Unfortunately, depending on your specific situation, the job may turn from intelligence operator to analysis "medic"—you will hustle to meet operational needs as quickly as they arrive. Usually, this is when theory takes a backseat to providing time-critical products. Yet, even during times of intelligence triage, a few quick notes concerning discourse analysis can help. For example, many well-organized briefings, summaries, and reports are readily available in classified and unclassified formats through the Internet. Specifically, your access to the high-speed Secret Internet Protocol Router Network system makes an incredible array of polished products available. In the trenches, you will depend increasingly on preanalyzed products as you pull down briefings to satisfy short-notice requests. These are excellent products; however, you need to keep in mind that most of these products are not targeted to your specific audience.

Erika Lindemann offers the communication triangle shown in figure 11 as a simple way to help define rhetorical problems.[2] The



Legend:
CIA, Central Intelligence Agency
DIA, Defense Intelligence Agency
MSIC, Missile and Space Intelligence Center

Figure 11. Communication Triangle

problem you will face is rapid adaptation of discourse products influenced by someone else's rhetorical perspective in order to satisfy your customers. As a quick and sound guide, the communication triangle can aid in the formulation of questions concerning the "relationship between terms [corners of the triangle]."[3] The triangle can be used to formulate questions concerning the author's relationship to the subject and audience as depicted in Lindemann's work.[4] Basically, you are "reverse engineering" the originating author's rhetorical process.

As you use products designed for other audiences, you must take on positions (fig. 12) of reader, then writer, editor, and, ultimately, briefer to your specific audience (commanders, crews, and others). Correspondingly, depending on the depth of your analysis, you can significantly enhance your final presentation.

Audience analysis, directly tied to the communication triangle, is critical to all forms of communication. "As you learn more about your audience, the possibilities for your own role as a writer [briefer] will become clearer."[5] This process can be energized by approaching and asking the audience for input. A good recommendation is that you should sit down with your new commanders and crews and ask them what they would

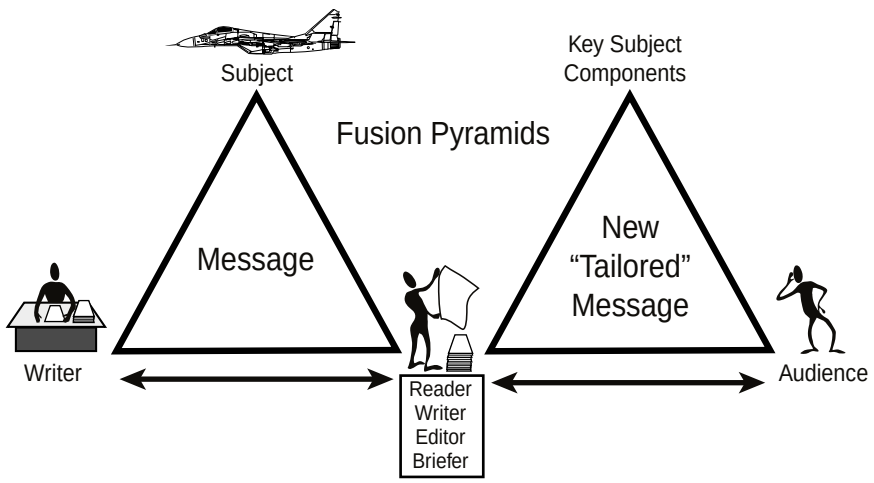
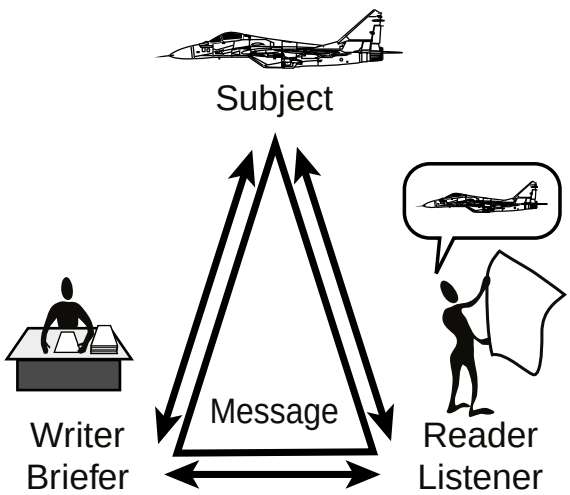


Figure 12. Communication Analysis

like to see. You will build tremendous ethos in the unit and significantly cut your presentation-tailoring time.

Additionally, analysts must ask some critical questions when they use the communication triangle. Specifically, you must understand your audience.[6] Development of an audience profile can help narrow and define audiences through a look at their ages, occupational specialties, and experiences.[7] As this writer (briefer)/reader (listener) relationship grows and matures, your communication triangle actually shrinks at the base; and your message moves with greater speed and clarity.[8] The new, enhanced triangle in figure 13 represents a comprehensive audience understanding, and the writer can use a medium that optimizes this advantage. The CIA, much like other intelligence organizations, skillfully uses audience analysis in order to tailor products "to the individual intelligence consumer's concerns."[9]



Chapter 8

Conclusion

> *So nations have armies to help them, rulers have ministers to assist them. When the helper is strong, the nation is secure; when the helper is weak, the nation is in peril.*
>
> —Sun Tzu
> *The Art of War*

Your primary job as analysts is to excel as the military's helpers to war fighters and decision makers. Hopefully, this discussion has assisted your "pursuit of expertise in analytic tradecraft" through a deeper understanding of rhetorical theory.[1] Rhetorical theory builds a superb foundation, enhancing the intelligence-analysis process at all levels of the discourse spectrum (from unit-level training to combatant-commander briefings). Specifically, the force of Foucault's power and discontinuity analysis provides an insightful analytical perspective.

As Admiral King emphasized, "It is particularly important to comprehend the enemy point of view in all aspects."[2] Importantly, the enemy point of view is in its greatest state of flux since the Cold War. The former Soviet Union, our Cold War "enemy," has transformed from a power-projection threat into an advanced weapons-proliferation concern. Although this transition is troubling, smaller, highly unconventional threats (countries, organizations, and threat systems) are now in the forefront, resulting in some of the greatest challenges for intelligence analysts. Consider the unconventional attacks orchestrated by Osama bin Laden, resulting in the near-simultaneous bombing attacks on the US embassies in Nairobi, Kenya, and Dar es Salaam, Tanzania, on 7 August 1998. Additionally, the 11 September 2001 attacks on the World Trade Center and the Pentagon underscored a critical need to modify our understanding of the enemy point of view.

As an unconventional analytical source, Foucault provides new power perspectives for intelligence analysis, and he gives

US Embassy Damaged by Terrorists in Tanzania

an unconventional look at an ever-growing unconventional threat environment. Foucault's analytical edge helps confront these threats "by refusing to separate off knowledge from power."[3] "His strategy has been to focus his work, both political and intellectual, on what he sees as the greatest threat—that strange, somewhat unlikely, mixing of the social science and social practices developed around subjectivity."[4] Foucault's theories address the human behind the satellite images and database numbers. He reminds you to "distinguish among events, to differentiate the networks and levels to which they belong, and to reconstitute the lines along which they are connected and engender one another."[5]

Some of you are already using many components of these powerful rhetorical tools. Some organizations, such as the CIA, are compiling key elements of these theories that directly apply to their craft. These theories work to bridge practical application gaps in the intelligence community—enhancing our ability to adapt and thwart failure. Eliot A. Cohen and John Gooch, authors of *Military Misfortunes: The Anatomy of Failure in War,* underscore the basic reasons for failure in military organizations:

"failure to learn, failure to anticipate, and failure to adapt."[6] Theory allows you to learn from rhetorical lessons of the past, resulting in an intelligence service that can anticipate and adapt to power flows, shifts, ruptures, and discontinuities. These authors also underscore the importance of the skill of adaptation (specifically referencing the US Navy's recovery from a string of setbacks during its 1940–42 antisubmarine warfare campaign): "Indeed, the ability to adapt is probably most useful to any military organization and most characteristic of successful ones, for with it, it is possible to overcome both learning and predictive failures. In the interim, however, the cost of such failures will be—and in the case was—high, in terms of blood, treasure, and time."[7] The end result of an enhanced understanding of theory is an adaptive intelligence organization that is able to provide a comprehensive view of the battle space to war fighters. As intelligence operators, you must strive to enhance your analytical growth through rhetorical theory—a force-multiplying education that extends our comprehension of an evolving, growing threat environment.

Notes

1. John Gannon, "Foreword," in Jack Davis, *A Compendium of Analytic Tradecraft Notes*, ed. F. Douglas Whitehouse (Washington, D.C.: Government Printing Office, 1997), vi.
2. Quoted in Naval Doctrine Publication 2, *Naval Intelligence*, 1994, 24.
3. Quoted in Michel Foucault, *The Foucault Reader*, ed. Paul Rabinow (New York: Pantheon Books, 1984), 7.
4. Ibid.
5. Ibid., 56.
6. Eliot A. Cohen and John Gooch, *Military Misfortunes: The Anatomy of Failure in War* (New York: Vintage Books, 1991), 26.
7. Ibid., 94.

Bibliography

Air Force Press. On-line. Internet, 10 March 1999. Available from http://www.af.mil.html.

Bizzell, Patricia, and Bruce Herzberg, eds. *The Rhetorical Tradition: Readings from Classical Times to the Present.* Boston: Bedford Books, 1990.

Brownstone, David, and Irene Franck. *Timelines of War: A Chronology of Warfare from 100,000 B.C. to the Present.* New York: Little, Brown and Co., 1994.

Central Intelligence Agency. *Agencies of the US Intelligence Community (USIC):1998.* On-line. Internet, 10 June 1999. Available from http://www.cia.gov/ic/ichome.htm.

———. *Analysis: Directorate of Intelligence in the 21st Century.* Washington, D.C.: Government Printing Office (GPO), 1996.

———. *The World Factbook.* Washington, D.C.: Brassey's, 1998. On-line. Internet, 10 June 1999. Available from http://www.cia.gov/cia/publications/factbook/country.html.

Cohen, Eliot A., ed. *Gulf War Air Power Survey.* 5 vols. Washington, D.C.: GPO, 1993.

Cohen, Eliot A., and John Gooch. *Military Misfortunes: The Anatomy of Failure in War.* New York: Vintage Books, 1991.

Coulthard, Malcolm. *An Introduction to Discourse Analysis.* 2d ed. New York: Longman Limited, 1985.

Davis, Jack. *A Compendium of Analytic Tradecraft Notes.* Edited by F. Douglas Whitehouse. Foreword by John Gannon. Washington, D.C.: GPO, 1997.

DOD News Briefing. On-line. Internet, n.d. Available from http: http://www.defenselink.mil/news/Jul999/t07011999_t0701sd.html.

Dulles, Allen. *The Craft of Intelligence.* New York: Harper and Row, 1963.

Dunnigan, James F., and Austin Bay. *A Quick and Dirty Guide to War: Briefings on Present and Potential Wars.* 3d ed. New York: William Morrow and Co., 1996.

Fillingham, Lydia A. *Foucault for Beginners.* New York: Writers and Readers Publishing, 1993.

Foss, Sonja K., Karen A. Foss, and Robert Trapp. *Contemporary Perspectives on Rhetoric.* 2d ed. Prospect Heights, Ill.: Waveland Press, 1991.

Foucault, Michel. *Aesthetics, Method, and Epistemology: Essential Works of Foucault, 1954–1984.* Edited by James Faubion. New York: New Press, 1998.

———. "The Archaeology of Knowledge." *The Rhetorical Tradition: Readings from Classical Times to the Present.* Edited by Patricia Bizzell and Bruce Herzberg. Boston: Bedford Books, 1990.

———. *The Foucault Reader.* Edited by Paul Rabinow. New York: Pantheon, 1984.

———. "The Order of Discourse." In *The Rhetorical Tradition: Classical Times to the Present.* Edited by Patricia Bizzell and Bruce Herzberg. Boston: Bedford Books, 1990.

———. *This Is Not a Pipe.* Translated and edited by James Harkness. Los Angeles: University of California Press, August 1983.

Hirsch, E. D., Jr. *The Dictionary of Cultural Literacy*. 2d ed. Boston: Houghton Mifflin Co., 1993.

Holman, Hugh C., and William Harmon. *A Handbook to Literature*. 5th ed. New York: Macmillan, 1986.

Joint Publication 2-01. *Joint Intelligence Support to Military Operations,* 1996.

Kent, Sherman. "The Need for an Intelligence Literature." *Studies in Intelligence*, spring 1955, 3. On-line. Internet, 2 February 1999. Available from http://www.odci.gov/csi/books/shermankent/2need.html.

Kozaryn, Linda. *Cohen, Shelton Say NATO's Patience, Precision Paid Off.* On-line. Internet, 5 July 1999. Available from http://www.defenselink.mil/news/June 1999/ n06111999_9906113.html.

"Leadership: Combat Leadership." Lecture. Squadron Officer School, Maxwell AFB, Ala., Class 97D, 1994.

Lindemann, Erika. *A Rhetoric for Writing Teachers*. 3d ed. New York: Oxford University Press, 1995.

Melton, H. Keith. *The Ultimate Spy Book*. New York: DK Publishing, 1996.

National Reconnaissance Office. *Who We Are*. On-line. Internet, 20 March 1999. Available from http://www.nro.odci.gov/background.html.

Naval Doctrine Publication (NDP) 2. *Naval Intelligence*, 1994. On-line. Internet, 11 July 2003. Available from http://www.nwdc.navy.mil/Library/Documents/NDPs/ndp2/ndp20001.htm.

Ong, Walter J. *Orality and Literacy: The Technologizing of the Word*. New York: Routledge, 1995.

Patterns of Global Terrorism: 1998. On-line. Internet, 20 June 1999. Available from http://www.state.gov/www/global/terrorism/1998Report.

Reid, Stephen. *The Prentice Hall Guide for College Writers*. 4th ed. London: Prentice Hall, 1998.

Saint-Exupéry, Antoine. *Flight to Arras*. Translated by Lewis Galantiere. New York: Harcourt Brace Jovanovich, 1942.

Saussure, Ferdinand de. "Nature of the Linguistic Sign." In *Professing the New Rhetorics: A Sourcebook*. Edited by Theresa Enos and Stuart Brown. Boston: Blair Press, 1994.

Tobey, Ronald C. *Foucault, Michel*. On-line. Internet, 11 March 1998. Available from http://www.kaiwan.com/~lucknow/horus/guide/cm108.html.

Tomlin, Russell S., et al. "Discourse Semantics." In *Discourse as Structure and Process*. Edited by Teun van Dijk. London: Sage, 1997.

Tzu, Sun. *The Art of War*. Boston: Shambhala, 1988. On-line. Internet, 10 March 1999. Available from http://www.af.mil.html.

Van Doren, Charles. *A History of Knowledge: Past, Present, and Future*. New York: Ballantine Books, 1991.

Index

airborne command, control, and surveillance systems, 30
Allied Force. *See* Operations.
analysis, 1–6, 8–9, 11, 14–19, 22–23, 25, 27–31, 33, 36, 39–41, 43–45, 48–50, 53, 55
analytic tradecraft, 3, 42, 52, 55
Aristotle, 7–9
arrangement, 7
artifacts, 13–14, 16–18
Art of Rhetoric, 6–7
Art of War, The, 14
audience analysis, 49–50

Balkan Ghosts: A Journey through History, 27
Balkans, 40
Bay, Austin, 41
Bentham, Jeremy, 28
Bosnia, 40
Brownstone, David, 41
Burke, Kenneth, 45

canons, 7
Central Intelligence Agency (CIA), 2–3, 5, 12, 14, 36, 42, 44, 48, 50–52, 56
Cicero, Marcus, 25
Clausewitz, Carl von, 23
Clausewitzian principles, 24
Cohen, Eliot A., 45, 56
Cohen, William S., 35
coherent representation, 17
Cold War, 55
collection, 11–15, 42–43
combatant commander, 31, 36
communication
  paradigms, 7
  triangle, 48–51
Compendium of Analytic Tradecraft Notes, 42, 52
Corax of Syracuse, 6
Corona, 13–15
credibility, 8
critical analysis, 9
cultural literacy, 50–51

Dar es Salaam, Tanzania, 55
deception, 17, 42–44
Desert Shield. *See* Operations.
Desert Storm. *See* Operations.
devices for exclusion, 22
Directorate of Intelligence, 5, 51
discourse
  community, 51
  formation, 33
  infrastructure, 37
  mechanism, 15
  power flows, 37
dissemination and integration, 12, 18
Dunnigan, James F., 41

11 September 2001, 55
embassy, 56
enhanced communication triangle, 50
essential elements of information (EEI), 16, 18
ethos, 7–8, 50
exploitation phase, 15

F-117, 24
finished intelligence, 15, 18
fog and friction, 24
Fontana, Alessandro, 23
Forrest, L., 17
Foss, Sonja K., 22
Foucault, Michel, 1, 3, 5, 11, 19, 21–25, 27–31, 33–34, 36–37, 39, 43–44, 52–53, 55–56
Franck, Irene, 41

Gannon, John, 3
Gooch, John, 45, 56
Green Ramp, 27
Gulf War. *See* Persian Gulf War.
Gulf War Air Power Survey, vol. 1, *Planning and Command and Control,* 35

Hirsch, E. D., Jr., 50

information, 3, 6–8, 18, 36, 42–44, 51–53
  access to, 31, 35
  age, 5
  analysis, 17
  fusion of, 15
  key elements of, 11,
  management, 16–17
  value of information of the enemy, 1

integrated air defense system, 30
intelligence, 1–19, 24–25, 28, 30–32, 35–37, 39, 41, 45–48, 50–51, 53, 55–57
  analysis, 1–2, 4, 17, 28, 41, 45, 55
  community, 1, 3, 10, 12, 18, 46, 56
  cycle, 1, 11–13, 18–19, 41
  discourse, 2
  finished, 15
  integration, 17
  operators, 5, 57
  "pulled," 18
  "pushed," 16, 18
  sources, 16
  specialist, 1
Internet, 12, 31, 48
invention, 7
Iraqi
  aircraft shelter, 19
  area of operation, 36
  military architecture, 36
  pivot points, 35
  power structure, 36
  president, 36. *See also* Saddam Hussein.
irruptive, 21

Joint
  Guardian. *See* Operations.
  Publication (JP) 2-01, *Joint Intelligence Support to Military Operations*, 11
  surveillance, target attack radar system (JSTARS), 30
Jomini, Antoine Henri de, 24
  warfare theory, 24

Kalugin, Oleg, 13
Kaplan, Robert, 27
Kent, Sherman, 2
Kim Il Sung, 39
Kim, M., 17
King, Ernest, 1
Kosovo, 24, 27, 35, 40–41

Lindemann, Erika, 48
logos, 7–8

Marshal Tito, 40
memory, 7, 51
message, 15, 31, 44, 50–53
military
  discourse community, 51
  literacy, 51
Military Misfortunes: The Anatomy of Failure in War, 56
mnemonics, 7
modern intelligence specialist, 1
modulation, 7

Nairobi, Kenya, 55
National Reconnaissance Office (NRO), 13–14
NATO, 30, 35
Naval Doctrine Publication 2, *Naval Intelligence*, 12, 16

Ong, Walter, 45, 52–53
Operations
  Allied Force, 35
  Desert Shield, 36
  Desert Storm, 11, 36
  Joint Guardian, 35
operationally focused instruction, 19
oral communication, 53
Orality and Literacy: The Technologizing of the Word, 52
oratory, 5
Osama bin Laden, 55

panopticon, 28–31, 39, 44
Pasquino, Pasquale, 23
pathos, 8
pedagogy, 11
Pentagon, 55
Persian Gulf War, 35
physical power, 34–35
Poitiers, France, 21
Pope Air Force Base (AFB), North Carolina, 27
Powell, Enoch, 41
power
  analysis, 4, 22, 29–30, 33, 36, 39–40
  architecture, 31–32
  flow, 31, 34–36, 39, 41, 44–45
  mutations, 40
  ruptures, 24, 40
"Probable Course of Action," 6
processing and exploitation, 12, 15
product, 15, 17–18, 51
production phase, 15

propaganda, 5
psychopathology, 21
Pu, M. M., 17
"pursuit of expertise in analytic tradecraft," 55

reconnaissance aircraft, 14–15
"rhetoric is an action," 5–6
rhetorical
  template, 4, 9
  vision, 1
Richards, I. A., 45

Saddam Hussein, 36
secondary orality, 53
Secret Internet Protocol Router Network system, 48
Serbian military infrastructure, 35
Sicily, 6
Sun Tzu, 14, 28, 55
Syracuse, Corax of, 6

tactician, 22–23, 39
technical paradigm shifts, 8
Timelines of War: A Chronology of Warfare from 100,000 BC to the Present, 41
Tomlin, Russell L., 17
trip wire, 41–42, 45
  events, 39, 41
tropes, 5

University of Arkansas, 2

warning signs, 42–43
World Trade Center, 55

Yugoslavia, 40

The Role of Rhetorical Theory in Military Intelligence Analysis

A Soldier's Guide to Rhetorical Theory

Air University Press Team

Chief Editor
Hattie D. Minter

Copy Editor
Joan Hickey

Book Design and Cover Art
Daniel M. Armstrong

Composition and Prepress Production
Mary P. Ferguson

Quality Review
Joan Dawson

Print Preparation
Joan Hickey

Distribution
Diane Clark

This Page Is Intentionally Left Blank

NAVAL POSTGRADUATE SCHOOL

MONTEREY, CALIFORNIA

THESIS

EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL WITHIN THE HOMELAND SECURITY ENTERPRISE

by

Roger L. Stokes

December 2013

Thesis Co-Advisors: Kathleen Kiernan
John Rollins

Approved for public release; distribution is unlimited

THIS PAGE INTENTIONALLY LEFT BLANK

REPORT DOCUMENTATION PAGE		Form Approved OMB No. 0704–0188

Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instruction, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202–4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704–0188) Washington, DC 20503.

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE December 2013	3. REPORT TYPE AND DATES COVERED Master's Thesis

4. TITLE AND SUBTITLE EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL WITHIN THE HOMELAND SECURITY ENTERPRISE	5. FUNDING NUMBERS
6. AUTHOR(S) Roger L. Stokes	
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) Naval Postgraduate School Monterey, CA 93943–5000	**8. PERFORMING ORGANIZATION REPORT NUMBER**
9. SPONSORING /MONITORING AGENCY NAME(S) AND ADDRESS(ES) N/A	**10. SPONSORING/MONITORING AGENCY REPORT NUMBER**

11. SUPPLEMENTARY NOTES The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government. IRB Protocol number ____N/A____.

12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited	12b. DISTRIBUTION CODE A

13. ABSTRACT (maximum 200 words)

The purpose of this thesis was to examine the employment and adherence of the intelligence cycle process model within the National Network of Fusion Centers and the greater Homeland Security Enterprise by exploring the customary intelligence cycle process model established by the United States Intelligence Community (USIC). This thesis revealed there are various intelligence cycle process models used by the USIC and taught to the National Network. Given the numerous different training entities and varied intelligence cycle process models, challenges exist with providing a well-defined training program that ensures consistent and clear intelligence cycle process model employment. Finally, this thesis offers an overview pertinent to researchers and/or practitioners regarding the viability of employing the intelligence cycle process model as the principle guide for domestic intelligence activities.

This thesis employed a qualitative research method that analyzed and interpreted publicly available academic and policy information gathered from government and nongovernment institutions regarding the conceptual and practical intelligence cycle process model narratives. A case study analysis was conducted of the April 15, 2013, Boston Marathon bombing as a platform to discuss the active and effective employment of the intelligence cycle process model by the National Network.

The principal conclusion offers while literature clearly agrees the intelligence cycle process model is a cyclical structure of actions, literature also finds there are common themes suggesting the intelligence cycle does not sufficiently describe how the intelligence process works at the operational stages of domestic intelligence activities within the National Network.

14. SUBJECT TERMS Domestic intelligence, intelligence cycle, intelligence, fusion centers, national network, homeland security enterprise, homeland security intelligence enterprise, US Intelligence Community, 28 CFR Part 23, national criminal information sharing plan, information sharing environment.	15. NUMBER OF PAGES 117
	16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UU

NSN 7540–01–280–5500 Standard Form 298 (Rev. 2–89)
Prescribed by ANSI Std. 239–18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL WITHIN THE HOMELAND SECURITY ENTERPRISE

Roger L. Stokes
Senior Intelligence Officer, U.S. Department of Homeland Security, Dallas, TX
B.S., Excelsior College, 2002
M.A., University of Oklahoma, 2003

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF ARTS IN SECURITY STUDIES
(HOMELAND SECURITY AND DEFENSE)

from the

NAVAL POSTGRADUATE SCHOOL
December 2013

Author: Roger L. Stokes

Approved by: Kathleen Kiernan, PhD
Thesis Co-Advisor

John Rollins
Thesis Co-Advisor

Mohammad Hafez, PhD
Chair, Department of National Security Affairs

THIS PAGE INTENTIONALLY LEFT BLANK

ABSTRACT

The purpose of this thesis was to examine the employment and adherence of the intelligence cycle process model within the National Network of Fusion Centers and the greater Homeland Security Enterprise by exploring the customary intelligence cycle process model established by the United States Intelligence Community (USIC). This thesis revealed there are various intelligence cycle process models used by the USIC and taught to the National Network. Given the numerous different training entities and varied intelligence cycle process models, challenges exist with providing a well-defined training program that ensures consistent and clear intelligence cycle process model employment. Finally, this thesis offers an overview pertinent to researchers and/or practitioners regarding the viability of employing the intelligence cycle process model as the principle guide for domestic intelligence activities.

This thesis employed a qualitative research method that analyzed and interpreted publicly available academic and policy information gathered from government and nongovernment institutions regarding the conceptual and practical intelligence cycle process model narratives. A case study analysis was conducted of the April 15, 2013, Boston Marathon bombing as a platform to discuss the active and effective employment of the intelligence cycle process model by the National Network.

The principal conclusion offers while literature clearly agrees the intelligence cycle process model is a cyclical structure of actions, literature also finds there are common themes suggesting the intelligence cycle does not sufficiently describe how the intelligence process works at the operational stages of domestic intelligence activities within the National Network.

THIS PAGE INTENTIONALLY LEFT BLANK

TABLE OF CONTENTS

I. INTRODUCTION....1
A. PROBLEM STATEMENT....5
B. OVERVIEW....7
C. RESEARCH OBJECTIVES AND METHODOLOGY....10

II. LITERATURE REVIEW....13
A. DEFINING KEY INTELLIGENCE ENTERPRISES AND THE TERM "INTELLIGENCE"....15
B. INTELLIGENCE CYCLE PROCESS MODELS....19
C. CORE ISSUE....21
D. HOMELAND SECURITY ENTERPRISE AND NATIONAL NETWORK INTELLIGENCE CYCLE TRAINING....32

III. DOMESTIC INTELLIGENCE AND EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL....37
A. DOMESTIC INTELLIGENCE ACTIVITIES – NATIONAL SECURITY FOCUS....37
B. DOMESTIC INTELLIGENCE POLICY....40
C. EXPLOITING DOMESTIC INTELLIGENCE AUTHORITIES – ABUSES....44
D. USIC MEMBERS – FBI, CIA, AND DOD/NSA....45
E. LOCAL LAW ENFORCEMENT....48
F. NATIONAL NETWORK OF FUSION CENTERS....49
G. DOMESTIC INTELLIGENCE - CULTURE....50

IV. INTELLIGENCE CYCLE PROCESS MODEL CASE STUDY – BOSTON MARATHON BOMBING....55
A. INTRODUCTION....55
B. SCENARIO....57
C. PHASE 1 – REQUIREMENTS/NEEDS....57
D. PHASE 2 – PLANNING/DIRECTION....59
E. PHASE 3 – COLLECTION....61
F. PHASE 4 – PROCESSING....63
G. PHASE 5 – ANALYSIS....64
H. PHASE 6 – DISSEMINATION....66
I. CONCLUSION....66

V. INTELLIGENCE CYCLE PROCESS MODEL AND THE HOMELAND SECURITY ENTERPRISE....71
A. HOMELAND SECURITY ENTERPRISE AND EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL....71
B. INTELLIGENCE CYCLE PROCESS MODEL TRAINING....72
C. STATE AND LOCAL LAW ENFORCEMENT COMMUNITY....75
D. PRIVATE SECTOR....77

E. PRACTICAL CHALLENGES TO EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL 80
F. CONCLUSION 81
BIBLIOGRAPHY 87
INITIAL DISTRIBUTION LIST 95

LIST OF FIGURES

Figure 1. FBI Intelligence Cycle 24
Figure 2. The Iowa State Police Intelligence Cycle 24
Figure 3. CIA Intelligence Cycle 25
Figure 4. DoD Joint Publication Intelligence Cycle....25
Figure 5. The Prediction-Led Policing Business Process Model, RAND RR233–1.1 ...28

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF TABLES

Table 1. The Various Types of Organizational Intelligence Cycle Models and Attributes.....9
Table 2. Timeline Reflecting Intelligence Policy Engagement among Federal and Local Environment.....83

THIS PAGE INTENTIONALLY LEFT BLANK

LIST OF ACRONYMS AND ABBREVIATIONS

ACLU	American Civil Liberties Union
BUR	Bottom Up Review
CC	Community Coordinator
CFR	Code of Federal Regulation
CIA	Central Intelligence Agency
CINT	Chief Intelligence Officer
COC	Critical Operational Capability
COINTELPRO	Counterintelligence Program
D	Departmental
DHS	Department of Homeland Security
DNI	Office of the Director of National Intelligence
DoD	Department of Defense
DOJ	Department of Justice
EO	Executive Order
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
HSAC	Homeland Security Advisory Committee
HSE	Homeland Security Enterprise
HSEC SIN	Homeland Security Standing Information Needs
HSIE	Homeland Security Intelligence Enterprise
I&A	Office of Intelligence and Analysis
IACP	International Association of Chiefs' of Police
IALEIA	International Association of Law Enforcement Intelligence Analyst
ILP	Intelligence-Led Policing
IRTPA	Intelligence Reform and Terrorism Prevention Act
ISAC	Information Sharing and Analysis Center
ISE	Information Sharing Environment
JTTF	Joint Terrorism Task Force
MCCA	Major City Chiefs' Association

MCCCIE	Major City Chiefs' Criminal Intelligence Enterprise
NCISP	National Criminal Intelligence Sharing Plan
NSA	National Security Agency
USA PATRIOT	Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism
PM	Program Manager
S	Service
SLTPS	State, Local, Tribal, and Private Sector
TCL	Target Capabilities List
USIC	United States Intelligence Community

EXECUTIVE SUMMARY

The United States Intelligence Community (USIC) was not designed to serve as a concept intended to detect significant national security threats originating or residing within our nation's borders, but it was focused on foreign intelligence activities. Little research has been done to study the post-9/11 Homeland Security Enterprise (HSE) counterterrorism efforts supporting domestic intelligence activities and its reliance on the intelligence cycle process model. This thesis evaluates whether the intelligence cycle process model supports the performance of domestic intelligence activities, specifically within the National Network of Fusion Centers (National Network) and the greater HSE.

The unprecedented September 11, 2001, terrorist attacks brought into question the USIC intelligence collection capabilities and served as the catalyst for state, local, tribal and private sector partners into the HSE. The DHS 2011 National Network of Fusion Centers Final Report defined the HSE as federal, state, local, tribal, nongovernmental, and private sector entities. The HSE serves organized complex organizations and their relationships through the National Network. The National Network allows for the integration of the HSE as nontraditional intelligence entities employing intelligence collection and analysis. The National Network and broader HSE have become essential elements providing support to the national intelligence architecture.

Originally, the 1947 USIC structure and the function of its intelligence cycle process model was designed to provide essential information to the president, policymakers, federal organizations, and military communities. The 1947 USIC structure has expanded to its current structure that includes 17 organizations charged with conducting intelligence activities – both foreign and domestic. Today, the growth of the USIC and its purpose has expanded beyond federal elements to include the National Network and the HSE in order to enhance domestic intelligence capabilities.

An assessment of the limited information made available that focuses on domestic intelligence and the intelligence cycle employment reveals information gaps concerning its effectiveness and appropriateness within the post-9/11 HSE. While literature clearly agrees the intelligence cycle process model is a cyclical structure of actions, literature also finds there are common themes suggesting the intelligence cycle does not sufficiently describe how the intelligence process works at the operational stages of domestic intelligence activities within the National Network.

This thesis offers an overview pertinent to researchers and/or practitioners regarding the viability of employing the intelligence cycle process model as the principle guide for domestic intelligence collection activities. Intelligence derived from analyzed information through the intelligence cycle process serves as a principle tool for supporting the nation's counterterrorism efforts and offers law enforcement and homeland security officials with insights and advantages over terrorists. However, there are multiple intelligence cycle concepts within the USIC and the HSE. The various intelligence cycle process models range from a four-step process to a seven-step process.

There are various intelligence cycle process models used by the USIC and now being taught to the National Network by federally funded entities. As an example, the DHS Office of Intelligence and Analysis (I&A), the National Counterterrorism Center, the Memorial Institute for the Prevention of Terrorism (MIPT), the Department of Justice State and Local Anti-terrorism Training Program, and the International Association of Law Enforcement Intelligence Analysts (IALEA) each deliver intelligence training opportunities enthusiastic of the intelligence cycle process model. Given the number of different training entities and varied intelligence cycle process models, challenges exist with providing a well-defined training program that ensures consistent and clear intelligence cycle process model employment within the National Network.

A case study analysis of the April 15, 2013, Boston Marathon bombing illuminates adherence to the intelligence cycle process model as a proactive approach that may have prevented the bombing. This case study was selected in an effort demonstrate the conceptual intelligence cycle process model, in action. Additionally, it

offers the challenges with employing the intelligence cycle process model as an element of the 2003 National Criminal Information Sharing Plan (NCISP) in efforts to prevent terrorism.

The literature provided no USIC or HSE doctrinal information on the adoption of the intelligence cycle as a formal process by USIC or HSE members. Providing comprehensive, consistent intelligence cycle process training to the National Network may serve to decrease privacy concerns while also verifying a concerted federal effort in the fitting execution of domestic intelligence activities. Drawing on publicly available information from government, academia, and national security consortiums, analysis revealed broad acceptance of the intelligence cycle process model philosophy. However, literature provided by academic and operational practitioners support claims that the intelligence cycle process model is flawed and not practical in the operational environment. This thesis may serve as a basis for recommending additional research necessary for studying the intelligence cycle process model implementation and employment within the post-9/11 HSE and its effectiveness in preventing terrorist attacks and enhancing national security intelligence.

THIS PAGE INTENTIONALLY LEFT BLANK

ACKNOWLEDGMENTS

Jeremiah 33:3 – “Call unto Me and I will answer you, and tell you great and hidden things that you have not known.” (ESV)

I would like to thank my wonderful wife, Nikkia, and children, Xavier and Isaiah, for their support and sacrifices during the time spent away doing my academic work. May they forever live in the blessings of God.

Finally, I would like to thank my thesis advisors, Dr. Kathleen Kiernan and Mr. John Rollins, as their steady guidance throughout the thesis process was both insightful and encouraging. Thank you for your words of support and direction.

To the senior leadership, Mr. Scott McAllister and Mr. Robin Taylor, of the DHS Office of Intelligence and Analysis, State and Local Program Office for their support in making this endeavor a reality.

Moreover, to the men and women of the United States Intelligence Community, the United States Military, Federal and Domestic Law Enforcement, the Fire Service, Emergency Management and Emergency Medical Services who protect this nation on a daily basis. May God watch over and protect you.

THIS PAGE INTENTIONALLY LEFT BLANK

I. INTRODUCTION

The topic discussed in this thesis is important to the author, and as such, presents a degree of theoretical sensitivities. This thesis runs the risk of slight bias towards the intelligence cycle process model from the federal level and national security intelligence perspective; juxtapose the nontraditional criminal intelligence perspective at the state and local level. The author's own professional experiences as a retired intelligence collector with the U.S. Army Military Intelligence Corps/Defense Intelligence Agency, former Federal Bureau of Investigation Supervisory Intelligence Analyst and current DHS Senior Intelligence Officer have been useful in understanding the policy and practical challenges related to employing the intelligence cycle process model.

However, the intent of this research is to serve as an introduction and description of the issues necessary to explore employing the customary intelligence cycle process model established by the United States Intelligence Community (USIC) within the National Network of Fusion Centers (National Network) and the greater Homeland Security Enterprise (HSE). The information offered delivers an overview pertinent to researchers and/or practitioners regarding the viability of employing the intelligence cycle process model as the principle guide for domestic intelligence collection activities.

On September 11, 2001, the unthinkable happened. International terrorists residing in the US brought into question the USIC intelligence collection capabilities and served as the catalyst for state, local, tribal and private sector partners into the HSE. Immediately following the devastating strike, the nation focused all of its intelligence collection efforts on the prevention of future terrorist attacks from abroad and from within. Nine separate national strategies were written to address elements of homeland security. They include, in part, a National Intelligence Strategy published by the Office of the Director of National Intelligence (DNI) in 2005; a National Strategy for Homeland Security published by the White House in 2007; a National Counterintelligence Strategy published by the DNI in 2009; a National Security Strategy of the United States published by the White House in 2010; a National Counterterrorism Strategy published by the White House in 2011, and most recently a National Strategy for Information

Sharing and Safeguarding published by the White House in 2012. The lack of any national level guidance or strategy related to the collection of domestic intelligence within the HSE other than organizational relationships, classified, or otherwise appears to be a glaring oversight.

The DHS *2011 National Network of Fusion Centers Final Report* defined the HSE as federal, state, local, tribal, nongovernmental, and private sector entities.[1] The HSE serves organized complex organizations, and their relationships with the national intelligence architecture through the National Network. Collecting and analyzing information through the National Network combines state and local criminal intelligence and national intelligence to address transnational threats.[2] The National Network in partnership with the HSE provides an essential information collection and analysis function in efforts to prevent terrorist attacks within the homeland.

Within this complex HSE, there are several USIC intelligence cycle process models being taught. Given today's transnational threat environment, this thesis is intended to inform readers regarding the adaptation and adherence to the intelligence cycle process model within the HSE. The adherence to a consistent intelligence cycle process model within the National Network, as an internal entity of the complex HSE, is critical to producing common operating threat pictures at all levels of government.

The National Network is the integration of nontraditional intelligence entities into the practice of intelligence collection and analysis essential for supporting the national intelligence architecture. In order to examine the National Network's adeptness to adapt to the intelligence cycle process model, it is fitting to review the history of the USIC germane to the intelligence process. The USIC serves as a coalition of agencies and organizations that work both independently and collaboratively with the primary mission

[1] U.S. Department of Homeland Security, *2011 National Network of Fusion Centers Final Report*, May 2012, 2.

[2] 50 U.S. Code Section 402(i)(5) defines transnational threats as any transnational activity (including international terrorism, narcotics trafficking, the proliferation of weapons of mass destruction and the delivery systems for such weapons, and organized crime) that threatens the national security of the United States that includes any individual or group that engages in such activity.

to collect and produce intelligence. The USIC has evolved tremendously in size, structure, and scope since its creation more than 60 years ago following World War II and the 1947 National Security Act. However, the conceptual intelligence cycle process has essentially gone unchanged since its inception. Notwithstanding, the intelligence cycle process phases or steps have increased over the years.

Over the 60 years the USIC has existed, domestic intelligence activities have raised serious concerns regarding privacy, civil rights and civil liberties as a result of abuses of authority and illegal behavior by federal and local law enforcement intelligence entities. Providing federally funded training to the National Network that supports employing the intelligence cycle process model is once again raising concerns among privacy advocates and American citizens. Providing comprehensive, consistent intelligence cycle process training to the National Network may serve to decrease privacy concerns while also verifying a concerted federal effort in the proper execution of the intelligence process. Literature reveals even the best analysis will do nothing to affect national security and crime rates at the state and local level, if it does not influence practices within the National Network.

Chapter II offers a literature review essential for identifying critical premises, as well as contributions necessary for exploring the adherence to the intelligence cycle process model within the National Network. The main goal of the literature review is to understand intelligence cycle process models and to provide context for homeland security and intelligence professionals. Fundamental to this chapter is defining the USIC, the Homeland Security Intelligence Enterprise (HSIE), the HSE, and key intelligence terms. As important is the identification and illumination of the various intelligence cycle process models being used within the HSE.

The 1947 USIC structure has expanded to its current structure that includes 17 organizations charged with conducting intelligence activities both foreign and domestic. The 17-member USIC is composed of a community coordinator, six program managers, five departmental elements, and five services. The Office of the Director of National Intelligence serves as the USIC community coordinator. The six USIC entities that serve as intelligence program managers are the Central Intelligence Agency, the Defense

Intelligence Agency, the National Security Agency, the National Reconnaissance Office, Federal Bureau of Investigation (National Security Branch), and the National Geospatial-Intelligence Agency. The five departmental elements identified as USIC members within specific organizations are the Department of Energy's Office of Intelligence and Counterintelligence, the Drug Enforcement Administration's Office of National Security Intelligence, the Department of Homeland Security's Office of Intelligence and Analysis, the Department of State's Bureau of Intelligence and Research, and the Department of the Treasury's Office of Intelligence and Research. The five services identified as USIC members are US Air Force Intelligence, US Army Intelligence, US Coast Guard Intelligence, US Marine Corps Intelligence, and US Navy Intelligence.[3]

Originally, the 1947 USIC structure and the function of its intelligence cycle process model were designed to provide essential information to the president, policymakers, federal organizations, and military communities. Today, the growth of the USIC and its purpose has expanded beyond federal elements to include state, local, tribal, nongovernmental, and private sector entities necessary to enhance domestic intelligence capabilities.

Chapter III is intended to offer illustrations relevant to the challenges of executing domestic intelligence activities. The central points are identifying the national security focus of domestic intelligence policies, the exploitation of domestic intelligence authorities and cultural differences between the USIC and elements of the HSE that affect the employment of the intelligence cycle process model.

Chapter IV presents a case study of the April 15, 2013, Boston Marathon bombing in the context of the intelligence cycle process model adherence necessary to detect the threat and provide intelligence to policy and decision makers with information in order to prevent the bombing. This case study was selected in an effort demonstrate the conceptual intelligence cycle process model, in action, within the context of the National Network and the broader HSE. Additionally, the case study offers the challenges with employing the intelligence cycle process model within the National Network at the state

[3] "About the Intelligence Community," Intelligence.gov, accessed July 12, 2013, http://www.intelligence.gov/about-the-intelligence-community/.

and local level and supporting the 2003 National Criminal Information Sharing Plan (NCISP) efforts to prevent terrorism.

Chapter V is intended to offer a reading on the intelligence cycle process model and the HSE relevant to intelligence cycle model training and national integration of state and local law enforcement, the private sector, and implementation challenges given the complex HSE.

A. PROBLEM STATEMENT

The USIC was not designed to serve as a concept intended to detect significant national security threats originating or residing within our nation's borders[4] but was focused on foreign intelligence activities. This thesis evaluates if the intelligence cycle process model supports the performance of domestic intelligence activities within the National Network that serve as focal points within the state and local environment for the receipt, analysis, gathering, and sharing of threat-related information between the federal government and state, local, tribal, territorial and private sector partners.[5] Research provided little has been done to study the weaving together of local, state, and federal counterterrorism efforts[6] that support domestic intelligence activities and the reliance on the intelligence cycle process model.

The National Network has been in development since 2003 and was established to serve as intelligence and analytical hubs[7] at the state, local, tribal, and territorial level. The National Network is supported by training and technical assistance in employing the intelligence cycle process model from DHS, the Department of Justice (DOJ), and other

[4] Intelligence and National Security Alliance, *Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead*. White paper, Arlington: Homeland Security Intelligence Council, 2011.

[5] U.S. Department of Homeland Security, accessed June 7, 2013, http://www.dhs.gov/state-and-major-urban-area-fusion-centers.

[6] Frank J. Cilluffo, Joseph R. Clark, and Michael P. Downing, *Counterterrorism Intelligence: Law Enforcement Perspectives*, Counterterrorism Intelligence Survey Research, Homeland Security Policy Institute, George Washington University, September 2011.

[7] U.S. Department of Homeland Security, *Role of Fusion Centers in Countering Violent Extremism*, October 2012.

institutions. Providing federally funded training to the National Network on intelligence cycle process model variations, and their employment philosophies, serve as limitations to establishing fusion center baseline capabilities and their integration into national intelligence. Annual assessments are conducted on the National Network by DHS in efforts to evaluate baseline capabilities and their integration into national intelligence. The National Network completes an Online Self Assessment Tool that includes numerous multiple-choice and "yes/no" questions focused on the critical operational capabilities (COC) in support of the 2011 and 2012 DHS-led fusion center assessments.[8] While the COC questions focus on distinct aspects of the intelligence cycle process model, the 2011 and 2012 assessments do not evaluate the adherence to or wholly employing the intelligence cycle process model. A publication written by noted author and academic David Carter, who developed a local intelligence guide titled *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, affirms, "the need for a different approach to the intelligence cycle exists for the federal level compared to state, local, tribal and territorial elements because of different intelligence demands."[9]

The July 2010 DHS Bottom Up Review (BUR) that provides the results of a department-wide assessment reported, "there had been no systematic effort to ensure that these centers establish and maintain a baseline level of capability so that they are able to become fully integrated into national efforts to gather, analyze, and share information needed to protect our communities."[10] The 2010 BUR was addressed by the subsequent annual DHS-led National Network assessments. Notwithstanding, elements external to the National Network observed continued challenges with integrating local elements within the national intelligence architecture. A 2011 report by The Homeland Security

[8] U.S. Department of Homeland Security, *2012 National Network of Fusion Centers Final Report*, accessed October 8, 2013, http://www.dhs.gov/sites/default/files/publications/2012%20National%20Network%20of%20Fusion%20Centers%20Final%20Report.pdf.

[9] David Carter, U.S. Department of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed., January 2009, 14.

[10] U.S. Department of Homeland Security, *Bottom-Up Review Report*, July 2010.

Policy Institute's Counterterrorism Intelligence Survey Research indicated 62 percent of the intelligence chiefs representing major metropolitan police departments in the U.S. believed the "national [federal] intelligence enterprise was such that it left them unable to develop a complete understanding of their local threat environment"[11] — an intended product of the intelligence cycle process model.

B. OVERVIEW

Intelligence derived from analyzed information through the intelligence cycle process serves as a principle tool for supporting the nation's counterterrorism efforts and offers law enforcement and homeland security officials with insights and advantages over terrorists. However, there are multiple intelligence cycle concepts within the USIC and the HSE. The various intelligence cycle process models range from a four-step process to a seven-step process.

The first depicted model of an intelligence cycle process was documented in 1944 and titled the *Production of Military Intelligence, a Continuous Process*.[12] Moreover, in 1948, Robert Rigby Glass published a book titled *Intelligence for Commanders* becoming the first known academic reference to an intelligence cycle process.[13] Subsequently there have been numerous books about the USIC and the intelligence cycle process. Author Leo D. Carl refers to the intelligence cycle as a five-step process in his 1990 book titled *The International Dictionary of Intelligence*.[14] Author Robert M. Clark in his 2004 *Intelligence Analysis: A Target-Centric Approach* refers to the traditional intelligence cycle as a six-step process.[15] The Naval Postgraduate School's Center for Homeland

[11] Frank J. Cilluffo, Joseph R. Clark, and Michael P. Downing, *Counterterrorism Intelligence: Law Enforcement Perspectives*. Counterterrorism Intelligence Survey Research. Homeland Security Policy Institute. George Washington University, September 2011.

[12] Michael E. Bigelow, "A Short History of Army Intelligence," *Military Intelligence*, July-September 2012, 31.

[13] Sources and Methods: Part 4 – *The Traditional Intelligence Cycle and Its History*, accessed December 1, 2011, http://sourceandmethods.blogspot.com/2011/05/part-4-traditional-intelligence-cycle.html.

[14] Leo d. Carl, *The International Dictionary of Intelligence* (McLean, VA. International Defense Consulting Service, 1990), 183.

[15] Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (Washington, D.C.: CQ Press, 2004), 14.

Defense and Security Course NS4146 titled *Intelligence for Homeland Security*, by Dr. William Lahneman, refers to a seven-step process. The aforementioned noting of intelligence cycle process models reveals the diverse number of models and aids in identifying the potential challenges with providing consistent training and adherence to the National Network and the greater HSE. The DHS Homeland Security Advisory Council (HSAC), which provides advice and recommendations to the DHS Secretary on matters related to homeland security, noted effective intelligence and information fusion requires reliance on existing traditional USIC analytic processes. The HSAC defined "fusion" as a cyclic process that includes elements of a five-step intelligence cycle process.[16] This provides yet another version of the intelligence cycle process model. Table 1 provides a depiction of different intelligence cycle process models of USIC members, academia, and a state and local law enforcement element.

[16] U.S. Department of Homeland Security, *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion*. Homeland Security Advisory Council. April 28, 2005, 5–7.

Table 1. The Various Types of Organizational Intelligence Cycle Models and Attributes

	Requirements	Planning & Direction	Collection	Processing & Exploitation	Analysis & Production	Dissemination	Consumption	Evaluation & Feedback
CIA		X	X	X	X	X		
FBI	X	X	X	X	X	X		
U.S. Air Force		X	X	X	X (Production)	X (Integration)		
U.S. Army		X	X	X		X		
U.S. Marine Corps		X	X	X	X (Production)	X	X (Utilization)	
U.S. Navy		X	X	X (Processing)	X (Production)	X		
DoD Joint Pub		X	X	X	X	X (Integration)		X
HSAC		X (Requirements Development)	X		X (Analysis)	X (Tasking, Archiving)		X (Reevaluation)
	Requirements	Planning & Direction	Collection	Processing & Exploitation	Analysis & Production	Dissemination	Consumption	Evaluation & Feedback
IOWA DPS		X	X	X (Processing)	X	X		
NPS-CHDS	X		X	X	X	X	X	X
PENN STATE		X (Planning, Direction, Needs, Requirements)	X	X	X (Analysis)	X		

The single intelligence cycle attribute used by all within the various intelligence cycle models is the “collection” phase. There are various intelligence cycle process models used by the USIC and now being taught to the National Network by federally funded entities. As an example, the DHS Office of Intelligence and Analysis (I&A), the

National Counterterrorism Center, the Memorial Institute for the Prevention of Terrorism (MIPT), the Department of Justice State and Local Anti-terrorism Training Program, and the International Association of Law Enforcement Intelligence Analysts (IALEA) each deliver intelligence training opportunities on intelligence cycle process model. The complexities of HSE are intensified when observed through the lens of different training entities and varied intelligence cycle process models. Consistent and clear intelligence cycle process employment within the National Network presents challenges with integration into the national intelligence architecture without a uniform training.

C. RESEARCH OBJECTIVES AND METHODOLOGY

The research process applies the basic program evaluation principles to gather information on the intelligence cycle process model adherence within the National Network and greater HSE. The research objective seeks to evaluate whether the National Network and HSE members adhere to the intelligence cycle process model when performing public safety and homeland security related missions.

This thesis employs a qualitative research method that analyzes and interprets publicly available academic and policy information gathered from government and nongovernment institutions regarding the conceptual and practical writings relevant to the intelligence cycle process model. In addition to the academic and policy data gathered, the writer provides a case study analysis of the April 15, 2013, Boston Marathon bombing focused on practical adherence to the phases of a general intelligence cycle process model. The applied research method is intended to provide the framework for exploring the employment of the intelligence cycle process model within the current HSE. A case study approach was chosen in an effort to explore adherence to the intelligence cycle process within the National Network in context to its origin and intended purpose. It is in this setting that the writer explores the National Network's adherence to the intelligence cycle process model considering their integration as a critical state and local asset within the broader national intelligence architecture.

Employing the intelligence cycle process model within the National Network and the greater HSE presents privacy concerns. Literature reveals these privacy concerns are

focused on the collection of information on Americans who have not violated the rule of law. Privacy concerns among policymakers also exist regarding the proper collection of information in support of domestic intelligence activities engagement by public and private HSE entities. Lastly, scholars and practitioners present concerns questioning whether the intelligence cycle process model serves as effective analytic tradecraft in reducing strategic surprises associated with a threat while simultaneously enhancing operational law enforcement and intelligence elements.

THIS PAGE INTENTIONALLY LEFT BLANK

II. LITERATURE REVIEW

The significance of examining the intelligence cycle process model within the HSE is well intentioned given it was not originally designed or intended to detect significant national security threats originating or residing within our nation's borders.[17] The literature examined provided a spectrum of knowledge about the intelligence cycle process model within the pre- and post-9/11 domestic intelligence environment. The evaluation of intelligence literature provided by academic, organizational and nongovernment consulting institutions revealed minimal discourse concerning the intelligence cycle process employment to support domestic intelligence activities.

The research literature includes publications from within and outside the government by high-level policy organizations and academia. The concentration of government publications reviewed were congressional legislation associated with homeland security and intelligence, as well as homeland security intelligence reports and information sharing related products of the Government Accountability Office and Congressional Research Service. A review of public and nonprofit organizations serving as consultants to the intelligence community and homeland security provided intelligence journals and articles, as well as academic intelligence publications by the Department of Defense (DoD) and public institutions. Finally, as appropriate, USIC organizational and National Network documents were reviewed specifically relating to intelligence cycle process model training and policies.

The literature review provided no USIC or HSE doctrinal information on the adoption of the intelligence cycle as a formal process by USIC or HSE members. Additionally, there are no specific standards concerning intelligence processes for domestic intelligence collection, whether at the federal level or the state and local level. However, there are documents that provide guiding principles regarding domestic intelligence collection and the use of the intelligence cycle process. The principle document governing the USIC (federal-level) role relevant to domestic intelligence

[17] Intelligence and National Security Alliance, *Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead*. White paper, Arlington: Homeland Security Intelligence Council, 2011.

activities is Presidential Executive Order (EO) 12333. The DHS/DOJ endorsed guidelines for introducing the intelligence cycle process model into the National Network are the 2006 Fusion Center Guidelines[18] and the TCL[19] for state and local partners operating externally to the National Network. In March 2002, during an Intelligence Summit, the International Association of Chiefs of Police (IACP), an organization established in 1893 to serve as the professional voice of law enforcement, adopted the intelligence-led policing philosophy.[20] In 2011, the Major City Chief's Association (MCCA) initiated the Major City Chiefs' Criminal Intelligence Enterprise (MCCCIE) to better integrate state and local criminal intelligence and counterterrorism operations and address the deficiencies of standardizing integration and intelligence collection practices.[21] These guiding principles focus on the administration and management of the collection process, not necessarily a standardized employment of an intelligence cycle process model. An assessment of the limited information made available that focuses on domestic intelligence and the intelligence cycle employment reveals information gaps concerning its effectiveness and appropriateness within the post-9/11 HSE. This thesis attempts to explore whether the intelligence cycle is the best process model for domestic intelligence.

This literature review includes defining key intelligence enterprises, the term "intelligence" within the USIC and law enforcement, intelligence cycle process models, and training the intelligence cycle process to the HSE and National Network. The key intelligence enterprises discussed are the USIC, the Homeland Security Intelligence Enterprise (HSIE), and the HSE.

---

[18] U.S. Department of Homeland Security, *Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New Era; Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels; Law Enforcement Intelligence, Public Safety, and the Private Sector*, accessed July 16, 2013, http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

[19] U.S. Department of Homeland Security, *Target Capabilities List: A companion to the National Preparedness Guidelines*, September 2007, accessed July 16, 2013, http://www.fema.gov/pdf/government/training/tcl.pdf.

[20] International Association of Chiefs of Police, *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels*. Alexandria, VA, 2002.

[21] Major Cities Chiefs Criminal Intelligence Enterprise, accessed August 25, 2013, https://www.majorcitieschiefs.com/pdf/news/mcca_criminal_intelligence_enterprise_initiative_20120329.pdf.

A. DEFINING KEY INTELLIGENCE ENTERPRISES AND THE TERM "INTELLIGENCE"

The USIC is formally defined in EO 12333 titled *United States Intelligence Activities*. An EO serves as an official document to manage the operations of the federal government.[22] The EO 12333 is an extremely complex order that sets forth the foundation of the USIC and the administration's directions regarding "timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents."[23] Its support of national security consists of three key parts: Part 1) defines each intelligence community member and the particular roles and responsibilities; Part 2) focuses on the protection of civil liberties and privacy rights; and Part 3) provides relevant definitions. The 17-members consisting of the USIC are primarily concerned with foreign intelligence and counterintelligence, as prescribed in EO 12333, with the only agencies focusing on domestic intelligence are the

FBI and the newly created DHS.[24] EO 12333 was originally signed in 1981 under the Reagan Administration and since amended in 2008 under the Bush Administration because of the 9/11 terrorist attacks. EO 12333 provides the goals, direction, and responsibilities of USIC members performing intelligence activities within the U.S. There have been several amendments to EO 12333 since the original signing: in 2003 by EO 13284, in 2004 by EO 13355, and lastly in 2008 by EO 13470. The 2003 amendment by EO 13284 provided for the inclusion of the DHS Office of Intelligence and Analysis. The 2004 amendment by EO 13355 was designed to strengthen the management of the intelligence community. Lastly, the 2008 amendment by EO 13470 made administrative changes, to include language focused on state, local, and tribal governments as well as the private sector:

> State, local, and tribal governments are critical partners in securing and defending the United States from terrorism and other threats to the United

[22] National Archives, accessed July 27, 2013, www.archives.gov/federal-register/executive-orders/about.html.

[23] Ibid.

[24] Sephan J. Flanagen, *Managing the Intelligence Community*, International Security, vol. 10, no. 1, (Summer 1985), MIT Press, accessed June 13, 2012, http://www.jstor.org/stable/2538790.

> States and its interests. Our national intelligence effort should take into account the responsibilities and requirements of state, local and tribal governments and, as appropriate, private sector entities, when undertaking the collection and dissemination of information and intelligence to protect the United States.[25]

While every USIC member has the authority and responsibility for implementing EO 12333 within their respective organizations, the two chief organizations responsible for ensuring successful implementing and providing direction is the DNI and DOJ/FBI.

The DHS HSIE consists of three DHS headquarter elements that have an intelligence function: The Office of Intelligence and Analysis, the Homeland Infrastructure Threat and Risk Analysis Center, and the Intelligence Division of the Office of Operations Coordination and Planning. It also consists of the intelligence element of six operational components: U.S. Customs and Border Protection, U.S. Immigration and Customs Enforcement, U.S. Citizenship and Immigration Services, Transportation Security Administration, U.S. Coast Guard, and U.S. Secret Service.[26] While there is a described HSIE, the term *homeland security intelligence* has yet to be defined or codified in law.[27] Noted author Frances Townsend, the former Homeland Security Advisor under President Bush and former Chairwoman of the nonprofit, public-private organization Intelligence and National Security Alliance, defined *homeland security intelligence* as a discipline that depends on the successful fusion of foreign and domestic intelligence to produce the kind of actionable intelligence necessary to protect the homeland.[28]

The DHS Undersecretary for Intelligence and Analysis serves as the Department's Chief Intelligence Officer (CINT) responsible for leading the HSIE. The DHS' Management Directive Number 8110 titled *Intelligence Integration and Management*

---

[25] Executive Order 13470, *Further Amendments to Executive Order 12333, United States Intelligence Activities*, Part 1 1.1(f), accessed July 27, 2013, www.fas.org/irp/offdocs/eo/eo-13470.htm.

[26] Congressional Research Service, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress*, R40602, May 27, 2009, 3.

[27] Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, RL33616, January 14, 2009, 9.

[28] Frances Townsend, *Intelligence to Protect the Homeland - Taking Stock Ten Years Later*. Intelligence and National Security Alliance 1 2011, 3.

established the CINT position to effectively integrate and manage DHS intelligence programs, as well as serve as the principle for leading, governing, integrating, and managing intelligence functions throughout DHS.[29] The DHS CINT is tasked with being the primary connection between DHS and the USIC, as well as the primary source of information for state, local, tribal, and private sector partners. To date, there has only been two Senate confirmed DHS CINTs. The first CINT was the Honorable Charles Allen, a 40-year senior Central Intelligence Agency official who served as the first DHS CINT from 2005–2009 and was responsible for developing the department's intelligence architecture.[30] The second CINT was the Honorable Caryn Wagner, a 30-year DoD official who served as the DHS CINT from 2010 to 2012[31] and during her tenure provided a focus of "creating a true homeland security information-sharing enterprise through a greater focus on state, local, and major urban area fusion centers," as well as "unify and sustain the DHS intelligence enterprise."[32]

The HSE was defined by a DHS report on the National Network as federal, state, local, tribal, nongovernmental, and private sector entities.[33] Integration of the HSE into the national intelligence architecture was intended to occur through the National Network. Other than the 2011 DHS report, the examination of literature does not provide any other formal HSE definition, although the term is frequently used in government and academic articles. Similar to the term *homeland security intelligence*, the failure to provide a unified and accepted definition among stakeholders encumbers the ability to assess the effectiveness of the intelligence cycle process model.

---

[29] U.S. Department of Homeland Security, Management Directive 8110, *Intelligence Integration and Management*, accessed August 4, 2013, http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_8110_intelligence_integration_and_management.pdf.

[30] Chertoff Group, accessed August 4, 2013, http://chertoffgroup.com/bios/charles-allen.php.

[31] U.S. Department of Homeland Security, accessed August 4, 2013, http://www.dhs.gov/caryn-wagner.

[32] Anthony L. Kimery, *Homeland Security Today*, "DHS I&A Chief Outlines New Vision," May 13, 2010, accessed August 7, 2013, http://www.hstoday.us.

[33] U.S. Department of Homeland Security, *2011 National Network of Fusion Centers Final Report*, May 2012, 2.

Intelligence is a term that has multiple meanings dependent upon the literary contribution whether it has a USIC or law enforcement origin. An examination of literature commonly discussed what "intelligence" means or at least how an author intended to use the term. Prior to the terrorist attacks of September 11, 2011, academic and federal government literature largely referred to intelligence within the context of issues related to national security associated with defense, foreign policy, and internal (domestic) security.[34] However, the term "intelligence" within the context of law enforcement often refers to significant information that is relevant to an impending event and that will be a contribution to the positive outcome of a specific case.[35] Lowenthal subscribes that intelligence can be defined from three different perspectives: 1) "Intelligence as a product – intelligence that can be thought of as a product of the [process]," 2) "Intelligence as a process – intelligence [that] can be thought of as the means by which certain types of information are required and requested, collected, analyzed, and disseminated…," and 3) "Intelligence as an organization – intelligence…thought of as the units that carry out its various functions."[36]

In the post-9/11 environment, intelligence began to be more widely accepted and used among state, local, tribal, territorial, and private sector elements as key partners within the HSE. For the purpose of this thesis, "intelligence" is defined as the collective "functions [and] activities…which are involved in the [intelligence] process [model] of planning, gathering, and analyzing information of potential value to decision makers."[37]

[34] U.S. Department of Homeland Security, *2011 National Network of Fusion Centers Final Report*, May 2012, 4.

[35] Roger G. Dunham, Geoffrey P., Alpert, Jennifer E. Davis, and Robert W. Taylor, *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings* (6th ed., Waveland Press, 2010), 225.

[36] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C., CQ Press, 2012). 9.

[37] Leo D. Carl, *The International Dictionary of Intelligence* (McLean, VA. International Defense Consulting Service, 1990), 178.

B. INTELLIGENCE CYCLE PROCESS MODELS

A review of journals and scholarly publications provided descriptions of intelligence cycle process models. However, it was difficult uncovering its origination and the policies associated with its formal adoption within the USIC. According to the International Journal of Information Management, an international peer-reviewed journal, the use of the intelligence cycle was first derived from the U.S. Army.[38] In 1920, the Army's Chief of Staff attempted to establish the first Army-wide intelligence doctrine via the distribution of *Intelligence Regulations.*[39] Author Michael Bigelow, Command Historian with the U.S. Army Intelligence and Security Command, contends the first depicted model of the intelligence process was documented in 1944, under the title the *Production of Military Intelligence, a Continuous Process.*[40]

In 1952, intelligence collection, the single most common intelligence cycle attribute was defined as the procuring, assembling and organizing of information and served as the first step in the processing of intelligence information. It is now considered the third step or phase in the intelligence cycle process model and "…officially defined as 'the exploitation of sources of information by collection agencies and delivery of information to the proper intelligence-processing unit for use in the production of intelligence.'"[41] The 1952 definition focused on intelligence collection targeted against communist nation-states and not the domestic intelligence environment of today.

The intelligence cycle process model in simple discourse involves structured steps necessary for gathering required data in order to create knowledge. The created knowledge (intelligence) in the early years served executive and congressional policymakers primarily focused on Cold War adversaries in an attempt to uncover foreign intelligence activities and assist with supporting global national security interests.

---

[38] "Targeting Intelligence Gathering in a Dynamic Competitive Environment," *International Journal of Information Management*, 20, iss. 3, 2000: 184.

[39] Michael E. Bigelow, "A Short History of Army Intelligence." *Military Intelligence*, July-September 2012, 21.

[40] Ibid., 31.

[41] Leo D. Carl, *The International Dictionary of Intelligence* (McLean, VA. International Defense Consulting Service, 1990), 59.

Prior to the September 11 terrorist attacks, the FBI served as the principle federal agency responsible for domestic intelligence. In response to criticism by Congress following the attacks, the FBI initiated reforms to increase their collection and analysis of domestic intelligence. Nonetheless, critics contend FBI intelligence collection play a secondary role to their law enforcement mission.[42] Because of the September 11, 2001, Al-Qaida terrorist attacks that emphasized intelligence failures, the stated integration of the intelligence cycle process model became a common theme among public safety officials at the state, local, tribal, territorial and private sector levels. The new intelligence mission has by both necessity and practice expanded beyond the federal-level originally identified in the 1947 National Security Act and is now based on the principle of shared responsibility and partnership with state and local governments, the private sector, and the American people in a concerted national effort to prevent future terrorist attacks within the U.S.[43]

There are multiple intelligence cycle process model versions within the USIC, the HSIE and the HSE, which range from four-step process to a seven-step process. Many authors indicated that the intelligence cycle process model is more or less a common practice of how intelligence professionals perform the functions of intelligence. For the purpose of this thesis, the intelligence cycle is defined according to the official USIC definition as "the steps by which information is acquired and converted into intelligence and made available to consumers."[44] Similarly to the many academic descriptions of the intelligence cycle process models, USIC organizational models depend on the organization and its mission-space. The diverse number of intelligence cycle models stresses the need for an HSE-wide accepted intelligence cycle process doctrine.

[42] Eric Rosenbach, *Confrontation or Collaboration? Congress and the Intelligence Community*. Belfere Center for Science and International Affairs. The Intelligence and Policy Project. Background Memorandum for the 111th Congress. July 2009, 44–49.

[43] Office of Homeland Security, *National Strategy for Homeland Security*, July 2002, 2.

[44] Leo D. Carl, *The International Dictionary of Intelligence* (McLean, VA. International Defense Consulting Service, 1990), 183.

C. CORE ISSUE

The intelligence cycle process model continually strives to better understand the threat environment or a threat issue. Understanding is accomplished and supported by relying on past and present information necessary to deliver a probabilistic view of the future. The basic intelligence cycle process model involves sequenced steps necessary for gathering the information in order to create the desired understanding. While literature plainly reveals the cyclical structure of intelligence cycle process model, literature also suggests the intelligence cycle process model does not sufficiently describe how the intelligence process works at the operational stages of domestic intelligence activities within the National Network. Within the USIC, however, the intelligence cycle process model appears to be an academic process conducted primarily by analysts and not operational intelligence collectors. As an example, in a doctoral dissertation written by Ms. Bridget Nolen on USIC information sharing and collaboration she noted "An analyst will sometimes write a paper on a self-generated topic, but much of the time the analyst is responding to a 'tasking,' which means that a policymaker has a specific question that he or she wants a subject matter expert to answer. The analyst drafts a response as quickly as possible by putting together the available information from a variety of classified and open sources, and must then begin the arduous coordination process to ensure that other analysts in the Intelligence Community concur with the assessment. After the paper is coordinated, it must then go through many more layers of editing through management, and then a final edit for style, structure, and formatting before it can be published—that is, delivered to policymakers."[45]

A critical juncture in the process identified by Nolen is coordination. This corresponds with the independent phase "production" or the joint phase "analysis and production" dependent on which intelligence cycle process model is being used. During this phase, it is noted "...each paper an analyst writes is considered a 'community' product...,so it is important that other experts vet an analyst's work before the policy

[45] Bridget Rose Nolen, *Information Sharing and Collaboration in the United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center* (PhD diss., University of Pennsylvania, 2013), 90.

maker reads it. At this theoretical level, coordination makes sense. In practice, however, the coordination process frequently transforms into a battle over turf, a venue for blatant backstabbing, and a practice rooted in nitpicking and meaningless editing...."[46] Another cogent example identifying the challenges of finished intelligence—the theoretical end result of a perfectly functioning intelligence cycle process model—is provided from an interview excerpt "NCTC has to coordinate with everyone. It is difficult when DHS thinks they can call the editors personally and hold your piece because they think it interferes with their business project. Like with terrorist documents—we might write about how terrorists exploit student visas, and well, State issues the student visas and they do not like the fact that we are criticizing the loopholes in their system. So they'll hold the piece or try to kill it."[47] These issues point out the practical challenges with employing the intelligence cycle process model within the USIC established in 1947, accordingly, similar challenges are present within the complex National Network and the HSE.

Author Leo D. Carl reference to the intelligence cycle as a five-step process in his 1990 *The International Dictionary of Intelligence* includes: 1) Planning and Direction, 2) Collection, 3) Processing, 4) Production, and 5) Dissemination.[48] Author Robert M. Clark in his 2004 *Intelligence Analysis: A Target-Centric Approach* describes the traditional intelligence cycle as a six-step process: 1) Requirements, needs, 2) Planning, direction, 3) Collection, 4) Processing, 5) Analysis, and 6) Dissemination.[49] Lastly, the Naval Postgraduate School Center for Homeland Defense and Security's Course NS4146 titled *Intelligence for Homeland Security*, by Dr. William Lahneman offers to a seven-step process: 1) Requirements, 2) Collection, 3) Process and Exploitation, 4) Analysis and Production, 5) Dissemination, 6) Consumption and 7) Feedback. The aforementioned

[46] Bridget Rose Nolen, *Information Sharing and Collaboration in the United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center* (PhD diss., University of Pennsylvania, 2013), 90–91.

[47] Ibid., 98–99.

[48] Leo D. Carl, *The International Dictionary of Intelligence* (McLean, VA. International Defense Consulting Service, 1990), 183.

[49] Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (Washington, D.C.: CQ Press, 2004), 14.

noting of intelligence cycle process models reveals the diverse number of models and aids in identifying the potential challenges with providing consistent training and adherence to the National Network and broader HSE.

The DHS HSAC cyclic process included a five-step intelligence cycle process: 1) Planning and Requirements Development, 2) Collection, 3) Analysis, 4) Dissemination, Tasking, and Archiving, and 5) Reevaluation.[50] This provides yet another version of the intelligence cycle process model.

The four figures below serve as diagrams illustrating the diversity of intelligence cycle process models, similar to the table provided in Chapter I. While there are minor but important differences, not one of the four is exactly alike, although each element is a member of the national intelligence architecture.

[50] U.S. Department of Homeland Security, *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion*. Homeland Security Advisory Council. April 28, 2005, 5–7.

Figure 1. FBI Intelligence Cycle[51]

Figure 2. The Iowa State Police Intelligence Cycle[52]

[51] Federal Bureau of Investigation, accessed September 4, 2013, http://www.fbi.gov/about-us/intelligence/intelligence-cycle.

[52] Iowa Department of Public Safety, accessed September 4, 2013, http://www.dps.state.ia.us/intell/intellcycle.shtml.

Figure 3. CIA Intelligence Cycle[53]

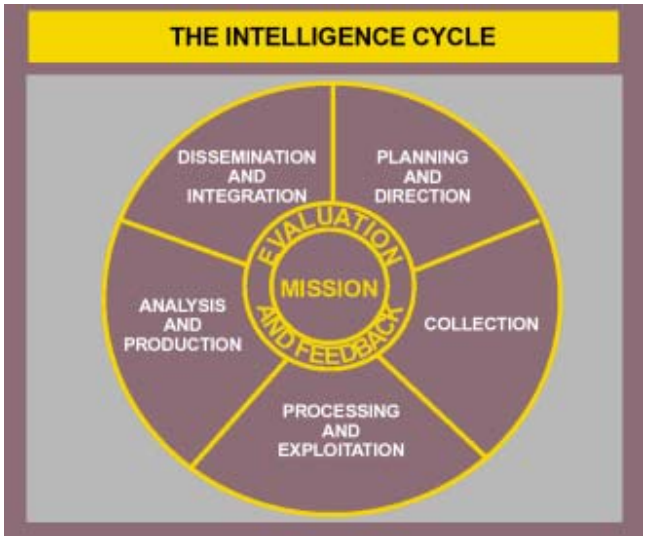


Figure 4. DoD Joint Publication Intelligence Cycle[54]

The integration of state, local, tribal, territorial and private sector elements as nontraditional intelligence partners of the HSE has shepherded the need to fundamentally change the requirement to provide intelligence not just to the federal level organizations, the president and Congress, but also to state and local policymakers and operational

[53] U.S. Central Intelligence Agency, accessed September 4, 2013, http://vmc.cia-dia.50megs.com/fboi/facttell/intcycle.htm.

[54] U.S. Department of Defense, accessed September 4, 2013, http://www.dodccrp.org/events/9th_ICCRTS/CD/papers/044.pdf.

entities. It involves evaluating the profound differences between providing classified information to policymakers, such as during the Cold War, and providing homeland security intelligence and threat information to the private sector, public organizations and U.S. Citizens in a post-9/11 domestic intelligence environment.[55]

The 9/11 Commission Act, Section 511 provides DHS shall establish a DHS State, Local, and Regional Fusion Center Initiative necessary for establishing partnerships with state, local, and regional fusion centers; specifically Section (b) (11) mandates providing training to state, local, and regional fusion centers.[56] The DHS I&A concurred with the responsibility per Section 511 to develop training curricula on the intelligence cycle process for state and local officials.[57] In satisfying this mandate, DHS deployed intelligence officers charged with managing the intelligence cycle in their areas of responsibility.[58] While fusion center personnel receive DHS sponsored intelligence cycle training from a variety of federally funded institutions, this is not the case for a majority of public safety officials operating outside the National Network such as the MCCCIE initiative.

The Major Cities Chiefs Association, an organization comprised of police chiefs and sheriffs from 63 of the largest law enforcement agencies in the U.S., initiated the MCCCIE in 2011. Serving as a significant representative of the state and local criminal intelligence community, the MCCCIE's aim is to better integrate state and local criminal intelligence and counterterrorism operations in support of the National Network by addressing the deficiencies of standardizing integration and intelligence collection

[55] Elaine C. Kamarck, *Transforming the Intelligence Community: Improving the Collection and Management of Information*. John F. Kennedy School of Government, Harvard University, IBM Center for The Business of Government, October 2005, 11.

[56] 110th Congress Public Law, Public Law 110–53, *Implementing Recommendations of the 9/11 Commission Act of 2007*.

[57] U.S. Department of Homeland Security, *DHS' Role in State and Local Fusion Centers is Evolving*. Office of Inspector General Report – OIG-09–12. October 2008. 16.

[58] U.S. Department of Homeland Security, *Responsibilities of Intelligence Officers*, accessed March 7, 2013, http://www.dhs.gov/deployed-intelligence-officers-and-protective-security-advisors.

practices within the state and local environment.[59] Figure 5 depicts a four-step Prediction-Led Policing Business Process Model that may be viewed in the context of the intelligence cycle process model. The Prediction-Led Policing Business Process Model is based on a concept established by the Center for Problem-Oriented Policing with the first two phases focusing on collecting and analyzing criminal information necessary for establishing predictions and the last two phases focus on response to the predictions.[60] The parallels between the intelligence cycle process model and the prediction-led policing process model is the critical need for information collection and analysis.

This critical segment of the HSE receives considerably less training on the intelligence cycle process model, although it oversees far more personnel than the National Network. There are questions law enforcement intelligence analysts use to ascertain a threat or the threat situation using the intelligence cycle process model that are not readily obvious to law enforcement investigators.[61] The contrasting perspectives associated with the intelligence cycle process model between law enforcement intelligence analysts and law enforcement investigators parallel the environmental setting within the USIC between intelligence analysts and operational intelligence collectors.

[59] Major Cities Chiefs Criminal Intelligence Enterprise, accessed August 25, 2013, https://www.majorcitieschiefs.com/pdf/news/mcca_criminal_intelligence_enterprise_initiative_20120329.pdf.

[60] RAND, *Predictive Policing – The Role of Crime Forecasting in Law Enforcement Operations*, Prediction-Led Policing Business Process Model, accessed October 3, 2013, http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.

[61] Timothy Connors, and John Rollins, Center for Policing Terrorism at the Manhattan Institute. *State Fusion Center Processes and Procedures: Best Practices and Recommendations* (Policing Terrorism Report, No. 2, September 2007), 3.

Figure 5. The Prediction-Led Policing Business Process Model, RAND RR233–1.1[62]

The terrorist events of 9/11 vastly transformed law enforcement communities across the U.S. and the approach to preventing and combating terrorism that focused on proactive posturing versus reactive engagement.[63] New transnational enemies possibly operating within the homeland in the form of international terrorists and transnational issues, such as narcotics and money laundering have risen in importance becoming more urgent than the previous Cold War era geopolitical concerns. As the intelligence and law enforcement communities have both become increasingly involved in the international aspects of terrorism, drug trafficking, and international organized crime, the National Network is positioned to access the USIC's considerable wealth of information on these subjects. However, in considering the fulfillment of these capabilities by the HSE, this issue has been the most difficult to resolve.[64]

[62] RAND, accessed October 3, 2013, http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.

[63] Roger G. Dunham, Geoffrey P. Alpert, Jennifer E. Davis, and Robert W. Taylor, *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings*, 6th ed, Waveland Press, 2010, 224.

[64] *The Intelligence Community in the 21st Century*: Staff Study - Permanent Select Committee on Intelligence House of Representatives 104th Congress, accessed March 5, 2013, http://www.gpo.gov/fdsys/pkg/GPO-IC21/html/GPO-IC21–13.html.

The HSIE, through DHS I&A, authorizes intelligence collection activities that serve to support the National Network and the HSE in efforts to identify emerging homeland security threats. The DHS I&A intelligence collection efforts of DHS Intelligence Officers supporting the National Network was detailed in a July 29, 2008 DHS Memorandum. On April 3, 2008, DHS CINT Honorable Charles Allen under DHS Intelligence Oversight procedures defined homeland security threats to include "all threats or hazards, regardless of origin, that relate to: critical infrastructure or key resources; a significant public safety, public health or environmental impact; political, societal and economic infrastructure; border security; the proliferation or use of weapons of mass destruction; or other potential catastrophic events including man-made and natural disasters."[65]

An examination of literature provides general knowledge and reveals minimal discourse concerning the intelligence cycle process model employment within the context of domestic intelligence collection activities, specifically within the National Network. DHS and other entities continue to provide training and instruction on various intelligence cycle process models to the 78 state and major urban area fusion centers that embody the National Network.

Lowenthal proclaims one of the stated goals of the U.S. intelligence process (intelligence cycle) is to have "analysis-driven collection." A short hand way of recognizing that collection priorities should reflect the intelligence needs required to produce analysis.[66]

There are disagreements in literature as writer Arthur S. Hulnick, a professor at Boston University who served seven years as an U.S. Air Force Intelligence Officer and 28 years with the Central Intelligence Agency (CIA), claims the intelligence cycle is really not a very good description of the ways in which the intelligence process works and "the notion that policymakers or intelligence consumers provide guidance to

[65] U.S. Department of Homeland Security, *Roles and Function*, Office of Intelligence and Analysis General Counsel Memorandum, July 29, 2008.

[66] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*. (Washington, D.C.: CQ Press, 2003), 60–61.

intelligence managers to begin the intelligence process is incorrect."[67] Robert Clark, a 42-year Intelligence Analyst, faculty member of the Intelligence and Security Academy and a professor of intelligence studies at the University of Maryland University College, likewise challenges the intelligence cycle process model's effectiveness and contends "intelligence is organized around the flawed concept of an intelligence cycle"[68] and "over the years the intelligence cycle has become somewhat of a theoretical concept…[and] when pressed many intelligence officers admit that the intelligence process 'really doesn't work like that.'"[69]

The evaluation of the intelligence cycle process model, based on the writers' presentation, suggest the theoretical intelligence cycle is a simple process beginning with customer needs and ending with providing a product that satisfies those needs. Inconsistencies with employing the intelligence cycle process model surface because of existing conflicts among intelligence and law enforcement analytic and operational components. With the inclusion of DHS into the USIC, along with state and local entities as key HSE elements, there exists an essential challenge—what intelligence process training should be provided to the National Network and HSE? In addition, is current intelligence cycle process training provided to the National Network and HSE appropriate and effective? Given literature overlooks a standardized intelligence cycle process model that does not exist. Furthermore, literature reflects significant historical abuses along with current events that illustrate challenges with domestic intelligence activities specifically collection.

Unlike at the federal-level within the USIC, the National Network made up of mainly law enforcement centric elements view the intelligence process from a different perspective. Prior to using the intelligence cycle as a business practice, state and local law enforcement integrated intelligence-led policing as the standard business practice for "analysis-driven collection." Law enforcement's acceptance of intelligence-led policing

[67] Arthur S. Hulnick, *What's Wrong with the Intelligence Cycle*. Intelligence and National Security 21. No. 6. December 2006. 959.

[68] Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach* (Washington, D.C.: CQ Press), 2004. 12.

[69] Ibid., 15.

advanced the goal of developing a universal process that would integrate both law enforcement and national security intelligence agendas. The result was the intelligence cycle process model[70] although some have affirmed there are fundamental differences between national security and local law enforcement intelligence. The fundamental differences that exist between the law enforcement perspective and traditional intelligence community perspective, regarding intelligence collection, results in a less than effective intelligence platform within the homeland.[71]

In a September 2011 publication by the Intelligence and National Security Alliance titled *Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead*, former FBI Executive Assistant Director for Intelligence Maureen Baginski, a former NSA senior intelligence official who headed the FBI Directorate of Intelligence created in 2005, claims that many federal intelligence and law enforcement professionals do not recognize the homeland security implications and intricacies of criminal information.[72] Jennifer Sims, a Senior Fellow for National Security at the Chicago Council on Global Affairs and a Visiting Professor in the Security Studies Program at Georgetown University along with Burton Gerber, a CIA Distinguished Intelligence Medal recipient and former 39-year CIA employee acknowledges, "[a] critical difference between law enforcement and traditional intelligence collection is that law enforcement gathers hard truth in the form of evidence; prosecutors and courts require this."

The intelligence collection phase under the intelligence cycle process model covers the gray area and makes estimations, which is what the consumer demands. The "gray area" centers on how to effectively perform domestic intelligence activities while employing the intelligence cycle process model among HSE members concurrently protecting privacy, civil liberties, and civil rights. Chapter III offers the historical and

[70] Roger G. Dunham, Geoffrey P. Alpert, Jennifer E. Davis, and Robert W. Taylor, *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings*, 6th ed, Waveland Press, 2010, 232.

[71] Jennifer E. Sims, and Burton Gerber, *Transforming U.S. Intelligence* (Washington, D.C., Georgetown University Press, 2005), 208–209.

[72] Intelligence and National Security Alliance, *Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead*. White paper, Arlington: Homeland Security Intelligence Council, 2011.

post-9/11 challenges of domestic intelligence activities, specifically the collection phase of the intelligence cycle process model.

The HSE receives intelligence training from many organizations, such as DHS I&A, DOJ Bureau of Justice Assistance, MIPT, the Institute for Intergovernmental Research, as well as many academic institutions. When combining the many versions of the intelligence cycle process model and the various organizations providing intelligence training on one of its many versions to the HSE, the question surfaces as to its effective adherence.

D. HOMELAND SECURITY ENTERPRISE AND NATIONAL NETWORK INTELLIGENCE CYCLE TRAINING

The previous section of the literature review focused on defining key intelligence enterprises, the term "intelligence" within the USIC and law enforcement, and the intelligence cycle process and its many variations. This section of the literature review will focus on training the intelligence cycle within the HSE and National Network.

The analysis of limited information made available regarding HSE and National Network intelligence cycle employment reveals gaps concerning its effectiveness and appropriateness within the post-9/11 environment. The HSE and National Network receive training from federal, government sponsored and academic institutions on the intelligence cycle process model with an emphasis on enhancing domestic intelligence capabilities to prevent future terrorist attacks.

Providing structured training on the intelligence cycle process model should make the most of the HSE and National Network efforts to detect, neutralize, and exploit terrorist strategies and tactics. Well-trained analysts within the National Network are critical to efficient intelligence analysis. However, even with pristine data, a lack of strong analytics may result in less-than-desirable intelligence products and operational outcomes.

Additionally, employing the intelligence cycle process model within the National Network and the greater HSE have presented several concerns. Among privacy advocates, there are privacy concerns regarding collection of information on Americans

who have not violated the rule of law. Among policy makers, there are concerns regarding the proper collection of information in support of domestic intelligence activities among public and private HSE entities. Lastly, among scholars and practitioners, there are concerns the intelligence cycle process model may not serve as an effective analytic tradecraft competency in reducing strategic surprises associated with a threat, while simultaneously enhancing operational law enforcement and intelligence elements. The literature review did not provide standardized doctrinal information on the adoption of the intelligence cycle as a formal process by USIC, HSIE or HSE members. However, guiding principles such as EO 12333 (as amended), the 2006 Fusion Center Guidelines, and the TCL provided a common framework to introduce the intelligence cycle process model.

The DHS State and Local Program Office, in conjunction with the DHS Federal Emergency Management Agency (FEMA) and DOJ provides intelligence cycle training opportunities to the National Network and HSE via the DHS/DOJ Fusion Process Technical Assistance Program and Services, the FEMA sponsored MIPT. There are a number of academic institutions that also provide intelligence cycle training, most notably the Naval Postgraduate School's Center for Homeland Defense and Security and the Michigan State University. The author and academic David Carter with Michigan State University developed a local intelligence guide titled *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies* highlighting the need for a different approach to the intelligence cycle at federal level when compared to state, local, tribal and territorial level based on different intelligence demands.[73]

Literature clearly agrees that the intelligence cycle is used as the traditional intelligence process at the federal level within the USIC. Because of the federal government's support to the state and local environment via the National Network, DHS provides instruction on the intelligence cycle process to state and local officials within

[73] David L. Carter, U.S. Department of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed., January 2009, 14.

the National Network and limited HSE elements. As highlighted by author David Carter, there is a cultural contradiction that exists in traditional law enforcement notwithstanding the recent focus on the intelligence-led policing (ILP) model that focuses on identifying criminal behavior, reporting criminal activity and preventing future crimes based on trends and patterns.

Mr. Carter acknowledges the private sector is often a legitimate consumer of law enforcement intelligence meeting the "right to know" and "need to know" in support of information sharing standards. Similar to the majority 18,000 U.S. law enforcement agencies, the private sector as a significant element of the HSE that owns an estimated 85 percent of the nation's critical infrastructure is generally not slated to receive federally funded intelligence cycle process training. Moreover, the private sector has a large personnel force who, if given the proper information, can significantly increase the "eyes and ears" on the street to observe individuals and behaviors that pose threats. However, there are information sharing issues that need to be resolved. For example, certain types of personal information may be inappropriate for law enforcement to release to the private sector. Conversely, proprietary information related to corporate products may also be restricted. Despite these limitations, there is a legitimate intelligence role for the private sector.[74]

Mr. David Cid, MIPT Executive Director, similarly recognizes the law enforcement cultural contradiction to intelligence and asserts avoiding strategic surprise is a principle function of intelligence that allows law enforcement to be anticipatory and proactive in efforts to prevent potential terrorist attacks. However, traditional measures of success in law enforcement, such as arrests, indictments, and seizures of property are secondary to prevention.[75]

Common themes within the literature advances intelligence cycle models as a key element of the USIC. The literature also reveals disagreements about its effectiveness at

[74] David L. Carter, White paper, *The Intelligence Fusion Process for State, Local and Tribal Law Enforcement*, Michigan State University, May 2006, accessed March 3, 2013, http://www.ncirc.gov/documents/public/intelligence_fusion_process.pdf, 7.

[75] David Cid, *Understanding Counterterrorism: A Guide for Law Enforcement Policy Makers and Media*, 2012, 264, 268.

the practitioner level, as well as its many variations based on organizational mission space. Finally, the literature overlooks or perhaps shortchanges the question of whether the intelligence cycle process model is effective or appropriate within the HSE and the National Network, while revealing the challenges of domestic intelligence collection, which will be focus of the following chapter.

THIS PAGE INTENTIONALLY LEFT BLANK

III. DOMESTIC INTELLIGENCE AND EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL

> We also have no official with sole and comprehensive responsibility for domestic intelligence. It is no surprise that gaps in domestic intelligence are being filled by ad hoc initiatives.
>
> – Judge Richard Posner, U.S. Court of Appeals

The focus of this thesis provides an academic inquiry into the intelligence cycle process adherence within the National Network and the greater HSE. The information contained in this publication may reflect the intelligence cycle process as an idealistic model while highlighting the challenges of adopting a standardized intelligence cycle process acceptable among homeland security professionals. Chapter III is intended to offer illustrations relevant to the challenges of executing domestic intelligence activities. The central points are identifying the national security focus of domestic intelligence policies, the exploitation of domestic intelligence authorities, and cultural differences between the USIC and elements of the HSE that effect the employment of the intelligence cycle process model.

A. DOMESTIC INTELLIGENCE ACTIVITIES – NATIONAL SECURITY FOCUS

The USIC, established by the 1947 National Security Act because of World War II, differs in many ways from its present structure. The 1947 National Security Act established a national effort to protect the U.S. from foreign actors in response to the Japanese attack on Pearl Harbor and the subsequent Cold War with the Soviet Union. As a result of the terrorist acts committed on September 11, 2001, the USIC changed to introduce two new members of the USIC; the DNI; and DHS I&A. The 9/11 attacks on the U.S. served as a motivator for yet another national effort to protect the U.S. from both foreign terrorists operating abroad and within U.S. borders. A national policy or doctrine

regarding a standard intelligence process is critical, since professional intelligence officers often think of their primary mission of information collection and analysis in terms of an "intelligence cycle."[76]

Historically, America has responded to the need for domestic intelligence in four ways. First, avoid it. There was less than a page-sized narrative devoted to intelligence in the 2002 National Strategy for Homeland Security. Second, construct ad-hoc arrangements without clear oversight and authority, which led to political abuse in the 1975 Church Commission Report. Third, allow the FBI and CIA to perform limited and highly scrutinized overt domestic intelligence collection activities per EO 12333. Fourth, assume the law enforcement community can substitute for intelligence.[77]

The National Network assumed a key role to address counterterrorism threat information sharing and intelligence analysis at the state and local level. The annual Fusion Center Assessments, a critical component of a broader Fusion Center Performance Program, is designed to measure pre-determined baseline capabilities and holistic performance of the National Network[78] fulfilling the shortcomings identified in the 2010 DHS BUR.

The DHS, in coordination with interagency partners, Fusion Center Directors, and other fusion center stakeholders, manages the annual assessment process that focuses primarily on measuring four COCs,[79] which contain elements of the intelligence cycle process model – collection, analysis, production, and dissemination. The 78 fusion centers that constitute the National Network completed the 2011 and 2012 Fusion Center Assessments allowing DHS to collect data necessary for measuring their progress in achieving baseline capabilities that include the COCs as key performance objectives within the National Network.

---

[76] Loch K. Johnson, and James J. Wirtz, *Intelligence and National Security: The Secret World of Spies-An Anthology* (Oxford, NY: Oxford University Press, 2008). 49.

[77] Henry A. Crumpton, *Intelligence and Homeland Defense. In Transforming U.S. Intelligence*, edited by Jennifer E Sims and Burton Gerber, 198–219. Washington, D.C: Georgetown University Press, 2005, 206–207.

[78] U.S. Department of Homeland Security, *2011 National Network of Fusion Centers Final Report*, accessed June 7, 2013, http://www.dhs.gov/2011-fusion-center-assessment.

[79] Ibid.

The first COC-1 is *receive*; the ability to receive classified and unclassified information from federal partners.[80] The second COC-2 is *analyze*; the ability to assess local implications of threat information using a formal risk assessment process.[81] The third COC-3 is *disseminate*; the ability to further disseminate threat information to other state, local, tribal, and territorial entities within their jurisdictions.[82] And lastly, the fourth COC-4 is *gather*; the ability to gather locally generated information, aggregate it, analyze it, and share it with federal partners as appropriate.[83] The COCs 1 and 4 are viewed in context of the intelligence cycle process model pertaining to "collection" and places emphasis on the vertical flow of information among federal agencies and state, local, tribal, territorial, and private sector partners. As previously mentioned and reflected in Figure 1, the single common attribute within the various intelligence cycle models is the "collection" phase. Chapter III of this thesis offers noted historical and current challenges to executing domestic intelligence activities under the collection phase of the intelligence cycle process model, a continuing concern for privacy advocates. The COCs 2 and 3 are logical sequenced actions of the intelligence cycle process model that are utterly contingent on the National Network's ability to fully execute the complete intelligence cycle process.

External to the National Network, DHS in close partnership with state and local partners developed the Target Capabilities List for general public safety officials, excluding law enforcement. The TCL describes the preparedness capabilities related to the four homeland security mission areas: Prevent, Protect, Respond, and Recover. The TCL identified critical elements of the intelligence cycle process model involved with gathering [collection], analysis, production and dissemination that states and localities should possess in order to prevent, protect, respond and recover from a terrorist incident. It defines and provides the basis for assessing preparedness of which include information gathering (collection), intelligence analysis and production as elements of the Prevent

[80] U.S. Department of Homeland Security, *2011 National Network of Fusion Centers Final Report*, accessed June 7, 2013, http://www.dhs.gov/2011-fusion-center-assessment.

[81] Ibid., 14.

[82] Ibid., 17.

[83] Ibid., 19.

Mission Capabilities. In 2009, the Heritage Foundation,[84] which is a conservative think tank whose mission is to formulate and promote conservative public policy, emphasized the significance of state and local capabilities in understanding the threat environment reported in a article titled *Effective Counterterrorism: State and Local Capabilities Trump Federal Policy*.

B. DOMESTIC INTELLIGENCE POLICY

The 2002 Homeland Security Act established DHS I&A, which was later amended by the 2007 Implementing Recommendations of the 911 Commission Act that established the DHS I&A State and Local Program Office. Both pieces of legislation created an organization designed to address the issues of information sharing to protect the homeland and partnering with state, local, tribal, territorial and private sector elements to ensure not only horizontal and vertical information sharing but also to leverage the HSE as contributors to the national intelligence architecture. Effective information sharing and the expansion of USIC capabilities is intended serve a more comprehensive approach in supporting the national efforts to protect the U.S. from future terrorist attacks.

The 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA), signed into law by President Bush made major amendments to the 1947 National Security Act and reintroduced the "…idea of a Director of National Intelligence (DNI) [that] dates to 1955 when a blue-ribbon study [was] commissioned by Congress. It was the attacks of September 11, however, that finally moved forward the longstanding call for major intelligence reform and the creation of a Director of National Intelligence."[85] As noted in Chapter II, EO 12333 sets forth the foundation of the USIC and the Administration's

[84] The Heritage Foundation, accessed June 7, 2013, http://www.heritage.org/about.

[85] Office of the Director of National Intelligence, accessed August 5, 2013, http://www.dni.gov/index.php/about/history.

directions regarding "timely and accurate information about the activities, capabilities, plans, and intentions of foreign powers, organizations, and persons and their agents"[86] in support of national security.

An EO serves as an official document to manage the operations of the federal government.[87] However, when EO 13470 in 2008 amended EO 12333, it included language focused on the responsibility of state, local and tribal governments, as well as the private sector to support U.S. intelligence activities. In order to support state, local and tribal governments, as well as the private sector integration into the HSE and support U.S. intelligence activities, DHS I&A, as well as other federal and academic elements, began delivering intelligence cycle process model training to the National Network and HSE.

The single common attribute used by various USIC intelligence cycle models is the "collection" phase. Nonetheless, the intelligence collection phase under the intelligence cycle process model within the post-9/11 HSE is considered a gray area because information is often required or expected from activities that are not necessarily violations of law, yet the information may be collected for the purpose of predictive analytic assessments for law enforcement and homeland security professionals. In 1952, intelligence "collection" was defined as the procuring, assembling and organizing of information and served as the first step in the processing of intelligence information according to *The International Dictionary of Intelligence* published by author Leo D. Carl. Today, it is considered the third step or phase in the intelligence cycle and "officially defined as 'the exploitation of sources of information by collection agencies and delivery of information to the proper intelligence-processing unit for use in the production of intelligence.'"[88] The 1952 definition was geared toward intelligence collection targeted against communist nation-states of the former Soviet Union and not the domestic intelligence environment of today.

---

[86] U.S. National Archives, accessed July 27, 2013, www.archives.gov/federal-register/executive-orders/12333.html.

[87] Ibid.

[88] Leo D. Carl, *The International Dictionary of Intelligence* (McLean, VA. International Defense Consulting Service, 1990). 59.

The September 11 terrorist attacks raised serious concerns regarding the sufficiency of the USIC intelligence collection capabilities and facilitated state, local, tribal and private sector partner assimilation into the newly established homeland security enterprise. The nation began focusing its intelligence collection efforts in order to prevent future attacks through the development of multiple national strategies between the White House and the DNI with minimal attention to domestic intelligence collection. The White House produced the 2002 National Security Strategy, the 2007 National Strategy for Homeland Security, and the 2010 National Security Strategy of the United States, the 2011 National Counterterrorism Strategy, and most recently the 2012 National Strategy for Information Sharing and Safeguarding. The DNI produced the 2005 National Intelligence Strategy and the 2009 National Counterintelligence Strategy. The first National Homeland Security Strategy published by the Bush administration in 2002 documented "Homeland security is based on the principle of shared responsibility and partnership with "state and local governments, the private sector, and the American people."[89] However, within the 2002 national strategy, there is no specific mention of domestic intelligence collection,[90] which remains consistent among the other referenced strategies.

Executive Order (EO) 12333 provides guidance for U.S. intelligence activities among USIC members, but it lacks a specific doctrine or "how to" concerning domestic intelligence collection to prevent repeating the law enforcement and intelligence mishaps of the past. The lack of doctrine may accelerate intelligence mishaps given the explicit language of Part 1.4 of EO 12333 that integrates state, local, and tribal governments, as well as private sector entities.

> [T]he Intelligence Community shall collect and provide information in accordance with priorities set by the President concerning activities to protect against international terrorism, proliferation of weapons of mass destruction, intelligence activities directed against the United States, international criminal drug activities, and other hostile activities directed against the United States by foreign powers, organizations, persons, and

[89] Office of Homeland Security, *National Strategy for Homeland Security*, July 2002, 2.

[90] Jennifer E. Sims, and Burton Gerber, *Transforming U.S. Intelligence*. Washington, D.C., Georgetown University Press. 2005. 206.

> their agents as well as take into account information needs relating to national and homeland security provided by state, local, and tribal governments and private sector entities.[91]

The federal government concentrates its support to nontraditional intelligence collectors (state, local, and tribal governments, as well as private sector entities) via the National Network. The National Network is a far-reaching change from the USIC that existed originally as part of a massive response to the challenge from the Axis powers in World War II and charged with responding to the challenges associated with the spread of Communism and the military might of the Soviet Union.

Most fusion centers within the National Network are law enforcement centric and recently integrated the Intelligence-Led Policing (ILP) model as the standard intelligence business practice. The term "Intelligence-led Policing" was coined in Great Britain to focus on key criminal activities[92] and its general philosophy was adopted by IACP in the March 2002 Intelligence Summit.[93] Author and academic David Carter, stated the emergence of ILP significantly enhances the law enforcement intelligence function.[94] However, as law enforcement agencies wrestle with the understanding of their new role in collecting and analyzing intelligence in support of the national intelligence architecture while at the same time managing crime in their jurisdictions, some authors judge introduction of ILP in the U.S. has been problematic.[95] Few agencies engage in proper intelligence-led techniques and ILP cannot be implemented effectively, if officers and analysts are not trained in the intelligence cycle process model in order to prevent crime

---

[91] Executive Order 12333, *United States Intelligence Activities* (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008).

[92] U.S. Bureau of Justice Assistance, *Intelligence-Led Policing: The New Intelligence Architecture*, September 2005, 9.

[93] International Association of Chiefs of Police, *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels*. Alexandria, VA, 2002.

[94] David L. Carter, *The Law Enforcement Intelligence Function: State, Local, and Tribal Agencies*, accessed March 3, 2013, http://www.hsdl.org/?view&did=469588.

[95] Roger, G. Dunham, Geoffrey P. Alpert, Jennifer E. Davis, and Robert W. Taylor, *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings*, 6th ed, Waveland Press, 2010, 232.

and terrorism.[96] According to the 2012 National Network of Fusion Centers Final Report, 100 percent of the National Network reported conducting or contributing to threat assessments, primarily focused on consequence, risk or vulnerability analysis[97] juxtapose proactively identifying threats supporting intelligence-led law enforcement activities necessary for preventing crime and terrorism. Purportedly, only 41 of 78 fusion centers (53.2 percent) contributed to national-level assessments, a statistic unchanged from the 2011 Assessment.

The International Association of Law Enforcement Intelligence Analyst (IALEIA), an organization established in 1980 to advance law enforcement intelligence analytic standards, defines ILP as "executive implementation of the intelligence cycle to support proactive decision making for resources allocation and crime prevention."[98] A consensus on the interpretation of the ILP philosophy between IACP and IALEIA has not been reached relative to standard employment of the intelligence cycle process model.

C. EXPLOITING DOMESTIC INTELLIGENCE AUTHORITIES – ABUSES

Expanding domestic intelligence capabilities initially began in the early part of the 20th century under President Theodore Roosevelt's administration.[99] Thirty-plus years prior to 9/11, challenges with domestic intelligence collection were uncovered during the 1970s Watergate, Rockefeller, Church, and Pike Investigations. The investigations involved overreach into U.S. domestic intelligence by the USIC and

[96] Roger, G. Dunham, Geoffrey P. Alpert, Jennifer E. Davis, and Robert W. Taylor, *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings,* 6th ed. (Waveland Press, 2010), 243.

[97] U.S. Department of Homeland Security, *2012 National Network of Fusion Centers Final Report*, accessed October 8, 2013, http://www.dhs.gov/sites/default/files/publications/2012%20National%20Network%20of%20Fusion%20Centers%20Final%20Report.pdf, 15.

[98] Lisa M. Palmieri, *Challenges Facing law Enforcement Intelligence*, 316.

[99] Loch K. Johnson, and James J. Wirtz, *Intelligence and National Security: The Secret World of Spies-An Anthology*. Oxford, NY. Oxford University Press. 2008, 6.

improper domestic intelligence activities by the Law Enforcement Community.[100] However, September 11, 2001, once again initiated the demand for increased domestic intelligence collection.

Domestic intelligence abuses may be viewed from two perspectives, political and multicultural. During the 1970s, the main topic of interest underlying the perceived threat to U.S. social structures centered on preventing the spread of communism by addressing perceived Soviet Union influence of social issues. In the post-9/11 environment, the topic centers on identifying the terrorist threat residing within the U.S. from groups or individuals aligned with radical violent and extremist ideology.

D. USIC MEMBERS – FBI, CIA, AND DOD/NSA

Members of the USIC, most notably the FBI and the CIA, as well as local law enforcement, conducted improper domestic intelligence collection activities under two programs. The FBI Counterintelligence Program known as COINTELPRO is well known for its domestic intelligence collection overreaches. The Center for National Security Studies,[101] a civil liberties think-tank founded in 1974 to prevent violations of civil liberties in the U.S., published several articles on COINTELPRO. Another grim domestic intelligence overreach involved the CIA's Operation CHAOS.[102]

Seymour Hersh in the New York Times first exposed the CIA's domestic operations on December 22, 1974. As a result, President Ford established the Rockefeller Commission to look into the CIA's domestic intelligence activities. The Rockefeller Commission detailed the CIA's mail intercept program described a separate domestic spying program run by the CIA's Office of Security called Project Resistance and

[100] *The Intelligence Community in the 21st Century: Staff Study* - Permanent Select Committee on Intelligence House of Representatives 104th Congress, accessed March 5, 2013, http://www.gpo.gov/fdsys/pkg/GPO-IC21/html/GPO-IC21–13.html.

[101] The Center for National Security Studies serves as a watchdog in defense of civil liberties, human rights and constitutional limits on government power. Policymakers, opinion leaders and journalists regularly seek the Center's expertise on both substantive and strategic issues, accessed August 5, 2013, http://www.cnss.org/pages/mission.html.

[102] Verne Lyon, *Domestic Surveillance: The History of Operation CHAOS*, accessed March 5, 2013, http://www.serendipity.li/cia/lyon.html.

mentioned an Office of Security program that gave seminars and training on lock-picking and surveillance to a number of local police departments.

The CIA's Operation CHAOS was designed to infiltrate American student organizations opposed to the Vietnam War to determine if there were foreign links.[103] The CIA Operation CHAOS existed for 5 years beginning in 1967 and ending in 1972, according to the Rockefeller report that revealed a compilation of some 13,000 different files, including files on 7,200 American citizens. However, the numbers may be on the low side; Operation CHAOS was tightly compartmented within the CIA and free from periodic internal review. For example, later reports of the number of state, local, and county police departments assisted by the CIA were put at 44, which is far more than the handful mentioned in the Rockefeller report.

The problems of collection guidance were the subject of a number of special studies to include the CIA's Inspector General in 1966 (known as the Cunningham Report).[104] In wake of revelations that the CIA had violated its charter by spying on U.S. citizens, a series of congressional investigations concluded there were violations of the law, as well as discovery of much wider range of intelligence investigation abuses.[105]

During the same period as CIA's Operation CHAOS, the FBI's COINTELPRO levied intelligence requirements on the CIA to collect information on U.S. citizens traveling abroad.[106] The FBI, established in 1908, was initially designated primarily as a law enforcement agency. However, under President Roosevelt's administration and because of World War II, the FBI's responsibilities expanded to include centralizing the authority for domestic intelligence.[107] Although originally created to investigate specific federal crimes, the FBI expanded into the notorious Hoover-era domestic intelligence

[103] Loch K. Johnson, and James J. Wirtz, *Intelligence and National Security: The Secret World of Spies-An Anthology*. Oxford, NY. Oxford University Press. 2008, 368.

[104] Scott D. Breckenridge, *The CIA and the U.S. Intelligence System* (Boulder, CO.: Westview Press. 1986), 56.

[105] Mark M. Lowenthal, *Intelligence: From Secrets to Policy* (Washington, D.C.: CQ Press, 2003), 21.

[106] Scott D. Breckenridge, *The CIA and the U.S. Intelligence System* (Boulder, CO.: Westview Press, 1986), 201.

[107] Ibid., 112.

agency that was famous for excess and overreach. Revelations of Hoover-era abuses prompted the FBI to refocus for a time on crime solving and a season of robust oversight and operational limitations on intelligence gathering followed. These limits were set forth in an internal set of rules, known since their creation as the "Attorney General's Guidelines."[108] The organizational setback is still a concern with the American public and civil liberties organizations. Because of 9/11, the Attorney General's Guidelines have once again undergone changes and currently it is titled the *Domestic Intelligence Operations Guide*. Thus, while the FBI has conducted investigations for both law enforcement and intelligence purposes throughout its history, their intelligence-collection activities prompt the most frequent calls for reform.[109]

During combat operations in Vietnam, U.S. Army intelligence agents gathered information on anti-war activists in support of the potential use of federal troops in the case of civil disturbances or urban riots. When the U.S. Army's domestic intelligence program became public knowledge in 1970 the public and political backlash caused a sever reduction at the end of the Vietnam War at perceived abuses.[110] The NSA, a DoD element recently came under public scrutiny concerning domestic intelligence collection activities. In the wake of leaks by former NSA contractor Edward Snowden, U.S. officials have faced growing questions about the kinds of information they are collecting about Americans, at what scale and under what authority. Intelligence officials reported collection efforts are important counterterrorism measures. Similar to the current privacy concerns regarding domestic intelligence collection activities by the FBI and the National Network, NSA has ties to past domestic intelligence collection abuses. The NSA created Project MINARET in 1969 to spy on peace groups and black power organizations. Federal agencies requested NSA to survey international communications of certain U.S. citizens traveling to Cuba. Beginning in 1967, requesting agencies provided names of U.S. persons in an effort to determine foreign influence on civil disturbances occurring

[108] Emily Berman, *Domestic Intelligence: New Powers, New Risks*. Brennan Center for Justice at New York University School of Law. 2011, 5.

[109] Ibid., 7.

[110] Michael E. Bigelow, "A Short History of Army Intelligence." *Military Intelligence*, July-September 2012, 45.

throughout the Nation and later, the widespread national concern over criminal activity such as drug trafficking and acts of terrorism, both domestic and international.[111]

The activities were likely a result of the lack of specific legislative and organizational guidance or doctrine regarding domestic intelligence collection. The U.S. intelligence collection array was largely built to respond to the difficulties of penetrating the Soviet target.[112] However, as the literature review highlights, when the collection phase on the USIC intelligence cycle is directed to support domestic intelligence, it has proved to be a detriment to civil rights without sound doctrine.

E. LOCAL LAW ENFORCEMENT

As early as the 1920s, law enforcement intelligence units maintained "dossier" files on individuals thought to be involved in some form with criminal activity, and in the 1950s, such files were maintained on individuals due to their political expressions or their placement on the fringes of mainstream society. Because of these files, the U.S. Supreme Court under Chief Justice Earl Warren ruled state or local law enforcement might be subject to civil liability.

This ruling commonly referred to as the "1983 suits" relied on a provision of the 1871 Civil Rights Act, codified as U.S. Code Title 42, Section 1983 – Civil Action for Deprivation of Rights. In the 1960s and early 1970s, lawsuits under the "1983 suits" targeting police intelligence units provided an individual could hold state and local law enforcement departments and their officers liable for maintaining records on individuals with no evidence of a crime.[113] Given a history in the 1960s and 1970s in which police

[111] U.S. Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities, Intelligence Activities – National Security Agency and Fourth Amendment Rights, October 29, 1975, accessed October 8, 2013, http://www.aarclibrary.org/publib/church/reports/vol5/pdf/ChurchV5_1_Allen.pdf.

[112] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*. Washington, D.C.. CQ Press. 2012, 83.

[113] David L. Carter, *Law Enforcement Intelligence: A Guide for State, Local and Tribal law Enforcement Agencies*, 2nd ed, 2009, 33.

intelligence units all too often violated citizen groups' First Amendment rights, there was a widespread movement to dismantle such capabilities.[114]

The NCISP drafted by the Global Justice Information Sharing Initiative Intelligence Working Group served to provide a model for intelligence process principles and policies by law enforcement elements. A key element of the NCISP supports policies that will protect privacy and constitutional rights while not hindering the intelligence process. As an example, the NCISP states a "privacy policy should stress the need for and importance of planning and direction (the first stage of the intelligence process). Although it is only one phase of the intelligence cycle, planning and direction guides the overall activities of the criminal intelligence function."[115]

F. NATIONAL NETWORK OF FUSION CENTERS

The National Network is susceptible to encountering like challenges with executing domestic intelligence activities. In December 2007, the American Civil Liberties Union (ACLU) published an article titled *What's Wrong With Fusion Centers?*" in which authors Michael German, ACLU Senior Policy Counsel and former FBI Supervisory Special Agent and Jay Stanley, an ACLU Senior Policy Analyst claims there has not been adequate public discourse regarding the National Network establishment prior to opening a state or major urban area fusion center charged with collection and sharing of intelligence information, specifically about American citizens and other residents. The article emphasizes civil rights abuses of the past by federal and local law enforcement and intelligence organizations while concluding like actions could potentially occur again without the proper legislative oversight and adequate checks and balances to monitor their operations.

The ACLU provided examples of a number of troubling intelligence products produced by fusion centers that were leaked to the public, such as a Texas fusion center

[114] Timothy Connors, and John Rollins, Center for Policing Terrorism at the Manhattan Institute. *State Fusion Center Processes and Procedures: Best Practices and Recommendations*. Policing Terrorism Report, No. 2, September 2007, 3.

[115] U.S. Department of Justice, Global Justice Information Sharing Initiative, *National Criminal Intelligence Sharing Plan*, October 2003, 12.

that released an intelligence bulletin describing a purported conspiracy between Muslim civil rights organizations, lobbying groups, the Iraq anti-war movement, a former U.S. Congresswoman, the U.S. Treasury Department and hip hop bands to spread Sharia law in the U.S. A Virginia Fusion Center reportedly issued a terrorism threat assessment describing the state's universities and colleges as "nodes for radicalization" and characterized the "diversity" surrounding a Virginia military base and the state's "historically black" colleges as possible threats.[116]

G. DOMESTIC INTELLIGENCE - CULTURE

As a result of the September 11 terrorist attacks, the 2001 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act also known as the USA PATRIOT Act, allowed greater latitude in domestic intelligence/law enforcement collection activities.[117] The USA PATRIOT Act represents a decision on the part of the president and Congress that the nation expects its defenders to be proactive against terrorism of all kinds.[118] In support of the proactive nature to defend the nation, DHS I&A has the responsibility per Section 503 of the 9/11 Commission Act to develop training curricula on the intelligence cycle process model for state and local officials[119] via the National Network in an effort to predict emerging threats.

In order to fully execute the USIC intelligence cycle process model, information fusion as an immediate and long-term strategic capability must be continually built upon to perform carefully informed analysis and assessments of homeland security information. In order to achieve such a capability, government agencies and organizations must have timely and appropriate access to information that supports the "collection" phase of the intelligence cycle process model. This remains a challenge

[116] American Civil Liberties Union, accessed August 7, 2013, http://www.aclu.org/spy-files/more-about-fusion-centers.

[117] Mark M. Lowenthal, *Intelligence: From Secrets to Policy*. Washington, D.C., CQ Press. 2003, 23.

[118] Loch K. Johnson and James J. Wirtz, *Intelligence and National Security: The Secret World of Spies-An Anthology*. Oxford, NY. Oxford University Press. 2008, 369.

[119] U.S. Department of Homeland Security, *DHS' Role in State and Local Fusion Centers is Evolving*. Office of Inspector General Report – OIG-09–12. October 2008, 16.

within the HSIE, specifically DHS I&A, as reflected in the DOJ Opinion of 28 Code of Federal Regulations, Part 23 specifically pertaining to DHS I&A. The opinion revealed;

> It has been brought to [DOJ] attention that some elements of the law intelligence information (which may include 'law enforcement sensitive' information) with the Department of Homeland Security (DHS), based upon a concern that it is not a 'law enforcement activity.' DOJ has consistently advised that the term does not require that an agency have law enforcement or investigative authority in order to qualify under an intelligence project's 'need to know' and 'right to know' criteria. Based on the description above, it appears that DHS, in performing its function of gathering information needed to protect the nation from foreign or domestic terrorist activity, is engaged in a 'law enforcement activity' and accordingly may be given access to criminal intelligence information that may be needed to properly carry out that function.[120]

The challenges with fusing information have been identified within HSIE as well as the HSE. The 2007 National Strategy for Homeland Security reported under the heading *Challenges in Homeland Security and Beyond* "although we have substantially improved our cooperation and partnership among all levels of government, private and nonprofit sectors, communities, and individual citizens, we must continue to strengthen efforts to achieve full unity of effort through a stronger and further integrated national approach to homeland security. Our information sharing capabilities have improved significantly, but substantial obstacles remain. We must continue to break down information barriers among federal, state, local and tribal partners and the private sector."[121]

In early August 2010, President Obama signed EO 13549 titled *Classified National Security Information Programs for State, Local, Tribal, and Private Sector (SLTPS) Entities*. This represented a significant step forward to facilitate classified intelligence and homeland security-related information sharing with SLTPS partners; to include putting in place a governance and oversight structure that would serve to ensure the uniform application of security standards within the executive branch and SLTPS

[120] U.S. Department of Justice Memorandum, *28 Code of Federal Regulations, Part 23*, March 31, 2005.

[121] The White House, *National Strategy for Homeland Security*, Washington: The White House, October 2007.

communities while maintaining consistency with existing policy and standards. This action now allowed classified information originating outside of DHS, and not otherwise covered by specific memorandum of understandings, to be disseminated by DHS to appropriately cleared nonfederal recipients in the National Network.

However, the policy and associated information sharing strategies often set forth by Washington are not readily accepted as they promulgate outside Washington, DC. In a professional environment, the writer observed and experienced unsuccessful intelligence and information sharing between SLTPS nontraditional intelligence recipients and federal HSIE and USIC entities because of differing organizational cultures. Due to the typical law enforcement culture and "lead-agency" law enforcement concept, the sharing of information with nontraditional law enforcement partners and the private sector remains a challenge. The October 2010 DHS Office of Inspector General Report emphasized this premise when it reported, "despite the overall improvements, DHS continues to face several information sharing challenges. Specifically, DHS component collaboration in the information sharing process needs improvement. In addition, unfinished intelligence products have not always been timely, and the production process for finished intelligence products should allow for more fusion center collaboration."[122]

The intelligence cycle process model collection phase depends on effective information sharing in order to produce value-added finished intelligence products for HSE policy and decision makers. With the expansion of USIC capabilities via SLTPS partners in support of the national intelligence effort, it is difficult to evaluate its effectiveness of the intelligence cycle process model in context of the lack of consistent intelligence cycle training and employment. Ms. Lisa Palmieri, a current DHS I&A Senior Intelligence Officer and former President of the International Association of Law Enforcement Intelligence Analysts, suggests the analysis phase of the intelligence cycle process model is problematic given the confusion between the terms intelligence and information among law enforcement officials as well as "…agencies employment of so-

[122] U.S. Department of Homeland Security, *Information Sharing with Fusion Centers Has Improved, but Information System Challenges Remain*, Office of Inspector General Report 11–04, October 2010.

called analysts who were either unaware of or untrained in analysis and who were merely collecting and disseminating raw data."[123]

Mr. Matt Mayer, counselor to the Secretary and Acting Executive Director for the Office of Grants and Training in DHS, visiting fellow at The Heritage Foundation, and President of the Buckeye Institute for Public Policy Solutions in Columbus, Ohio and Mr. Scott Erickson, who has studied and written on the proliferation of homegrown terrorism and the response by domestic law enforcement have specifically addressed the need for reform within the law enforcement culture in order to properly support their new counterterrorism role. Both assert that "uniformity of training must be a central aspect of any comprehensive shift in the domestic law enforcement culture" and "maintaining a mixed counterterrorism training regime [that includes the application of intelligence analysis] across the nation's 18,000 law enforcement agencies will inhibit the adoption of consistent and uniform standards for counterterrorism recognition and awareness." Symmetrical and uniform training standards would benefit the broader law enforcement community, as well as the public at large, by ensuring a consistent understanding of the threat of terrorism.[124]

[123] Lisa M. Palmieri, International Association of Chiefs of Police, "Information Vs. Intelligence: What Police Executives Need to Know," *The Police Chief*, vol. 72, no. 6, Alexandria, VA, June 2005.

[124] Matt A. Mayer, and Scott G. Erickson, *Changing Today's Law Enforcement Culture to Face 21st-Century Threats*. The Heritage Foundation. June 23, 2011.

THIS PAGE INTENTIONALLY LEFT BLANK

IV. INTELLIGENCE CYCLE PROCESS MODEL CASE STUDY – BOSTON MARATHON BOMBING

> No one can comprehend what goes on under the sun. Despite all their efforts to search it out, no one can discover its meaning. Even if the wise claim they know, they cannot really comprehend it. Ecclesiastes 8:17

A. INTRODUCTION

In an evaluation of performance metrics known as COCs for the National Network, the TCL for non-law enforcement elements, such as emergency managers, and the MCCCIE for the law enforcement community, this thesis intends to ascertain adherence to the intelligence cycle process model. To better understand the intelligence cycle process model's general effectiveness, the thesis examines existing public data made available to the author of the 2013 Boston Marathon bombing with respect to the National Network and HSE. Information made available regarding the 2013 Boston Marathon bombing will attempt to illuminate whether the National Network or the HSE adhered to the intelligence cycle process model in order to forecast or prevent the terrorist act.

The Boston Marathon bombing once again raised similar questions that surfaced after the September 11, 2001 terrorist attacks regarding law enforcement officials and intelligence analysts' ability to identify a potential terrorist attack. The Boston Marathon bombing serves as a platform to discuss the effective employment of the intelligence cycle process model by the National Network, and why it did not prevent the Boston bombing. This associated case study is intended to underscore key issues associated with employing the intelligence cycle process model at the state and local level by demonstrating its effectiveness prior to, during, and after the April 15, 2013, Boston Marathon bombing as an appropriate HSE intelligence process model. It is not focused on identifying possible solutions and providing potential courses of action. The case study framework and lessons learned from the Boston Marathon bombing may be useful to HSE agencies in developing and supporting intelligence processes suitable for the National Network. The information sources gathered for this case study were acquired

from public discussion of the issue in Congress, court documents, the press media and statements of senior state and local officials.

This case study uses the April 15, 2013, Boston Marathon bombing in the context of the intelligence cycle process model adherence necessary to detect the threat and provide intelligence to policy and decision makers with information in order to prevent the bombing. Additionally, the case study highlights the challenges with implementing the intelligence cycle process model within the National Network while ensuring security and safety from both domestic and international terrorism. Literature has highlighted the challenges with the intelligence cycle process model within the U.S. intelligence community, as well as the HSIE and HSE, and how difficult it is to lead a successful intelligence process to the point that a value-added intelligence product is produced with sufficient content and consensus to be useful to the organizations tasked to develop it. This is especially true in a National Network that lack the mature culture and uniform repeatable processes generally employed by organizations like those that comprise the 17-member USIC. Nonetheless, intelligence as an entity, process, and product within the HSE has the critical mission of preventing future terrorist attacks.

Using the intelligence cycle process model domestically to support the HSE in an attempt to think ahead and to understand what is going to happen in the future has reopened old wounds associated with abuse of power by law enforcement and intelligence entities. Instead of having to focus on domestic intelligence collection in an effort to identify state actors of foreign intelligence and security services as a result of Cold War labors, it is now necessary that intelligence collection must expand beyond the traditional USIC members in order to defeat terrorism and transnational criminal organization threats in a post-9/11 environment.

The National Network was another safeguard developed across the country since 9/11 to support the national intelligence architecture and prevent future terrorist attacks. They were expressly created to make sure law-enforcement agencies shared terrorist-related information developed by federal, state, and local law enforcement agencies. “It highlights a concern that we have and the need for agencies to share data on the subjects that they are investigating,” said Mike Sena, president of the National Fusion Center

Association.[125] DHS estimates it has pumped $1.4 billion into state and local fusion centers in their effort to support the National Network and assist with sharing intelligence and treat information necessary to prevent terror attacks across the country.[126]

The implementation of the intelligence cycle process model within the USIC, HSIE and HSE in order to determine its effectiveness has received mixed reviews. Given these interpretations, the Boston Marathon bombing will be used to assess the effectiveness of a six-step intelligence cycle process that embraces *Intelligence Analysis: A Target-Centric Approach* published in 2004 by author Robert M. Clark: 1) Requirements, needs, 2) Planning, direction, 3) Collection, 4) Processing, 5) Analysis, and 6) Dissemination.[127]

B. SCENARIO

On April 15, 2013, at 2:49 p.m. Eastern Standard Time, two pressure cooker bombs exploded during the Boston Marathon killing three people and injuring 264 others.

The suspects were identified later that day as Dzhokar and Tamerlan Tsarnaev.[128] Tamerlan Tsarnaev was subsequently killed by law enforcement, but Dzhokhar Tsarnaev while injured was able to escape. On April 19, 2013, during an unprecedented manhunt by thousands of law enforcement officers, Dzhokhar Tsarnaev was later captured and arrested.

C. PHASE 1 – REQUIREMENTS/NEEDS

The beginning of the intelligence cycle process model is identifying information needs/requirements from a defined customer base with the intent of providing the right

---

[125] Boston Globe, *FBI Did not Alert State's Anti-terror Unit to its Probe of Suspected Bomber in 2011*, accessed June 10, 2013, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

[126] The Boston Channel, *Effectiveness of Fusion Centers Questioned*, accessed June 20, 2013, http://www.wcvb.com/news/investigative/effectiveness-of-fusion-centers-questioned/-/12520878/20358362/-/bkveudz/-/index.html#ixzz2aHaeHk5x.

[127] Robert M. Clark, *Intelligence Analysis: A Target-Centric Approach*. Washington, D.C., CQ Press. 2004, 14.

[128] U.S. District Court for the District of Massachusetts, Criminal Complaint, *USA v. Dzhokar Tsarnev*, Case No. 13–2106-MBB, April 21, 2013.

intelligence product to the right end user to prevent future terrorist attacks. Homeland Security Standing Information Needs (HSEC SINs) form the foundation for information collection activities within the National Network to focus their collection, analytic, and reporting assets in support of the homeland security mission.[129]

There existed HSEC SINs made available to the National Network and the HSIE to identify and document information needs designed to prevent the Boston Marathon bombing. Additionally, in 2004 DHS issued a warning regarding explosive devices hidden in pressure cookers.[130] Likewise, according to a July 2007 National Intelligence Estimate entitled *The Terrorist Threat to the U.S. Homeland* an attack like the Boston bombing has been a concern for the U.S. government for years.[131] The DHS warning indicated pressure cooker bombs was as "a technique commonly taught in Afghan terrorist training camps."[132]

The Boston Regional Intelligence Center and the Commonwealth Fusion Center in Maynard,[133] which were designed to serve as clearinghouses for information about potential threats, were unaware that the FBI interviewed Tsarnaev as part of a three-month investigation after Russian agents alerted U.S. officials to his increasing radicalization, officials said.[134] Nor was information about Tsarnaev shared at the quarterly meetings the FBI had with local law enforcement leaders because according to

[129] U.S. Department of Homeland Security, accessed June 10, 2013, http://www.dhs.gov/more-about-office-intelligence-and-analysis-mission.

[130] CNN, *Boston Marathon Terror Attack Fast Facts*, accessed August 14, 2013, http://www.cnn.com/2013/06/03/us/boston-marathon-terror-attack-fast-facts.

[131] Statement for the Record Senator Joe Lieberman (Ret) House Committee on Homeland Security, *The Boston Bombings: A First Look*, accessed July 27, 2013, http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-SchwartzK-20130509.pdf.

[132] Newsdesk, *Israel Homeland Security*, "A "Pressure Cooker" Warning was Given a Few Times in Recent Years," accessed April 21, 2013, http://i-hls.com/2013/04/a-pressure-cooker-warning-was-given-in-2004/.

[133] The Boston Regional Intelligence Center and the Commonwealth Fusion Center of Maynard are elements of the National Network of Fusion Centers (National Network).

[134] Boston Globe, *FBI did not alert state's anti-terror unit to its probe of suspected bomber in 2011*, accessed June 10, 2013, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

the FBI, it did not rise to a specific level of concern.[135] "We were not privy to the tip,'' said David Procopio, the spokesman for the Massachusetts State Police, which oversees the Fusion Center, "They didn't share that information with us."[136]

The numbers of HSE nontraditional intelligence recipients are vast, including the 78 fusion centers that make up the National Network. Due to the enormous number of executives charged with establishing and implementing intelligence policy, two challenges are immediately discovered; who determines the requirement to have access to intelligence and information together with identifying who shoulders the responsibility of approving and establishing the priorities for satisfying documented intelligence needs. The National Network is unlike the USIC that can be task members to collect, analyze and produce national intelligence products by Intelligence Community Directives and Intelligence Community Policy Guidance.

Within Phase 1 of the intelligence cycle process model, it appears clear that the DHS HSEC SINs provided the necessary information needs (requirements) to the National Network in an effort to focus their assets on reporting potential terrorist activity in support of the homeland security mission. Nevertheless, the National Network does not have an executive body capable of issuing directives to state and local owned fusion centers that serve their respective jurisdictions.

D. PHASE 2 – PLANNING/DIRECTION

In an April 2009 statement by John E. Bateman, Assistant Commander, Texas Department of Public Safety to the Committee on House Homeland Security Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, he commented that the National Network was designed to be a network of multi-agency intelligence centers, sharing and analyzing information, and then passing that information on to decision makers and first line personnel in the field, allowing these groups to make

[135] The Boston Channel, *Effectiveness of Fusion Centers Questioned*, accessed June 20, 2013, http://www.wcvb.com/news/investigative/effectiveness-of-fusion-centers-questioned/-/12520878/20358362/-/bkveudz/-/index.html#ixzz2aHaeHk5x.

[136] Boston Globe, *FBI Did Not Alert State's Anti-terror Unit to its Probe of Suspected Bomber in 2011*, accessed June 10, 2013, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

better, more informed decisions as they work to thwart the individuals and groups intended to harm the U.S. While there have been, in the past, multi-agency taskforce operations on the enforcement side designed to address problems relating to crime and terrorism, the National Network is the first true comprehensive nationwide program to combine the analytical and informational capabilities of federal, state, county, local, and tribal agencies.[137]

The planning/direction phase of the intelligence cycle process model at the federal level is generally administered by the DNI and the respective USIC organization. However, within the National Network, there does not exist a centralized element to oversee the administration of this process. Although there existed HSEC SINs focused on preventing terrorist attacks, Senator Joseph Lieberman asked, "did the FBI enlist the help of state and local law enforcement, either on or off the JTTF to continue to watch the brothers, engage with their friends, associates and community leaders or monitor their Internet activities – including Tamerlan Tsarnaev's YouTube account, which openly recommended a collection of jihadist videos – for the purpose of assessing if either or both of the brothers were radicalizing"? Senator Lieberman commented the FBI does not have the resources or personnel to monitor all potential terrorist threats in this country and must rely on state and local law enforcement.[138]

The cultural and legal barriers to effective partnerships among national intelligence elements and the National Network prevent effective planning/direction within the HSE and the new national intelligence structure. The final report of the National Commission on Terrorist Attacks Upon the United States (9/11 Commission) described many instances in which, in the period leading up to September 11, 2001 potentially useful information was available but no one knew to ask for it, information was distributed only in compartmented channels, or information was requested but

[137] *CQ Homeland Security*, "Fusion Center Hearing," accessed August 22, 2012, http://homeland.cq.com/hs/.

[138] Statement for the Record Senator Joe Lieberman (Ret) House Committee on Homeland Security, *The Boston Bombings: A First Look*, accessed July 27, 2013,, http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-SchwartzK-20130509.pdf, 2013.

withheld on the basis of a determination that it could not be shared. Twelve years later, Congressional House and Senate members have identified similar challenges remain with threat notification, access to information, and database management of information that may have contributed the 2013 Boston Marathon bombing.

E. PHASE 3 – COLLECTION

The National Strategy for Homeland Security supports the collection of information resulting in actionable intelligence for law enforcement agencies to prevent terrorist attacks. The collection of this information combines state and local criminal intelligence and national intelligence. Historically, domestic intelligence collection is viewed as problematic for law enforcement criminal intelligence when American law enforcement agencies have three primary roles: 1) Solving crimes committed in the past, 2) Preventing crimes that are imminent, and 3) Collecting criminal intelligence to stop future crimes.

Law enforcement criminal intelligence collection is guided by 28 CFR Part 23. 28 CFR Part 23 requires the collection and maintenance of criminal intelligence information concerning an individual, only if there is reasonable suspicion or criminal predicate that the individual is involved in criminal conduct or activity, and only if the information is relevant to that criminal conduct or activity. Because the "reasonable suspicion or criminal predicate" thresholds may be both conjectural and subjective in nature, criminal intelligence information cannot be accessed by criminal suspects to verify that the information is accurate and complete. The protections and limitations set forth in 28 CFR Part 23 are necessary to protect the privacy interests of the subjects and potential subjects of a criminal intelligence system.[139]

The FBI said it took a number of investigative steps to check on the request, including looking at his travel history, checking databases for derogatory information and searching for Web postings. Agents also interviewed Tsarnaev's family members, the

[139] Institute for Intergovernmental Research, *Criminal Intelligence Systems Operating Policies (28 CFR Part 23) Training and Technical Assistance Program*, accessed July 27, 2013, http://www.iir.com/WhatWeDo/Criminal_Justice_Training/28CFR/.

FBI said, but did not detect terrorist activity.[140] Richard Falkenrath, an adjunct Senior Fellow for Counterterrorism and Homeland Security, claim the U.S. authorities support broadminded foreign intelligence-gathering techniques abroad while, "we're instead reliant on more restricted domestic intelligence techniques to identify terrorist before they attack."[141]

Although the FBI and CIA as USIC members conducted a collection of information to determine the threat, a spokeswoman for the Boston Police Department said the Boston Regional Intelligence Center also was never notified about the FBI investigation[142] that may have resulted in the ability to leverage state and local unique capabilities to collect valuable data. In the FBI's final analysis, it concluded there was little it could have done to prevent the Boston Marathon bombing due to constraints provided in federal law and Justice Department protocols.[143] Although federal-level protocols disallowed the FBI from further inquiry, the National Network was also prevented from serving as a force-multiplier in an effort to collect as much information as possible in determining the threat.

While collection is the common variable among various intelligence cycle process models, it is also the most challenging to accomplish given the history of domestic intelligence collection activities by federal agencies and local law enforcement. Within the National Network, collection is implied to address "all-threats," but state and local organizational policies are generally unclear on what information is to be collected and what collection techniques is to be used, notwithstanding explicit statements to protect privacy, civil liberties, and civil rights.

---

[140] CNN, *FBI Agent Interviewed Bombing Suspect in 2011*, accessed April 21, 2013, http://www.cnn.com/2013/04/19/us/boston-suspects-no-links/index.html.

[141] Council on Foreign Relations, *Domestic Intelligence and the Boston Bombings*, accessed August 7, 2013, http://www.cfr.org/counterterrorism/domestic-intelligence-boston-bombings/p30557.

[142] Boston Globe, *FBI Did Not Alert State's Anti-terror Unit to Its Probe of Suspected Bomber in 2011*, accessed June 10, 2013, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

[143] New York Times, *FBI Said to Find It Could Not Have Averted Boston Attack*, accessed August 6, 2013, http://www.nytimes.com/2013/08/02/us/fbi-said-to-conclude-it-could-not-have-averted-boston-attack.html?_r=0.

F. PHASE 4 – PROCESSING

The processing of information associated with the Boston Marathon bombing in the context of the intelligence cycle process model proved ineffective because of information sharing challenges and data overload. A FBI Supervisory Agent provided an emailed statement suggesting that state and local officials had ample access to information about the Tsarnaev investigation in 2011, through their participation on the FBI Boston JTTF[144] that include detectives and detective supervisors from the Boston Regional Intelligence Center. Additionally, the Boston Police Department maintains a close and ongoing working relationship with both the FBI and DHS through the intelligence personnel both agencies have assigned to work within the fusion center.[145] While fusion center (National Network) personnel are employed on the FBI Boston JTTF, what has surfaced is that the information was compartmentalized to a point it provided a barrier and prevented a timely notification of potential threat information and intelligence to senior state and local decision makers.

An added challenge to processing information for determining an intelligence value is data overload. Richard DesLauriers, head of FBI Boston stated the FBI's assessment of Tsarnaev was "…one of about 1,000 such assessments conducted by the Boston task force…"[146] leading up to the Boston Marathon bombing. In relation to the processing of information associated with the Boston Marathon bombing, congressional members evoke many of the same themes associated with September 11, 2001. Representative Michael McCaul, Chairman of the House Homeland Security Committee, declared "My fear is that the Boston bombers may have succeeded because our system

[144] Boston Globe, *FBI Did Not Alert State's Anti-terror Unit to Its Probe of Suspected Bomber in 2011*, accessed June 10, 2013, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

[145] *Congressional Testimony of Boston Police Commissioner Edward F. Davis, III before the House Committee on Homeland Security*, accessed July 27, 2013, http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-SchwartzK-20130509.pdf, 2013.

[146] Wall Street Journal, *Boston Hearings Delve into FBI Alerts*, accessed August 14, 2013, https://www.online.wsj.com/article.

failed,"[147] and Representative Bernie Thompson announced "We cannot ignore that once again it has taken a tragedy to reveal problems in our vast, varied and numerous federal databases."[148]

G. PHASE 5 – ANALYSIS

Analysis in many respects is as difficult to attain as the collection aspect. One critical challenge is the intergroup dynamics between law enforcement investigators and intelligence analysts. Ms. Lisa Palmeiri, noted law enforcement is undergoing a real transformation and recognizing that intelligence is different from simple information as police executives have recognized only a clear comprehension of the analytic process will support public safety officials in protecting the nation.[149] Boston's Commissioner Edward Davis stated his detectives may have concluded the same findings as the FBI in that there was no information (back then) that would have caused further investigation of the Tsarnaev's.[150] What is not stressed in both the FBI findings and the Boston Commissioner's statement is the skill-set and analytic tradecraft employed by supporting analysts. This issue is compounded when dealing with the associated challenges of intelligence management, as well as interagency intelligence collaboration. As an example, how do you effectively balance the demands of current real-time crime intelligence needs and the competing demands for longer-range predictive analysis?

A 2011 The Homeland Security Policy Institute's Counterterrorism Intelligence Survey Research report, indicated 62 percent of the intelligence chiefs representing major metropolitan police departments in the U.S. believed the "national [federal] intelligence enterprise was such that it left them unable to develop a complete understanding of their

[147] Wall Street Journal, *Boston Hearings Delve into FBI Alerts*, accessed August 14, 2013, https://www.online.wsj.com/article.

[148] Ibid.

[149] Lisa M. Palmieri, International Association of Chiefs of Police, "Information Vs. Intelligence: What Police Executives Need to Know," *The Police Chief*, vol. 72, no. 6, Alexandria, VA, June 2005.

[150] Wall Street Journal, *Boston Hearings Delve into FBI Alerts*, accessed August 14, 2013, https://www.online.wsj.com/article.

local threat environment."[151] Likewise, in the September 2011 Intelligence and National Security Alliance publication, experts agree that many federal intelligence and law enforcement professionals do not recognize the homeland security implications and intricacies of criminal information.[152]

Without the information possessed by FBI Boston, the Boston Regional Intelligence Center analysts were never in a position to help federal authorities connect the dots on a potentially dangerous person. They could not evaluate the relevance of Tsarnaev's six-month trip to Russia in 2012; assess whether his potentially extremist views may have further hardened after he returned to his home in Cambridge; or decide whether authorities needed to interview him again.[153]

In hindsight to the Boston Marathon bombings, the DNI as part of a full interagency review ordered a review and assessment now under way by the U.S. intelligence and law enforcement community. The initial intelligence review had focused largely on regional militant connections the men had in Russia or Central Asia. Initially, before the FBI identified the men, the review was looking at any indications of a threat emerging from overseas against the U.S. Once the identities of the men became known, with their possible ethnic Chechen background, the focus shifted. The USIC is tasked under the review with checking any intelligence gathered overseas while the FBI will focus on what is known inside the United States.[154] As part of the great HSE, the National Network has not been revealed as an element of the review, or the significant role it may have played in preventing the bombing.

---

[151] Frank J. Cilluffo, Joseph R. Clark, and Michael P. Downing, *Counterterrorism Intelligence: Law Enforcement Perspectives*. Counterterrorism Intelligence Survey Research. Homeland Security Policy Institute. George Washington University. September 2011.

[152] Intelligence and National Security Alliance, White paper, *Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead*. Arlington: Homeland Security Intelligence Council, 2011.

[153] Boston Globe, *FBI did not alert state's anti-terror unit to its probe of suspected bomber in 2011*, accessed June 10, 2013, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

[154] CNN, *FBI Agents Interviewed Bombing Suspect in 2011*, accessed April 21, 2013, http://www.cnn.com/2013/04/19/us/boston-suspects-no-links/index.html.

H. PHASE 6 – DISSEMINATION

The dissemination of a possible intelligence product may have centered on the differences in the understanding of what was identified as "intelligence" necessary for sharing information associated with the Boston Marathon bombing. The general inclination among law enforcement practitioners is that intelligence is information that leads to successful law enforcement activities. Within this context, the FBI Boston JTTF may have arrived at the conclusion there was no need to share information regarding the bombers. The USIC however, describes intelligence as information that has undergone a formal process, typically using a variation of the intelligence cycle process model. According to a U.S. official familiar with intelligence information on the Boston Marathon bombings, initial indications were that the two suspects do not have direct links to any major al Qaeda group or affiliates, or to a new significant terrorist threat to the U.S.[155] Equally within the context of statement of the U.S. official, the intelligence information referenced was not provided to the National Network, specifically the Boston Regional Intelligence Center.

The National Network, specifically the Boston Regional Intelligence Center, was not in a position to publish an intelligence product identifying concerns and issuing a warning regarding explosive devices hidden in pressure cookers. There is no available public literature or empirical data supporting the use of the intelligence cycle process model associated with information processing was used in respect to producing indications, watch and warnings intelligence in an effort to prevent the Boston Marathon bombing. The issues associated with the adherence of the intelligence cycle process model underscore the challenges that remain within the National Network relative to the effectiveness of the intelligence cycle process model.

I. CONCLUSION

The writer's analysis of the 2013 Boston Marathon bombing offers the National Network nor the HSE adhered entirely to the intelligence cycle process model in order to

[155] CNN, *FBI Agents Interviewed Bombing Suspect in 2011*, accessed April 21, 2013, http://www.cnn.com/2013/04/19/us/boston-suspects-no-links/index.html.

forecast or prevent the terrorist act. This type of event was forecasted nine years earlier in 2004 when DHS issued a issued a warning regarding explosive devices hidden in pressure cookers, also there existed HSEC SINs to identify and document relevant information needs. In addition, a National Intelligence Estimate entitled *The Terrorist Threat to the U.S. Homeland* was issued in July 2007 designating an attack like the Boston bombing was a concern for the U.S. government.[156]

The writer identified several key issues underscored in the April 15, 2013, Boston Marathon bombing associated with employing the intelligence cycle process model at the state and local level as an appropriate HSE intelligence cycle process model. Adherence to the intelligence cycle process model revealed its ineffectiveness due to delays in access to relevant information between the FBI and local law enforcement. Recognizing that successful counterterrorism efforts require effective information sharing, Section 1016 of the 2004 IRTPA (Public Law 108–458), building on the August 27, 2004, EO 13356, "*Strengthening the Sharing of Terrorism Information to Protect Americans*," required the creation of the Information Sharing Environment (ISE) for terrorism information. What also emerges is the challenge of identifying and prioritizing to whom and what information is to be shared by agencies within the HSE that supports the requirements/needs process.

The 9/11 Commission Report that described instances leading up to September 11, 2001, clearly reflected that potentially useful information was available, but no one knew to ask for it; information was distributed only in compartmented channels, or information was requested but withheld on the basis of a determination that it could not be shared. Each challenge is linked to effective adherence of the intelligence cycle process model, specifically planning and direction (Phase 2), collection (Phase 3), processing (Phase 4) and analysis (Phase 5) within the National Network and in this case similar to the Boston Marathon bombing. This exposes the continued need to address the

[156] Statement for the Record Senator Joe Lieberman (Ret) House Committee on Homeland Security, *The Boston Bombings: A First Look*, accessed July 27, 2013, http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-SchwartzK-20130509.pdf.

ISE designed to support sharing and access to terrorism information, including information from the intelligence, law enforcement, military, homeland security, and other communities.

Individual departments and agencies have their own policies and procedures for information sharing, but there is no single government-wide agreement on what constitutes appropriate information sharing. Different standards exist among agencies (and even within agencies) for the designation and dissemination of terrorism information, resulting in different views on who requires the information and when and how the information is needed and processed. Because information protection standards vary, decisions on reconciling the need to protect information and the need to share information have been inconsistent and have contributed to the creation of cultures that support information segregation. A fundamental change must occur so that, in the dynamic setting of the new ISE, the right information is available to the right people at the right time.[157]

Consistent with the work of the Information Systems Council under Section 5 of EO 13356, one of the ISE's goals is to remove technology as a barrier to improved information sharing. For the most part, the technology needed to improve interoperability and information sharing is available today; and it should be an enabler rather than a barrier. While it is true that users face a vast and confusing array of systems, databases, networks and tools, in most cases this vast and confusing array is caused not by technological barriers, but by the policies, protocols, and sometimes security and legal concerns that prevent us from connecting the systems and sharing information in an optimal way.[158]

An area that remains to be developed is an appropriate identity-based screening system, to include biometrics and an improved visa threat analysis system. Law enforcement agencies have had to rely more on traditional investigative techniques to

[157] Office of the Director of National Intelligence, *Preliminary Report on the Creation of the Information Sharing Environment*, accessed August 8, 2011, http://www.ise.gov/sites/default/files/preliminaryreport.pdf.

[158] Ibid.

detect terrorist travel concerns, which resulted in the arrest of two U.S. citizens in New York after allegations they planned to travel to Somalia to join al-Shabaab.[159] The lack of a direct mechanism to share terrorism-related information between law enforcement agencies, along with the sheer amount of data that a JTTF in a major city has to sort through, are two issues that should be addressed in light of these attacks.

[159] Stephanie Hanson, *Al-Shabaab*, August 10, 2011, accessed August 24, 2011, http://www.cfr.org/somalia/al-shabaab/p18650.

THIS PAGE INTENTIONALLY LEFT BLANK

V. INTELLIGENCE CYCLE PROCESS MODEL AND THE HOMELAND SECURITY ENTERPRISE

A. HOMELAND SECURITY ENTERPRISE AND EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL

Intelligence can no longer be defined in the context of ascertaining the capabilities and intentions of other nation-states abroad while systemically providing access to such intelligence to only an elite community of federal level intelligence analyst and collectors. The 9/11 terrorist attacks brought the intelligence function and the associated intelligence cycle process model to the forefront of the HSE. The post-9/11 HSE requires an intelligence cycle process model with the capability to operationalize intelligence gaps necessary for preventing terrorist acts from international terrorist groups operating abroad and within U.S. borders, domestic terrorist groups and homegrown violent extremists. It also requires providing timely results of intelligence cycle process model information (intelligence) to federal, state, and local customers. It is essential that officials responsible for the various aspects of homeland security fully realize the robust capacity of the national intelligence architecture. The U.S. government has the responsibility to dutifully and deliberately consider the Nation's approach and actions given the complexity and uniqueness of operating within the domestic intelligence realm.[160]

In order to maximize the capabilities of the HSE, the intelligence cycle process should address both a dynamic "top-down" and "bottom-up" approach as a contributor to the national intelligence architecture. The USIC traditional intelligence cycle process model is a "top-down" approach that was originally constructed to addresses military and national policy maker information needs. National policymakers requested information and assessments concerning foreign capabilities and threats and their potential to affect U.S. interests abroad, as well as U.S. preparations for defeating military foreign threats. A "bottom-up" approach to the intelligence cycle process model provides state and local decision makers, public safety officials and the private sector the ability to influence and

[160] The White House, *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the U.S.*, December 2011, 3.

shape national interest through fusion centers operating within the National Network at the state and local level. There exists a credible need for a new intelligence process model that integrates the post-9/11 HSE and with it a need to train these diverse groups. Developing an intelligence process that integrates both, a "top-down" and "bottom-up" approach provides a comprehensive evaluation of the threats to homeland security that affect all levels of government and engages multiple public safety disciplines.

B. INTELLIGENCE CYCLE PROCESS MODEL TRAINING

Members of the USIC have developed organizational institutions to train its intelligence elements on the intelligence cycle process model most fitting their organization. The CIA has the Sherman Kent School for Intelligence Analysis that provides specialized training in the craft of intelligence analysis.[161] In 2005, the FBI established the Intelligence Career Service comprised of intelligence analysts, language specialists and surveillance specialists personnel with intelligence training at the College of Analytical Studies. It was later changed to the Center for Intelligence Training to provided basic and advanced training for FBI analysts and agents.[162] The Department of Defense provides intelligence training via individual service institutions and jointly through the National Intelligence University located within the Defense Intelligence Analysis Center that focuses on the profession of intelligence and offers an in-depth curriculum intended to enhance the analytical skills and competencies of intelligence analysis.[163] The DHS I&A Training Branch established the Homeland Security Intelligence Training Center to strengthen DHS intelligence enterprise capabilities, enhance collaboration among the intelligence offices of the department's components, and provide specialized intelligence training to state and local officials.[164]

---

[161] U.S. Central Intelligence Agency, *Training Resources*, accessed August 10, 2013, https://www/cia/goc/offices-of-cia/intelligence-analysis/training-resources.html.

[162] U.S. Department of Justice, Federal Bureau of Investigation, *National Security Branch*, September 2006, accessed August 10, 2013, http://www.hsdl.org/?view&did=480684.

[163] U.S. Defense Intelligence Agency, accessed August 10, 2013, http://www.dia.mil/university/.

[164] U.S. Department of Homeland Security, *The Department Develops its Own Professional Intelligence Workforce*, January 14, 2009, accessed August 10, 2013, http://ipv6.dhs.gov/journal/leadership/labels/Intelligence%20and%20Analysis%20Directorate.html.

The DHS also supports formal degree granting opportunities with tailored intelligence instruction through the Naval Postgraduate School – Center for Homeland Defense and Security.

In October 2007, the DOJ Global Justice Information Sharing Initiative commonly referred to as Global, published the *Minimal Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States*. Global serves as a federal advisory committee to the U.S. Attorney General on critical justice information sharing initiatives.[165] The Global training philosophy is intended to "…develop a culture of information analysis and information sharing within the law enforcement communities…"[166] Global defines the intelligence cycle as "an organized process by which information is gathered, assessed and distributed in order to fulfill the goals of the intelligence function. It is a method of performing analytic activities and placing the analysis in a usable form."[167]

Global identified objectives for law enforcement intelligence analyst, intelligence managers/commanders, executives, and officers. Within these objectives is a standard for training the intelligence process/cycle that includes topics to be considered: Collection, analysis, dissemination, production, collation, evaluation, and assessment within a three-hour block of instruction for law enforcement analysts and managers.[168] The law enforcement officer basic criminal intelligence officer provides for 40-minutes of training to include the officer's role and responsibilities in the intelligence process/cycle.[169] Global does not identify sequential steps common within the USIC nor provide illustrations of the intelligence cycle.

Though HSE partners, specifically state and local officials, have limited opportunities to attend in-residence training opportunities at the USIC member

[165] U.S. Department of Justice, Global Justice Information Sharing Initiative, Findings and Recommendations, *Minimal Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States*, Version 2, October 2007.

[166] Ibid., 1.

[167] Ibid., 41.

[168] Ibid., 4, 8.

[169] Ibid., 18.

institutions, there are far more intelligence focused training opportunities presented to state and local officials through on-site mobile training events sponsored by a number of elements. Through the DHS/DOJ Fusion Process Technical Assistance Program and Services, DHS FEMA sponsored MIPT and the Institute of Intergovernmental Research delivers on-site mobile training opportunities to the National Network, as well as the state and local members of the HSE. In order to effect the required change, some have opined the need to establish as national center for intelligence training in conjunction with a national intelligence strategy. Although a national center has not been established, the Governor of Texas designated the Texas Department of Public Safety, Intelligence and Counter-Terrorism Division (DPS-ICT) as the proponent for intelligence for the State of Texas. The DPS-ICT, in concert with criminal justice professors at Texas State University, has initiated a project intended to create a certification program providing statewide training and an education baseline for all analysts in Texas.[170] While many have echoed the sentiment regarding specific intelligence training to state and local law enforcement, there has been little realization of the kind of training that state, local, and tribal law enforcement communities need to be truly effective homeland security partners.[171]

The need for integration of the state and local environment into nation's intelligence effort was a principal finding of the USIC assessments in the wake of the 9/11 attacks and desired goals of subsequent national strategies. In addition to the USA PATRIOT Act, the 2004 IRTPA provided the DNI and is responsible for establishing intelligence community-wide policies. Yet, there remain challenges and practical implementation with the intelligence cycle process model and domestic intelligence collection by the HSE, as noted in the previous chapter. It is critical to recognize and define how the USIC intelligence cycle process model is to be employed within the HSE at the state and local level. Equally significant is ascertaining if a standardized

[170] Texas Department of Public Safety, *IDP's for Intelligence Analysts at the Texas Department of Public Safety PowerPoint*, accessed October 7, 2013, www.iafie.org/resource/resmgr/2012_conference/mullins.pptx.

[171] Law Enforcement Assistance And Partnership, *A Law Enforcement Assistance and Partnership Strategy, Improving Information Sharing Between the Intelligence Community and State, Local, and Tribal Law Enforcement*, 5.

intelligence cycle process model exists that is capable of being employed effectively within the USIC, the HSIE, as well as the HSE. As noted in previous chapters, there are many versions of the intelligence cycle process model that is generally aligned to an organizations' mission space and numerous intelligence training venues theoretically serving to provide some aspect of training on the intelligence cycle.

C. STATE AND LOCAL LAW ENFORCEMENT COMMUNITY

A key element of the HSE is the state and local law enforcement community. Intelligence in law enforcement has historically been misunderstood, underutilized, and even misapplied. With 18,000 local and state law enforcement agencies in the U.S., there is a critical need to provide and coordinate education, training, and professional services related to domestic intelligence collection activities and the employment of a standardized intelligence cycle process model. There are many misconceptions about the meaning and application of intelligence within law enforcement, although the IACP Criminal Intelligence Sharing Plan provides "intelligence is the combination of credible information with quality analysis - information that has been evaluated and from which conclusions can be drawn.[172]

Ms. Lisa Palmieri suggests the intelligence cycle process model is not fully explored in the law enforcement community within the context of criminal investigations because case information collected during an investigation is often considered "peripheral to proving the elements of the crime." Additionally, Ms. Palmeiri claims the training of law enforcement officials and intelligence analysts has not been institutionalized necessary for incorporating "intelligence as an element of policing culture [that] would address the challenge of evaluating intelligence analysts in police agencies."[173]

Various reports identify more than 800,00 law enforcement officials nationwide responsible for public safety. Being able to provide intelligence products that support

[172] David L. Carter, U.S. Department of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed., January 2009, 10, 13.

[173] Lisa M. Palmieri, Law Enforcement Intelligence Units and International Association of Law Enforcement Intelligence Analysts, *Challenges Facing Law Enforcement Intelligence*, 2011, 313.

more than 800,000 state and local law enforcement officials and the private sector requires a new approach to the intelligence cycle process model. Given the 18,000 state and local law enforcement agencies operating within the HSE, and the misconceptions about intelligence, the type of products disseminated generally fails to satisfy varied and numerous customer needs.

In the 1970s, standards were introduced requiring police departments to articulate "criminal predicate" before beginning intelligence operations on members of the community. In the 1980s, the Regional Information Sharing System was established and implemented through the Criminal Intelligence Operating Policies at the federal level - 28 CFR Part 23.[174] A noticeable distinction exposes the current USIC intelligence cycle process model in that it does not require criminal predicate, on the other hand, 28 CFR Part 23 does not address the collection of information for policymakers, yet both are in use within the HSE in support of domestic intelligence collection activities.

Police officers' and sheriff's believe that in order to be effective in preventing terrorism and related criminal activity; it is essential that they fully participate in the intelligence cycle process at both the federal and nonfederal levels. Additionally, they must become advocates for law enforcement intelligence products that meet their information needs and ensure law enforcement intelligence and other information is shared with their communities.[175] The current USIC intelligence cycle process model paradigm fosters aggressive, active intelligence gathering. It anticipates the threat before it arises and plans preventive action against suspected targets. In contrast, the law enforcement paradigm fosters reactions to information provided voluntarily, uses ex post

[174] Roger G. Dunham, Geoffrey P. Alpert, Jennifer E. Davis, and Robert W. Taylor, *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings*, 6th ed. (Waveland Press, 2010), 226–227.

[175] Law Enforcement Assistance And Partnership, *A Law Enforcement Assistance and Partnership Strategy, Improving Information Sharing Between the Intelligence Community and State, Local, and Tribal Law Enforcement*, 1.

facto arrests and trials governed by the rule of law, rules of evidence, and the protection of the rights of American citizens.[176]

Although law enforcement agencies need background information or "strategic intelligence" regarding patterns of criminal activity (e.g., analysis indicating that increasing quantities of cocaine are flowing through harbors in southern Florida), they tend to give higher priority to tactical information (e.g., a tip that a specific cargo vessel is scheduled to off-load a shipment of cocaine at a specific dock in Miami on the night of August 4). However, national policymakers require a continuous stream of information about countries, groups, and individuals working against U.S. interests. There is no end-point to these requirements; even a favorable evolution of events does not mean the end of the need for up-to-date information. In many cases at the federal level, the need for intelligence is more important than the need for dealing with a particular incident.

D. PRIVATE SECTOR

In addition to the National Network, primarily supported by state and local law enforcement, there is a philosophy to integrate and maintain relationships with the private sector to support the needs of the national intelligence architecture. The are 15 private sectors Information Sharing and Analysis Centers (ISAC) considered operational organizations that collect, analyze, and share threat and vulnerability information to protect critical infrastructure.[177] These private sector elements with specialized capabilities can and are being used to address national security concerns and homeland security threat issues. These ISACs[178] are: the Communications ISAC; the Electric Sector ISAC; the Emergency Services ISAC; the Financial Services ISAC; the National Health ISAC; the Information Technology ISAC; the Multi-State ISAC; the Maritime Security ISAC; the Nuclear Energy Institute; the Public Transportation ISAC; the Surface Transportation ISAC; the Real Estate ISAC; the Research and Education ISAC; the

[176] Richard A. Best Jr., Congressional Research Service, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, RL30252, December 3, 2001, 9.

[177] Mark A. Randol, Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, RL33616, January 14, 2009, 14.

[178] National Council of Information Sharing and Analysis Centers, accessed August 10, 2013, http://www.isaccouncil.org/memberisacs.html.

Supply Chain ISAC; and the Water ISAC, all of which enhance information sharing and serve as analytic centers within the private sector.

With the integration of private sector elements into the HSE and their value-added to information sharing, questions arise as to the intelligence cycle process model being trained by the elements mentioned previously. The success of U.S. intelligence at home will increasingly depend on a new form of domestic intelligence collection against specific threats and on the forging of a deep partnership with the American nation, from local law enforcement to the private sector.[179]

Within the governance structure of the National Network, the *Baseline Capabilities for State and Major Urban Area Fusion Centers* provides fusion centers "shall have a governance structure that provides appropriate representation for the jurisdictions and disciplines in the center's area of responsibility," and as an example it reflects "including representatives from…the Information Sharing and Analysis Centers…" in support of Fusion Center Guidelines 3, 4, and 5.[180] In highlighting the role of fusion centers in national security, DHS posits "The national security enterprise must reach beyond the capabilities of the federal government and national intelligence community to identify and warn about impending plots that could impact the homeland, particularly when the individuals responsible for the threats operate within the United States and do not travel or communicate with others overseas."[181] Given DHS I&A's responsibilities as a USIC member, it has the largest customer set than any other intelligence community member.

This thesis summarizes there are no fewer than an estimated 175 federal, state, local law enforcement, and private sector establishments contributing to the responsibility for sharing homeland security information through the conduct of collecting, analyzing

[179] Jennifer E. Sims, and Burton Gerber, *Transforming U.S. Intelligence* (Washington, D.C.: Georgetown University Press, 2005), 198.

[180] U.S. Department of Homeland Security and U.S. Department of Justice, *Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines***,** September 2008, 23.

[181] U.S. Department of Homeland Security, *State and Major Urban Area Fusion Centers*, accessed February 24, 2012, http://www.dhs.gov/files/programs/gc_1156877184684.shtm.

and disseminating threat information based on the number of USIC member organizations, HSIE elements, fusion centers, FBI Field Intelligence Groups, and private sector ISACs. At the federal level, there are 17 members of the USIC; within the USIC there are 56 FBI Field Intelligence Groups as elements of the FBI National Security Branch; three (3) DHS headquarters elements and six (6) operational component intelligence elements that make up the HSIE for a total of (9); at the state and local level there are 78 DHS/DOJ recognized fusion centers; and at the private sector level 15 ISACs. These 175 entities that make up the HSE has received or may receive some form of training on the varied intelligence cycle process models from various federal level, federally sponsored or academic institutions.

The number of intelligence cycle process models, as well as the amount of intelligence consumers, is as varied as the number of intelligence producing entities. Policymakers exist at all levels of government, law enforcement elements operate at all levels of government and other public safety officials provide prevention, protection, recovery, and response resources at all levels of government. Additionally, the private sector, likewise, supports the prevention, protection, recover, and response mission spaces that integrates the business community yet another intelligence consumer. Because of the post-9/11 HSE, these entities now serve as key partners in the first phase of the intelligence cycle – planning and direction. However, a vital question surfaces; who is responsible for determining the planning and direction, as well as prioritizing, what should be collected in order to ensure appropriate finished intelligence is produced and disseminated as an end-result of the intelligence cycle process model? Can the National Network serve as an effective analytic element at the state and local level for such an enormous customer base?

Additionally, with the diverse numbers of intelligence cycle process models and the assorted training venues another question remains; is it appropriate to employ the intelligence cycle process model in an effort to detect significant national security and homeland security threats originating or residing within our nation's borders provide it was not designed and intended to serve as such? Further, is it possible to evaluate the

USIC intelligence cycle process model in the performance of domestic intelligence collection activities at the state and local level in support of the HSE?

A new intelligence cycle process model would provide an opportunity for a more cohesive community of stakeholders who could both exploit training and educational opportunities to the benefit of the collective whole.

E. PRACTICAL CHALLENGES TO EMPLOYING THE INTELLIGENCE CYCLE PROCESS MODEL

Two key challenges to employing the USIC intelligence cycle process model is defining the term *homeland security intelligence* and the lack of access to information necessary to provide a comprehensive threat picture. A challenge to adopting a standardized intelligence cycle process model within the HSE may be associated with the fact the term *homeland security intelligence* has not been defined or codified in law.[182] The closest definition provided by law is the term *homeland security information* provided in the 2002 Homeland Security Act that states it is;

> any information possessed by a federal, state or local agency that (a) related to the threat of terrorist activity, (b) relates to the ability to prevent, interdict or disrupt terrorist activity, (c) would improve the identification or investigation of a suspected terrorist or terrorist organization, or (d) would improve the response to a terrorist act.

There are clear challenges associated with effectively employing initial phases of the intelligence cycle process model - planning and direction, as well as collection - at the state and local level given the independent nature of stakeholders. What element serves as the compromising authoritative body for determining planning and direction for the National Network and broader HSE? What element ensures access to information when it is incomplete due to information sharing disputes between agencies (whether cultural or procedural)? What element shoulders the responsibility to address the lack of standardized training given the various forms of intelligence cycle process models? As argued previously, proper planning and direction, as well as efficient information

[182] Mark A. Randol, Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, RL33616, January 14, 2009, 9.

collection within the HSE, increases the performance of the final intelligence product aimed at providing situational awareness and a common threat picture for all stakeholders.

The U.S. counterterrorism strategy and its implementation have seen little progress since the terrorist attacks of 9/11. The "shared responsibility" proposition has not been fully realized in the sharing of intelligence and threat information at all levels of government or the "whole of government" approach to counterterrorism investigations. This concern directly affects DHS' ability to share intelligence and threat information with state, local, and private sector partners as mandated by the 9/11 Commission Act, particularly given that the DHS State and Local Program Office has a mandated role to support the National Network as state and local intelligence collection and analytical centers.

F. CONCLUSION

Within this thesis, the writer identified several critical moments in U.S. history that initiated major intelligence reform at the federal level, as well as the state and local levels of government. The attack of Pearl Harbor in 1947 and the subsequent involvement in World War II, initiated the creation of the USIC per the 1947 National Security Act. In 1981, President Ronald Reagan issued EO 12333 *United States Intelligence Activities* in order to address domestic intelligence collection abuses by federal level government agencies. During the same general period, the "1983-suits" were legal actions brought against local police intelligence units in the 1960s and 1970s for violating citizen groups' First Amendment rights. This period facilitated the establishment of IALEA and the establishment of 28 CFR Part 23 that provides guidance for criminal intelligence. The tragic and horrible attack on the U.S. by international terrorist on September 11, 2001, initiated the creation of DHS, and subsequently, the DHS I&A State and Local Program Office charged with providing federal level support to the National Network and HSE. After 9/11, the IACP endorsed ILP and the Major City Chiefs' initiated the MCC Criminal Intelligence Enterprise.

Table 2, constructed by the author, provides a visual snapshot of the gaps in synchronizing federal level intelligence initiatives and integration. While the post-9/11 National Network was not established until 2003, history reveals a pattern of addressing domestic intelligence collection issues. Based on the information reflected, one can deduce the timeframe gaps between federal level intelligence doctrine and intelligence cycle process employment and the establishment of local level intelligence guidance and intelligence process endorsement. As an example, there was 24 years from the initiation of the first U.S. Army-wide intelligence doctrine to the first documented intelligence cycle process model [1920–1944] and 27 years until the creation of the USIC [1920–1947]. There was 33 years from the creation of the USIC to the establishment of the IALEA, formalizing efforts to professionalize law enforcement analysts and the establishment of the Regional Information Sharing System operating under 28 CFR Part 23 [1947–1980]. The IACP, which was established in 1893, did not endorse intelligence-led policing until 19 years later in 2002, the same period in which DHS was created under the 2002 Homeland Security Act. In 2007, the 9/11 Commission Act established the DHS I&A State and Local Program Office for the specific purpose of providing federal level intelligence support to the National Network created in 2003. Establishing intelligence training guidance at the state and local level, external to the National Network occurred in 2007 with the Major City Chiefs' establishment of the Major City Chiefs' Criminal Intelligence Enterprise four years later in 2011. The White House supported the intelligence progress at the state and local level and issued EO 13470 in 2008 that amended EO 12333 to include the state and local environment within the U.S. Intelligence Activities guidance, as well as establishing EO 13594 two years later in 2010 that provided guidance for state and local access to national security information. The intent of the aforementioned chronology of intelligence initiatives is to provide a visual snapshot of the gaps between time in the synchronizing of federal level intelligence initiatives and integration of the National Network and the broader HSE.

Table 2. Timeline Reflecting Intelligence Policy Engagement among Federal and Local Environment

Date	Organization	Intelligence Initiative
1920	U.S. Army	U.S. Army-wide intelligence doctrine
1944	U.S. Army	First documented intelligence cycle process model
1947	White House & Congress	Established U.S. Intelligence Community
1980	International Association of Law Enforcement Analyst	Professionalize law enforcement analytic cadre and increase capabilities
1980	Regional Information Sharing System	RISS established and implemented through the Criminal Intelligence Operating Policies at the federal level - 28 CFR Part 23
1981	White House	Established Executive Order 12333 - U.S. Intelligence Activities; provides guidance for U.S. intelligence activities among USIC members
2002	International Association of Chiefs' of Police	Established in 1893; endorsed intelligence-led policing
2003	National Network of Fusion Centers	Established state & local intelligence and information sharing network
2007	DHS I&A	Establish a DHS State, Local, and Regional Fusion Center Initiative necessary for establishing partnerships with state, local, and regional fusion centers; specifically section (b) (11) mandates providing training to state, local, and regional fusion centers
2007	DOJ Global Justice Information Sharing Initiative	Published the minimal criminal intelligence training standards for law enforcement and other criminal justice agencies in the U.S.
2008	White House	Amended EO 12333 via EO 13470 to include state & local environment
2010	White House	Established EO 13549; provided state & local access to classified national security information
2011	Major City Chiefs'	Established Major City Chiefs' Criminal Intelligence Enterprise

In theory, the intelligence production cycle, otherwise known as the intelligence cycle, is the process by which information is acquired and converted into an assessment or estimate begins and ends with the policy maker. Ideally, policymakers advise the managers of the USIC collection and production organization of their informational needs. In practice, it is often up to intelligence managers to gauge and anticipate policy maker's needs because policy makers have never been particularly diligent or effective in articulating their informational needs. Yet, today DHS I&A field deployed personnel not only provide training on the intelligence cycle process model, but they are also requested to manage the intelligence cycle in their area of responsibility to include the sharing of threat-related information between SLTPS partners and the federal government. Throughout the literature review and case study, the writer offered the intelligence cycle process model serves as a theoretical concept allowing academic comprehension by nonintelligence individuals. The writer also reasoned, based on the interpretation of literature, case study to include professional experience and observation, the practical employment of the intelligence cycle process model at the strategic and operational levels within the post-9/11 HSE has not fully been studied in order to evaluate its effectiveness or appropriateness.

This document was intended to provide awareness of employing the intelligence cycle process model and initiate dialogue regarding standardizing an intelligence cycle process within the HSE. The writer acknowledges there are possible challenges with attempting to standardize the intelligence cycle process model. The obvious challenges to the enormous task of standardizing a domestic intelligence cycle process given the numerous and varied stakeholders at the federal, state and local level are identifying who would serve as the principle oversight and/executive agency for standardizing such a training program. While the DNI is the executive agency for the USIC, additional thought would have to be given to integrating the state and local level, as well as the private sector. At the state and local level, the National Fusion Center Association represents the National Network, and they are in an executive position to provide influence for the training requirements. Similarly, the IACP, the MCCIE, and IALEIA serve as influencing bodies for elements external to the National Network. The private sector as critical

elements of the HSE may prove as the most challenging when integrating key elements into discussions of standardizing the intelligence cycle process model.

Another challenge deals with building consensus among the numerous and varied HSE stakeholders regarding the design of an intelligence cycle process model that appropriately addresses USIC intelligence requirements and the intelligence information needs for nontraditional intelligence elements. In proposing and developing a new intelligence cycle process model, considerations must be given to the varying analytic and operational paces of the intelligence, law enforcement, and private sector environments. The timeframe provided for pure USIC analytic and operational differ significantly from the analytic and operational environments of the National Network, the great law enforcement and private sector communities.

In conclusion, drawing on publicly available information from government, academia, and national security consortiums, analysis revealed broad acceptance of the intelligence cycle process model philosophy. However, literature provided by academic and operational practitioners support claims that the intelligence cycle process model is flawed and not practical in the operational environment. This thesis may serve as a basis for recommending additional research necessary for studying the intelligence cycle process model implementation and employment within the HSE and its effectiveness in preventing terrorist attacks and enhancing national security intelligence.

THIS PAGE INTENTIONALLY LEFT BLANK

BIBLIOGRAPHY

A Complex Organization United Under a Single Goal: National Security. http://www.intelligence.gov/about-the-intelligence-community/.

American Civil Liberties Union. "More About Fusion Centers." http://www.aclu.org/spy-files/more-about-fusion-centers.

Berman, Emily. *Domestic Intelligence: New Powers, New Risks*. Brennan Center for Justice at New York University School of Law, 2011.

Best, Jr., Richard A. Congressional Research Service, *Intelligence and Law Enforcement: Countering Transnational Threats to the U.S.*, RL30252, December 3, 2001.

Bigelow, Michael E. "A Short History of Army Intelligence," *Military Intelligence*, July-September 2012.

The Boston Channel. *Effectiveness of Fusion Centers Questioned*, http://www.wcvb.com/news/investigative/effectiveness-of-fusion-centers-questioned/-/12520878/20358362/-/bkveudz/-/index.html#ixzz2aHaeHk5x.

Boston Globe. *FBI Did not Alert State's Anti-terror Unit to Its Probe of Suspected Bomber in 2011*, http://www.boston.com/politicalintelligence/2013/04/25/fbi-did-not-alert-state-anti-terror-unit-its-probe-suspected-bomber/RLHZM6GHRotZ6ciIYxmiKP/story.html.

Breckinridge, Scott D. *The CIA and the U.S. Intelligence System*. Boulder, CO.: Westview Press, 1986.

Carl, Leo D. *The International Dictionary of Intelligence*. McLean, VA. International Defense Consulting Service, 1990.

Carter, David L. U.S. Department of Justice, Office of Community Oriented Policing Services, *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies*, 2nd ed., January 2009.

———. White paper, *The Intelligence Fusion Process for State, Local and Tribal Law Enforcement*, Michigan State University, May 2006. http://www.ncirc.gov/documents/public/intelligence_fusion_process.pdf, 7.

———. *The Law Enforcement Intelligence Function: State, Local, and Tribal Agencies*, http://www.hsdl.org/?view&did=469588.

Cid, David. *Understanding Counterterrorism: A Guide for Law Enforcement Policy Makers and Media*, 2012.

Cilluffo, Frank J., Joseph R. Clark, and Michael P. Downing. *Counterterrorism Intelligence: Law Enforcement Perspectives*. Counterterrorism Intelligence Survey Research. Homeland Security Policy Institute. George Washington University. September 2011.

Clark, Robert M. *Intelligence Analysis: A Target-Centric Approach*. Washington, D.C.: CQ Press, 2004.

CNN. "FBI Agents Interviewed Bombing Suspect in 2011." http://www.cnn.com/2013/04/19/us/boston-suspects-no-links/index.html.

CNN. "Boston Marathon Terror Attack Fast Facts." http://www.cnn.com/2013/06/03/us/boston-marathon-terror-attack-fast-facts.

Connors, Timothy, and John Rollins. Center for Policing Terrorism at the Manhattan Institute. *State Fusion Center Processes and Procedures: Best Practices and Recommendations*. Policing Terrorism Report, No. 2, September 2007.

Council on Foreign Relations. *Domestic Intelligence and the Boston Bombings*, http://www.cfr.org/counterterrorism/domestic-intelligence-boston-bombings/p30557.

Crumpton, Henry A. "Intelligence and Homeland Defense". *Transforming U.S. Intelligence*, edited by Jennifer E Sims and Burton Gerber, 198–219. Washington, D.C: Georgetown University Press, 2005.

CQ Homeland Security. "Fusion Center Hearing." http://homeland.cq.com/hs/.

Dunham, Roger G., Geoffrey P. Alpert. Jennifer E. Davis, and Robert W. Taylor. *Intelligence-Led Policing and Fusion Centers, Critical Issues in Policing: Contemporary Readings*, 6th ed, Waveland Press.

Executive Order 12333. *United States Intelligence Activities* (As amended by Executive Orders 13284 (2003), 13355 (2004) and 13470 (2008).

Executive Order 13470. Further Amendments to Executive Order 12333, United States Intelligence Activities, Part 1 1.1(f), www.fas.org/irp/offdocs/eo/eo-13470.htm.

Flanagen, Sephen J. "Managing the Intelligence Community", *International Security*, vol 10 no. 1 (Summer 1985), MIT Press, http://www.jstor.org/stable/2538790.

Hanson, Stephanie. *Al-Shabaab*. August 10, 2011, http://www.cfr.org/somalia/al-shabaab/p18650.

The Heritage Foundation. *Leadership For America*, http://www.heritage.org/about.

Hulnick, Arthur S. "What's Wrong with the Intelligence Cycle". *Intelligence and National Security,* 21. no. 6. December 2006.

Institute for Intergovernmental Research. *Criminal Intelligence Systems Operating Policies (28 CFR Part 23) Training and Technical Assistance Program,* http://www.iir.com/WhatWeDo/Criminal_Justice_Training/28CFR/.

Intelligence and National Security Alliance. *Intelligence to Protect the Homeland: Taking Stock Ten Years Later and Looking Ahead*. White paper, Arlington: Homeland Security Intelligence Council, 2011.

International Association of Chiefs of Police. *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels*. Alexandria, VA, 2002.

Iowa Department of Public Safety. *Division of Intelligence: Intelligence Cycle*. http://www.dps.state.ia.us/intell/intellcycle.shtml.

Johnson, Loch K., and James J. Wirtz. *Intelligence and National Security: The Secret World of Spies-An Anthology*. Oxford, NY. Oxford University Press. 2008.

Kamarck, Elaine C. *Transforming the Intelligence Community: Improving the Collection and Management of Information*. John F. Kennedy School of Government, Harvard University, IBM Center for the Business of Government, October 2005.

Kimery, Anthony L. *Homeland Security Today*, "DHS I&A Chief Outlines New Vision", May 13, 2010, http://www.hstoday.us.

Law Enforcement Assistance and Partnership. *A Law Enforcement Assistance and Partnership Strategy, Improving Information Sharing Between the Intelligence Community and State, Local, and Tribal Law Enforcement*.

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*. Washington, D.C.. CQ Press. 2003; 2012.

Lyon, Verne. *Domestic Surveillance: The History of Operation CHAOS*, http://www.serendipity.li/cia/lyon.html.

Major Cities Chiefs Criminal Intelligence Enterprise. https://www.majorcitieschiefs.com/pdf/news/mcca_criminal_intelligence_enterprise_initiative_20120329.pdf.

Masse, Todd. Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, RL33616, August 18, 2006.

Mayer, Matt A., and Scott G. Erickson. *Changing Today's Law Enforcement Culture to Face 21st-Century Threats*. The Heritage Foundation. June 23, 2011.

The National Council of Information Sharing and Analysis Centers. http://www.isaccouncil.org/memberisacs.html.

Newsdesk. *Israel Homeland Security*, "A "Pressure Cooker" Warning was Given a Few Times in Recent Years", http://i-hls.com/2013/04/a-pressure-cooker-warning-was-given-in-2004/.

New York Times. FBI Said to Find It Could Not Have Averted Boston Attack, http://www.nytimes.com/2013/08/02/us/fbi-said-to-conclude-it-could-not-have-averted-boston-attack.html?_r=0.

Nolen, Bridget Rose. *Information Sharing and Collaboration in the United States Intelligence Community: An Ethnographic Study of the National Counterterrorism Center*, PhD diss., University of Pennsylvania, 2013.

Office of the Director of National Intelligence. *Leading Intelligence Integration*, http://www.dni.gov/index.php/about/history.

———. Preliminary *Report on the Creation of the Information Sharing Environment*, http://www.ise.gov/sites/default/files/preliminaryreport.pdf.

Office of Homeland Security. *National Strategy for Homeland Security*, July 2002.

Palmieri, Lisa M. *Challenges Facing Law Enforcement Intelligence*, Law Enforcement Intelligence Units and International Association of Law Enforcement Intelligence Analysts, 2011.

———. International Association of Chiefs of Police, "Information Vs. Intelligence: What Police Executives Need to Know", *The Police Chief*, vol. 72, no. 6, Alexandria, VA, June 2005.

RAND. *Predictive Policing – The Role of Crime Forecasting in Law Enforcement Operations, Prediction-Led Policing Business Process Model*, http://www.rand.org/content/dam/rand/pubs/research_reports/RR200/RR233/RAND_RR233.pdf.

Randol, Mark A. Congressional Research Service, *Homeland Security Intelligence: Perceptions, Statutory Definitions, and Approaches*, RL33616, January 14, 2009.

———. Congressional Research Service, *The Department of Homeland Security Intelligence Enterprise: Operational Overview and Oversight Challenges for Congress*, R40602, March 19, 2010.

Rosenbach, Eric. *Confrontation or Collaboration? Congress and the Intelligence Community*. Belfere Center for Science and International Affairs. The Intelligence and Policy Project. Background Memorandum for the 111th Congress. July 2009.

Sims, Jennifer E., and Burton Gerber. *Transforming U.S. Intelligence*. Washington, D.C., Georgetown University Press, 2005.

Sources and Methods: Part 4 – *The Traditional Intelligence Cycle and its History*. http://sourceandmethods.blogspot.com/2011/05/part-4-traditional-intelligence-cycle.html.

Texas Department of Public Safety. *IDP's for Intelligence Analysts at the Texas Department of Public Safety PowerPoint*, www.iafie.org/resource/resmgr/2012_conference/mullins.pptx.

"Targeting Intelligence Gathering in a Dynamic Competitive Environment". *International Journal of Information Management*, vol. 20, no. 3, 2000.

Townsend, Frances. *Intelligence to Protect the Homeland -Taking Stock Ten Years Later*. Intelligence and National Security Alliance, 2011.

U.S. Bureau of Justice Assistance. *Intelligence-Led Policing: The New Intelligence Architecture*, September 2005.

U.S. Central Intelligence Agency. *Training Resources*, https://www/cia/goc/offices-of-cia/intelligence-analysis/training-resources.html.

———. http://vmc.cia-dia.50megs.com/fboi/facttell/intcycle.htm.

U.S. Congress. *110th Congress Public Law, Public Law 110–53, Implementing Recommendations of the 9/11 Commission Act of 2007*.

———. *The Intelligence Community in the 21st Century: Staff Study - Permanent Select Committee on Intelligence House of Representatives 104th Congress*, http://www.gpo.gov/fdsys/pkg/GPO-IC21/html/GPO-IC21–13.html.

———. Statement for the Record Senator Joe Lieberman (Ret) House Committee On Homeland Security, *The Boston Bombings: A First Look*, http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-SchwartzK-20130509.pdf, 2013.

———. *Congressional Testimony of Boston Police Commissioner Edward F. Davis, III before the House Committee on Homeland Security,* http://docs.house.gov/meetings/HM/HM00/20130509/100785/HHRG-113-HM00-Wstate-SchwartzK-20130509.pdf, 2013.

U.S. Defense Intelligence Agency. http://www.dia.mil/university/, http://ipv6.dhs.gov/journal/leadership/labels/Intelligence%20and%20Analysis%20Directorate.html.

U.S. Department of Defense. http://www.dodccrp.org/events/9th_ICCRTS/CD/papers/044.pdf.

U.S. Department of Homeland Security. *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion*. Homeland Security Advisory Council. April 28, 2005.

———. *Roles and Function*, Office of Intelligence and Analysis General Counsel Memorandum, July 29, 2008.

———. *DHS' Role in State and Local Fusion Centers is Evolving*. Office of Inspector General Report – OIG-09-12. October 2008.

———. *The Department Develops Its Own Professional Intelligence Workforce*, January 14, 2009.

———. *Bottom-Up Review Report*, July 2010.

———. *Information Sharing with Fusion Centers Has Improved, but Information System Challenges Remain*, Office of Inspector General Report 11-04, October 2010.

———. *2011 National Network of Fusion Centers Final Report*, May 2012.

———. *Role of Fusion Centers in Countering Violent Extremism*, October 2012.

———. *2012 National Network of Fusion Centers Final Report*, June 2013.

———. *State and Major Urban Area Fusion Centers*, http://www.dhs.gov/files/programs/gc_1156877184684.shtm.

———. *Responsibilities of Intelligence Officers*, http://www.dhs.gov/deployed-intelligence-officers-and-protective-security-advisors.

———. http://www.dhs.gov/more-about-office-intelligence-and-analysis-mission.

———. *Fusion Center Guidelines Developing and Sharing Information and Intelligence in a New Era; Guidelines for Establishing and Operating Fusion Centers at the Local, State, and Federal Levels; Law Enforcement Intelligence, Public Safety, and the Private Sector*, http://it.ojp.gov/documents/fusion_center_guidelines_law_enforcement.pdf.

———. *Target Capabilities List: A companion to the National Preparedness Guidelines*, September 2007, http://www.fema.gov/pdf/government/training/tcl.pdf.

———. Management Directive 8110, *Intelligence Integration and Management*, http://www.dhs.gov/xlibrary/assets/foia/mgmt_directive_8110_intelligence_integration_and_management.pdf.

U.S. Department of Homeland Security and U.S. Department of Justice. *Baseline Capabilities for State and Major Urban Area Fusion Centers: A Supplement to the Fusion Center Guidelines*, September 2008.

U.S. District Court for the District of Massachusetts. Criminal Complaint, *USA v. Dzhokar Tsarnev*, Case No. 13-2106-MBB, April 21, 2013.

U.S. Department of Justice, Federal Bureau of Investigation. Inspection Division Commendation Memorandum to Mr. Roger Stokes, October 27, 2006.

———. Federal Bureau of Investigation. National Security Branch, September 2006, http://www.hsdl.org/?view&did=480684.

———. Federal Bureau of Investigation. http://www.fbi.gov/about-us/intelligence/intelligence-cycle.

———. Global Justice Information Sharing Initiative, *National Criminal Intelligence Sharing Plan*, October 2003.

———. Global Justice Information Sharing Initiative, Findings and Recommendations, *Minimal Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States*, Version 2, October 2007.

U.S. Department of Justice Memorandum. *28 Code of Federal Regulations, Part 23*, March 31, 2005.

U.S. Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities, *Intelligence Activities – National Security Agency and Fourth Amendment Rights*, October 29, 1975, http://www.aarclibrary.org/publib/church/reports/vol5/pdf/ChurchV5_1_Allen.pdf.

Wall Street Journal. "Boston Hearings Delve into FBI Alerts," May 9, 2013. https://www.online.wsj.com/article.

The White House. *National Strategy for Homeland Security*, Washington: The White House, October 2007.

———. *Strategic Implementation Plan for Empowering Local Partners to Prevent Violent Extremism in the U.S.*, December 2011.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center
   Ft. Belvoir, Virginia

2. Dudley Knox Library
   Naval Postgraduate School
   Monterey, California

This Page Is Intentionally Left Blank

governmentattic.org
"Rummaging in the government's attic"

Description of document:	United States Cryptologic History, Sources in Cryptologic History, Volume 4, A Collection of Writings on Traffic Analysis, Vera R. Filby, Center For Cryptologic History, National Security Agency, 1993
Requested date:	02-August-2012
Released date:	11-June-2013
Posted date:	24-June-2013
Source of document:	National Security Agency Attn: FOIA/PA Office (DJ4) 9800 Savage Road, Suite 6248 Ft. George G. Meade, MD 20755-6248 Fax: 443-479-3612 (ATTN: FOIA/PA Office) On-Line Request Form

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

-- Web site design Copyright 2007 governmentattic.org --

NATIONAL SECURITY AGENCY
CENTRAL SECURITY SERVICE
FORT GEORGE G. MEADE, MARYLAND 20755-6000

Serial: MDR-68578
11 June 2013

This responds to your 2 August 2012 request for the declassification review of the following NSA document: *A Collection of Writings on Traffic Analysis*. The material has been reviewed under the Mandatory Declassification Review (MDR) requirements of Executive Order (E.O.) 13526 and is enclosed. We have determined that some of the information in the material requires continued protection from public release.

Some portions deleted from the document are currently and properly classified in accordance with E.O. 13526. The information denied meets the criteria for classification as set forth in Section 1.4 subparagraphs (c) and (d) and remains classified TOP SECRET, SECRET and CONFIDENTIAL as provided in Section 1.2 of E.O. 13526.

Additionally, section 3.5 (c) of E.O. 13526 allows for the protection afforded to information under the provisions of law. Therefore, the names of NSA/CSS employees and information that would reveal NSA/CSS functions and activities have been protected in accordance with Section 6, Public Law 86-36 (50 U.S. Code 402 note).

Since your request for declassification has been partially denied you are hereby advised of this Agency's appeal procedures. Any person denied access to information may file an appeal to the NSA/CSS MDR Appeal Authority. The appeal must be postmarked no later than 60 calendar days after the date of the denial letter. The appeal shall be in writing addressed to the NSA/CSS MDR Appeal Authority (DJ5), National Security Agency, 9800 Savage Road, STE 6881, Fort George G. Meade, MD 20755-6881. The appeal shall reference the initial denial of access and shall contain, in sufficient detail and particularity, the grounds upon which the requester believes the release of information is required. The NSA/CSS MDR Appeal Authority will endeavor to respond to the appeal within 60 working days after receipt of the appeal.

Sincerely,

BLAKE C. BARNES
Chief
Declassification Services

Encl:
a/s

sources in cryptologic history number 4

~~TOP SECRET~~ NO. 114

united states cryptologic history

A Collection of Writings on Traffic Analysis

~~THIS DOCUMENT CONTAINS CODEWORD MATERIAL~~
~~NOT RELEASABLE TO CONTRACTORS~~

Declassified and approved for release by NSA on 06-11-2013 pursuant to E.O. 13526 - MDR 68578

CH-E32-93-05

national security agency
central security service

~~TOP SECRET~~

This monograph is a product of the National Security Agency history program. Its contents and conclusions are those of the authors, based on original research, and do not necessarily represent the official views of the National Security Agency. Please address divergent opinion or additional detail to the Center for Cryptologic History (E324).

Contents of this publication should not be reproduced or further disseminated outside the U.S. Intelligence Community without the permission of the Director, NSA. Inquiries about reproduction and dissemination should be directed to the Center for Cryptologic History, National Security Agency, Fort George G. Meade, MD 20755-6000, ATTN: E324.

UNITED STATES CRYPTOLOGIC HISTORY

Sources in Cryptologic History

Volume 4

A Collection of Writings on Traffic Analysis

Vera R. Filby

CENTER FOR CRYPTOLOGIC HISTORY

NATIONAL SECURITY AGENCY

1993

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

Table of Contents

Page

Foreword vii

Preface ix

A Capsule History of Traffic Analysis 1

The First Quarter Century

Fundamentals

What Good is Traffic Analysis? ..... ROBERT H. SHAW 5
Establishing Communications Norms ..... [redacted] 11
Chatter Patterns: A Last Resort ..... WAYNE E. STOFFEL 15
A Note about NRs ..... [redacted] 25

Views of the Automated Future

Some Thoughts concerning Traffic Analysis Mechanization ..... ROBERT S. BENJAMIN 27
Cleaning the Augean Stables or How Much TA Can a Computer Do? ..... FRED MASON 33
Traffic Analysis or [redacted] Data Transmission Systems ..... [redacted] 41
Traffic Analysts of the Future ..... [redacted] 45

Callsign Stories

[redacted] ..... [redacted] 49
Recovery of a Vietnamese Communist Callsign System ..... [redacted] 71
True Base: Two Tales ..... [redacted] 73
Maybe It's Related to the Phases of the Moon ..... [redacted] 81
[redacted] ..... JAMES D. DELANEY 87

Miscellany

Area Studies and Their Place in Traffic Analysis ..... [redacted] 101

P.L. 86-36

P.L. 86-36
EO 1.4.(c)

The 1970s

Fundamentals

The Reality of Communications Changes 105
A Note about Organizing TA Problems 109
[redacted] 111

Mechanization

Address to Traffic Analysis Mechanization Forum ..... MAJ. GEN. JOHN E. MORRISON 113
Introduction to Traffic Analysis Mechanization .. ROBERT S. BENJAMIN 115
Automation of a TA Process ..... TIM MURPHY 129
How Clean Does a Database Need to Be? 139
The Hand Is Not Quicker than the Eye 141

Traffic Analysis and Mathematics

The Lost Indicator ..... DR. RALPH W. JOLLENSTEN 143
Applications of Set Theory to Traffic Analysis 151
TA, CA, Logic, Math – Where Do They Intersect (TACALOMA) 155

Anxieties

Let's Not Lose Our TA Skills 171
Letters 175

Miscellany

Simplicity in Color ..... C. GAROFALO 179
The Impact of ARDF on Traffic Analysis ..... ALLEN L. GILBERT 181
Barometer – Readers' Comments 183
How Many Angels Can Stand on the Head of a Case Notation? 185

The 1980s and Beyond

Fundamentals

Traffic Analysis: A Current Perspective ..... JAMES HOPPER 187

TA and Computers

There's a New World Coming--Are You Ready? ... [redacted] 195
In Pursuit of: Faster Horses, Younger Women, Older Whiskey, and More Money 199
Computerizing Traffic Analysis 203

Professional Concerns

Traffic Analysis: Specialty without a Portfolio 215

New Areas of Interest

[redacted] 221

Hail and Farewell

The Future of Traffic Analysis 241
Valedictory of a Traffic Analyst ..... JOSEPH STARR 245

Author's Biography 249

Sources and Additional Readings 251

P.L. 86-36

Foreword

If the professional field of traffic analysis has had its ups and downs, the need for its skill and art has never really diminished. Like Mark Twain, its early demise has been reported at regular intervals, but, happily, has always proved premature. Even though the discipline may change as a career field, the value to the cryptologic mission of contributions made by traffic analysis - and traffic analysts - continues.

Captain Duane Whitlock, USN, a veteran of cryptologic activity on Corregidor before World War II, speaking at the 1992 Symposium on Cryptologic History at NSA, emphasized and reemphasized the indispensability of traffic analysis. In that period of crisis before Pearl Harbor, traffic analysis worked closely to support cryptanalysis, and during periods when systems were unreadable, TA constituted the only means of following developments in the armed forces of a potential enemy.

Half a century after the attack on Pearl Harbor, we need to understand that despite more sophisticated collection and processing, traffic analysis still makes basic and vital contributions to the national mission.

Vera Filby has collected a number of thought-provoking articles on traffic analysis into one handy volume. This reader serves many purposes, not the least of which is to stimulate us into considering how the field has changed, what roles traffic analysis has played in the past, and what it can do for the cryptologic mission in the future.

Reduced to slogans, this is a good book for times like these, and these are good times for a book like this.

DAVID A. HATCH
Director,
Center for Cryptologic History

Preface

In 1989 NSA Senior Executive [redacted] proposed the creation of a series of readers in cryptology to make more readily available some of the literature in the several cryptologic disciplines that has accumulated over the years in the National Security Agency. The present collection of occasional articles on traffic analysis (TA) is offered to the cryptologic community as a first contribution to what it is hoped will be a continuing program. The articles reflect the times and circumstances of their creation and thus present a picture of traffic analysis across a span of nearly half a century.

Sources were mainly the *NSA Technical Journal* (published 1956-1981), *COMMAND* (1968-73), *Cryptolog* (1974-present), and *Cryptologic Quarterly* (1981-present). Articles on various aspects of TA, along with letters to the editor and TA problems, published in these and other journals, amounted to some 300-350 pages, making selection imperative. Several of the articles describe TA techniques. Many concern the problems, both technological and professional, attendant on the automation of TA. Others recount TA stories and successes. Some originated as briefings or addresses.

Choices for this collection were hard since almost all the candidates were worthy of inclusion. The selections are arranged by subject within three chronological periods: the first twenty to twenty-five years, the 1970s, and the 1980s. The TA problems were omitted for lack of space. It is hoped they may eventually be published separately.

The items included may seem a scant production for forty-odd years. But they are personal writings, voluntary offerings to communicate ideas, to teach, to present an argument, to tell a story. They are on a quite different plane from the technical and related production of traffic analysis: SIGINT technical reports; astronomical numbers of technical records, supplements, files, messages, working aids, and weekly TA notes; professional studies, reviews, and development plans; and training aids and manuals. A training manual, *Radio Traffic Analysis*, by Robert S. Benjamin, published in 1955, was a major literary production. This exhaustive treatise was the training standard and bible for traffic analysts for many years.

VERA R. FILBY

~~FOR OFFICIAL USE ONLY~~

A Capsule History of Traffic Analysis

THE FIRST QUARTER CENTURY

During the early years of the Armed Forces Security Agency and NSA, little was published to record the development of TA. But in the mid-1960s, evidence of an attention to TA as a discipline and career and concern for its status and future began to appear in written articles. This was in tune with the Agency's growing concern for the state of cryptologic disciplines, which resulted in the establishment of the professionalization program. In 1967 the beginnings of a TA library were established, and in 1968 the Techniques and Standards group, P1, and the TA Career Panel sponsored a TA workshop. Papers presented at its several sessions were later collected in response to a call for TA documentation. In October 1968 the first issue of *Command* was published, and the following year the Communications Analysis Association was formed.

Computers have been used in TA applications since the 1940s, but it was in the mid-1960s that the first wave of the computer revolution began to cause tremors in the work force. Many analysts were distrustful and apprehensive, both for their discipline and for their careers; but others were ready and eager to participate in the development of automation. Communication between analyst and computer programmer was a serious problem. Part of the eventual solution was in training traffic analysts to become computer programmers.

THE 1970s

The momentum begun in the late 1960s led to the Traffic Analysis Mechanization Forum in February 1970, where twenty-four briefings were presented. This was followed by the Traffic Analysis-Mathematics Symposium in May 1971 with twenty briefings. Compilations of these briefings were published in P1.

The level of energy, thought, and activity in the study of traffic analysis declined in the mid-1970s. Automation, decreased need for TA in targets where the communications structure had been largely recovered or where communications had become exploitable, and limitations in Agency fiscal resources reduced the size and depressed the morale of the TA work force. Early retirements, resignations, and moves into data systems, management, and other areas thinned out the ranks. Training requirements fell so low that the sole TA instructor remaining in the National Cryptologic School (NCS) had time for other duties.

THE 1980s AND BEYOND

Although the decline in Agency strength had reversed by the beginning of the 1980s, TA as a career remained at the same level, despite the fact that the volumes of traffic pouring into the data banks continued so vast that much of it could not even be looked at, while at the same time new communications and advanced systems appeared and had to be dealt with. Many analysts were still trying to get used to – or resigned to – computers, and they suffered prolonged frustration and dissatisfaction with systems they found unhelpful. Nevertheless, by the mid-1980s new waves of computerization had swept through the Agency, and a computer environment eventually prevailed.

A growing awareness of a need for cryptologic renewal characterized the early 1980s. The prospect of a future of struggle against new and increasingly complex signals underscored the need to enhance the vigor, skills, and creativity of the work force. It became clear also that future problems would call for multidisciplined approaches.

In the 1980s studies were undertaken to assess the situation and plans formed to deal with it. Programs and projects, both major and minor, were set in motion. One of these was RELOAD. Project RELOAD's stated purpose was to restore analytic and reporting responsibilities to the field, where during many years of centralization analytic skills had weakened. RELOAD became the driving force for rejuvenation and change both at headquarters and overseas, and its effects continued to proliferate throughout the decade.

Under RELOAD, a Traffic Analysis Working Group (TAWG) began in 1986 to examine the traffic analysis career field. The group's final report, presented as the Traffic Analysis Focus Plan in 1989, recorded its finding that major systemic reforms were needed and provided a list of proposals and actions taken. One of the proposals was the creation of an Intelligence Analysis career field combining TA and Intelligence Research -- an idea that had been put forth in earlier years but discarded. This time it was accepted, and beginning in 1987 working groups developed career structures, established professional standards, and identified training needs. Their prolonged efforts culminated in the inauguration of the Intelligence Analysis career field on 1 January 1991.

RELOAD and technical change resulted in a greatly increased need for training. To meet it, the NCS recruited more instructors and greatly expanded the use of adjunct faculty. By 1989 the TA faculty were teaching or developing a total of nineteen courses, and more than forty adjunct instructors were certified to teach one or more courses. To recognize outstanding talent, the TAWG established the Gold Nugget Award; the first was presented in 1989.

The NCS held a TA Curriculum Review in mid-December 1990. During the course of the presentations, it appeared that the prospect for TA in the 1990s ranges from the conventional to the experimental, from traditional net reconstruction and callsign recovery of low-level military targets to invention of strategies for solving the most sophisticated digital signals structures. The need for TA is undiminished, and the challenge for the profession is greater than ever.

Acknowledgment

Thanks are due to [redacted] for her encouragement and support in the making of this collection. Without the access to her files she so generously offered, it could not have been produced.

VERA R. FILBY

The First Quarter Century

What Is Good Traffic Analysis?[1]

ROBERT H. SHAW[2]

What is good traffic analysis? The posing of this question in these words by Mr. G. H. Vergine has raised in my mind a large number of points that while by no means original, seldom seem to be available in one place at one time. This paper is likely, therefore, to take on something of the appearance of a list. I do not apologize; I think a list is needed, and I hope that some of the topics enumerated here will be expanded in workshops to come.

1. To develop the concept of good traffic analysis, it is necessary first to be clear on the prior question of what traffic analysis is, and what its relationship may be to other SIGINT disciplines.

1.1. Historically, SIGINT (or COMINT, as it was almost exclusively at first) was initially conceived as a unified whole, the response of vaguely named communications intelligence entities to the presence of exploitable transmissions. The great growth of communications during and after the Second World War and the great diversification of techniques of transmission, encryption, keying, and read-out, led to an inevitable specialization of the analytic people, and in due course cryptanalysis, traffic analysis, signal analysis, substantive analysis, intercept, collection, computery and all the rest became, first, fields of primary concern to different units, and, later, disciplines of their own. Ineluctably, SIGINT came to be looked at as the sum of autonomous parts rather than as a conveniently divided whole; and now interdisciplinary working is something to be striven for, rather than the obvious circumstance of professional life. All these disciplines are interwoven. A traffic analyst has no vested interest in staking out a preserve of his own called traffic analysis; he has a vested interest in contributing by his own techniques to what is known through all techniques about a target.

1.2. The classic definitions of traffic analysis date from the Second World War. Typical might be that of the U.S. Navy (DNSC5, *Communications Instructions, 1944*, Chapter 4): "Traffic analysis is the obtaining of intelligence from communications by means other than cryptanalysis." This sort of early definition brigades many newer disciplines in as constituent parts of the discipline of traffic analysis and thus creates much jurisdictional controversy today. What about SIT (Special Identification Techniques) substantive analysis, and so on? What about collateral? The confusion is obvious in today's world, where efforts to restrict traffic analysis are resisted by the traffic analyst, and where the main object of SIGINT gets lost in a slather of hurt feelings and administrative slack. It is worth considering that the naming of what one does is of much less consequence than the doing.

---

1. This article was originally published as *P1 Informal No. 10* (T/A #2), dated March 1967.

2. Dr. Shaw, one of the "brightest and best" at NSA and its predecessor agencies, died in early March 1971. See the necrology in the *NSA Technical Journal*, Vol. XVI, No. 2, Spring 1971.

1.3. Technically speaking, the one set of techniques always excluded from traffic analysis is cryptanalysis. At the outset, no one was in any doubt about what that meant: it meant that traffic analysts did not try to decrypt texts of messages. Often they gave information to the people who did; often they gave information to the people who tried to solve the callsign systems; but traffic analysts were concerned with what were called message externals – everything that could be learned about a message and its many kinds of meaning by studying that message in the form in which it was uttered by the originating command or bureau. The raw material of traffic analysis is traffic: messages, chatter, callsigns, times, frequencies, signal strengths, addresses, authenticators, net structures, message lengths, precedences, plaintext transmissions, etc.

1.4. Certain of these raw materials of traffic analysis turned out in the long run to be of sufficient complexity to require the creation of subdisciplines to deal with them. Perhaps the first to come into prominence was the matter of callsigns. Endless reams have been written arguing whether cryptanalysis may sometimes be involved, but that such cryptanalysis is heavily dependent on traffic analytic identification of commands through uses of various callsigns (so-called "continuities"), and that the results of such cryptanalysis are of interest to the SIGINT producing agencies only. The mere labeling of traffic is in itself of no more lasting interest than the discovery that a dash followed by two dots represents the letter *D*. Good traffic analysis identifies continuities, and perhaps even equates them with commands; good cryptanalysis recovers callsign systems from those continuities; the resulting identifications are useful in many ways to text cryptanalysts, to substantive analysts, and to traffic analysts. The nonproducing world is unruffled by even the most brilliant results in this area.

1.5. Traffic analysis has been nibbled away at in another way: a highly automated discipline of signal analysis and SIT has grown up. Spreading from advanced collection procedures on the one hand and from advanced identification and location techniques on the other, this discipline both answers questions and asks them. To the traffic analyst it is a source of very refined raw material. He pays for it by having to pass his results back so that the procedure may be improved. Dealings among traffic analysts, signals analysts, and SIT people are also of local concern only and are valuable only insofar as they enhance the value of the information about locations, movements, actions and intentions, which is the real product of SIGINT and the ultimate justification for a SIGINT effort.

1.6. A principal function of traffic analysis is the determination of the activity of a country, or of a function of that country, by deduction from the characteristics of signals. Plaintext signals can be of considerable help in what they say, in the relationships they imply, and in the essentialia that are not said. It follows that traffic analysts should give grave thought to all the plain text they see, in headings, texts, or chatter. On some circuits there is so much plain text that it can be used as a source of intelligence in its own right, neglecting its origin. It was to deal with this situation that the discipline of substantive analysis was created and set apart from traffic analysis. The relationship of a traffic analyst to substantive analysts should therefore be that of information exchange: the traffic analyst refers a wordy circuit to the substantive analyst, who in return tells the

traffic analyst what commands, or what kinds of commands, are talking, and what those commands are up to. Once again each helps the other, and their mutual conversation in its raw form is not of interest outside the producing community.

1.6.1. On circuits only lightly involved in plain text, the traffic analyst must expect to do both jobs.

1.6.2. Particular note should be made of the great desirability of [redacted] Cryptanalysts, traffic analysts, and substantive analysts have a common interest in this project and should have equal opportunity to contribute to it. The results may show up anywhere, so that the files should be generally accessible within the producing community.

1.7. And that reminds us that people are forever telling traffic analysts something relating to their problem. This so-called "collateral" is intended to assist the traffic analyst in the interpretation of what he sees. There is a tendency on the part of many traffic analysts to busy themselves at once to confirm or deny the collateral. This rather misses the point, although occasionally it is possible and valuable to do so. Collateral is *already* known; one must not expect to make the welkin ring by repeating it aloud, even if it is not contradicted by indications in the traffic. The collateral is made available to the analyst so that something new may emerge. *Verbum sap*

2. What, then, should good traffic analysts be doing? When we know that, we can evaluate their work meaningfully.

2.1. They work toward the identification of stations and, through them, of commands. In the course of this, they may be lucky enough to uncover previously unknown subordinations (so-called "order of battle"), although there is a continuous and active danger of confusing communication with command. The real purpose of these identifications, apart from an occasional new and unexpected recovery, is.

2.2. The establishment of continuity. The purpose of continuity is to permit the following from day to day of the traffic of a known command, in order to find out what that command is up to. The study of the activities of known commands is a principal justification for traffic analysis.

2.3. There are by-products at this point, prominent by-products that have a tendency to become primary objects in the minds of analysts. One of these by-products is the material necessary to solve callsign systems. No one outside the producing community cares about this, in spite of the number of reports one sees. (Have you ever considered the probable reaction of the secretary of defense on learning that today the Second Field Army is known as 7X03? He is unlikely to declare a national holiday.) Another is the material necessary to analyze the activity of the commands. This also is of internal interest only. (Go ahead; *tell* the secretary of defense that 7X03 had 114 messages today but only 111 yesterday, and see what he says.) If consumers demand reports of such material, they are

very specifically criticizing the performance of the traffic analysts; they are, in fact, telling the producing agency that it has done an incomplete or incompetent job.

2.4. Traffic analysts should make every effort to be current. Working with the superficies of traffic, they are generally dealing in transient operation phenomena, and nothing is so old as yesterday's newspaper.

2.5. They support other SIGINT activities. They provide cryptanalysts with link data and with busts; they provide signal analysts with confirmation; they provide substantive analysts with material. They must not stop reading when they come to a BT; to do so is to create a jurisdictional stupidity which, if persisted in, can undo any meaningful understanding of the traffic.

2.6. They produce intelligence (or, in the common barbaric jargon, "intelligence information"). That means something beyond listing the raw material from which intelligence may be generated, something beyond wild guessing about the meaning of observed phenomena. (Navy readers will recall with glee the WWII TA report that the U. S. Navy had got a new, secret ship capable of incredible speed, "Heard off Cuba at 0913A, it was heard again at 1753Z at Port Lyautey; its callsign today is NERK.") It is not even the writing up of an intellectual marking signal: "We are still here, but we can't think of anything to say." Silence is golden; it takes more than gold, therefore, as openers for the silent mouth.

3. It might be said, therefore, that good traffic analysis is

3.1. *Traffic analysis.* It is not reporting, remembering, reviewing, or regurgitating. It is not a listing of phenomena. It is not the publication of intelligence of interest only to producers. It is information about the doings of organizations, information pertinent to the decision-making function of executive departments of our government.

3.2. *Defensible.* Any piece of TA output should have an *apparatus criticus* that will be fully explanatory and that will stand painstaking examination. Without it, a TA report is an unsubstantiated guess that will simply promote wild speculation and bring its originator into disrepute.

3.3. *Timely. Verbum sap.*

3.4. *Informative.* It may even contain predictions; this is greatly to be desired, if the predictions are carefully thought out and carefully justified. Predictions of routine communications/changes are, of course, beneath contempt except as working aids; predictions of fluctuation of target activity can be of the greatest value. Defensive traffic analysis predicted the Okinawa invasion and permitted the JCS to reschedule what might otherwise have been a disaster.

3.5. *Comprehensive.* The traffic analyst has the broadest scope of any SIGINT professional. His raw material is anything transmitted (except the plain texts of encrypted messages; if he can get them, he can use even those). It should never be said of a TA result that it failed to consider some known fact. A good traffic analyst, therefore, is a

person who knows how to balance comprehensiveness and timeliness: he is not panicked into publishing raw material, nor is he coerced into over-researching an item whose value lies in its immediate delivery

3.6. *Concise.* There is little to say that cannot be said in ten sentences. The footnoting, of course, can (and probably often should) take up a dozen pages, but the point of the item should be seen at once.

3.7. *Accurate. Verbum sap.*

4. What I am really suggesting is that the traffic analyst should begin each day with sixty seconds of meditation on what he is going to do, and end it with sixty seconds of meditation on what he has done. And honesty is a great virtue.

Establishing Communications Norms

P.L. 86-36

[redacted]

Communications norms can be described as what traffic can be expected, when it can be expected, and how it can be expected. The establishing of communications norms (referred to for the remainder of this paper as norms) is one of the most underrated procedures in COMINT. It is probably because the techniques in establishing norms appear so self-evident that analysts seldom "have time" to really know their target.

One might ask, why establish norms? In a period of high intercept volume and low analytic resources, it is often said, "I don't have the time – other things are more important." Well, let's take the time here and see if other things really are more important. To do this, you would just have to pin the analyst down as to what are the other things that are more important. After much hesitation and more vague and nebulous statements, you will probably find that the analyst is referring to what I'll call the production of "obvious intelligence." Obvious intelligence is what can be derived from a message after it has been converted to plain language. This is not intended to imply that obvious intelligence is not important, but frequently (too frequently) our translations do little more than provide a consumer with the same information he has either already received or will soon receive from a non-COMINT source. Somehow, competition with the press doesn't seem to be one of the Agency's objectives.

Obvious intelligence as defined above is available to anyone who can read. Once received or reduced to plain language, there is not special talent in deriving intelligence. On the other hand, there is very valuable intelligence to be derived by what is not said or in what is said in a different manner than usual. This type of information I'll call "subtle intelligence." As communications stand-downs are often the first indications of an imminent crisis, abnormal communications also have great potentials as sources of valuable intelligence. The unique and most important aspect of abnormal communications is that usually they provide intelligence not otherwise available – even by reading the messages.

Communications norms can only be established over a period of time as opposed to instant intelligence, which can be derived from reading a message. This is another reason why most analysts prefer and practice the "get rich quick" technique of rapidly searching through haystacks to find the one needle (which may or may not even be there) that will spell out "WAR WILL BE DECLARED TOMORROW." Should such a message ever be found, it would probably still be necessary to turn to a traffic analyst to find out who sent it.

While all abnormal communications may contain intelligence, it may not always be valuable intelligence. Each abnormality must be subjected to an evaluation of why it deviated from the norm. The traffic analyst would be well advised to consult other

professionals prior to reaching any conclusions as to why. At the same time, however, he should be very conscious of the fact that in the vast majority of cases he is better qualified to interpret COMINT phenomena than the consumer. He should take care to insure that his interpretation is restricted to COMINT facts.

Having discussed what norms are and why it is desirable to establish them, let's turn to how we establish norms. In the words of one of our former directors, "First there must be a signal." However, because of the restricted subject of this paper, all future discussion will be made under the assumption that the analyst is working with individual groups of homogeneous traffic.

Some care must be taken to distinguish between establishing norms and recovering technical data such as those used for TEXTA.[1] For example, a group composed of control and six outstations may appear as control and four outstations when examined from a "normal working" point of view. Likewise, certain frequencies may appear on TEXTA that would not appear on a normal frequency study. A large volume of traffic is not necessary to recover TEXTA data, but norms are established more easily, and they are more dependable with large volumes of traffic.

Since it was assumed that the analyst is working with traffic identified to case notation, recovery of calls, frequencies, etc., will already have been made and recorded on TEXTA. The analyst's job is now to determine the normal working. The different types of sorts in which the traffic can be put are numerous, and it would be beneficial to investigate various machine programs to do the bookkeeping.[2] Short of using a machine program, however, a good basic approach is to put each case in date order. A further breakdown of time within date is helpful and often recommended in training manuals, but past experience has revealed that the benefits gained are usually not as great as the cost in the additional time required. Specific norms are not established with the same degree of ease, and the types of sorts and logs used are dependent upon what norm(s) the analyst is attempting to determine.

Initially, traffic from each case notation should be examined separately. A log listing date/time of intercept, frequency, and actual contact is a good start. Having logged the above information, the analyst should begin analysis of the logs in an attempt to answer questions that would enable him to determine the norm. The specific questions to be answered are limited only by the imagination of the analyst, but discretion should be used to insure that the answers to each question will be worth the effort required to find out. The above-mentioned discretion is a very important ability of an analyst. Intelligence of some sort can be obtained from every bit of information, but its value is a factor of the probability of the occurrence of the conditions under which it will be useful. In other words, don't analyze solely for the pleasure derived in performing analysis.

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

1. TEXTA means Technical Extracts of Traffic Analysis. A system of recording and maintaining a database of technical information on communications targets.

2. Traffic Analysis Processing System (TAPS) and TANGERINE.

First, let's look at some of the items that can be determined by looking down the date of intercept column. A simple visual examination will reveal any "missing" dates during the period being examined. The missing dates will often show a pattern. A common pattern is no traffic every seventh day, and a comparison of the pattern and a calendar will probably reveal that the missing days are Sundays (or whatever day of the week the people of the target country consider the Sabbath). Don't be concerned if there are no missing days of intercept; communications of more advanced targets are active seven days a week. Either way you have just established your first norm – the group normally operates seven days a week or the group normally does not work on Sunday. At this point the analyst is cautioned to make sure he understands the working of his intercept source. This common pitfall can best be illustrated by the analyst who had established the norm that the group he studies operated only five and a half days a week closing down at noon on Saturday until Monday.

PPLL 886386
EE001144(¢¢)

Examination of the time of intercept column of the log will show the normal hours of operation and schedules. Once again as mentioned above, care should be taken not to recover the intercept source's hours of operation. Often the difference between the time the group begins operation and the time it stops is the same as the hours of a regular day's work or at most maybe sixteen hours a day (two eight-hour shifts).

Schedules are not as easy to establish as hours of operation. The main reason for this is that rarely does the analyst have the benefit of cast-iron coverage. A good intercept operator often makes up for sparse cover. He notes when he hears his target, and the next day he will usually be looking for that case at the same time. This results in the same approximate time being recorded for several days in a row, and it also establishes another norm. The other side of the coin is also true, however. Certain elements in collection management in our agency have caused a great deal of emphasis to be placed on the "productivity" of our intercept positions. Often this results in undesirable pressure being brought to bear at the source of intercept. In their efforts to make their positions productive, analysts spend less time searching for new schedules and placing more and more reliance on the few already recovered.

Another hindrance in establishing schedule norms is that operators at sites will often copy only "messages." Several receivers are used simultaneously and known schedules are checked out, but unless a message is being passed there is usually nothing to indicate to the analyst that the group was active at such and such a time. The disadvantage here is twofold. First, while the intercept operator may know when to look for a certain group, the odds are high that the analyst is not aware of the schedule. Second, after the norm has been established, a missed schedule by the target (which should have high intelligence value) would appear to an analyst exactly the same as the group coming

up on schedule but not passing a message (probably of no great intelligence value) and therefore heard but not copied by the intercept operator.

Schedules are much more difficult to an analyst than they are to the intercept operator. Often a good tech exchange letter to the source expressing the analyst's views and asking specific questions will help establish schedule norms very quickly.

Analysis of the frequency column of the log will increase the list of norms, which should be getting fairly large by now. The frequency normally employed can be easily determined by visual observation, but to establish norms beyond this, it is usually necessary to analyze the frequency column in conjunction with the date, time of intercept, and/or call-up columns. The same is true of the call-up column. In isolation, analysis will show only those stations that are normally contacted, but these norms can be refined greatly by further analysis between two or more columns of the log.

With relatively little effort so far, the analyst has managed to build up quite a set of norms. The log can now be expanded to include message headings and a column for type of traffic. The columns to be used for the message headings will vary, but almost all will include message number, precedence, date/time of origin, addresses, originator, and group count.

Without going into the detail given in the first part of the log, it should be noted that certain norms can be established by analysis of each column in isolation, but the possibilities are almost unlimited when analyzing each column with one or more other columns.

As was stated earlier in this paper, different norms are established with varying degrees of difficulty. There will be absolutely no doubt about the validity of certain norms. Others may be questionable, but the exercise of trying to establish norms will allow the analyst to identify those areas that need more intercept and analysis. This should result in better tech exchange and support and thereby make better use of collection resources.

Once the norms have been established, the analyst can quickly scan the daily intercept (without logging) and with a high degree of confidence separate the small percentage of abnormal traffic. The remainder of his time can be sent interpreting the abnormal traffic and thereby coming up with valuable unique intelligence.

P.L. 86-36

[redacted] in a lecture to our senior intelligence class, once said if he had three wishes they would be (1) to know everything in the world, (2) to be able to report it to parties capable of doing something about it, and (3) to have them believe it. Establishing good communications norms will enable to traffic analyst to continue to provide the intelligence community with unique intelligence when the linguist and cryptanalyst are truly stumped. At his point, the problems are just beginning as we are faced with the problem of "having them believe it," but, oh, what a wonderful problem with which to be faced.

Chatter Patterns: A Last Resort

WAYNE E. STOFFEL

A possible method of identifying radio operators by their reaction to standard situations occurring in chatter, for use when conventional techniques fail.

BACKGROUND

The success or failure of most traffic analysis problems depends primarily upon the analyst's ability to achieve continuity.[1] Simply defined, continuity involves bridging a communications change by equating a given element appearing before the change with a different element appearing after it. The term continuity refers to the discovered relationship between the given element and its replacement, *without reference to the underlying meaning*. For example, we may by various methods discover that callsign ABC during November was replaced by DEF during December, and thus achieve continuity from ABC (November) to DEF (December). Note that the time factor is intimately involved in the relationship between ABC and GHI is more accurately termed an equation or co-location and is not a continuity in its pure sense. Continuity can exist between ABC and DEF without any knowledge of the location, identity or function of ABC or DEF. The importance of the distinction between continuity and other forms of equation lies in the fact that once any knowledge is gained about ABC, it automatically applied to DEF (and vice versa). If we discover that ABC served the Chief of Staff, 12th Division, Greenville, for his contacts with subordinate regiments on the Division administrative/logistic net, this information applied to DEF, in toto. On the other hand, about GHI we can only say (with any certainty) that it is located at Greenville. (Depending upon the type of equation made between ABC and GHI, we may further be able to say that GHI also serves 12th Division *or* that it also serves an administrative/logistic function).

A direct cryptanalytic analogy to continuity can be recognized by considering a simple substitution system involving a matrix with changing coordinates. For example, the following matrix has been recovered for 1 April:

1. A number of countries today go to surprising lengths to suppress in their communications system distinctive characteristics that might serve to disclose their identity. Among the more common methods of suppressing characteristics is that of frequently changing certain communication elements, such as callsigns, frequencies, schedules, procedure, routing, and address symbols. Since it is often necessary for the traffic analyst to study several months of material on a given net before concrete intelligence results can be developed, and since communications elements may change as often as twice each day, he must, somehow, find a way to nullify the effect of these frequent changes in order to pull homogeneous material together for study. He may note certain characteristics that do *not* change frequently (for instance, that a given station sends a distinctive service message each day at 1100), which can serve as identifying features. When he is successful in nullifying a communications change, the traffic analyst refers to the result as *continuity*.

	4 2 1 8 • • •
2	A D R L • • •
9	P B O C
3	M - E T
1	- K N -
•	•
•	•

On 2 April, assumption of the probable word "**ATTACK**" yields.

47	23	23	47	63	55
A	T	T	A	C	K

	7 5 - 3 - - -
4	A D R L • • •
6	P B O C
2	M - E T
5	- K N -
•	•
•	•

It can then be stated, if the assumed word "**ATTACK**" proves correct, that row coordinate 4 on 2 April *is continuity of* row coordinate 2 on 1 April. It can also be shown that cipher value 57 on 2 April *is continuity of* cipher value 14 on 1 April. In this second case, we have achieved continuity without knowing what the actual plain value is. Finally, we can say that cipher value 43 on 2 April is continuity of cipher value 28 on 1 April. In this instance, when 43c (2April) = 28c (1 April) is proved, and 28c (1 April) = Lp, then 43c (2 April) = Lp.

The more frequently an element changes, the more important continuity becomes (since it is virtually the only consistent method for achieving enough depth on a given element so that a study of its underlying nature and purpose can be undertaken), and the harder it is to get. Most of us can sympathize with the unfortunate analyst whose formerly stable problem suddenly adopts twice-daily changing callsigns, frequencies, addresses and discriminants.[2]

On problems involving fast-changing elements, continuity is usually achieved by means of whatever characteristics are available that can be trusted to be unique. If many are available, the easiest, fastest or most economical methods are, of course, tried first,

2. Traffic analysts will recognize that, for the sake of simplicity, the complexities of the various classes of equations and their accompanying validations have been avoided in this presentation. Other readers are warned that many validities have been avoided in this presentation. Other readers are warned that many a "Donnybrook" can and does develop between traffic analysts on these very factors.

while the more intricate and time-consuming methods are held in reserve for tough cases. It often happens that certain nets develop a stubborn streak that defies description (in mixed company) and, despite application of the most time-consuming routines, manage to remain intact and featureless.[3] Where all else has failed, the analyst may well find the following proposed routine useful.

INTRODUCTION

Most people are creatures of habit, particularly when performing a routine task, and radio operators are no exception. There have been considerable experimentation with and study of the variable characteristics of a Morse operator's transmitting habits or "fist" in an effort to develop a systematic process of recording and analysis which would permit ready recognition of the individual at the key. There is, however, a large area of variable operator habit which has remained virtually unexplored during recent years: habitual operator characteristics as displayed in routine chatter exchanges.

A good many traffic analysts can recall a specific instance where a unique or rare procedure signal was consistently used by a certain net or station and, in the last resort, could thus be relied upon to identify its user. There may be few, however, who can recall conducting a comprehensive and systematic search for such characteristics in order to achieve continuity and identification.

What follows is an outline proposal for a routine of systematic search for unique chatter or conversation characteristics that can be used for continuity or co-location purposes. For the most part, specific details are avoided except for examples, since they will vary from problem to problem. It will be seen that the routine is not readily usable on large problems, and may, in fact, be suitable only on limited problems where the area of inquiry is relatively small and all standard methods of achieving continuity have failed. An obvious prerequisite would be a significant volume of activity transmitted by the stations under study, with some assurance that a fairly complete (preferably verbatim) copy of chatter has been recorded by the intercept operator.

BASIC ASSUMPTIONS

It can be empirically demonstrated that regardless of the degree of conformity enforced by the target's COMSEC service, different operators use different operators use different combinations of procedure signals to express the same ideas, but that each operator tends to be consistent with himself.

3. This situation tends to exist to a greater or lesser degree on most problems, although it can can be appreciated that the point is ordinarily glossed over in discussion unless the words "additional personnel" are injected into the conversation at a suitable point.

The writer's contention is that these habits are more widespread than is generally supposed and that, under admittedly special circumstances, a systematic routine will disclose a sufficient number of them to permit continuity to be developed.

Expert chatter readers will recognize that operator chatter must be treated as a distinct, albeit peculiar, language.[4] Despite the best intentions of the signal officer who compiles an extensive set of procedure signals for radio operations, the "plain" side of his "code" is generally restrictive. In actual operational use, a given procedure signal (prosign) tends to lose its rigidity and takes on a more general *concept* or *idea* form (particularly where it is used so often as to be easily recognized without "looking it up"). Thus the prosign QTR can be shown to have the fixed meaning ("The correct time is – hours"), whereas in actual usage among experienced operators, it embodies the general concept of *time* and is so used in a wide variety of contexts.[5] Complementing the tendency of experienced operators to generalize prosign meanings is the equally strong tendency to minimize and abbreviate words and prosigns in order to conserve both time and energy. "Ham" chatter displays this quite clearly.[6] It is not difficult to visualize how a relatively isolated segment of a radio network could gradually evolve a "local dialect" distinct from that of the rest as a result of improvisation under these pressures. Certainly a regimented COMSEC system with a firm domination over the radio schools could suppress some of this variation, but if we confine ourselves to studying experienced operators, it is likely that some recognizable variance and individuality will occur.

A SAMPLE PROBLEM

If distinctive operator habits do, in fact, exist, how do we go about finding and recording them? Evidently, if a way can be found to catalog the *situations* that confront a radio operator most frequently, we can collect his *responses* to any given recurring situation and by observation determine whether his reaction is fixed by habit or is variable. For example, we might select as a favorable starting point several hours of intercept between station A and station B during which a number of messages were sent by each station. As a recurring situation, we might select *message transmission* and further restrict our examination to the station responses during the period immediately before starting each message. We might find

4. A more precise analogy has been suggested that compares chatter to a codebook usage wherein (a) the vocabulary is not precisely suited to the material being encoded and (b) the code is large enough so that code clerks tend to use combinations of common, memorized groups in preference to rarer but more precise and economical groups that must be looked up each time they are needed.

5. For example, the interrogative for "QTR?" is listed as "What is the correct time?" The prosign QSY means "I shall send on ___ kilo[hertz] and its interrogative form (QSY?) is interpreted as "On what frequency shall I send?" or "Should I change frequency?" The compound "QTR QSY?" may well be used to mean "When should I change frequency?"

6. For example, the prosign "CUL" is a "Ham" contraction of "See or contact you later."

Example 1

A: *QTC*	(I have traffic for you.)
B: GA	(Go ahead.)
A: C AS	(Yes, stand by.)
B: C	(Yes.)
A: BT	(Break Sign – attention, etc.)
A: NR.....	(Goes into preamble.)

Examination of the same basic situation a short time later when station A was again about to transmit a message showed that after receiving "GA," station A again said "C AS" (Yes, stand by) and after receiving the affirmative from the other end began his transmission with a break sign. A third message still later in the same schedule begins with the same exchange, and it now begins to look as if we have found a starting point.

A quick look at the activity of station B shows that the two messages it sent were also preceded by identical chatter exchanges.

Example 2

B: QTC AAA	(I have an "AAA"[7] message for you)
A: AS	(Stand by)
B: C	(YES)
A: GA	(Go ahead)
B: C AS	(Yes. Stand by)
A: C AS	(Yes. I'll stand by)
B: C (pause) BT	(Yes. Break sign – attention)
(Then into preamble)	

Let us now examine what we have so far in the way of possible habits:

(a) When *offering* a "QTC," both station A (Example 1) and station B (Example 2) sent "C AS" after receiving "GA" from the other end. Each then preceded the preamble with "BT," but station B (Example 2) used the compound "C (pause) BT."

(b) When receiving a "QTC," station A (Example 2) responded with "AS" before giving the "GA," while station B (Example 1) gave "GA" immediately. When responding to "C AS," station B (example 1) gave the brief answewr "C," while station A (Example 2) used what may be a variant form – "C AS."

Later the same day, another exchange of messages is found between stations A and B. During this later schedule, two messages from station A are preceded by

7. "AAA" in this instace refers to type or priority of message (e.g., "2nd priority" or "service").

Example 3

A: QTC
B: GA
A: C (pause) VVV QTC
(goes into preamble).

and one message from station B is preceded by

Example 4

B: QTC
A: GA
B: C AS
A: C
B: C (pause) BT
(goes into preamble)

It is quickly seen that the behavior of station B is essentially unchanged but that of station A shows no parallel with what went before. Our choice at this point is quite simple – either station A has changed operators or the "habit" is not sufficiently strong. The resourceful analyst would study carefully the chatter exchange during the opening of this second schedule for any evidence of a new operator at station A (extensive tuning, authentication, etc). If the "new operator" hypothesis does not appear sound, other types of habit must be sought. On the other hand, if it *does* appear sound, examination of suspected continuities from previous or successive dates should show whether the time of change is fixed (i.e., the end of one duty tour and the beginning of another). It would appear that once the duration and change times of operator shifts can be established, analysis can proceed at a much faster rate, since the change times will allow the analyst to sort activity for any given date into tentatively homogeneous groups.[8]

Thus far, our accumulated results are far from impressive. Where can we look for other habits? Two situations obviously related to the one examined above would be the area immediately following the message (message closure and receipting exchange) and any "in-text" servicing (receiving station interrupting to ask for repeats while the message is still being transmitted) or "post-text" servicing (after the message is finished but before receipt is acknowledged), but there must surely be other areas that could be equally profitable.

TYPICAL SITUATIONS

We may find it useful to consider a typical schedule between two stations and examine the successive situations that confront the radio operator. Since certain of these will tend to recur within the same schedule (e.g., opening traffic, as in the example above), while

8. Some care must still be exercised in watching for cases where extra operators are put to cope with heavy traffic volumes, or for any other situation having the same effect.

others by their very nature will tend to occur only once in any given schedule, it is convenient to distinguish between the two *types*, since the former is much more useful as a starting point (one is bothered less by possible operator changes, and only one schedule is generally needed for initial isolation of a tentative habit) while the latter comes into use, for the most part after some initial foothold has been achieved. For purposes of convenience, we shall call the former *primary* and the latter *secondary habits*.

2. Tuning

Immediately after initial contact, various adjustments of tone, power, and frequency must usually be made before reception is considered good enough for the transaction of business. The exchanges may range from a short, terse and businesslike operation to a long, temperamental and often humorous argument. Unless they occur frequently, these longer-winded battles are of little use to the type of study being described,[9] and attention should be concentrated upon the shorter and more lucrative exchanges.[10] The first schedule after a frequency change usually contains much more tuning chatter than do subsequent schedules on that same frequency.

3. Recognition

Recognition exchanges may occur with or without a specific system such as an authentication chart or table of challenges and responses. They are most often seen on the first schedule after a new operator comes on duty, although some signal plans seem not to require their use unless messages are to be exchanged, while others obviously specify such use on every schedule. Many experienced operators prefer to rely on aural recognition of "fist" characteristics and frequently ask the other end to "send V's" (QSV) or adopt *some* other device toward the same end.[11]

4. Opening Traffic

The exchanges treated in some detail (see examples 1-4) may be preceded by statements from *both* operators that they have traffic to be transmitted. In this situation, agreement must be reached on an order of transmission, and such an exchange may be a good source of secondary habits.

5. Preamble and Text Handling

This category embraces a wide variety of characteristics, some of which are generally recognized as useful. In order to find *operator* habits, one must recognize that the operator

9. Except, of course, for the laudable purpose of recreation.

10. In analyzing these exchanges, it is useful to remember that frequently the operator does not have direct access to the transmitter itself and must relay adjusting instructions to a remote transmitter site by telephone.

11. This use of QSV should not be confused with the more extensive use during tuning or equipment adjustments. When the sending occurs early in the schedule, it is not always easy to distinguish between the two, but its use in the recognition sense is usually unmistakable when, during later operations, consistent mis-encipherment of procedure, etc., arouses clearly recognizable operator suspicions about an operator's identity.

is here working from a printed or written record, so that the order of preamble elements, for example, is controlled (in most problems) by their arrangement on the message form while breaks and separators may generally be attributed to the operator himself. Here also belongs the situation where the operator realizes he has mis-sent a portion of the text, sends an error sign, and corrects the mistake. In this category, one is most definitely at the mercy of the intercept operator, and one is likely to find him completely absorbed in copying the text (to the exclusion of nontextual transmissions).

6. "Break-in" Servicing

The receiving operator, under signal instructions, is allowed to "break-in" during text transmission to ask for verification or repeats of certain passages which he has missed or which seem doubtful. Where this happens (and where the intercept operator provides a verbatim record of the exchanges), primary characteristics may be found, since a number of prosigns are usually available for use in this situation, and requests for repeats can and do take several forms.

7. Closing Traffic

Most signal instructions will provide for some prosign such as **BT**, **BK** or **K** to mark the end of text, but some operators use additional compounds for emphasis, or to remind the other end that there are still more messages to be transmitted. As special case, traffic sent by broadcast methods is usually sent twice, and the procedure used to separate the two consecutive transmission frequently shows strong habit patterns.

8. Post-Message Servicing and Receipting

From the transmitting operator's point of view, a given message has not been "cleared" until the other end officially receipts for it. If the other end is not satisfied that his "copy" is correct, he will not give a receipt (**QSL**) until he has verified the questionable passages. Although the situation is slightly different from that described in "Break-in Servicing," habits found in one situation would be likely to show up in the other. As a special case, servicing may be asked for during a later schedule and, if it can be shown that the message has already been "cleared" (i.e., that a **QSL** was given), this "late" servicing may well result from an inability to decrypt the message.[12] The servicing request in this instance may differ from "break-in" or "post-message" servicing only to the extent that the involved message must be clearly identified (i.e., by serial number or other unique indicator).

9. Breaks, Waits, and Interruptions

We are here concerned, not with pauses that appear to be a fixed part of habits rising out of other situations (i.e., the pause before message transmission as shown in the first examples above), but rather with the nonroutine or unexpected interruptions that cause temporary or permanent breaks in a given schedule. Among the situations that can be

12. Such information might be particularly useful to the cryptanalyst.

expected to produce habitual responses [13] are intervention of other schedules, equipment failures, interference, operator changes, shortage of transmitters and interruptions by other stations.

On especially long waits, the transmitting operator may key certain characters or compounds to "hold" the other end, in the general sense of "Hang on, I'm still here" or "Keep listening, I'll only be another minute or so." The actual signals sent during this "hold keying" may well be unique to each operator, but again we are dependent upon verbatim intercept copy if this characteristic is to be used.

10. Next-Appearance Discussions

Once the business of a given schedule has been transacted and the schedule is about to be terminated, some mention is usually made of the next appearance. Where contact times and frequencies are predetermined by the signal instructions, this mention is not likely to exceed a very perfunctory "Watch for me; I'll watch for you." On the other hand, the discussions may well involve times and frequencies. Either situation will yield useful secondary habits. As a special case, satisfactory contact may not have been achieved, and ensuing discussions about another time and frequency may yield significant habits if the situation recurs.

11. Sign-Off

The actual termination of a schedule frequently involves a little ritual that is difficult to describe to one who has never heard it. Between operators who are used to working with each other, it is usually fairly rapid and highly stylized.[14] While this area should not be ignored as a source of habits, a departure from the routine specified in the signal instructions is frequently the result of tacit agreement between *both* operators and must be treated accordingly.

12. Special Circumstances

The above categories obviously do not complete the list of situations which may be useful on any given problem. If the net under examination regularly changes frequencies in midschedule, the chatter exchanges before and after each change merit some observation. Another special case involves the use of a matrix or table for prosign encipherment. Aside from the obvious benefits such a system can provide where local usage makes it effective for net or complex identification, the *use* of each *cell* in the matrix can be likened to the use of a comparable *prosign*. Thus, habitual use of certain cells or the formation of various compounds is just as useful as the prosigns themselves. This principle

13. Obviously, interruptions caused by flood, fire and other emergencies cannot be expected to appear often enough to be a fruitful source of habitual responses.

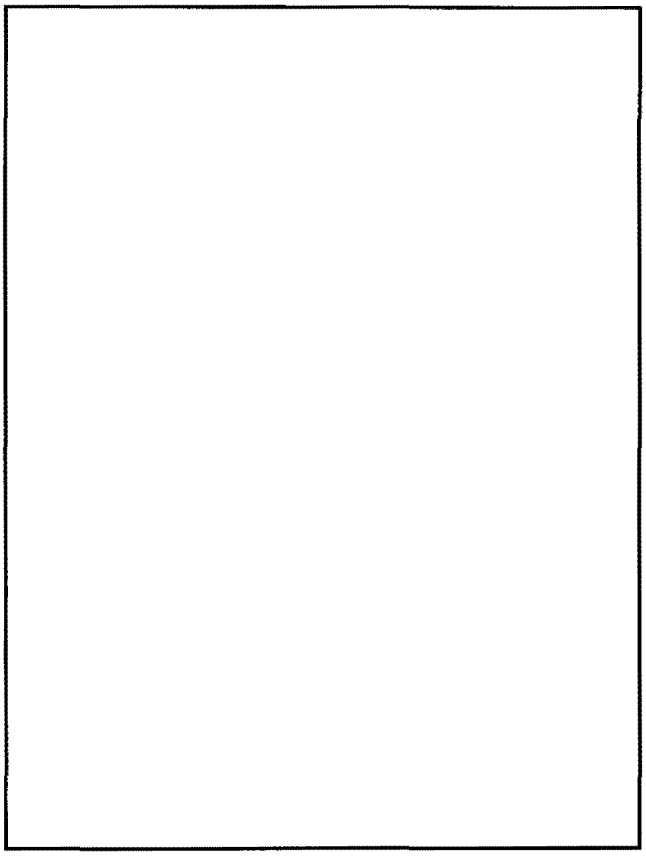
14. A typical exchange sometimes used by U.S. personnel, where conformity to COMSEC regulations is not rigidly enforced, involves the transmission EF (dit, di-di-dah-dit) and the answer EE (dit, dit), which approximates the rhythm of the familiar "Shave and a haircut..."

also applies to related systems, such as authentication, wherever habits can form as a result of allowing the operator a free choice in selection among a number of variables.

CONCLUSIONS

It will be evident that the proposed approach to maintaining continuity through chatter analysis has application only in limited cases. Because of its complexity, it may well be attempted only as a last resort and would undoubtedly require the services of a skilled chatter reader.

P.L. 86-36



On some problems, one or two distinctive habits may be sufficient, while on others a wide variety of situations may need to be examined before individual operators can be distinguished. It may be found useful, when looking for habits, to keep a similar running record of those responses *which are the same for all operators*, on the theory that such responses have been specified by the signal instructions or form a "local dialect." Such a list would be helpful in later examinations of a related net or complex, since it would define situations where habits are *not* likely to be found. (It might also become a useful *net identification* tool.)

It should be emphasized that the "habits" we seek in this approach are not tendencies to act in a given manner, but are more nearly instinctive reactions or reflexes to recurrent stimuli. Where these reactions are found to be quite variable, it may be assumed that the operator concerned lacks sufficient experience to have developed such habits or that the situation is rare enough so that he has not developed a reflexive response.

The approach may be useful, not only for continuity development in selected areas, but for inter-net equations after other evidence has narrowed the area of search to reasonable proportions, and to bridge communications changes where continuity is available both before and after, but not across, the change.

A Note about NRs

P.L. 86-36

[redacted]

A number range is an NR range, or so I have always thought. It is, of course, useful in recovering continuities and colocations, and the rate at which its member numbers are used up gives a relative measure of the tempo of activity of the user of the NR range. Recently, however, several interesting anomalies in NR usage on the Vietnamese Communist (VC) problem have triggered some thoughts about the behavior of NR ranges.

I recall sermonizing about my conviction that fewer errors occur in the NR (you may read "Radio Station Serial Number" for NR throughout this article) than anywhere else in the message. Errors, in this context, are those committed by the *target* and not by our ability to perceive what was sent (i.e., not intercept, or logging, or forwarding, or machine errors on *our* part). The argument underlying this belief centers on the use of the NR as a control or reference number: one refers to a message by means of that NR. Any ambiguity or conflict would cause difficulties in even the most primitive filing system. For that reason, one can imagine the keeping of a log book; each sheet of the log could have, down the left side of the page, the string of consecutive numbers that will become NRs as each message is logged onto the sheet. A neat, pretty picture – but not always correct.

In the course of looking at one particular VC NR range, it became apparent that, from time to time, *duplicate* NRs on consecutive messages did occur. At first, each instance was attributed to an intercept or recording error on our part, but in some instances the messages were re-sent on later dates with the same offending duplicate NRs. There is at least one explanation for such duplicates. The VC evidently do not like to send long messages and usually break up long texts into short messages of roughly 75–100 groups. Each part then gets its own NR and group count, and one of the parts will carry the file date and time for the whole batch. We might see five consecutive messages, only one of which carries a file date and time; it is as if all five messages were block-filed at one time. It seemed significant that none of the duplicates were *within* one of these batches of messages. Where duplicates occurred, they were invariably between the first message of a batch and the message preceding it. Often the earlier member of the duplicate pair was a single message filed late in the evening (later than the "typical" file times for that station) and carrying a high precedence. From time to time, we have captured radio station documents, and one frequently encountered is a small log book that is a rough diary of schedules met, significant (to the VC operator) chatter, and message preambles sent or received. Where duplicate NRs have occurred, it seems possible that the first message, carrying high precedence and needing to be sent out "after normal hours," simply was not logged in properly (such things have been known to happen around here, too) or that no log, as such, was kept at all by the station – the activity log book contained all preambles and could easily be checked to see what the next unused number should be. The pages of

these books are quite small, and the last previous message would often be logged on some earlier page. Instead of logging in, say, NR 76 on the line immediately below the entry for NR 75, in a formal NR log, one might simply leaf back through the activity log book for the last outgoing message. It would be easy to miss the entry of a single message, if most message entries contained strings of from five to fifteen messages, or if the message was not properly logged in. Thus, in the example, the leafing back for the last-used number, NR 75 might be missed, either because it was only a single entry and easily overlooked or because it was mishandled after hours and perhaps was not even logged. In any event, it seems clear that a *separate* NR log was not being maintained at that station.

Another aspect related to how the NR log was kept was evident in the circular NRs of one station: he used the block 100–399 to one set of outstations and 400–699 to another set. Each time one or the other ranges reverted, it was evident that the station was undecided about whether the ranges began at 100 and 400 or at 101 and 401. Over a long period, both starting points were used about equally often. Clearly, no preprinted logs could be the basis for such indecision. It could be accounted for either by the small operator log mentioned above or by a *blank* NR log (i.e., not preprinted with numbers).

A third "happening" seems, at first glance, to clash with the behavior described above. On 1 January 1969, the station that had been using the 100–399 and 400–699 circular series changed a number of aspects of its operation, including its NR patterns. In particular, both of these circular ranges were replaced by 1–100 ranges. In one circular series (but not the other), the number 44 was omitted. The omission is easily proved, since other serials occur in crypt indicators that do not omit 44. On the face of it, this could be explained by assuming that the station used a preprinted log containing an error in it. And that may indeed be the real explanation. But there is another possibility. Many of the VC documents captured and turned in to us for study bear the unmistakable signs of repeated usage. VC units in the field are short of paper and have learned, by writing lightly with pencil and later erasing, to stretch the life of each available scrap of paper. (Whether this fundamental difference between VC and U.S. methods has had any impact upon the course of the war will be left to historians and philosophers to debate.) It seems at least possible that some sort of log was kept during the *first* "pass" from 1 to 100, during which 44 was omitted in error. When the series reverted to 1, out came the trusty eraser and all but the NR was erased on each successive line as needed.

An NR range is an NR range, and its principal uses are still related to continuity, colocation, and tempo of activity. But subtle variations in *how* the range is used may, now and then, give us a little insight into the activities of the humans who use the NR range. All this presumes, of course, that the target country has not yet extended its COMSEC activities into the area of NRs.

Some Thoughts Concerning Traffic Analysis Mechanization

ROBERT S. BENJAMIN

Paradoxically, traffic analysis mechanization *will save manpower* but should not decrease and may even increase the amount of "real" traffic analysis work that remains to be done. NSA and the cryptologic community have always had far more things to do on most analytic problems that could be done with available human resources. Many of these things that have to be done prior to important analysis have, in the past, involved hours of logging, summarizing, counting, verification, some degarbling, and other similar operations. These are the things that machines can do best – once material is in a *machinable medium* that permits its being fed to a computer for automatic data handling. On the other hand, only people are capable of assessing the *meaning* of the various phenomena discovered in the process of organizing and reducing the data.

The scope of traffic analysis ranges between the first recorded results at an intercept station and the issuance of SIGINT end-product reports that detail traffic analytic findings in a form suited for intelligence consumers. Practically anything that goes on in the long series of complex processes between antenna and product, wherein "data" (signals) are gradually being transformed into increasingly meaningful information, is of concern to the traffic analyst. The traffic analyst works with signals collection people in directing intercept cover; he stands ready to assist the cryptanalyst in the latter's efforts to cryptanalyze message texts; he writes end-product reports for intelligence consumers or contributes basic data for integration into such reports. He works similarly with a multitude of other experts in various other SIGINT and COMSEC specialties.

The nature of traffic analysis is going to change; the change will come slowly at first, but we will be shifting gears in the next few years, and we must be ready for it. Material will be coming to us in predigested form – the more clerical parts of our job will in the near future be done to an increasing extent by machines. And we must develop and exchange ideas concerning the new working methods now appearing. A deeper order of creative thinking will be called for. Once mechanization systems are begun and databases are established, the use to which the data are put will be limited only by the imagination of those using the particular system. The *manual* part of analysis will be done more and more by machine; the *mental* part must be done by people.

SHOULD ANALYSTS LOOK AT HARD COPY?

People faced with machine output in one of its many forms often wonder whether they should continue to examine hard copy intercept. The answer to this question depends on a number of considerations – two, principally:

a. Hard copy should be examined until the analyst convinces himself of the accuracy and utility of the machine product.

b. Hard copy should be examined *if and only if* there is a real advantage to be gained.

A complete version of the intercept will probably have to be available for "back-up" use in many instances - just as the New York telephone directory must be available even though one doesn't read it page-by-page. This "back-up" traffic may be in hard copy, microfilm, or in a machine recorded form, and should be retained for a reasonable period. It should be available for emergency use to permit analytical reentry into traffic external systems (callsigns, etc.) when the machine "digests" are insufficient and to permit occasional spot checks of the efficiency and reliability of the system.

One thing is sure–extensive recopying and counting from hard copy should *not* be done. Summaries will be prepared by machine, as will detailed files concerning data elements and data items under consideration.

The traffic analyst is no longer limited to the traditional "sort and list" output of traffic analytic data. Machine output now may be in many other forms. To cite a few examples: summary listings (prints), printed matrices (coordinate tables of various kinds), printed "net reconstructions," decks of punched cards with "interpreted" (printed) information on them, answers received at a remote inquiry station (electric typewriter) communicating with a data bank in a remote computer, and "soft copy" displayed on a scope resembling a television screen (which may be photographed, if need be). Every few months, new forms of useful output seem to be appearing, resulting from computer industry developments, and from cooperation within NSA between so-called "machine people," R/D people, and analysts.

LARGE PROBLEMS VS. SMALL PROBLEMS

All those techniques of traffic analysis that depend upon collecting, summarizing and analyzing masses of data for achieving answers will lend themselves to mechanized treatment. But creativeness and judgment will be necessary

a. to design the logic for the mechanization in the first place,

b. to interpret the results obtained from machine output,

c. to improve and extend the capabilities of the particular system by discovering new ways to use it and new ways of producing even better information, and

c. to know when to go to hard copy intercepted traffic for answers that the machine system cannot give. Hopefully, proper interpretation of machine output will give a good part of these answers.

The one-of-a-kind type of occurrence is trickier and does not lend itself to machine analysis so readily. Such an occurrence may be recognized by a human being at an earlier point (in the field, for instance) and appropriately indicated, tagged, or reported in some suitable reporting medium. Or a scan of the hard copy material by an analyst *knowing what to look for* and taking fullest advantages of what has already been done by machine, may show up one-of-a-kind occurrences that may be significant. Whether a "hand scan" of hard copy will be profitable will depend upon the target, the requirements, and the circumstances.

The very, very small analytic problems are often cited as examples of things that need not be mechanized. This remains to be seen. Even in these small problems, however, certain data are necessarily a part of overall SIGINT requirements for coverage accounting reasons and must be mechanized. To the extent that an analyst can profit from what is already being mechanized, so much the better.

PENDING DEVELOPMENTS

There is a need to apply to traffic analysis methods like those called "management by exception" techniques now used in mechanized data handling in the business world. However, before such "analysis by exception" techniques can be used, norms must be established so that the computer can recognize occurrences or phenomena outside these norms. Admittedly, the establishment of norms is not an easy task. Machine scanning and selection methods involving the search for material containing certain desired "words" or the elimination of material containing unwanted "words" are a class of "exception" techniques.

Many people are working on developing many projects that relate to traffic analysis mechanization. Some projects that come to mind are

STRUM (Standard Technical Report Using Modules)

TAPS (Traffic Analysis Processing System - a flexible family of programs)

TIPS (Technical Information Processing System)

SPECOL ("Special Computer Oriented Language" – an experiment in data correlation and retrieval)

TEXTA Mechanization

ZITO (produces soft copy of a scope)

AG-22 (Paper-tape producing typewriter).

TRAPEZE (System to produce formatted reports from AG-22 paper-tape output.

Each of the above projects is significant enough to deserve being treated at great length, but that is beyond the scope of this article. And there are many other important projects that could be mentioned.

We urge individual analysts to learn more about machine processing. The National Cryptologic School offers several excellent courses to introduce the "layman" to the general idea of using machines, and other such courses will be devised in the months and years ahead.

Learning a programming "language" is another way to gain familiarity with machines. These so-called "higher programming languages" are machine-independent in that *compilers* are available that enable programs that have been written using these languages to be run on different computers, even computers made by different manufacturers. FORTRAN is one such language, but FORTRAN lends itself more readily to mathematical computation than to the handling of traffic analytic data. Showing more promise for data handling is COBOL, a language designed for business applications, which can handle alphabetical as well as numerical information. Courses in either of these languages can provide the traffic analyst with a good conceptual base. There are other "programming languages" in existence, or being developed, that are suitable for information handling.

As TIPS Pilot is developed, simple formatted interrogative statements through a RYE remote station will enable any analyst or manager to ask a wide range of questions and get rapid answers from the RYE computer concerning information in the TIPS files. Subsequent versions of TIPS – TIPS I and TIPS II (TIPTOES) – will add many refinements in future years.

However, analysts need not learn computer programming to use mechanization, but they should become familiar enough with machines to feel comfortable when confronted with the idea of mechanized data. Machine prints will not look like conventional "hard copy," but they will spare the analyst many, many hours of drudgery and permit him to spend his time really analyzing and synthesizing. Whole new areas of techniques will open up; for example, machine prints of TAPS output have shown phenomena not at all readily apparent in the hundreds of input entries that were combined, reduced, and presented to analysts in summary form. Interpreting these phenomena calls for a high order of thinking and judgment.

In summary, analysts on analytic problems that aren't already using machines should be exploring ways to use them, particularly since STRUM, AG-22 and the like will soon present a machinable input for practically all problems. And, of course, machine people need to know more about traffic analytic problems; at best, it isn't easy to dredge meaning out of the mass of confusing data facing the traffic analyst, and the more that machine people understand this, the more help they will be to this important aspect of SIGINT production.

Acknowledgments

I should like to express my appreciation for the review and helpful comments by Mr. James Taylor, C4103; Mr. Robert Grove, C416; Mr. George Hicken, C03; [redacted] A03; and Dr. Walter W. Jacobs, E.

Cleaning the Augean Stables
or
How Much T/A Can a Computer Do?

FRED MASON

One of the labors of Hercules was to clean the stables of King Augeas. These housed three thousand very healthy oxen and hadn't been cleaned in twenty years. Rather than trying a shovel, Hercules was smart enough to turn two rivers through the stables.

T/A has a comparable task. Manually, T/A is a desperate attempt to clean up the constantly augmented flood of intercept, in the belief that there may be one or more valuable needles in the original haystack. And the collectors are so damned healthy!

The computer seems to offer a way of doing it by dropping the input into electronic rivers. These, if properly directed, can multiply the human effort and wash, massage, organize, compare with the past, and separate the input–putting the debris here and a small pile of shining needles there.

How much of this can the computer, in fact, do? Part I attempts to define T/A, and Part II attempts to answer the computer question.

PART I. TRAFFIC ANALYSIS

1. Glittering Generalities

The purpose of SIGINT is to make available to supported commanders a reconstruction of the target Order of Battle (O/B) and changes thereto as derived from target emissions – and in time to permit educated command decisions to be made.

Order of Battle answers the command question about the opponent, "What forces oppose me? What are their titles, types, echelons, command relationships, equipment, morale, strength, locations, deployments?" It is a static description of the target at a moment in time.

Changes in O/B update the answer by establishing a vector; he was here then, now he's there; his O/B change is describable and sometimes measurable in amount and direction. Such intelligence vectors assist the commander to understand target changes in capabilities and to estimate hostile intentions.

2. Serendipity

SIGINT attempts to accomplish its purpose in several ways. One school of SIGINT thought has it that in combat all is flux; that little can be equated from day to day; and that the valuable SIGINT answers will be derived from exploitation of readable traffic (cryptanalysis) and the unusual, the compromise, the momentarily understandable in an ever-changing environment (traffic analysis).

This approach is Serendipity – the happy faculty for finding valuable things unexpectedly. Cryptanalysis has put a massive effort into reading as much encrypted text as possible, using substantial computer support to break into and exploit traffic. (The best way to find the most four-leaf clovers is to examine the entire lawn.)

Traffic analysis is governed by fewer rules and varies more in its application. Serendipity is also systematized by using a small number of full-time omnivorous readers who see all intercepted traffic, all reports on it, and all friendly correspondence relating to the situation. Ideally, their memories are photographic and their knowledge of O/B encyclopedic. They ignore all that does not excite their curiosity but seize anything with known indicators or with interesting unknown features. They then assemble all other traffic from that net and from any other net with the same SOI or displaying the same indicators or features. From this section of input is deduced the activity, often only after extensive study. But the reading of new material must continue, so that higher priority compromises, or additional data on the one being exploited, won't be missed. And collection must be redirected in order to pick up more of the activity.

SIGINT tries to take "unexpectedly" out of the Serendipity definition by collecting as much as possible and by examining it all for exploitability. From the serendipitous approach comes most of the SIGINT headlines – the front page stories.

And there is no question of its value. But it is unpredictable. It produces immense detail on a minor unit one day and on the entire O/B the next, but by its nature it cannot sustain its effort on any one subject. There is always a new fire to put out. Often, by itself it cannot answer the commander who asks, "Do all of the forces that opposed me yesterday still oppose me? How have they changed? Are there new ones?"

3. Continuity

As opposed to Serendipity (Crypt or T/A), which monitors the entire stream of intercept but selects only a small porter for exploitation, Continuity, i. e., traffic analysis, must process it all. It must sustain the effort, carry knowledge gained from compromise forward into overtly different communications structures, keep continuity, keep track of all of the units opposing us yesterday, and identify new ones. This is cleaning the stables.

Intercepted communications come in "sets," messages and chatter exchanged between two or more callsigns representing command or staff functions of one or more military units. The most repetitive terms in each set are the calls used, and the most useful term (because it is not arbitrary) is the frequency applied by the intercept operator. These are

the built-in terms labeling a set. They often are enough to identify the set, but the terms occurring in messages and chatter must usually be used as well.

Since calls and frequencies (and other terms) change frequently, the same *net* may be presented by many *sets* over a period of time. And each major unit controls many nets, an army group or military district often having as many as one hundred nets potentially active at the same time (plus the nets of its subordinates). These represent the different command and staff functions of the unit, working with different combinations of organic and subordinate command and staff functions, and with many alternate nets (morse, voice, and printer parallels).

Fortunately, the collection of terms and the typical formats into which they fit (like sentence structure) are usually sufficiently revealing to permit the intercept operator and traffic identification analyst to label them with some accuracy–at least as to country and service.

So traffic analysis – the proper labeling of each set of intercept, of each radio station, and of each activity – begins at the intercept set. Based on the initial set label (case notation), the intercept is sorted, and more or less homogeneous piles are given to each analyst for further processing.

Continuity is the "Alias" problem; set 542 is the same as set 821, which was the same as set 127, etc. Done exhaustively, it reveals only the number of nets active. It does not reveal who the stations are, where they are, what functions they represent, or where the net fits into the network. It does permit the application of the answers in one set to all of the other sets of which the set is a continuity.

Serendipity, either as a separate function or that of the continuity analyst in the course of his processing, provides the who, where, what, and structural location of the net. Continuity carries it forward.

4. Battlefield Vocabularies

Most of the categories of military communications terms are encoded for electrical transmission. A list of arbitrary terms is *generated* (calls, addresses, codewords, etc.) according to some sort of system. From the semifixed list are *selected* subsets of terms for each period according to other, local systems. And the selected subsets are *allocated* to various users according to still other systems. Frequencies follow the same scheme, except that they are not arbitrarily generated; they are selected and allocated according to locally devised systems.

For each period, then, the selected subset is matched against a list of plaintext meanings. The plaintext list (units in O/B order, command and reporting phases, etc.) does not change very much over a long period of time. The encoded terms for transmission change frequently and usually provide for a number of alternate terms each period. Change in the plaintext list of units usually indicates change in O/B.

There are two stages in the traffic analytic attack on the problem of battlefield vocabularies. The first is the isolation of terms in a category which presumably come from one subset: calls used by one or more related nets that possibly come from one callsign book; addresses used in an area presumably selected according to a common set of rules from a master list; frequencies used by related nets and presumably allocated from the same subset; etc. The collections of terms so isolated are input in the second stage, that of solving the systems of *generation* of the master list, of *selection* from the master list for the period being examined, and the *allocation* of the selected subset to the corresponding plaintext list of terms.

Generally, there is little point in trying the second stage (solution) until the first stage is accomplished with some accuracy. And the first stage depends upon the success of the continuity effort, since a single set of data will not, normally, provide enough terms to permit successful attack.

Success in any part of the attack makes the whole much easier, (e.g., solution of the callsign book generation system permits set and nets to be associated rapidly, which then provides collections of data for attack on the frequency problem).

5. Activity

Continuity and the solution of battlefield vocabularies, as discussed above, provide the skeleton of Order of Battle. Changes in O/B from one time to the next provide inferential information about target intentions: e.g., this division has been resubordinated from Army A to Army B; the capability of Army B is thereby measured and inferences may be drawn about its intentions, etc.

Better information is often available. The cryptanalytic solution of enciphered text and the traffic analytic solution of plain text and brevity codes often give more direct and valid information about capabilities and intentions. Grids give relative unit positions and artillery (tube, missile, and bomber) targets. Codewords give implementation times for activities and may, if solved, define the activity. ELINT cuts may reveal concentrations of radars in defense of troop concentrations or locate beacons for airborne drops.

The Serendipity approach acts, almost entirely, on the isolation of such revealing texts and then finds all related nets to build that part of the network for the period. And it may well be that this is all that is possible in a fluid battle area of some size.

Continuity attempts to account for all units, both active and inactive. If it can be accomplished, this complements serendipity by providing information on the existence of reserves and uncommitted and inactive units, and by providing the skeletal O/B to which interesting activity can be related.

PART II. THE COMPUTER

1. The Computer is an Idiot

So, too, is a shovel, a lever, and a quill pen. The difference lies in the time lag between human control and mechanical or electronic action. A shovel, lever, or quill pen is used directly and immediately by a human being; a computer is programmed for use in the future.

Directing action at second hand and in the future is very difficult, particularly if it is impossible to predict what may be sensed at the time the action is required.

You drive your car at some speed towards an intersection. Without conscious thought you identify all fixed scenery and all moving objects. You compute their probable positions at the point of time at which you will be in the intersection and, semiautomatically, you hit the brake, accelerate, or continue at your previous speed. But just try to get the car safely through the intersection by briefing a non-driver (the programmer), who will in turn instruct (program) a rote passenger on what to sense and what, in each possible circumstance, to instruct the blind driver to do.

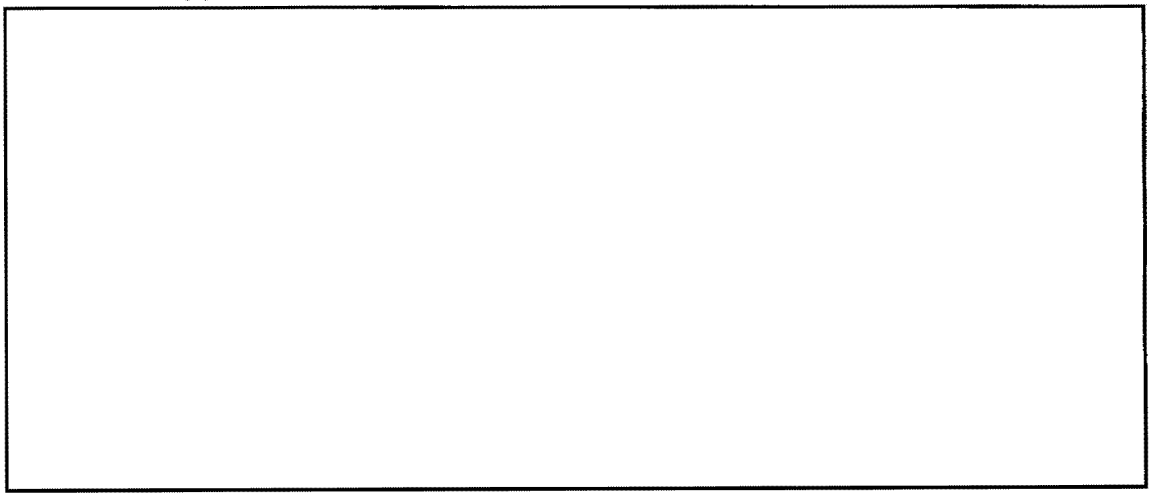
The difficulty lies in trying to explain what you have done, step by little step, when you have written a sentence with your quill pen or driven your car.

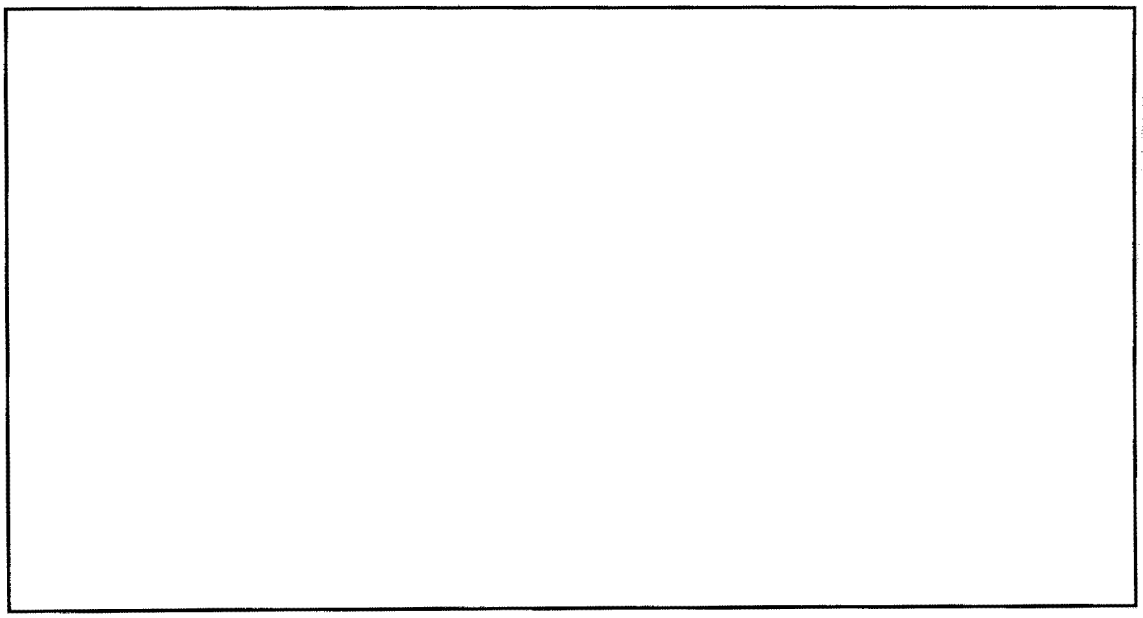
If it can be done, it multiplies your power very considerably. The computer, properly instructed, can drive a hundred cars as well as one. For this reason, it is a challenge and well worth trying.

2. What is the Computer Now Doing For T/A?

Programs now in being, or shortly to be implemented, accomplish a great deal of the clerical work previously done by traffic analytic personnel. In most cases the computer attempts no identification of call, or set, or net with specific military units or nets, but groups like things together and applies the best label added to the intercept by humans. The following process illustrates the type of computer-analyst interplay now in being.

P.L. 86-36
EO 1.4.(c)

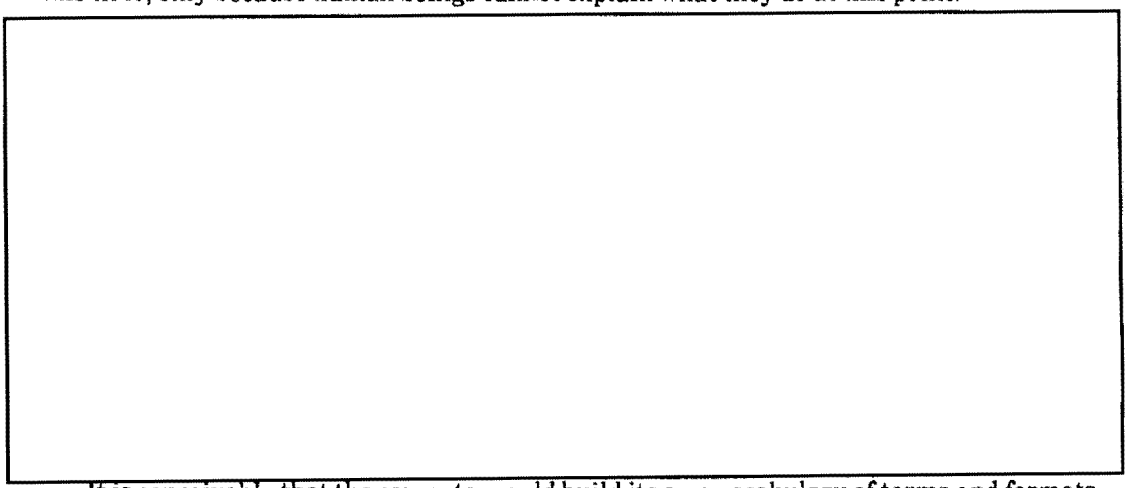




The characteristic of the above type of process is the control of the system by the analyst; if it is used as one of his tools and all of the tables and files in the system are maintained currently, it will work well for him; if the tables are not maintained, it will cause the input to degenerate. The analyst is necessary to the system.

3. What Could the Computer Do?

The manual T/A payoff is in the identification of O/B and of activity. Much of this is concealed by the periodically changing battlefield vocabulary, which humans deal with as "The Game": "sounds like"; "in this context may be"; "the activity around it suggests it may be a synonym for"; etc. It is not believed that this is within the computer capability at this time, only because human beings cannot explain what they do at this point.



It is conceivable that the computer could build its own vocabulary of terms and formats from its input, applying to each the best identification of the set from which it came. A

new set could then have its terms and formats compared to the computer vocabulary and all identifications of previous sets retrieved. The retrieved identifications might then be examined statistically. The computer output might be

This set is (65%) division X

It is (20%) artillery, (5%) SSm

Callsign ABCD is (25%) the umpteenth motorized rifle regiment

Best guess as to case is.....(42%), or.....(29%)

This set is a continuity of sets.....(82%),.....(74%),.....(68%)

4. The Computer in Combat

Those functions now accomplished or suggested for batch processing could be done in much smaller batches, approaching on-line processing. The computer could materially assist in sorting, selecting, and identifying intercept sets and activity and could, as well, guide intercept, if the callsign history could be directly queried. (The previous identification and analytic comment – "want" or "don't want" – could be made immediately available).

Portability is feasible with solid-state computer components, and size is approaching the manageable. The problem lies in analytic use. Unless analysts are trained in and appreciate the multiplication of their power possible through intelligent use of the computer, it should not be used. The machine will only hamper the successful manual operation.

5. Present Problems

The feeling still persists that the computer is an expensive, mystic black box and that it must operate efficiently at all costs. Its priesthood still carries this belief to the point where its efficiency is emphasized at the expense of the T/A problems it serves. It is not comparable to a quill pen, kept sharpened and ready for instant use when needed, as well as being adaptable to the needs of the moment. It is more like a railroad, with trains leaving on schedule (more or less). If you happen to want to go to that point at that time, climb aboard (after having applied for a ticket well in advance). But to change the composition of the train or its destination or its scheduled times is almost beyond the passenger's capability.

Not because of characteristics inherent in the computer, but rather because of the management of this tool, the computer is not adaptable, not flexible, not responsive to T/A needs – except in the case of those needs that are continuing and that can be conceived whole and perfect when the process was first requested.

6. Conclusion

The computer can perform many of the functions that traffic analysts do manually. It can group data into homogeneous piles. It can apply previous annotations to sets of data and to terms. It can sort and list. It can select data or discard them, based on previously determined criteria. It can provide a sizable memory with total recall. It can continue a process whose rules have been defined

PPLL.886386
EBO1144(¢¢)

The computer cannot, at the moment, solve the unusual. A new system or a nonstereotyped sentence cannot be given meaning by the computer until an analyst instructs the computer. (It can, however, collect the unusual for the analyst.)

The computer cannot, at the moment, be used to solve the little T/A problems, such as solving a frequency rota or running out a callsign pattern or solving a key sequence. Most of these problems are hand generated by target signal personnel and change frequently. By the time the analyst explains to the computer what to do, he can solve the problem himself.

The computer, then, is a tool, a big tool. It can materially assist the traffic analyst in his work and do most of the clerical labor associated with T/A. The system does not now permit it to be used as a little tool or a fine tool. And it is no more than a tool.

Build a road with a stream shovel; don't use the shovel to open a door! And yet I think that maybe, if I could tinker with it a bit and try a few things, I could open that door with the computer. Certainly, a better road could be built.

Traffic Analysis on [redacted] Data Transmission Systems

P.L. 86-36

[redacted]

Conventional traffic analysis has never been a glamorous job. It conjures up a picture of untidy desks piled high with traffic of various hues and drawers bursting with much-thumbed tools of the trade – callsign tables, network diagrams and, of course, that inevitable odd file of mysterious unidentified bits and pieces that is never thrown away because it is such a convenient place to put more unidentified bits and pieces. Amidst this scene we find that most maligned representative of the COMINT community, the traffic analyst, continuing his never-ending battle against the nonstop flow of paper and wiping his carbon-stained fingers all over his clean white shirt in a gesture of despair. His plight is known to all of us, and many have done sterling work to try to emancipate him. But despite some machine aid, the lot of the traffic analyst working on conventional communications, morse, radioprinter, and voice has not changed very much in twenty years.

P.L. 86-36
EO 1.4.(c)

The advent of [redacted] data transmissions threatened an even greater amount of paper unless new techniques were developed. As a result of these new techniques, there appeared on the scene a new breed of clean-shirted traffic analyst whose previously cluttered desk is now rarely used except perhaps for lunch.

What are these data transmission systems that so successfully changed the face of traffic analysis? They are very much in vogue these days, and the air and air defense forces of many nations, including the United States and USSR have turned to such systems to augment and sometimes replace their existing facilities for air surveillance reporting and weapons control. Basically, a data transmission system permits the automatic transmission of formatted information by means of digital coded impulses and gives a greatly increased traffic capacity coupled with speed and accuracy.

Two such systems are in current operational use by the [redacted]

To analyze and exploit the information transmitted in a data system, it is necessary to process and present it in a form suitable for analysts. [redacted]

P.L. 86-36
EO 1.4.(c)

[redacted] And so the idea of traffic analysis from a display was born in 1961. [redacted]

It is probably necessary at this juncture to placate the skeptics amongst the old hands who will have none of this nonsense and allay the fears of the new entrant who feels he was not born with enough hands. What is this traffic analysis that can be done at a display and how is it carried out?

[redacted]

[redacted]

P.L. 86-36
EO 3.3(h)(3)

It may seem that the new concept of traffic analysis demands a super breed of analyst – a combination of radar operator, machine specialist and data traffic analyst. It is true that more is demanded of the analyst, but experience has shown that the novelty of the new approach and the results obtained from it have whetted the appetite of those morse traffic analysts who have been transferred to data analysis, with the result that they have adapted themselves to the new techniques with a minimum of training. Air and air defense analysts are, of course, weaned on the interpretation of tracking, and machine handling has been made very simple as almost every requirement of the analyst has been covered in programming while operating consists of little more than pressing the required pushbuttons on the control panel.

Although the technique of traffic analysis from displays is still in its infancy, its

[redacted]

Although it was an air/air defense data system and the threat of unmanageable amounts of paper that resulted in this new method of traffic analysis using an immediate combination of man and machine and replacing the paper by displaying the data, it should not be construed that analysis by display will be limited to the air/air defense world or even to data systems. Traffic analysis involves looking at paper, a lot of paper. It involves sorting this paper and inevitably re-sorting. Obviously such procedures call for machine aid, and in many areas this help is available or planned on a larger scale. But in almost every case this help will be in the form of machine listings, perhaps alleviating the sorting problem, but replacing one lot of paper with another. Perhaps the reader can see a use for displays instead of listings for his own problem. Perhaps a "quick look" would permit enough discrimination to reduce the volume of listings to a minimum. It is hoped that this introduction to traffic analysis or [redacted] data transmission systems, traffic analysis from displays, will open up a new world to the many who did not know of its existence and that it will stimulate further ideas on how to handle traffic.

Traffic Analysts of the Future

P.L. 86-36

[redacted]

Let us take a glimpse into the future – a future much different from today. I want to convey a man-machine concept that visualizes a fairly complete computer complex from intercept collection to the storage and retrieval of intelligence by the consumers from their desks. This sort of data processing assembly line would contain numerous computers with process computers controlling other computers but with humans at certain vital points along the way. Traffic analysis is one of the subsystems in this assembly line. I want to fire the imagination of the traffic analysts, managers, data systems analysts, R & D types, and others so that some day we can put the pieces of the assembly line together. Certain operations in the assembly line can best be done by humans until we advance the state of the art in artificial intelligence. In the meantime, we want to make it as easy as possible for the humans.

In this assembly line concept, the output of one stage must be compatible with the input to the next stage or process without extensive conversion, reformatting, or other changes.

The concept visualizes that as the data flow through the system on a real-time basis, a human can call data from mass storage, state the processes (programs) to which they should be subjected, and display the results at any stage desired. Based on the results, the analyst would then specify additional processes until he is satisfied with the results.

Let us visualize how a traffic analyst of the future may work. First, he will work from a console instead of a desk. The console would probably contain at least two CRTs or TV-type displays plus an electric typewriter and light pen. All of these would be connected to a remote computer for the proper man-machine relationship.

Now suppose our traffic analyst wants to get continuity on a very important net for day X. All data are in a mass storage device to which the computer has access. He states his problem on the keyboard in stereotyped English, e.g., "Get all unidentified data from file X for day Y." (This can be further defined as data from certain intercept stations.) "Build and compare net structure with XXMT50101 using Program _____." "Display net structure of XXMT50101 on scope 1 and best match other nets on scope 2." After visual observation of all possibilities, the analyst wants more information on new net number 2. He asks for a display of the crypt systems used by both nets if messages were passed.

Then he asks for a comparison of traffic volume, address groups, etc. Having satisfied himself that the net is correctly identified, he types on the keyboard, "Identify new net structure number 2 as XXMT50101." This activates a program that updates all records in the master file with the new information.

After going through all his assigned nets and maintaining continuity, he calls for the display of all remaining unidentified nets. One group of control and three outstations has now appeared for several days. The analyst calls for a display of the group on a geographic mask with all stations geographically located by the previous day's direction finding. Then he reviews callsign, frequency, cryptosystems, usage and other elements to determine the echelon of the group. With two or three possibilities, he requests an order-of-battle (OB) display showing units located on a geographic overlay. In this way he can compare net structure with order-of-battle of units known to be in the same geographic area. After several tries, he finds a unit which fits so far as echelon structure, but one of the outstation location does not fit. Considering the possibility that the OB may not be up to date, the analyst requests a display of the OB overlay for the last two months on the second display scope showing day-by-day overlays at a two-second interval. With this technique he notes that one unit has been moving. By projecting the movement up to the latest information, he concludes that the unidentified outstation and the one unit are the same. In addition, he now has later information as to the location of the unit. He adds this information to the OB database so that tomorrow when the intelligence consumers interrogate the OB files for new information, this new location of a military unit will be produced.

Identifications are then made on the keyboard, and all records in the file are brought up to date.

Barometer-Readers' Comments P.L. 86-36

The future envisaged by [redacted] bothers me, in that it presumes a traffic analyst (and a consumer) who controls the situation, who asks the right questions of the computer. He queries the computer for new data on his assigned nets (or units) and then asks for all other unidentified nets, from which he selects and develops a new net. This suggests that, if he is preoccupied with other tasks, he needn't ask and *nothing* will arrive on his desk (or CRT). TA need not be done?

If this is not true–and, in fact, he must ask–then why the query at all? A set of mandatory queries ("Give me all, massaged") need be programmed only once and the computer will provide the data routinely. This is, I believe, the TA function. The target, not the analyst, controls the problem. The analyst (collectively) is *required to examine all of the intercept* and do something with it. If a mountain of material comes in, he must cope with a mountain, not just pick out bits he predetermines as being his.

It's like a police department. Does it sit in its police station asking questions about the status of Hollywood and Vine? Or does it patrol the whole city? Who can judge in advance where a crime will occur?

You cannot ask *all* of the right questions unless (1) there are a very limited number of possible questions and (2) you know all the possible questions.

Sincerely, Fred Mason

Sir:

In reference to Mr. Mason's letter in *COMMAND*, dtd March 1969, I don't believe Mr. Mason has heard about management by exception. The advantage of computers is that they can be programmed to look at the unusual. We do have a mountain of intercept, but it is not necessary for a human to look at it all. The computer looks at it all and finds the unusual or unidentified to which the human can devote all his intellect. Let's use machine for the routine and free humans to be analysts. Most analysts like to piddle around with the intercept because they can see tangible progress – that is, process so many papers. Most junior traffic analysts would not know what to do if they were faced with real analysis.

[redacted] PFLL 886386

Mr. Mason's rebuttal:

Management by exception? Maybe. Analysis by exception? I don't believe in it. Along with our primary mission of reporting all changes in O/B is our continuing obligation to reaffirm the status of all known target forces – to always expand, amplify, flesh out the static O/B skeleton. As a premise, we have never fully described O/B; there is always more we could say about a target. If this is true, neither we, nor our consumers, nor the computers, know enough about our target to say "All is normal, don't report." The fact of "normal" activity is reportable.

It has to do with indications of imminence. No one asks that we report everything, but no one permits us to suppress anything either. It is a very thin line we walk, this Pearl Harbor complex. For instance, it is "normal" for any one of fifty people to be in my little cubicle. At what point is it abnormal? When ten are here at once? Twenty? Fifty? It is now "normal" for Soviet crews to man missile sites in Egypt. If there are now X such crews, 2X is a 100 percent increase, surely reportable. But 3X is a 50 percent increase over 2X probably reportable. 4X is only a 331/3 percent increase over 3X; 5X a 25 percent increase; 6X = 20 percent; 7X = 162/3 percent; 8X = 14.3 percent. Is there a threshold below which we stop reporting? Or keeping a count? Or let the computer withhold intercept from us?

I'll go a step or two down the road. The computer is fully qualified (with a lot of analytic guidance) to summarize, to reduce the daily mountain to a comprehendible molehill. But the molehill must be regularly and exhaustively examined, refined, compared with previous molehills – and by humans. The validity of this map must be confirmed and reconfirmed by comparison with the mountain it represents (and the mountain itself is only a small sampling of the voluntary overt utterings of secretive "bad guys.")

Fred Mason

PRL 886386
EO 1.4(c)

A Brief Quarter Century of Soviet Crypto/Traffic Analysis

[redacted]

INTRODUCTION

The earliest piece of Soviet communications intercepted by the U.S. was dated early 1944,[1] according to my crypto/traffic analysis (C/TA) records. Since that time we have experienced many varied and complex problems in the TA field. We all know that TA deals with the items of communication that make it possible for the transmission of a message–the analysis of the text of which becomes cryptanalysis. In turn, C/TA is that special area where a cryptanalytic attack is made on the elements of TA in the attempt to assemble order, primarily military order of battle.

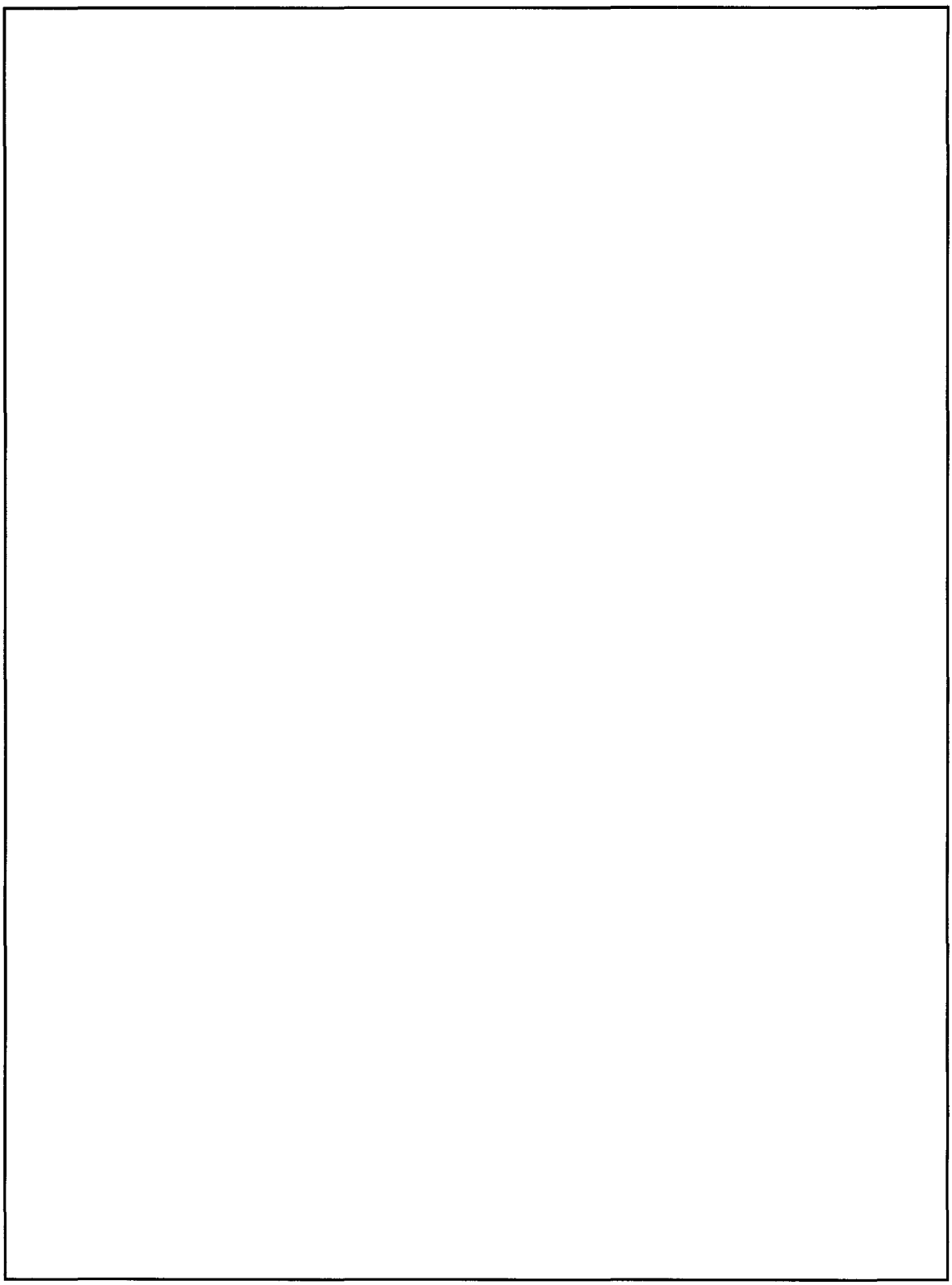
I have chosen as the base for C/TA the twenty-five years NSA has devoted to Soviet communications. The progressive improvements of these systems from an elementary state to certainly the most sophisticated yet indicates the degree and effort the Soviets have taken to deny the SIGINT community C/TA success. Also, we can be reasonably sure of the existence of strong Soviet influence in the communications of other Communist countries.

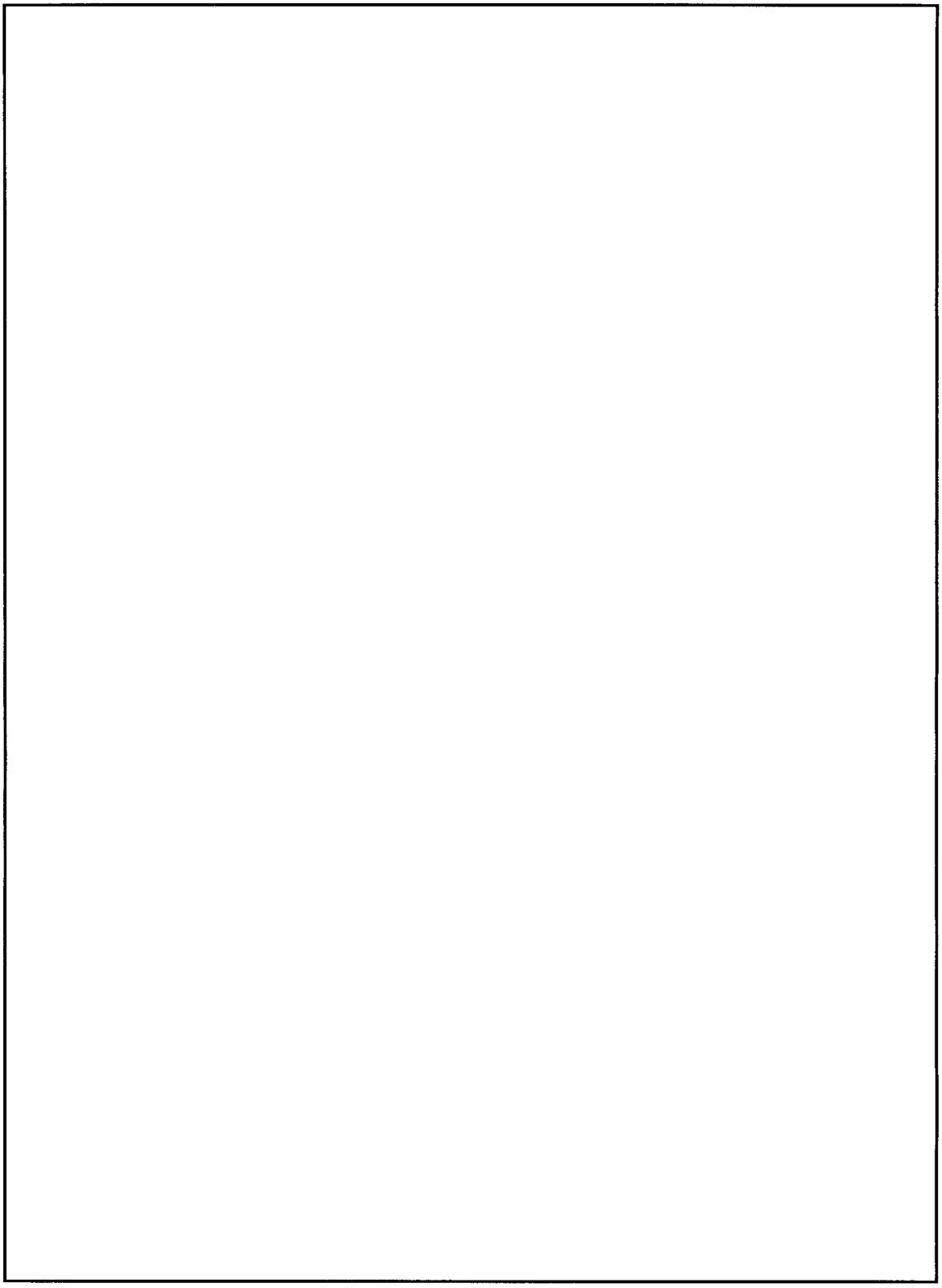
This paper is confined to callsign systems analysis.

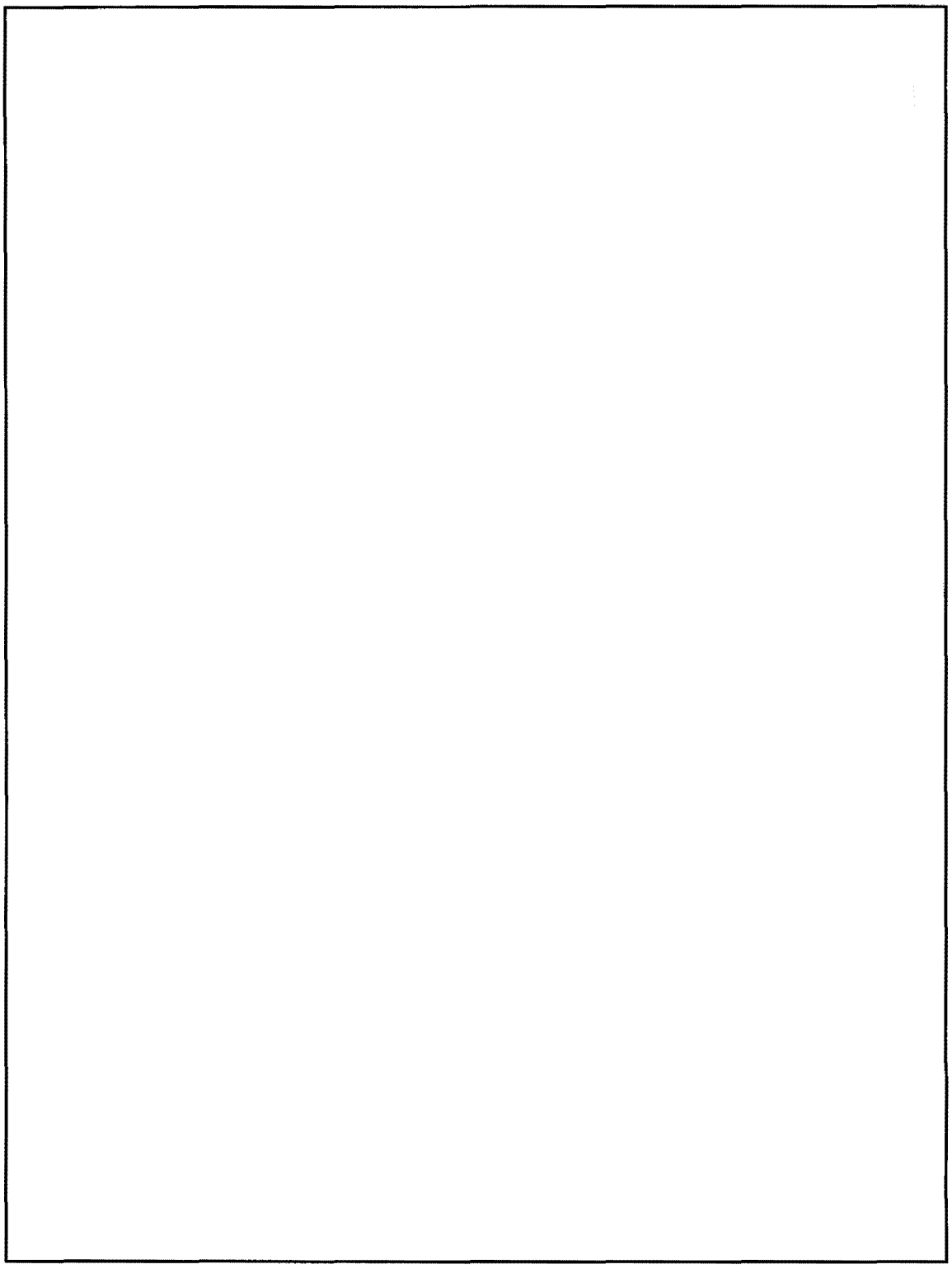
THE PRIMITIVE YEARS

While the United States C/TA effort did not actually begin until about 14 February 1944, we glean an insight into the earlier Soviet posture from captured German documents. We may summarize the period prior to 1 November 1948 as one in which very limited control was exercised over communications of the military forces by the military cipher office in Moscow. [redacted]

1. The U.S. Navy was already working on Russian traffic in Alaska in 1943. Mr. Frank Raven [redacted] and, according to him, the British began passing Russian traffic to the U.S. in 1940 or 1941. The author cannot further document this earlier period and, therefore, would be grateful for assistance from anyone possessing a documentation or recalling the contents thereof to set the record straight.

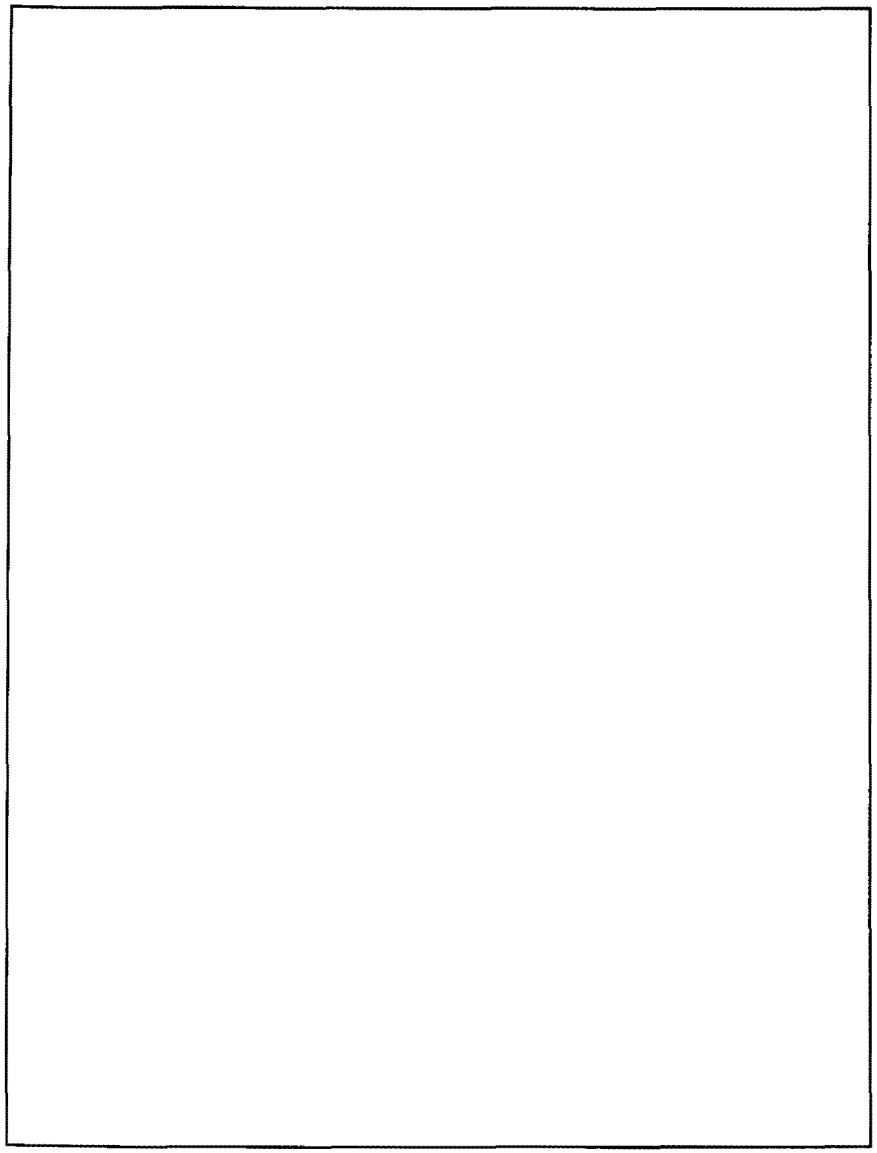




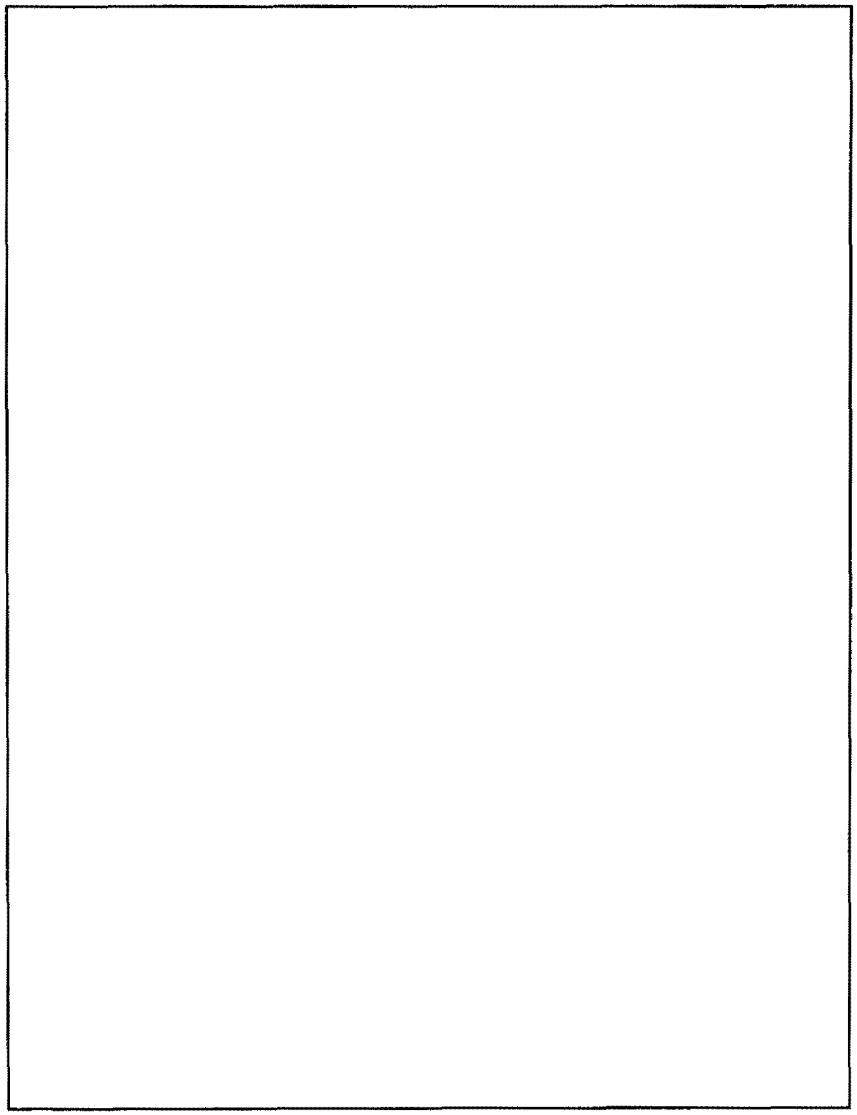


These have been the highlights, briefly told, yet symbolizing the culmination of many sympathetic efforts on these varied systems–each of which represented a greater challenge than its predecessor. I am proud to have served the C/TA effort during the part quarter century, and I envy the role of C/TA of the future because of the inevitable technical challenges.

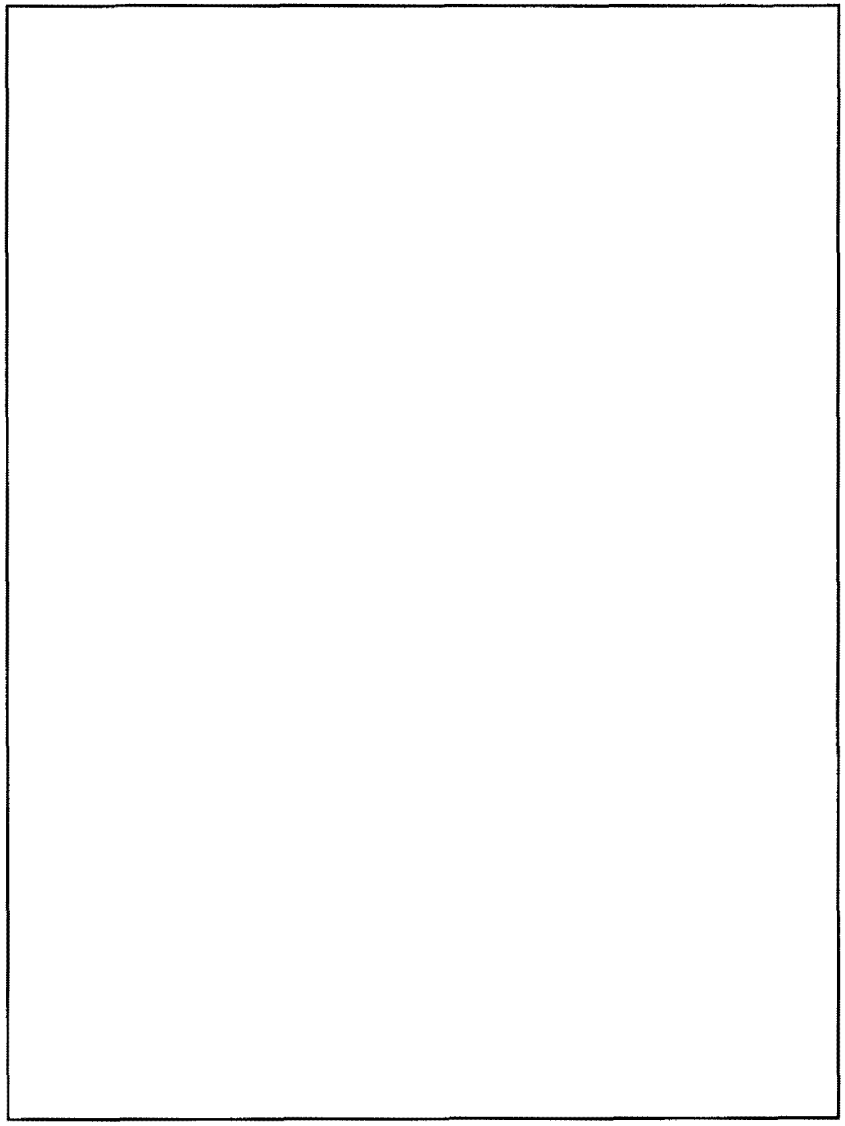
P.L. 86-36
EO 1.4.(c)



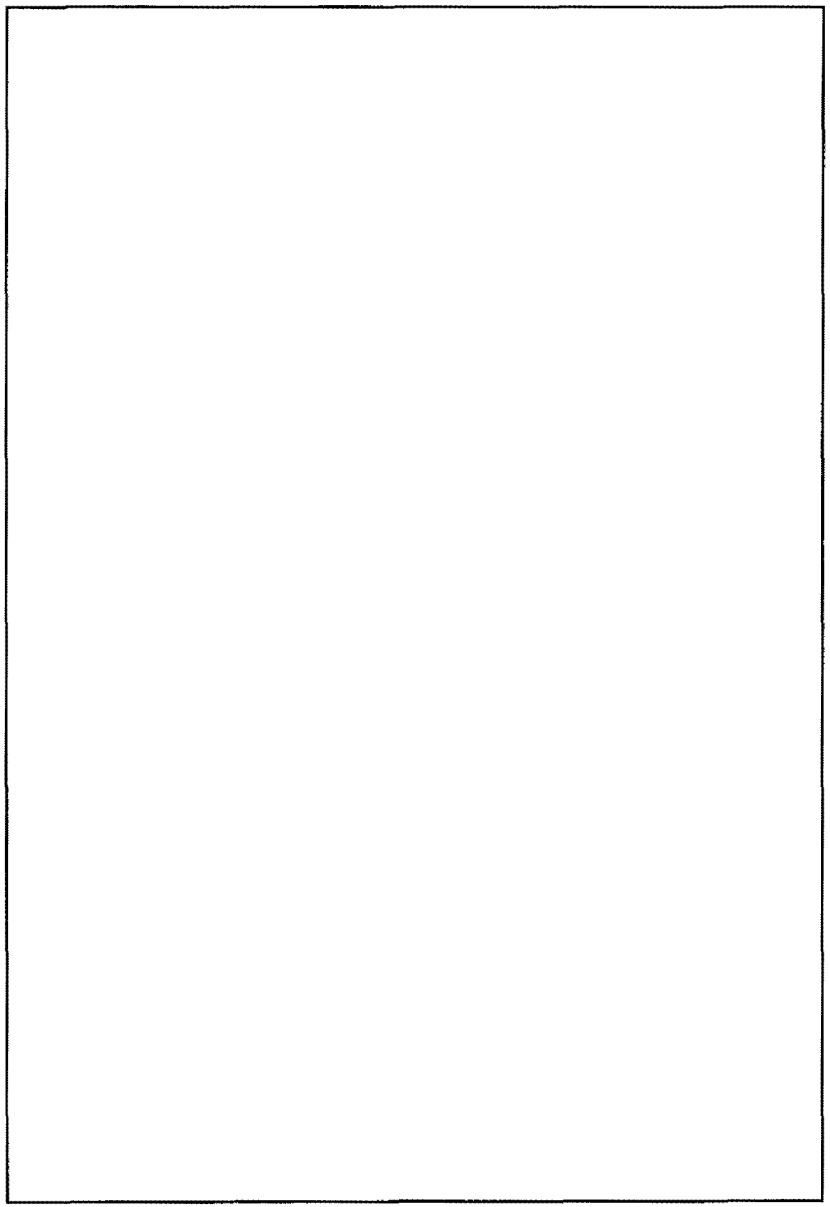
P.L. 86-36
EO 1.4.(c)



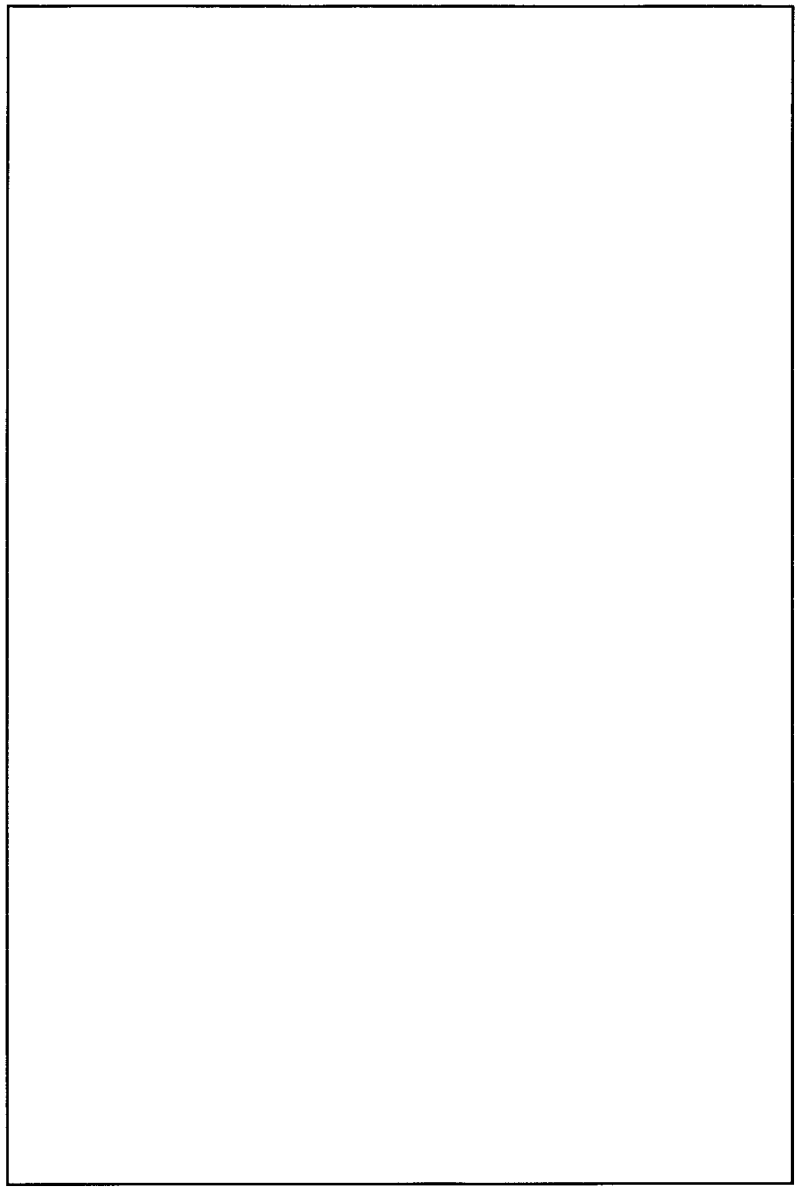
P.L. 86-36
EO 1.4.(c)



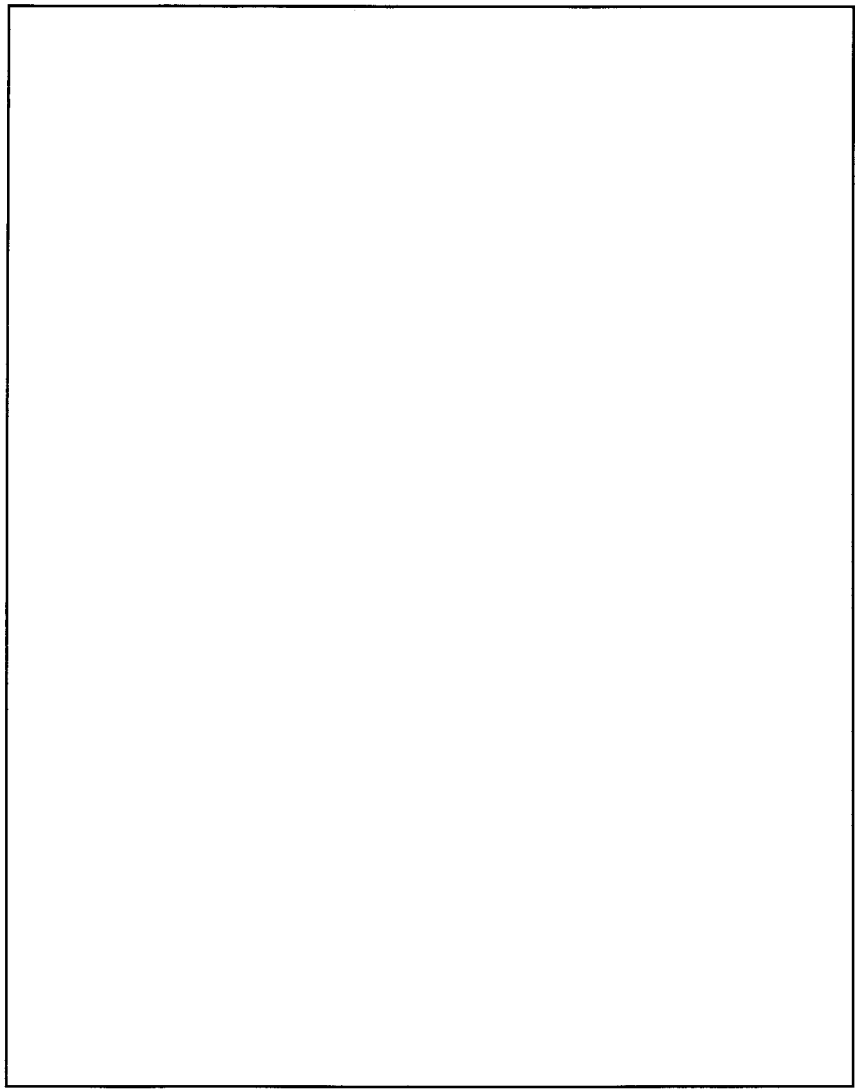
P.L. 86-36
EO 1.4.(c)



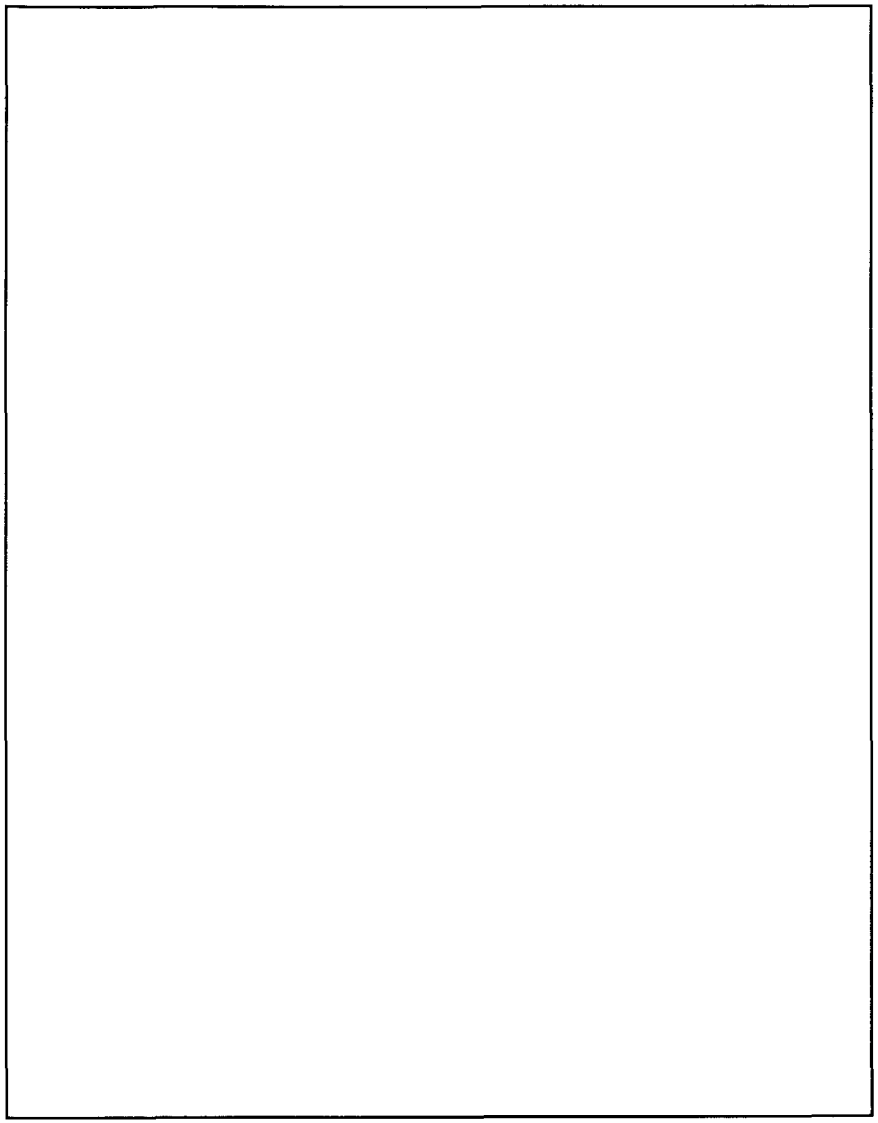
P.L. 86-36
EO 1.4.(c)



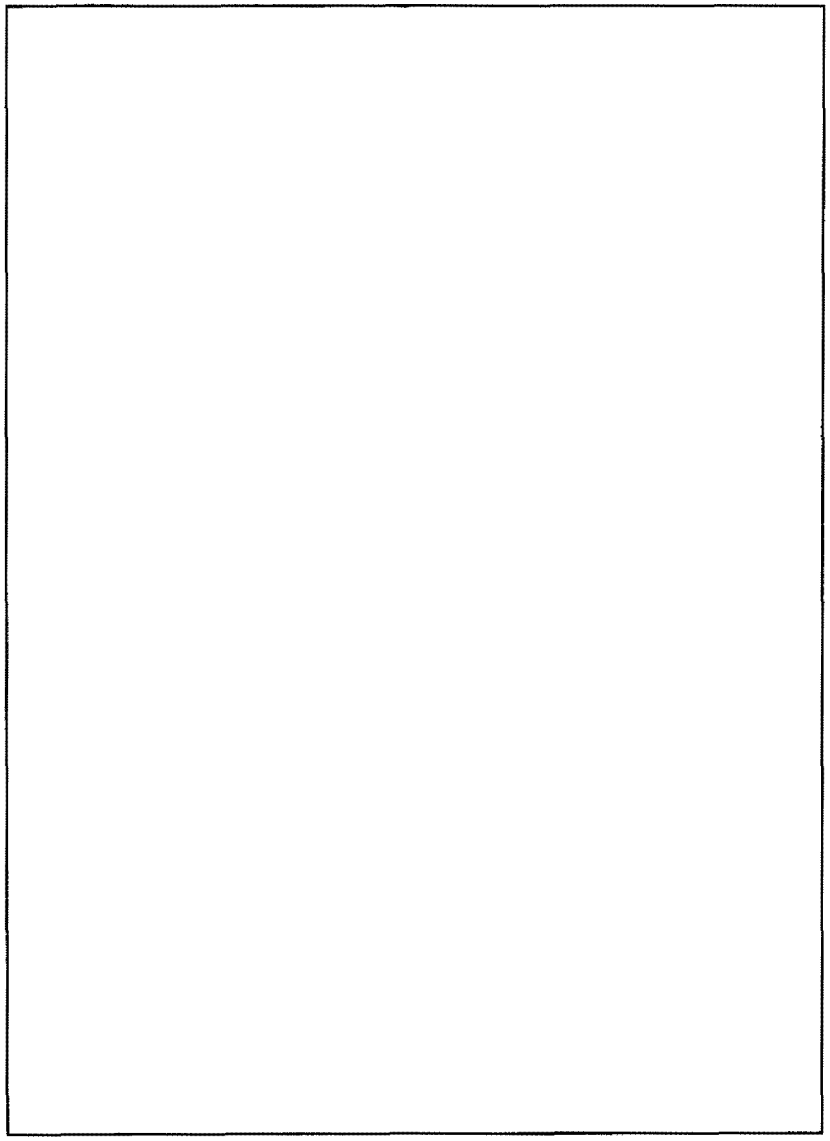
P.L. 86-36
EO 1.4.(c)



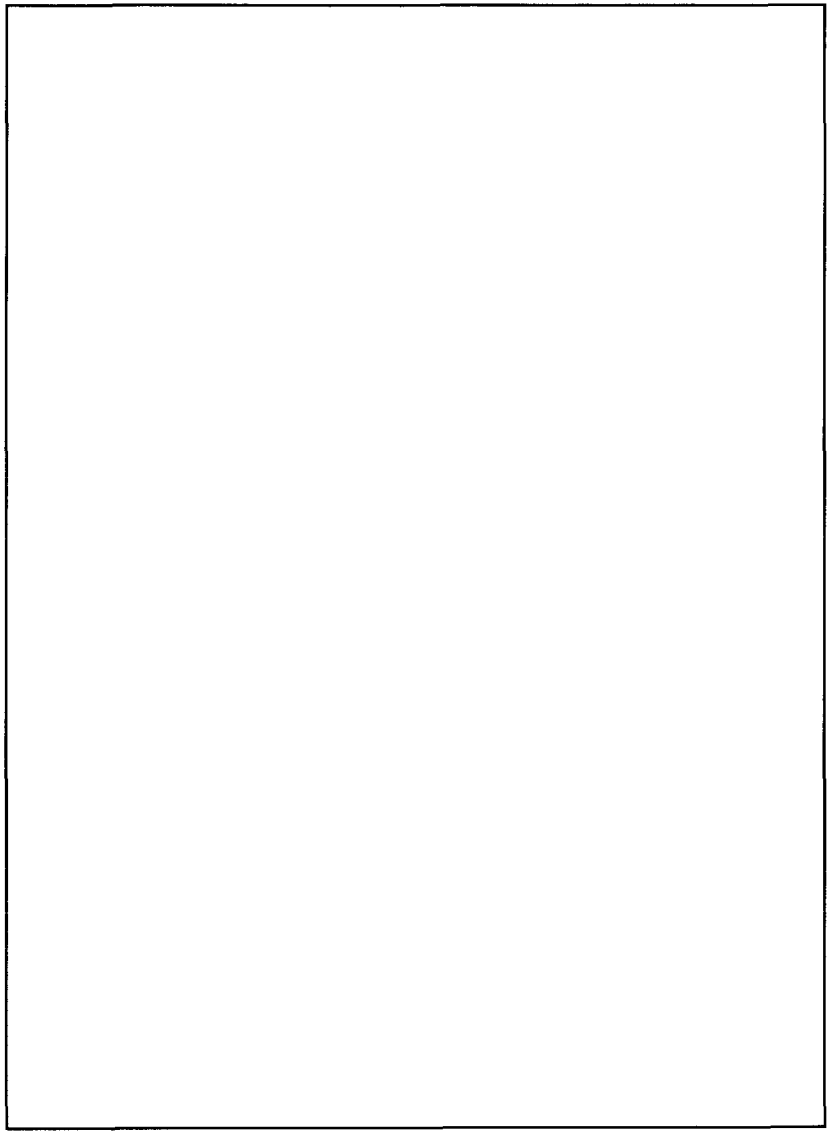
P.L. 86-36
EO 1.4.(c)



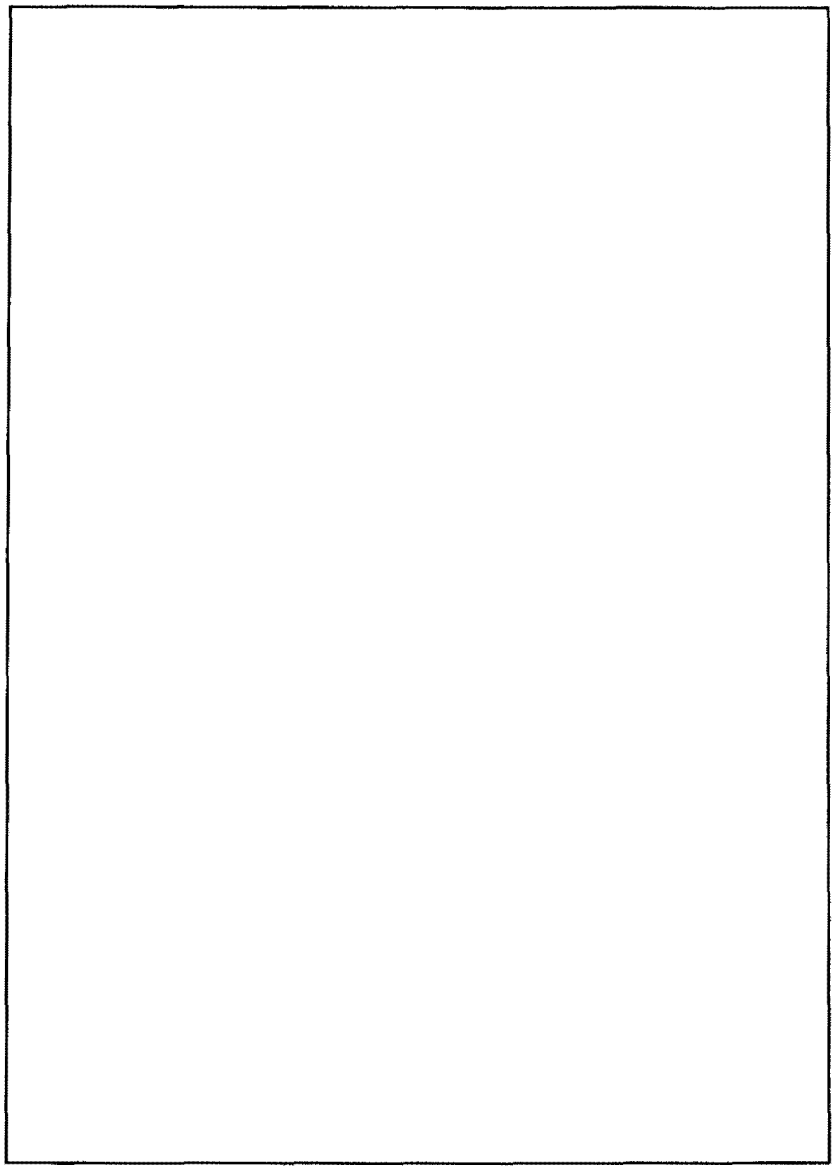
P.L. 86-36
EO 1.4.(c)



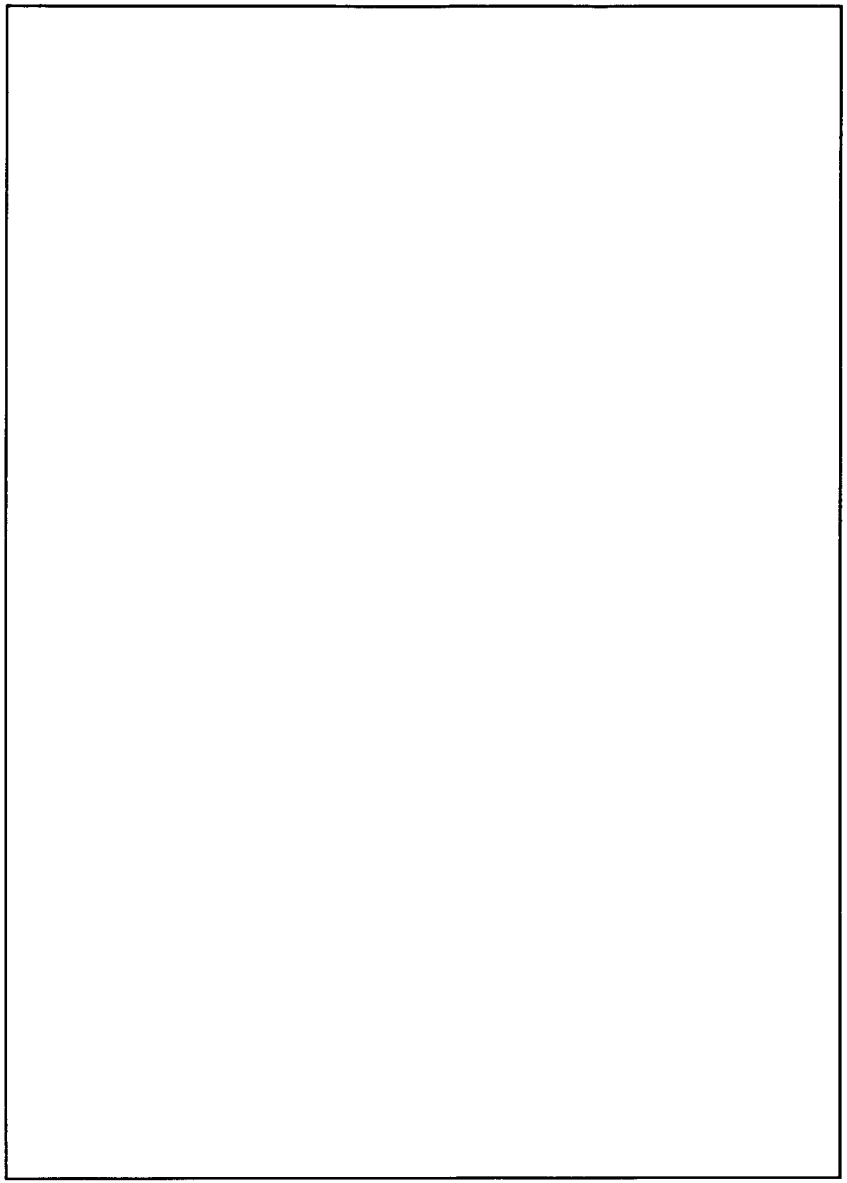
P.L. 86-36
EO 1.4.(c)



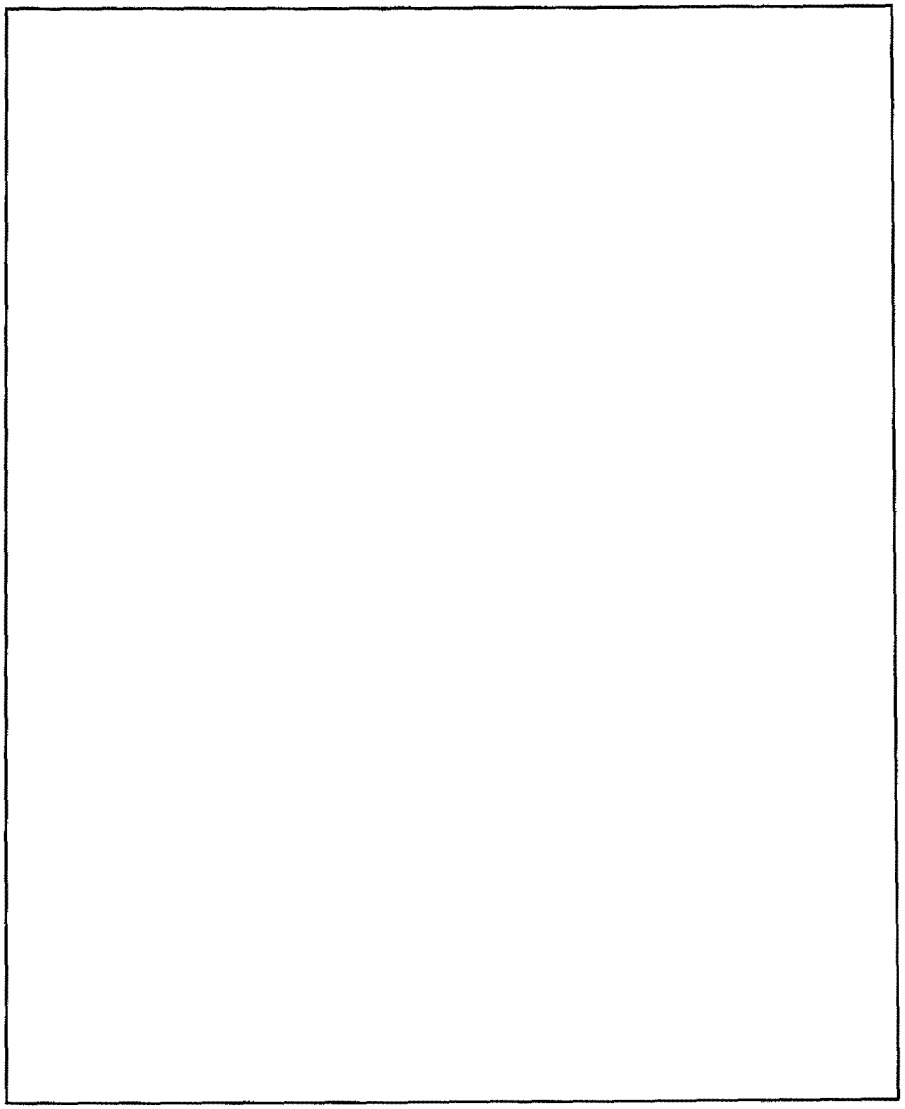
P.L. 86-36
EO 1.4.(c)



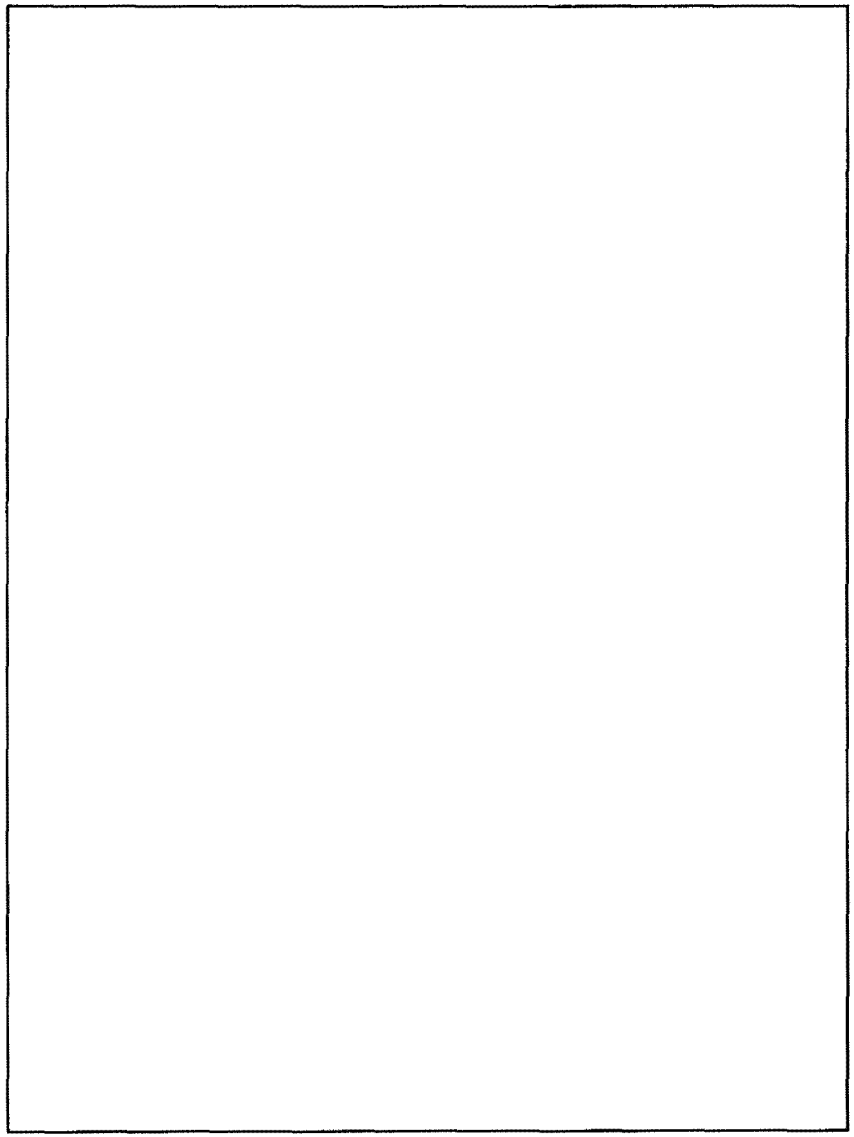
P.L. 86-36
EO 1.4.(c)



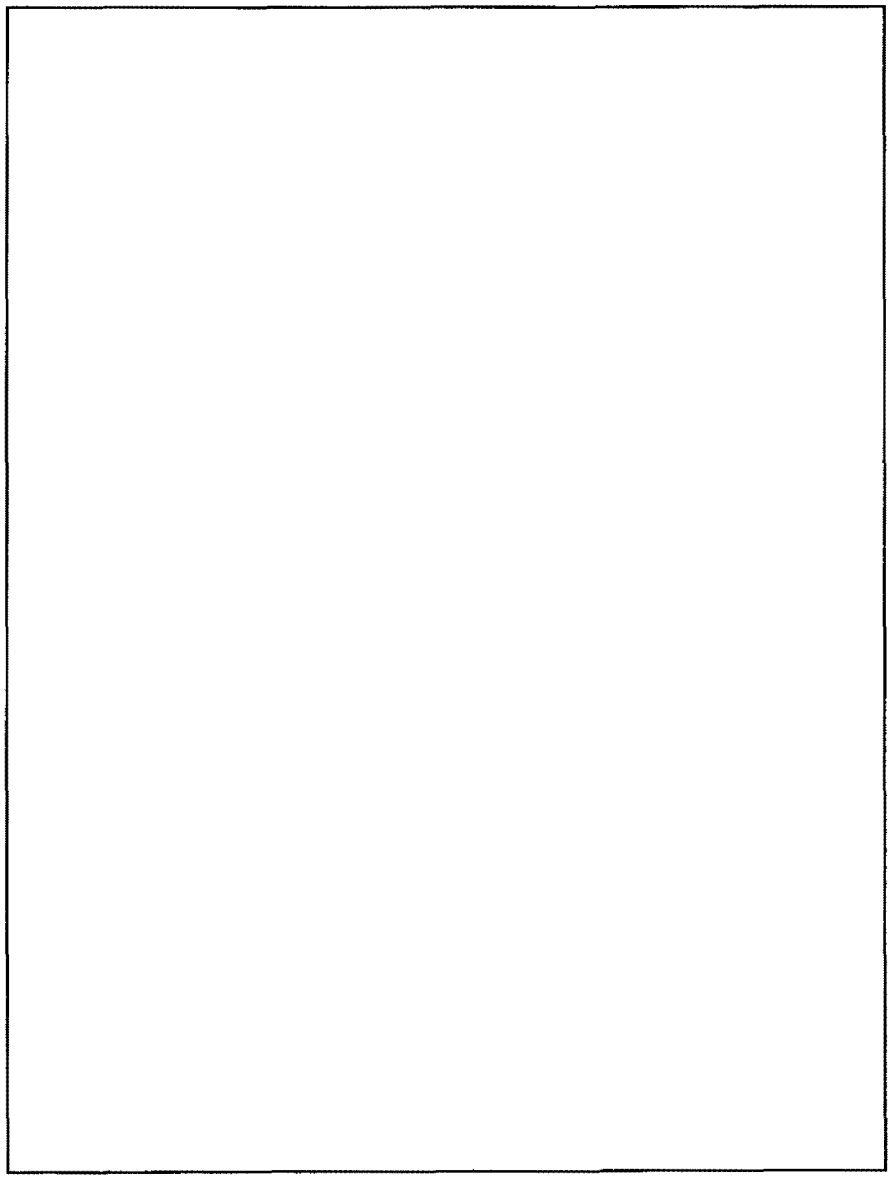
P.L. 86-36
EO 1.4.(c)



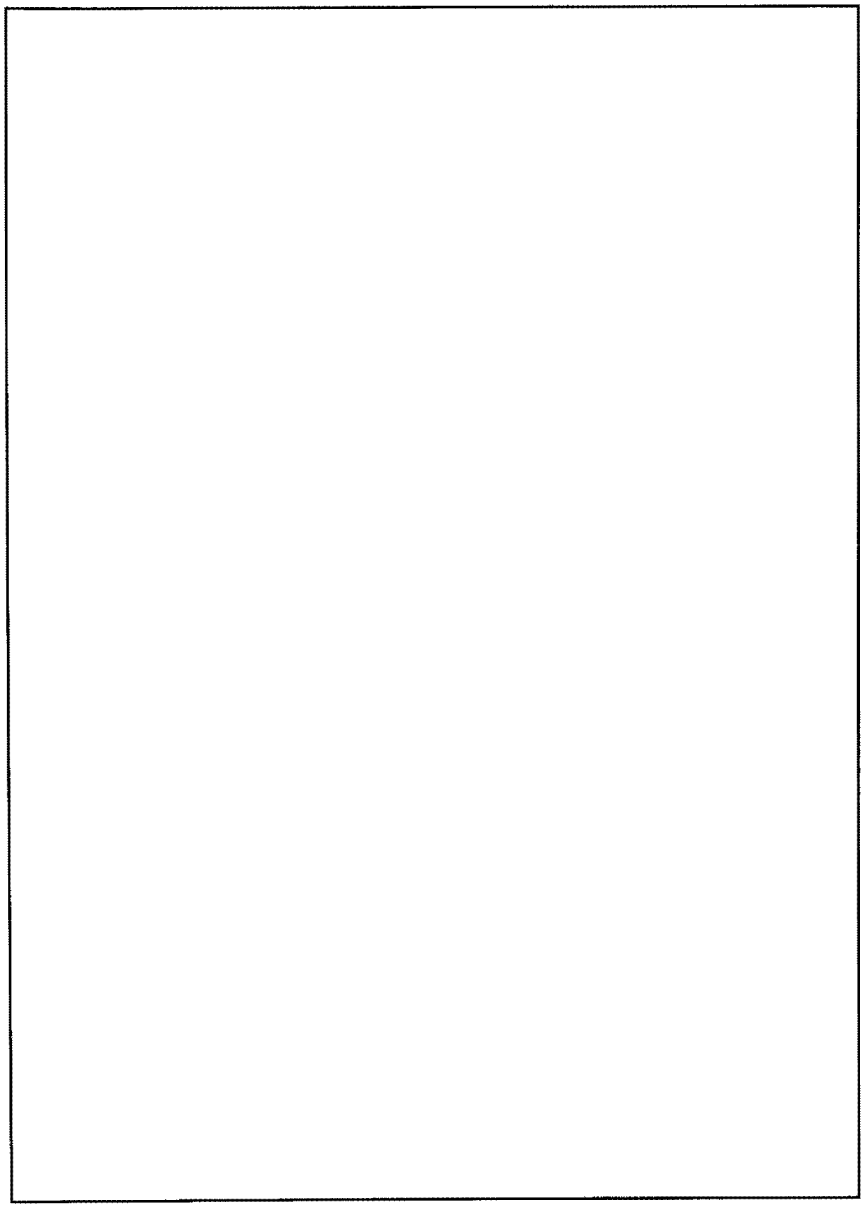
P.L. 86-36
EO 1.4 (c)



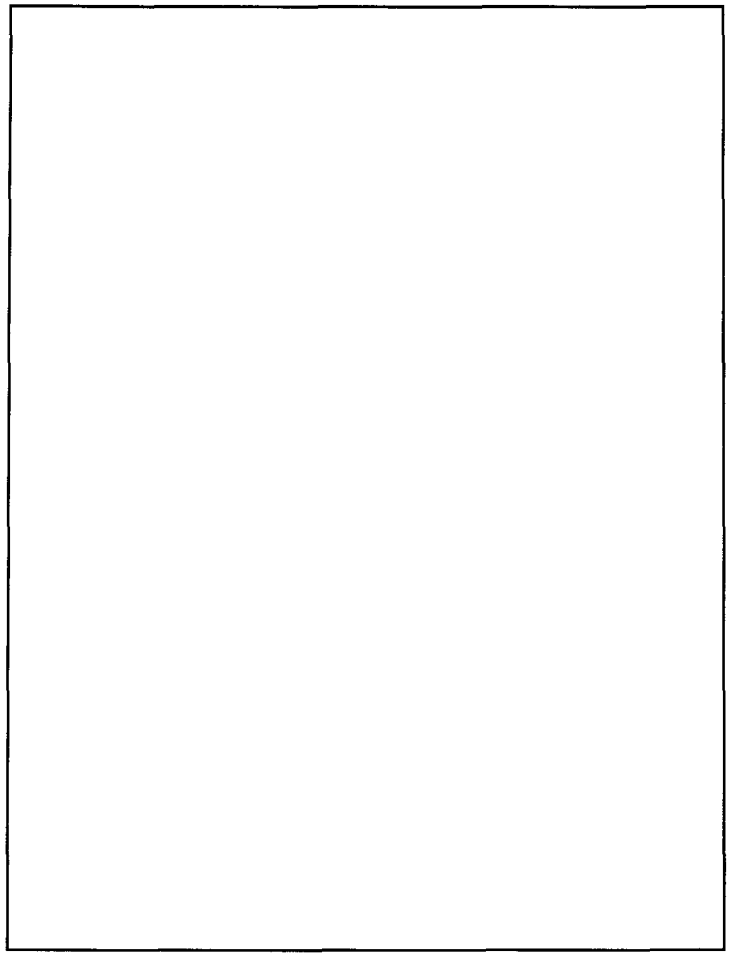
P.L. 86-36
EO 1.4.(c)



P.L. 86-36
EO 1.4.(c)



P.L. 86-36
EO 1.4.(c)



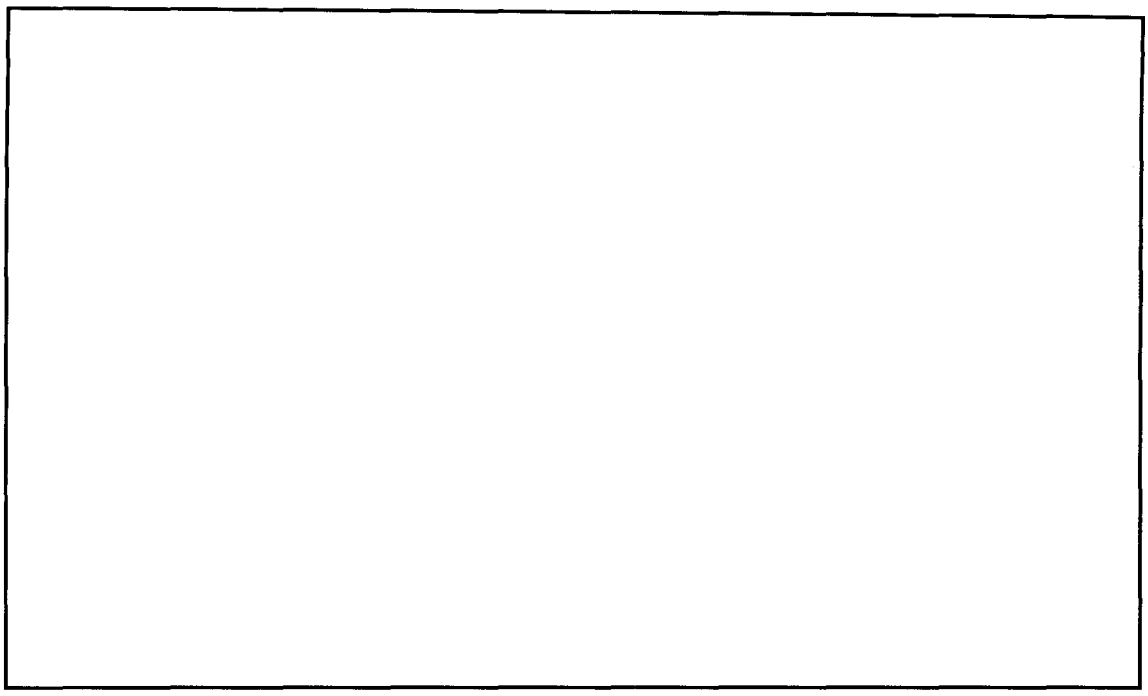
Recovery of a Vietnamese Communist Callsign System

[redacted] P.L. 86-36

The recovery of the Vietnamese Communist callsign system now titled AO1 (V61A, Abigail-1) clearly demonstrates the value of historical research toward the full understanding of a presumably obsolete signal plan, in that it facilitated recovery of its successor system. P.L. 86-36 EO 1.4.(c)

[redacted]

P.L. 86-36
EO 1.4.(c)



True Base: Two Tales (U)

P.L. 86-36

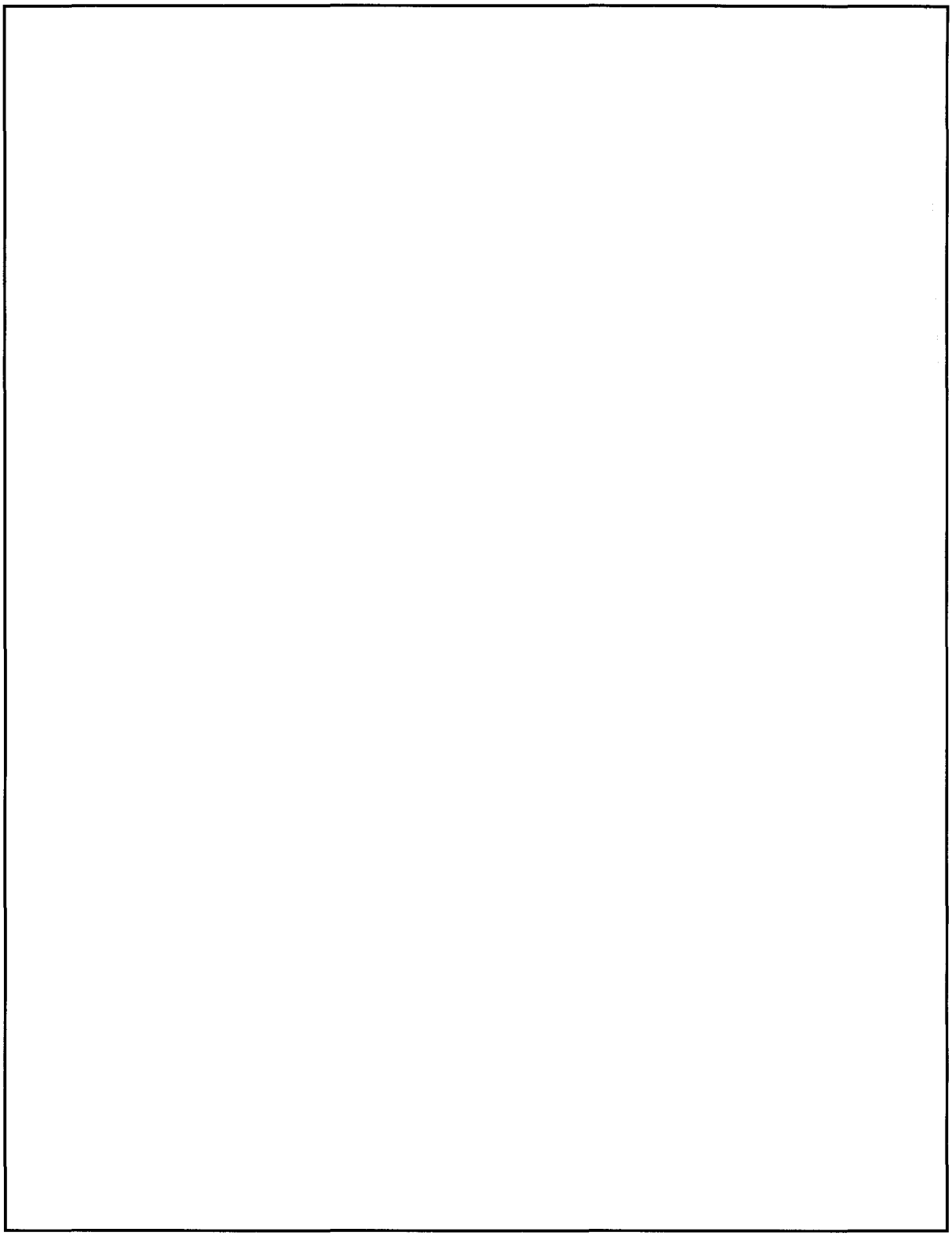
[redacted]

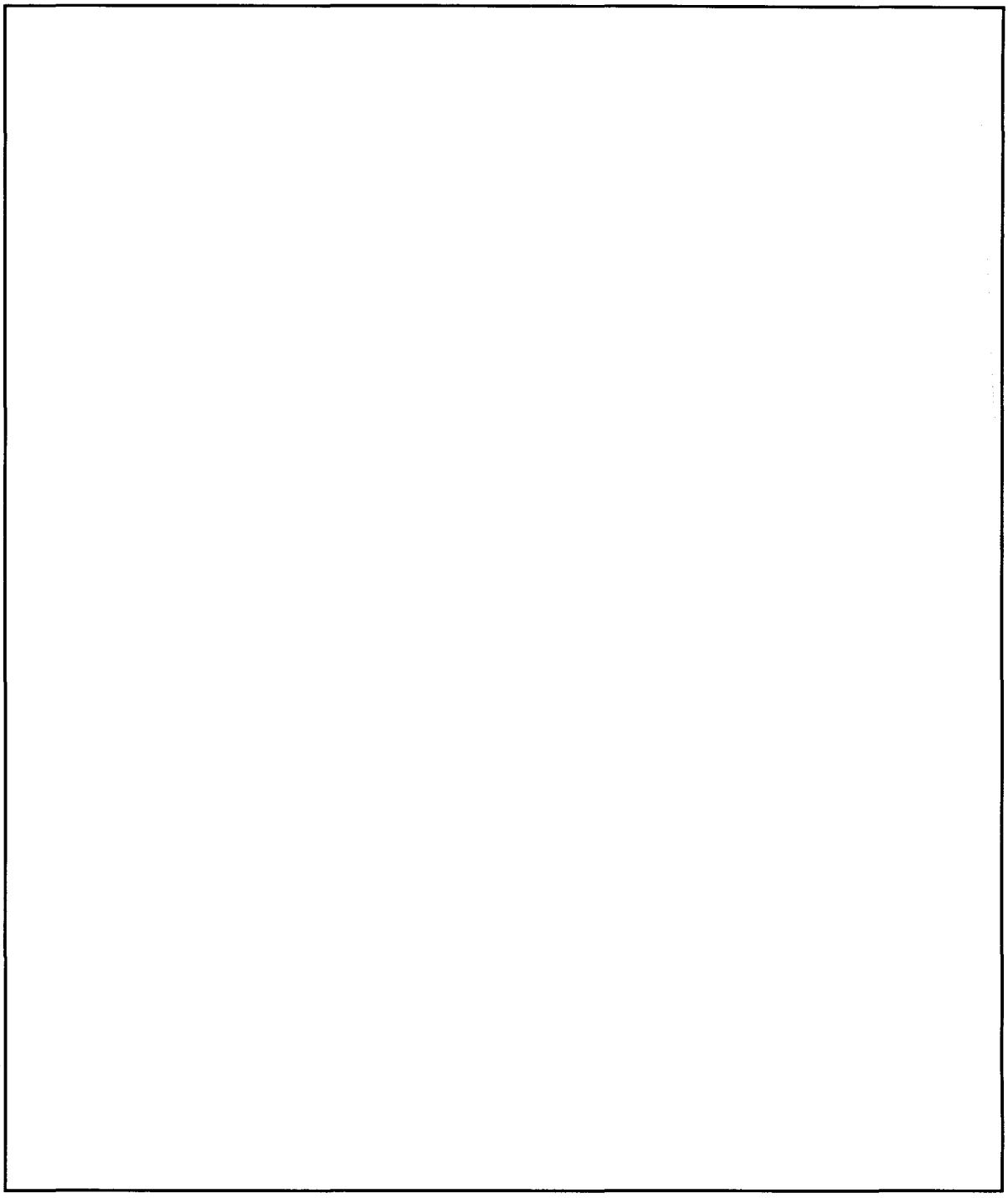
Both of these tales are true. Some of the details have been changed, but not necessarily to protect the innocent. They both have to do with the same thing: what happens to our knowledge about a target when we put one of its systems on true base.

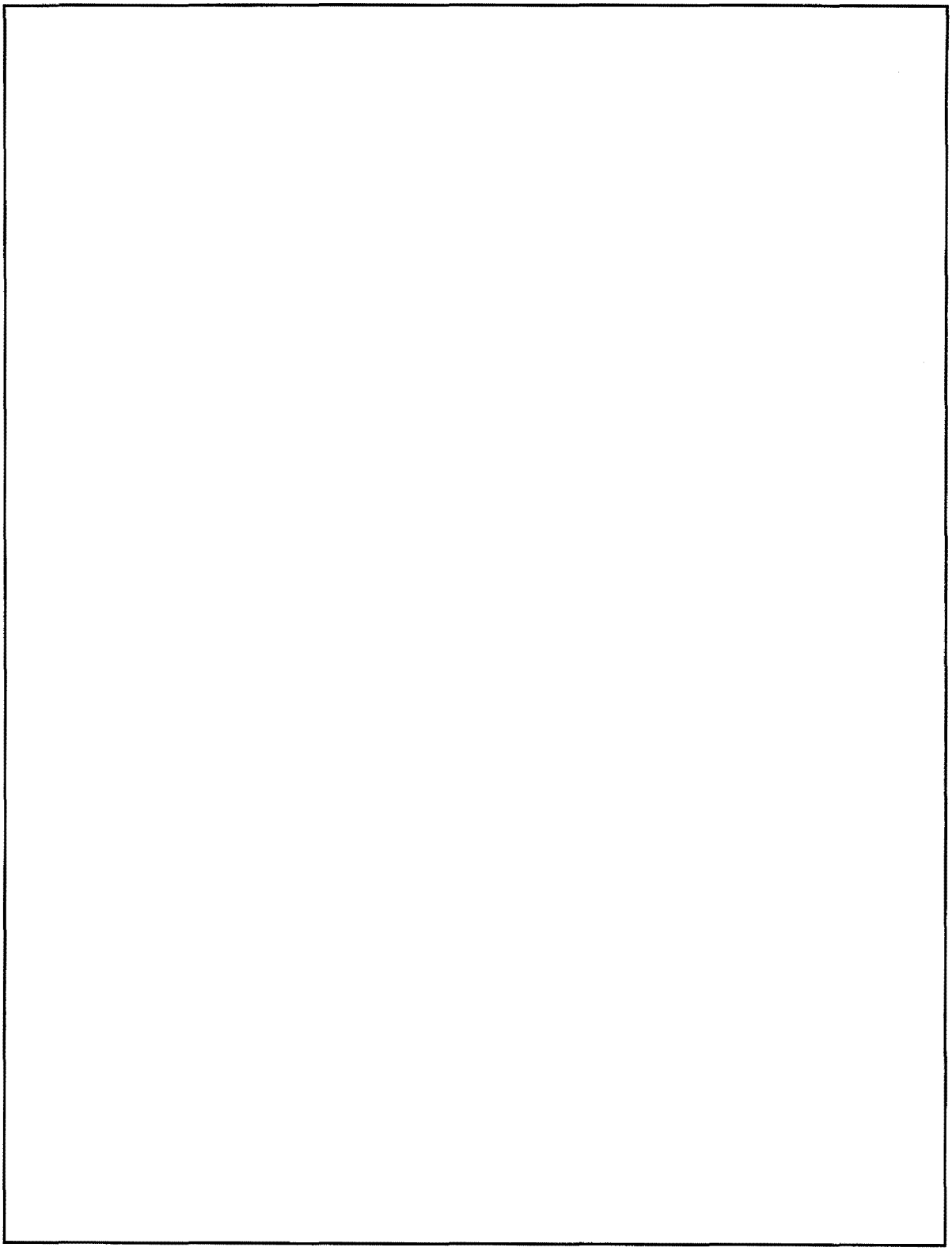
P.L. 86-36
EO 1.4.(c)

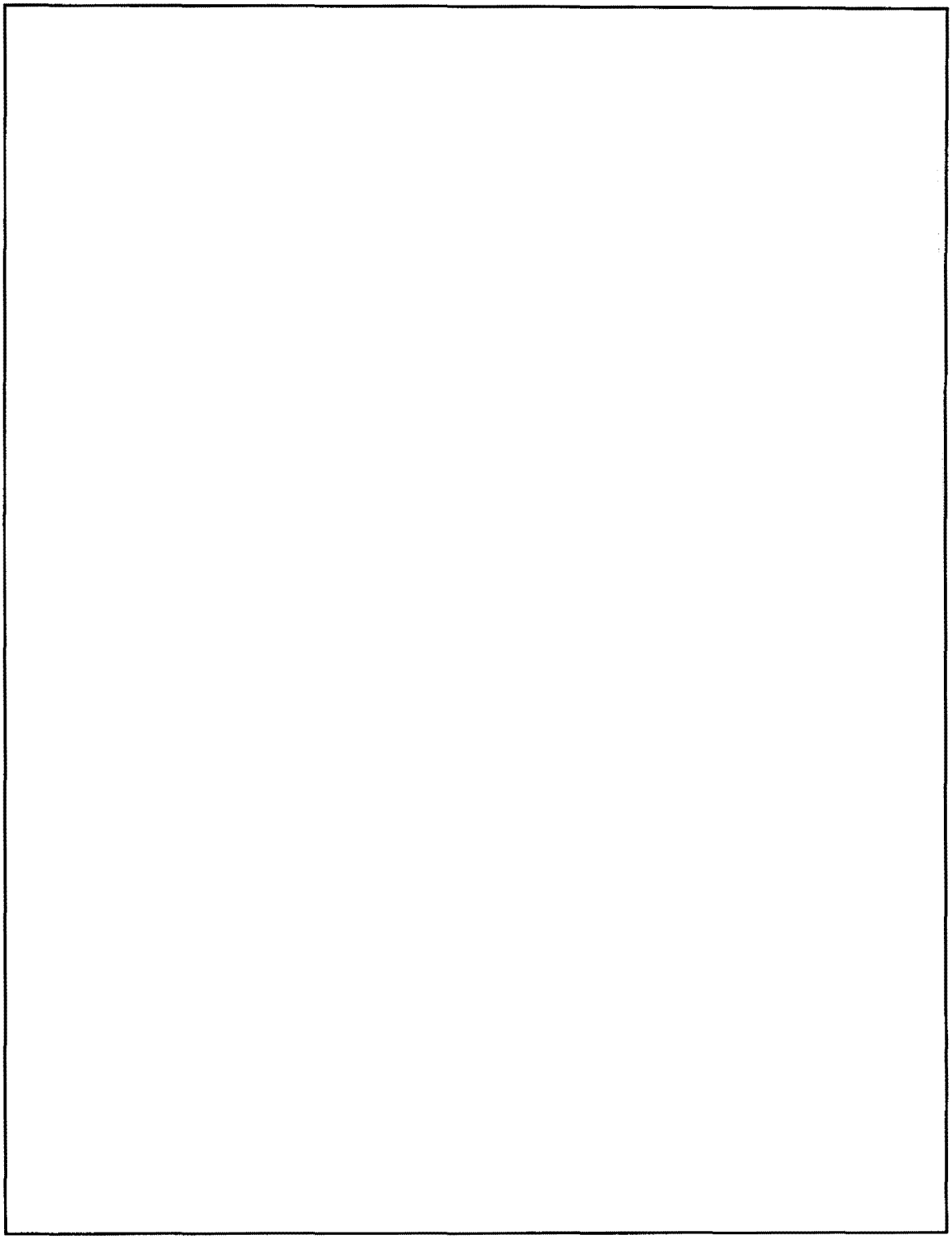
FIRST TALE

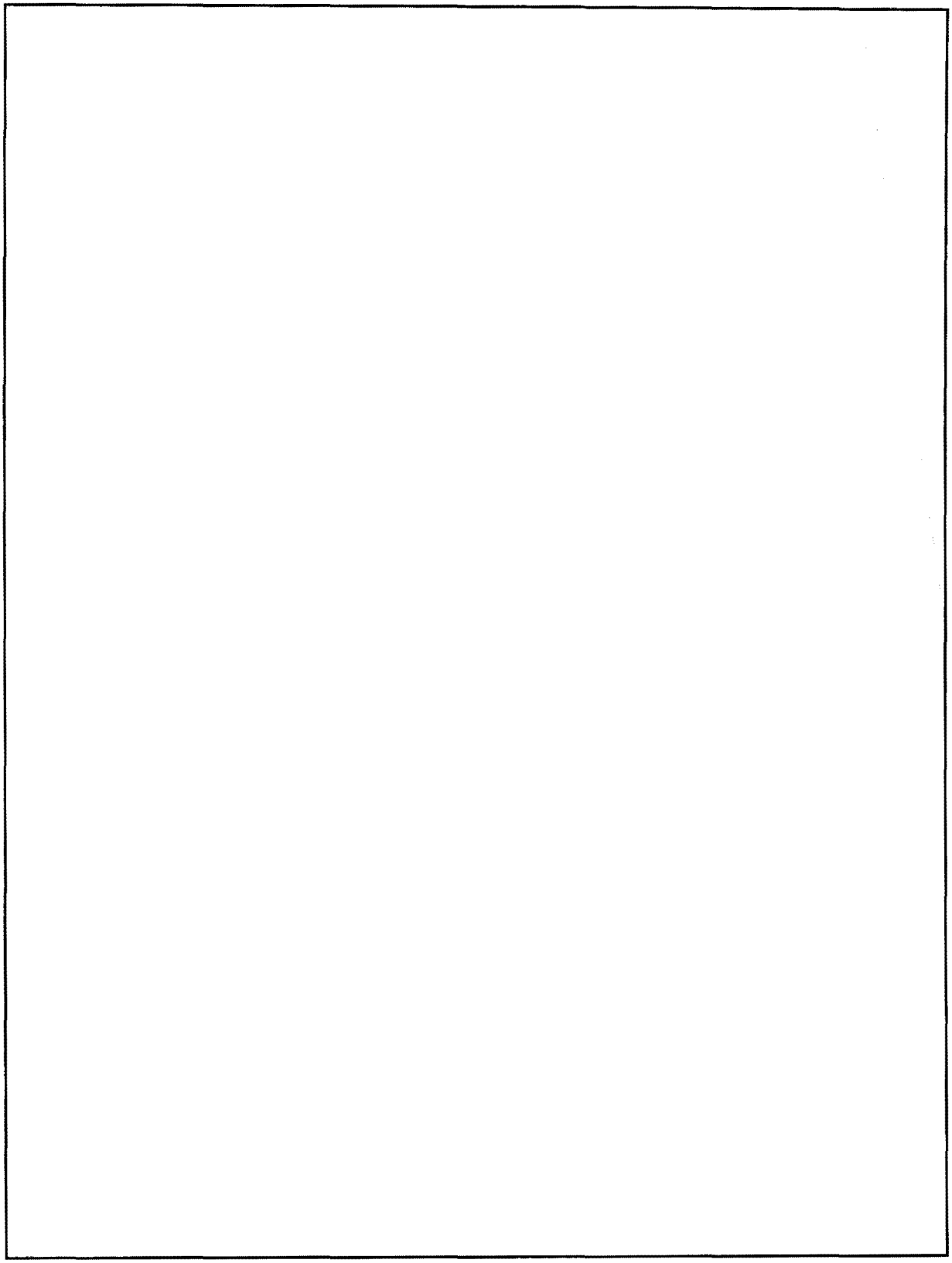
[redacted]

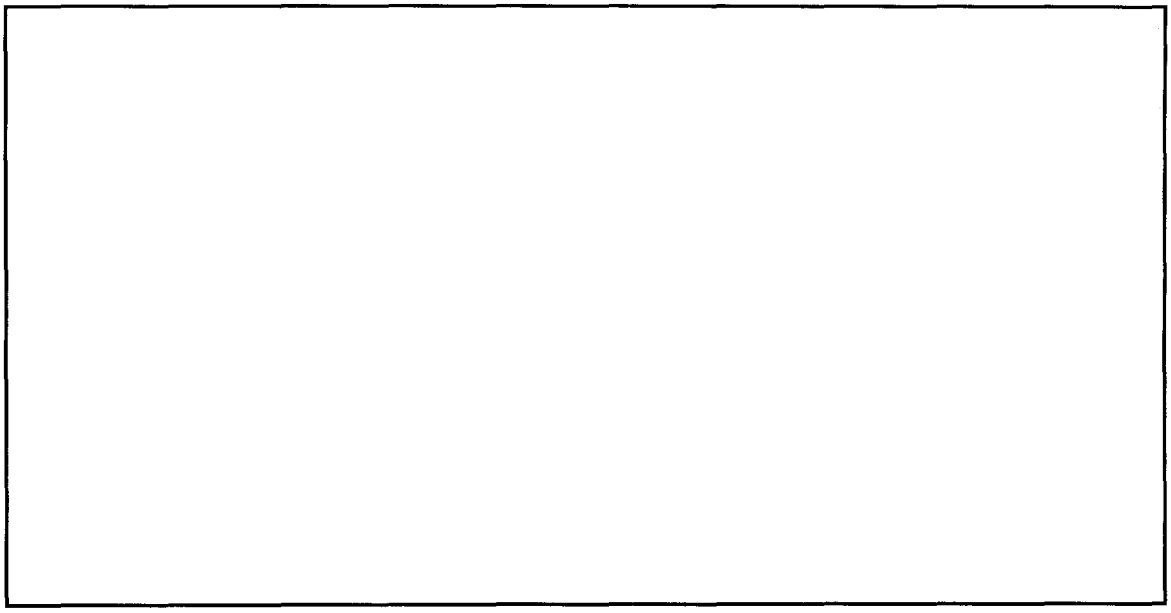












P.L. 86-36

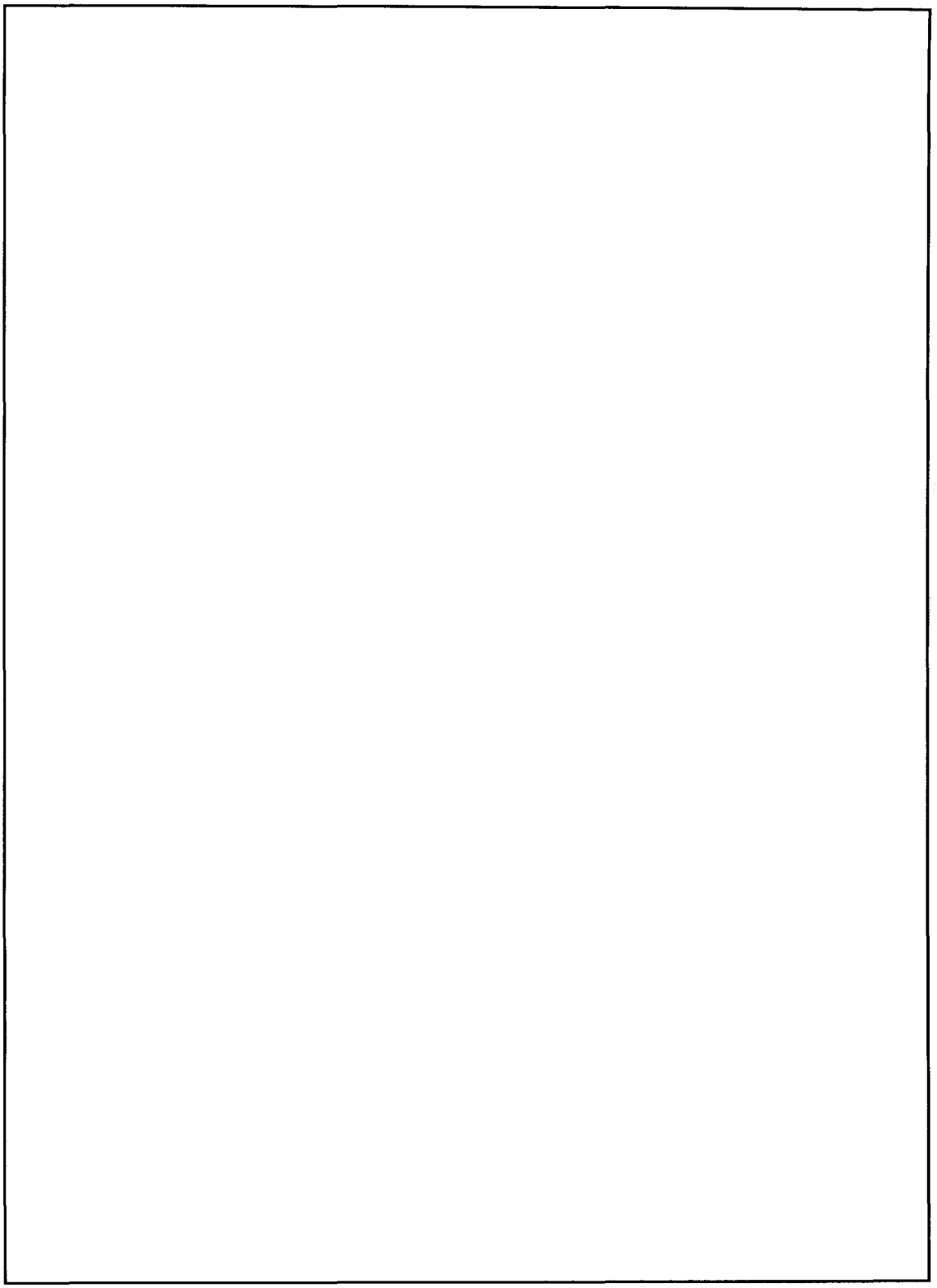
Maybe It's Related to the Phase of the Moon

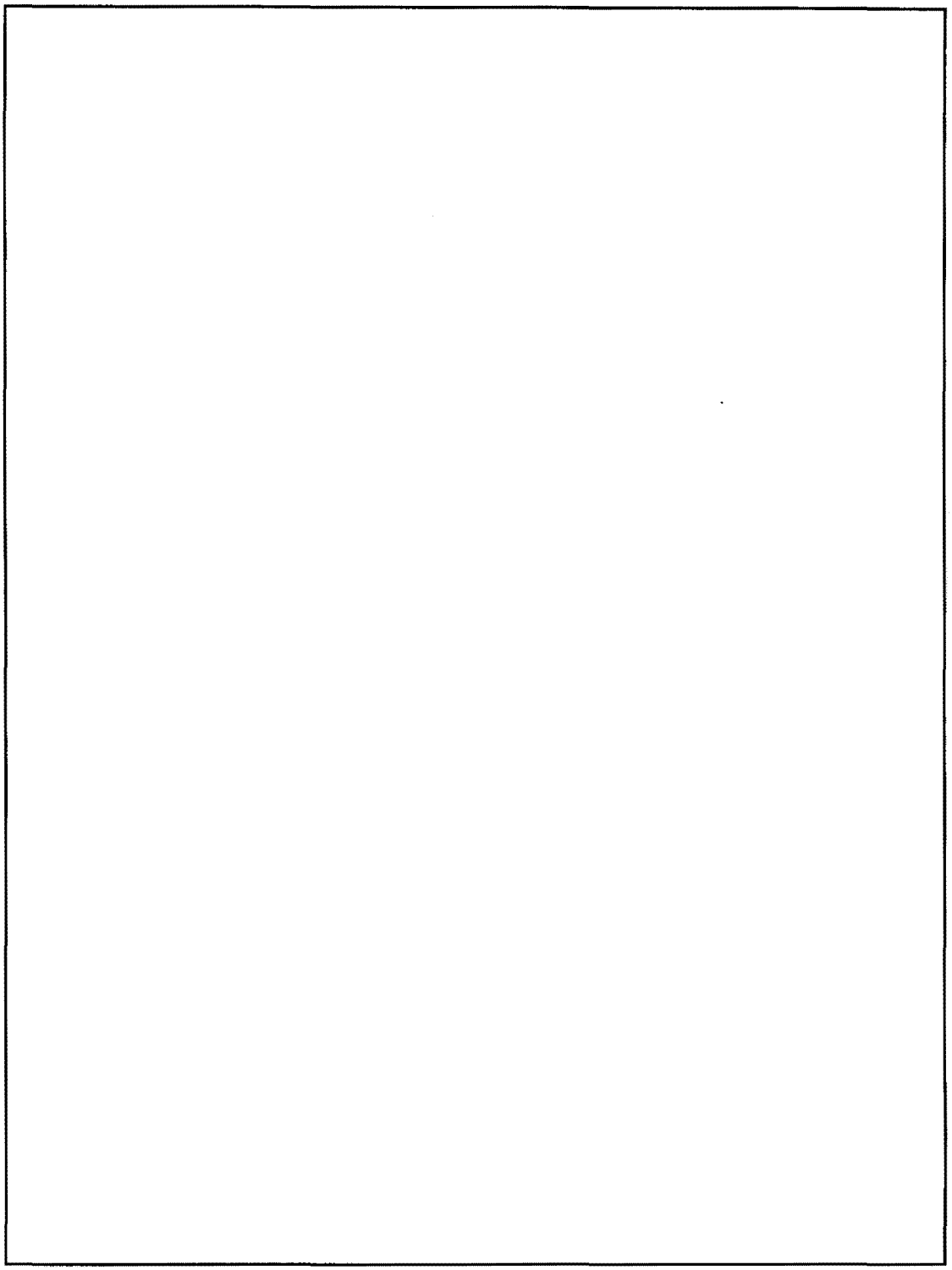
P.L. 86-36
EO 1.4.(c)

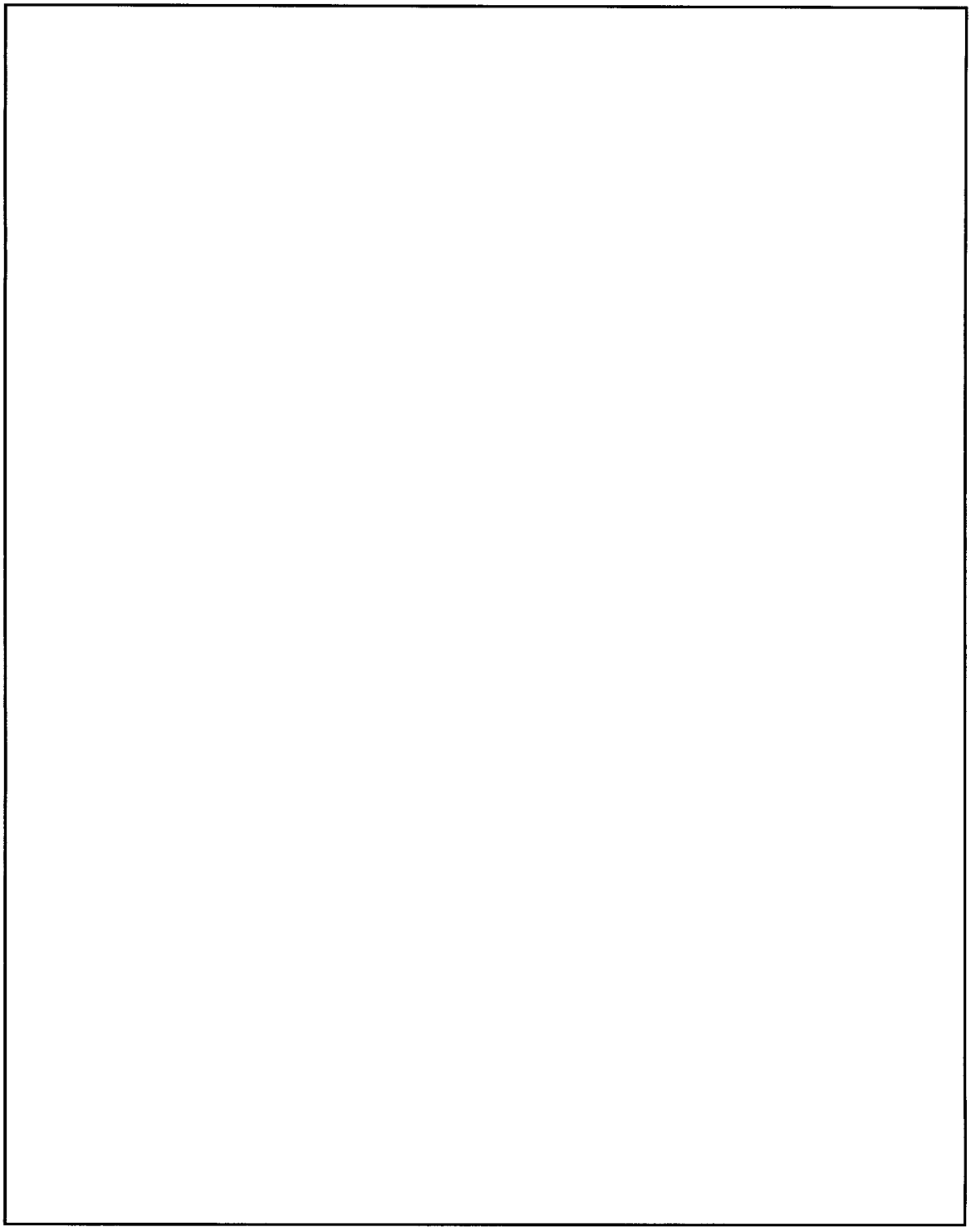
[redacted]

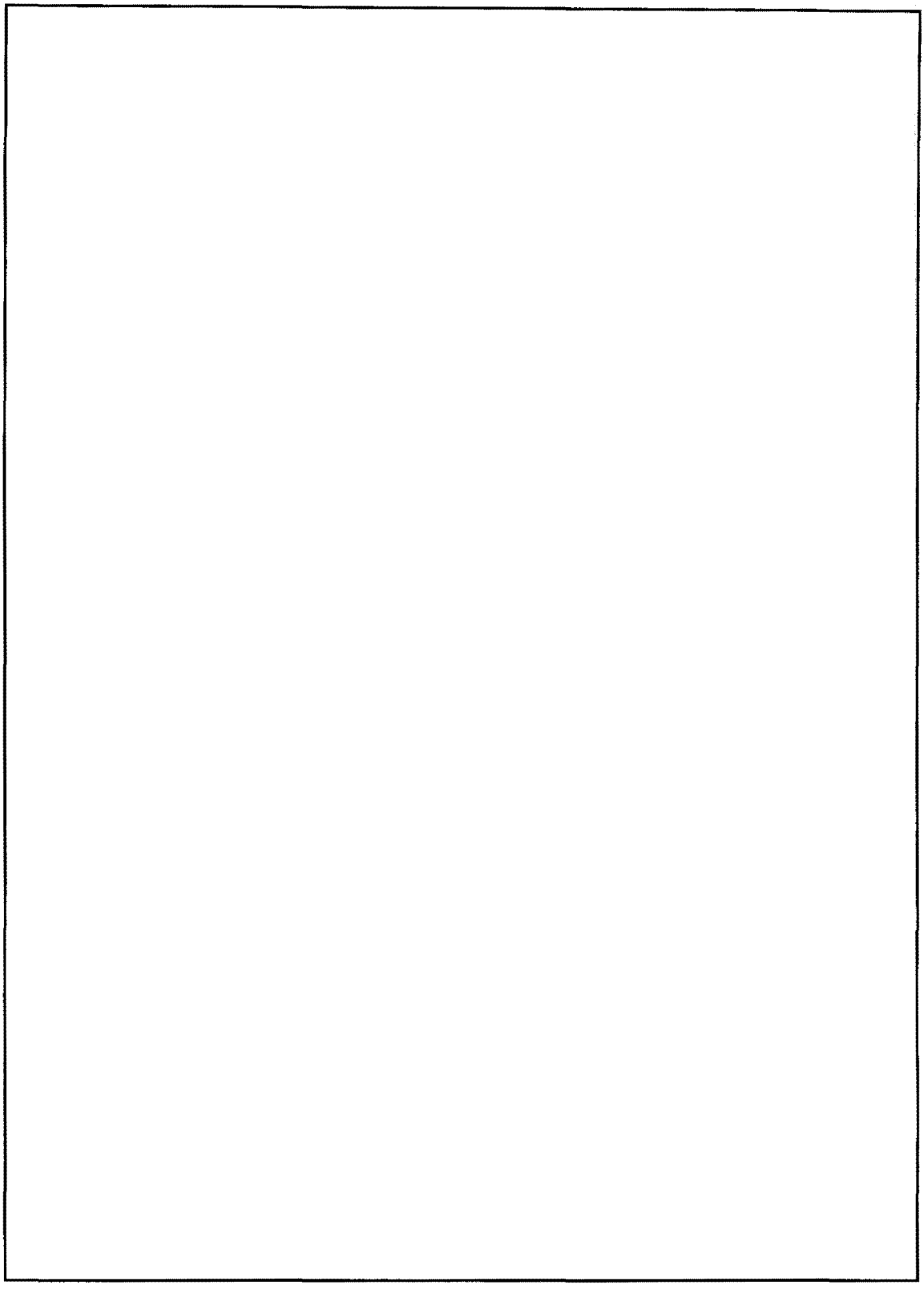
This story of the dissection of a callsign system proves the validity of that old saw "Many a true word is spoken in jest." It proves a lot of other things, too – among them that it ill behooves the cryptanalyst to dismiss the word spoken in jest too quickly. But you may ask what a cryptanalyst is doing "dissecting" a callsign system in the first place – isn't that a job for a traffic analyst? Well, in case some of us haven't yet learned the lesson that you can't really draw a line between the work of the cryptanalyst, the traffic analyst, and the linguist, this story provides a bit more proof of that, too.

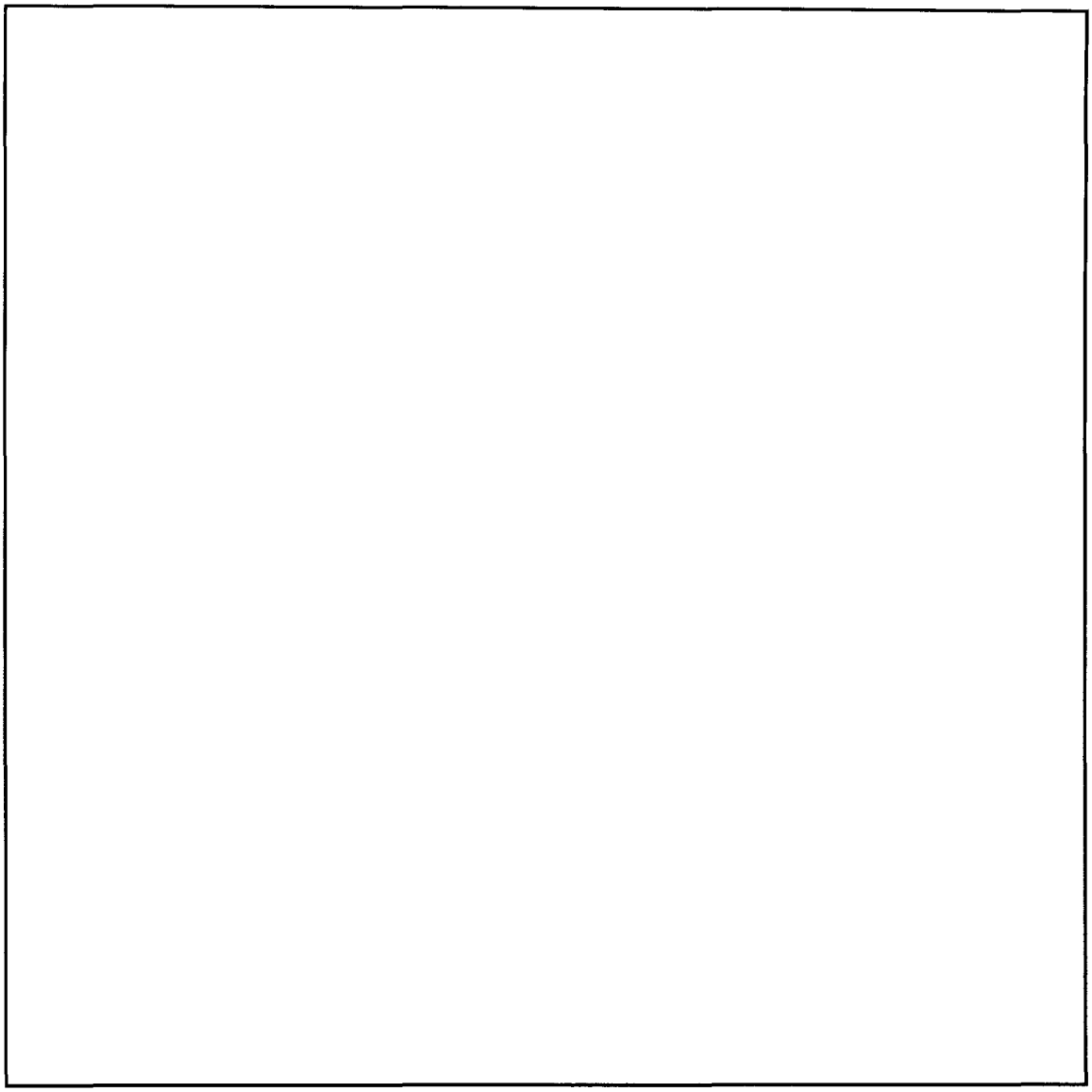
The reader has probably guessed by now that the title of this piece was the "true word spoken in jest." But it wasn't really spoken entirely in jest, because we knew that many of the [redacted]









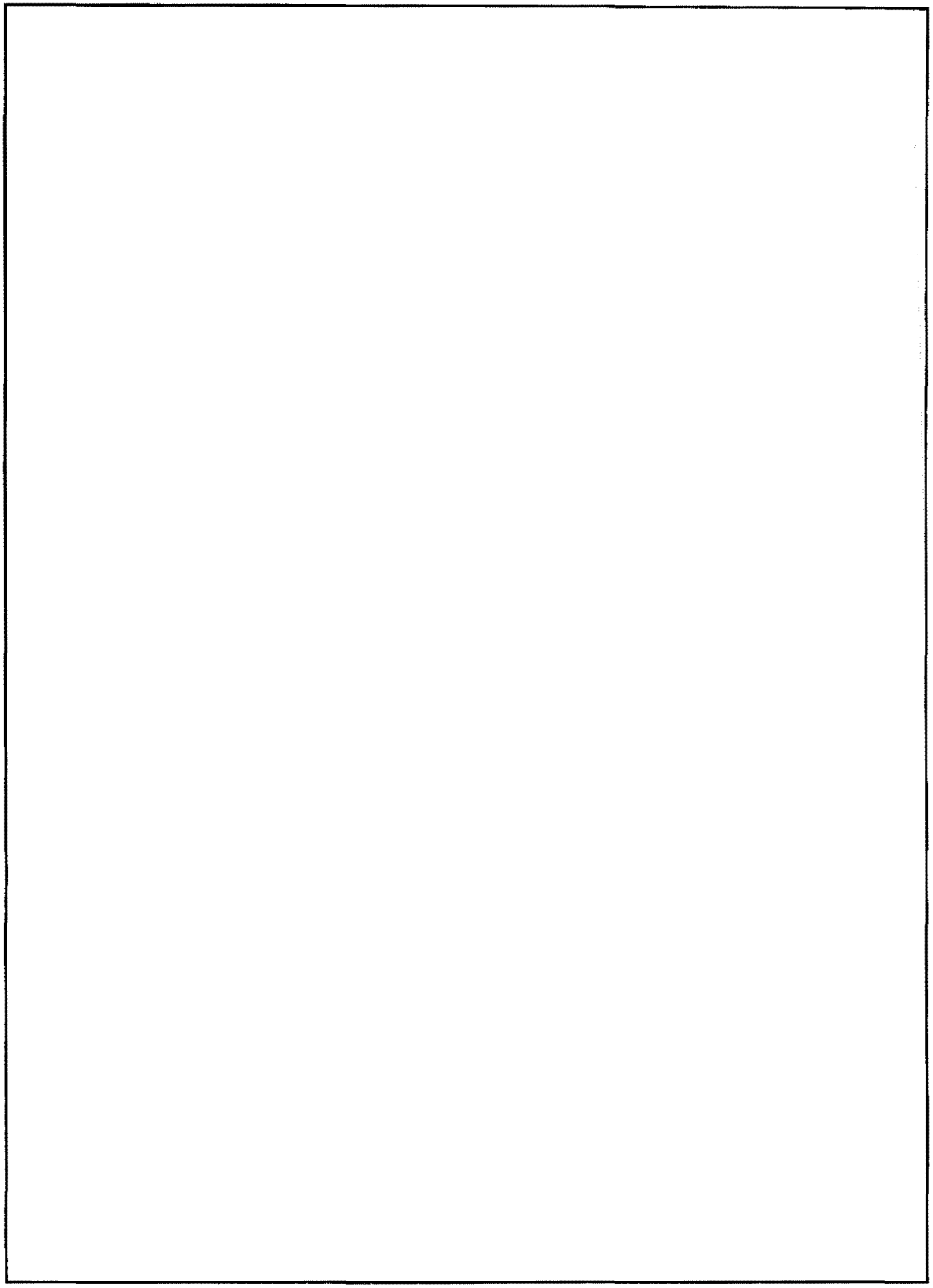


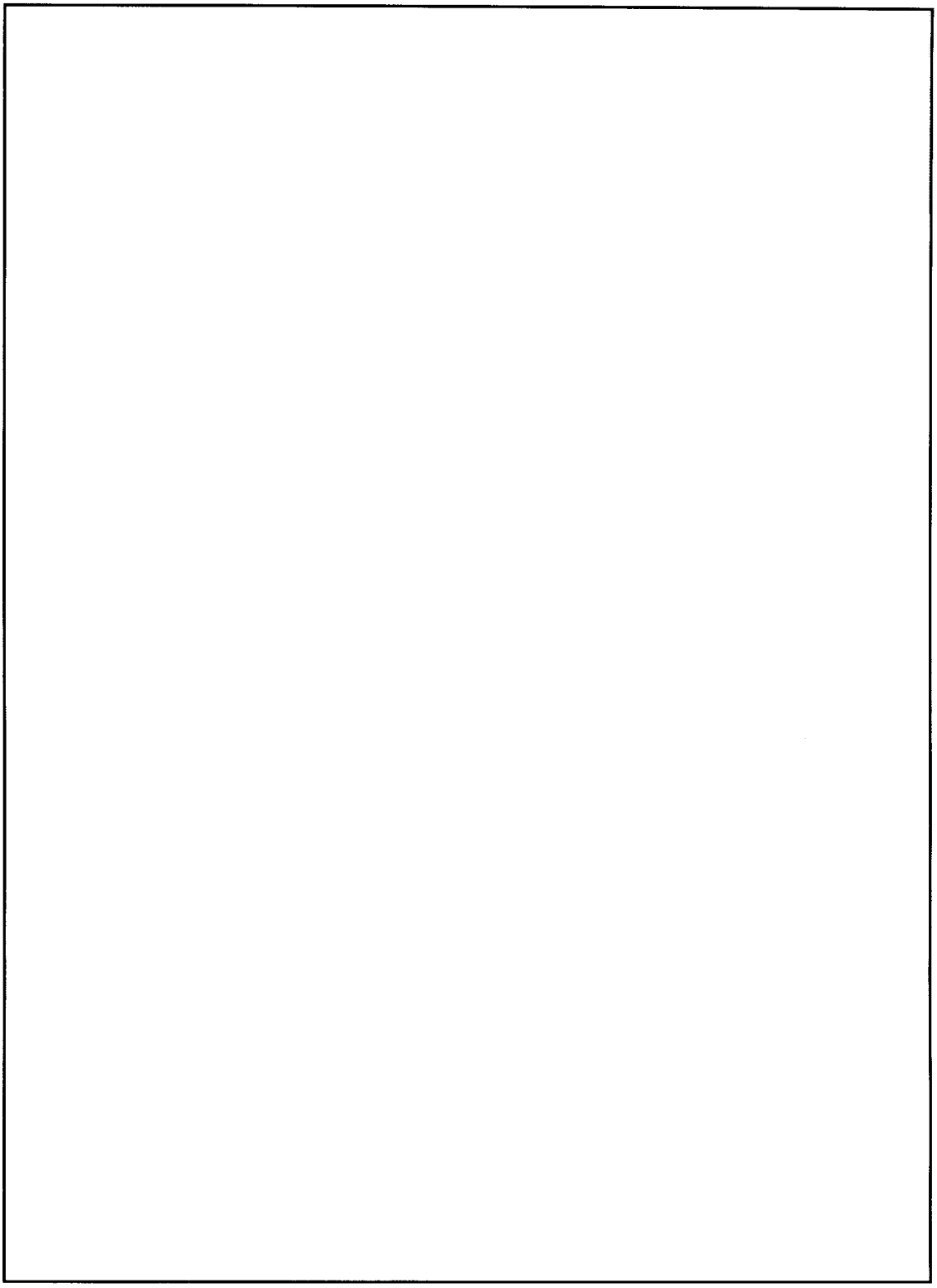
[redacted]

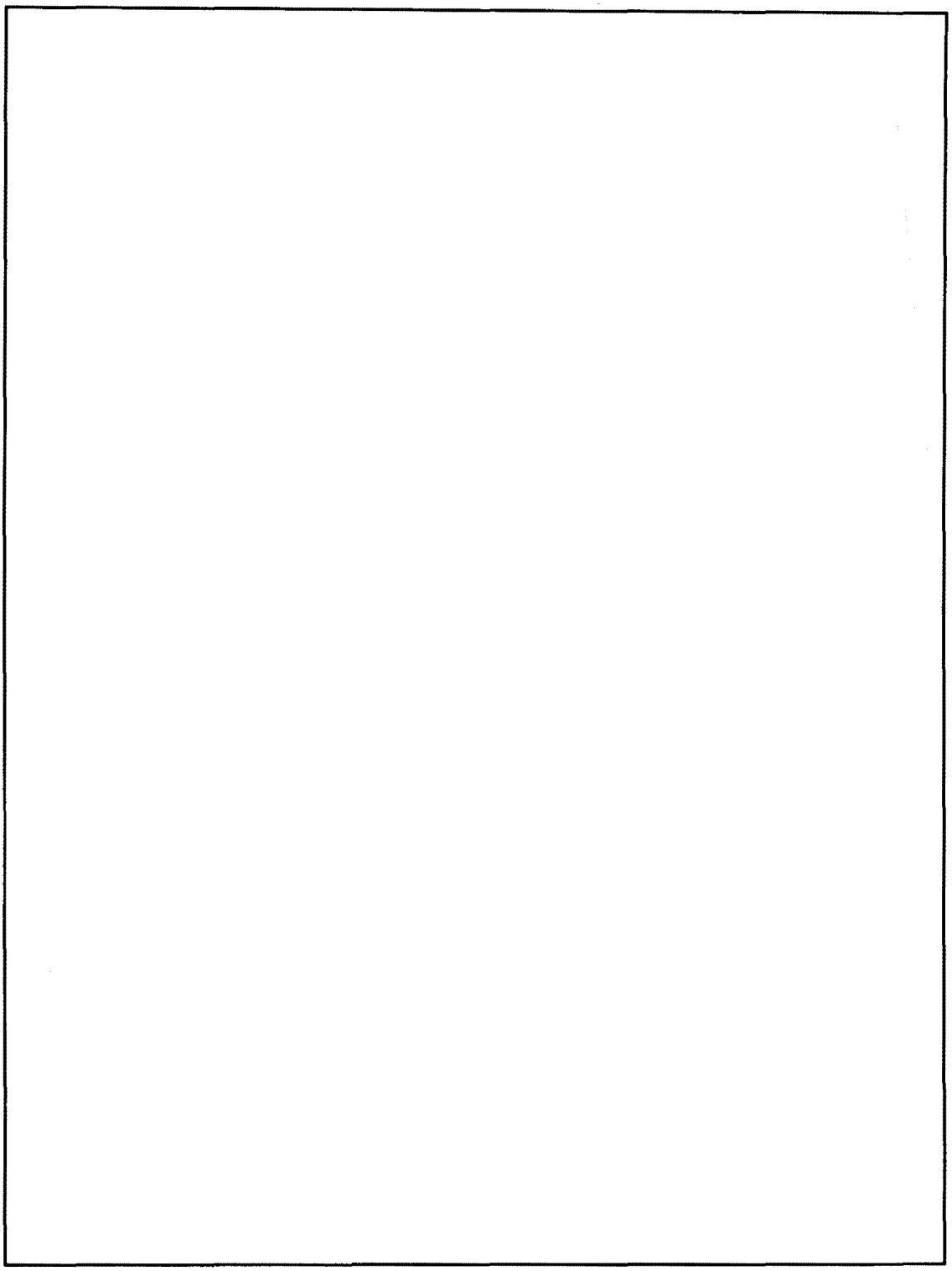
P. L. 86-36
EO 13526 1.4(c)

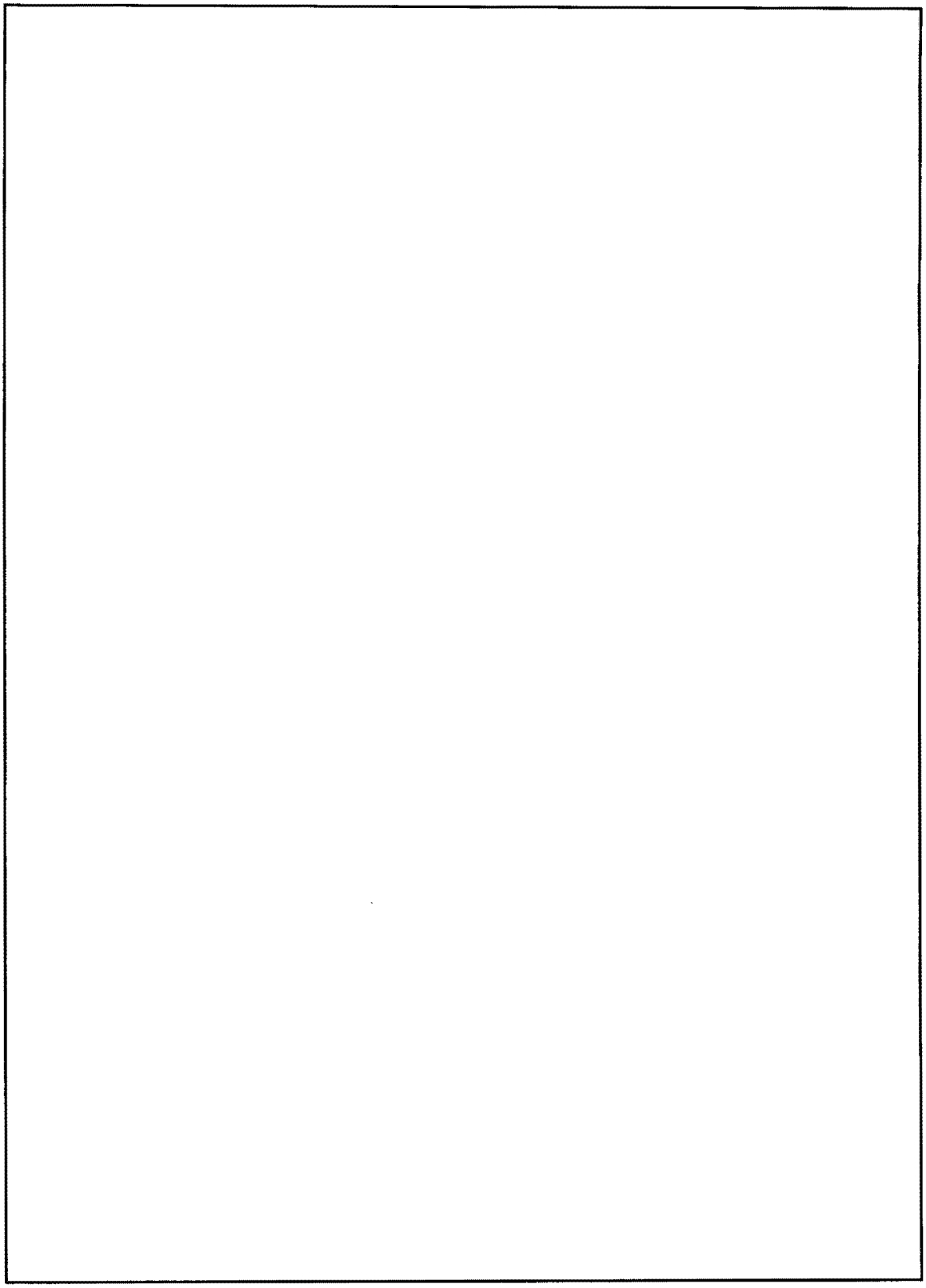
JAMES D. DELANEY

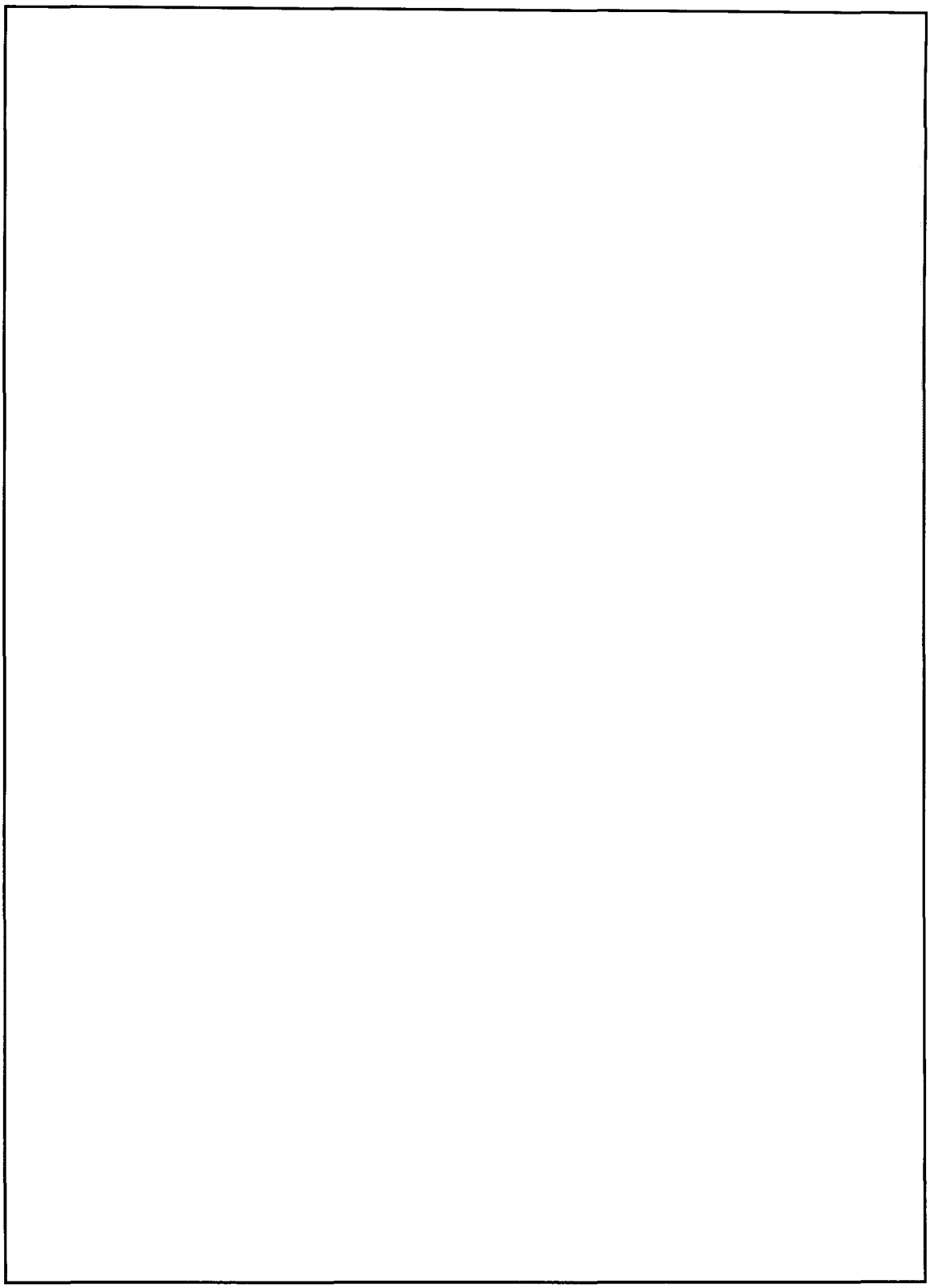
[redacted]

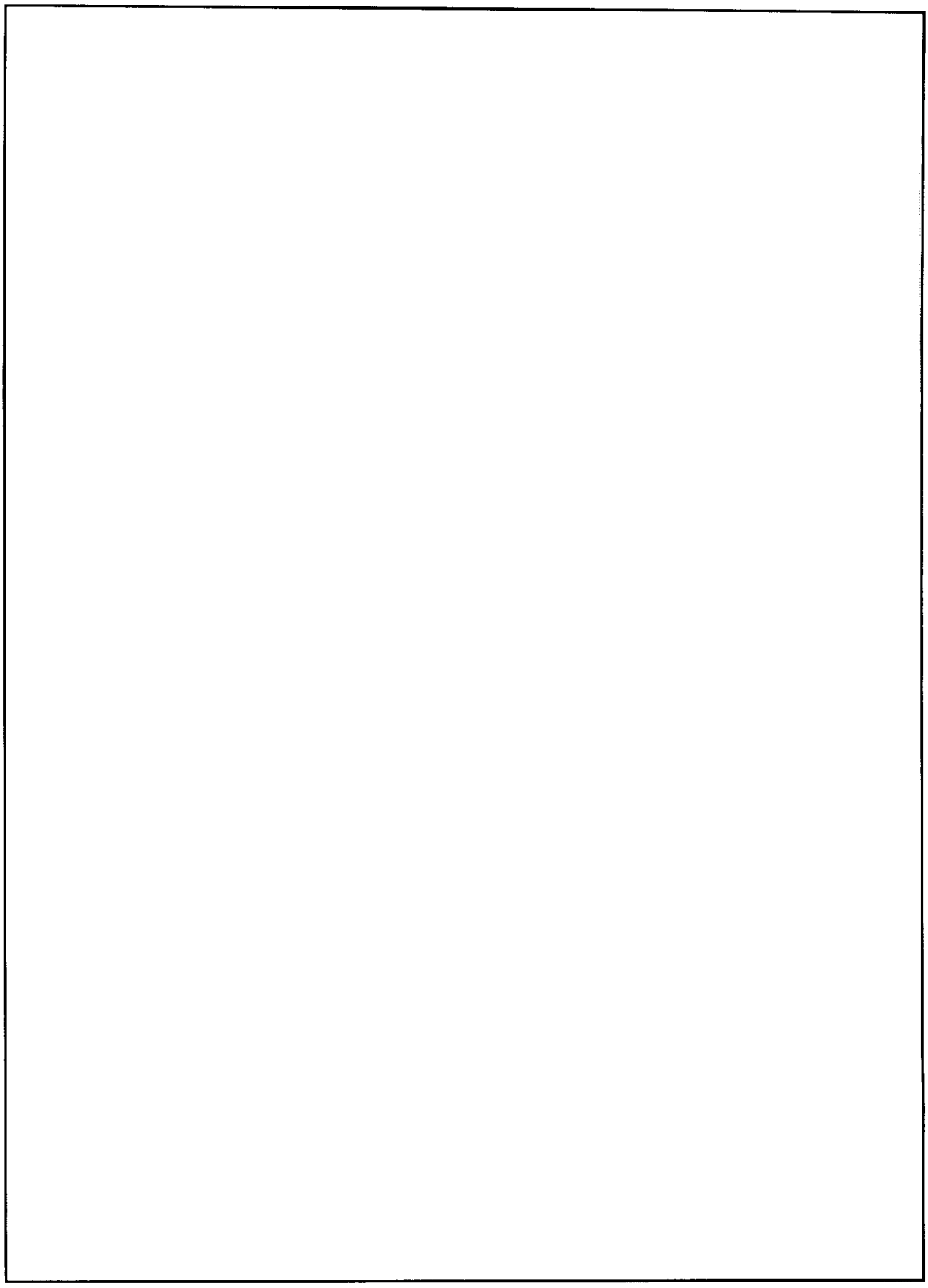


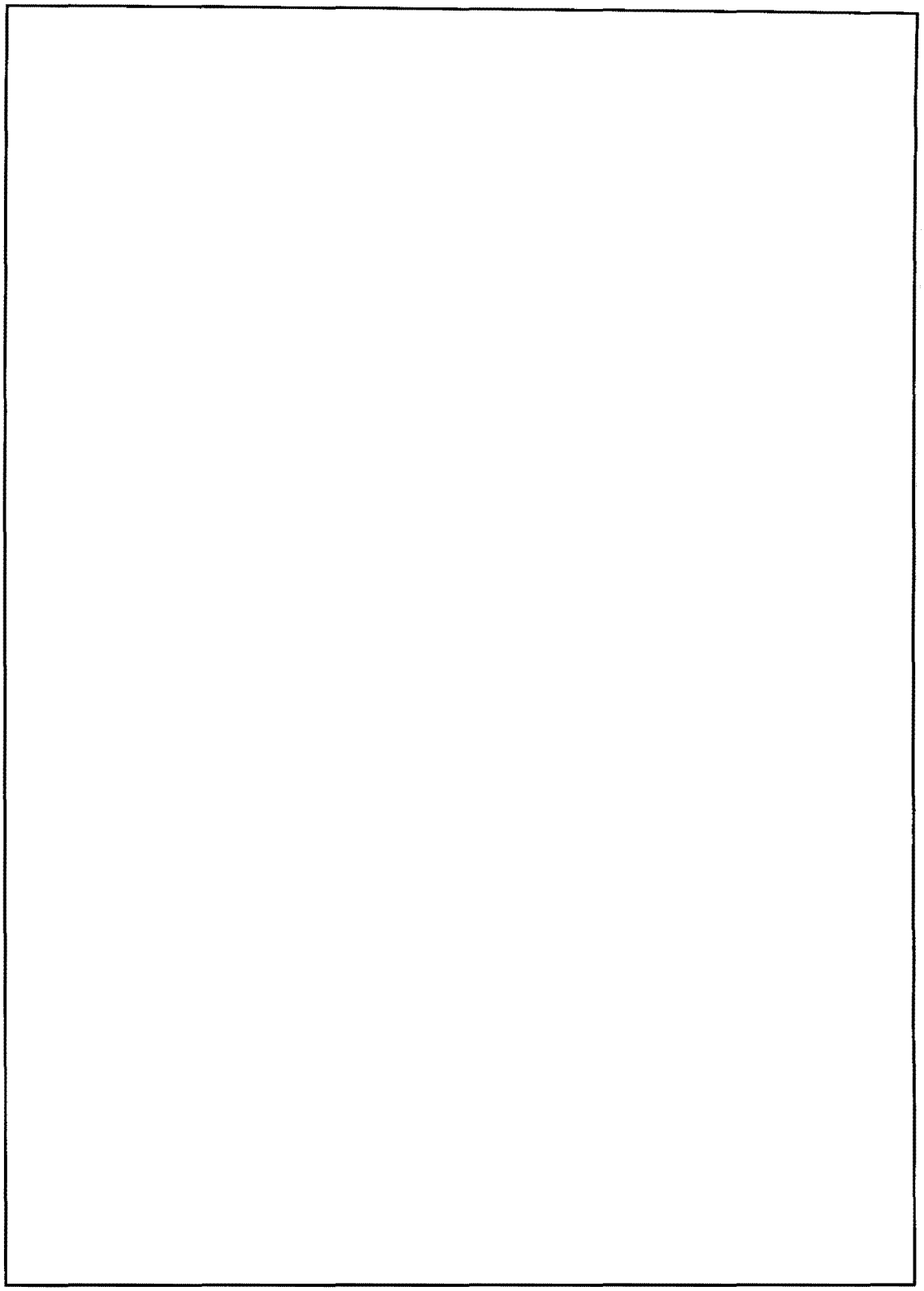


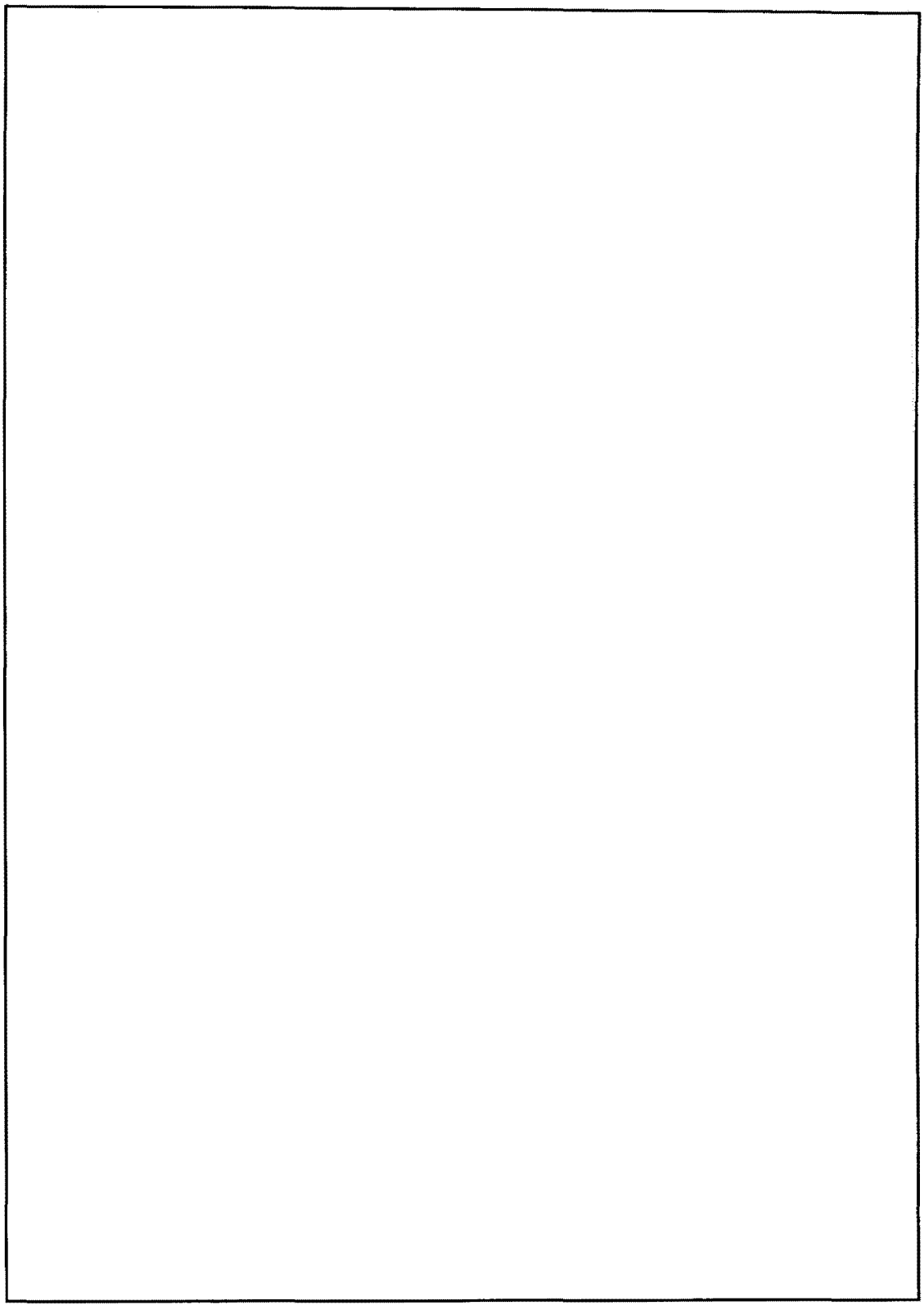


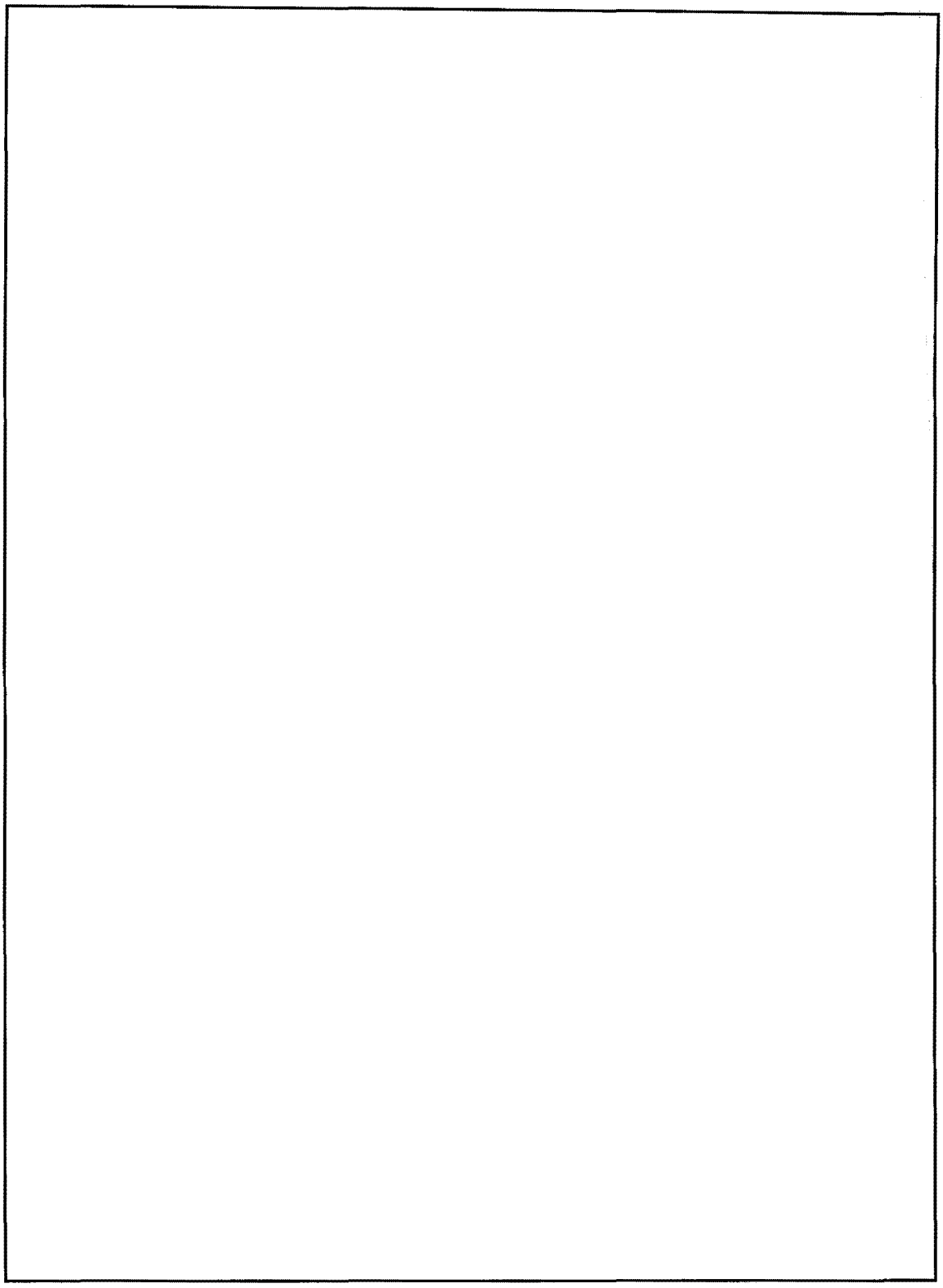


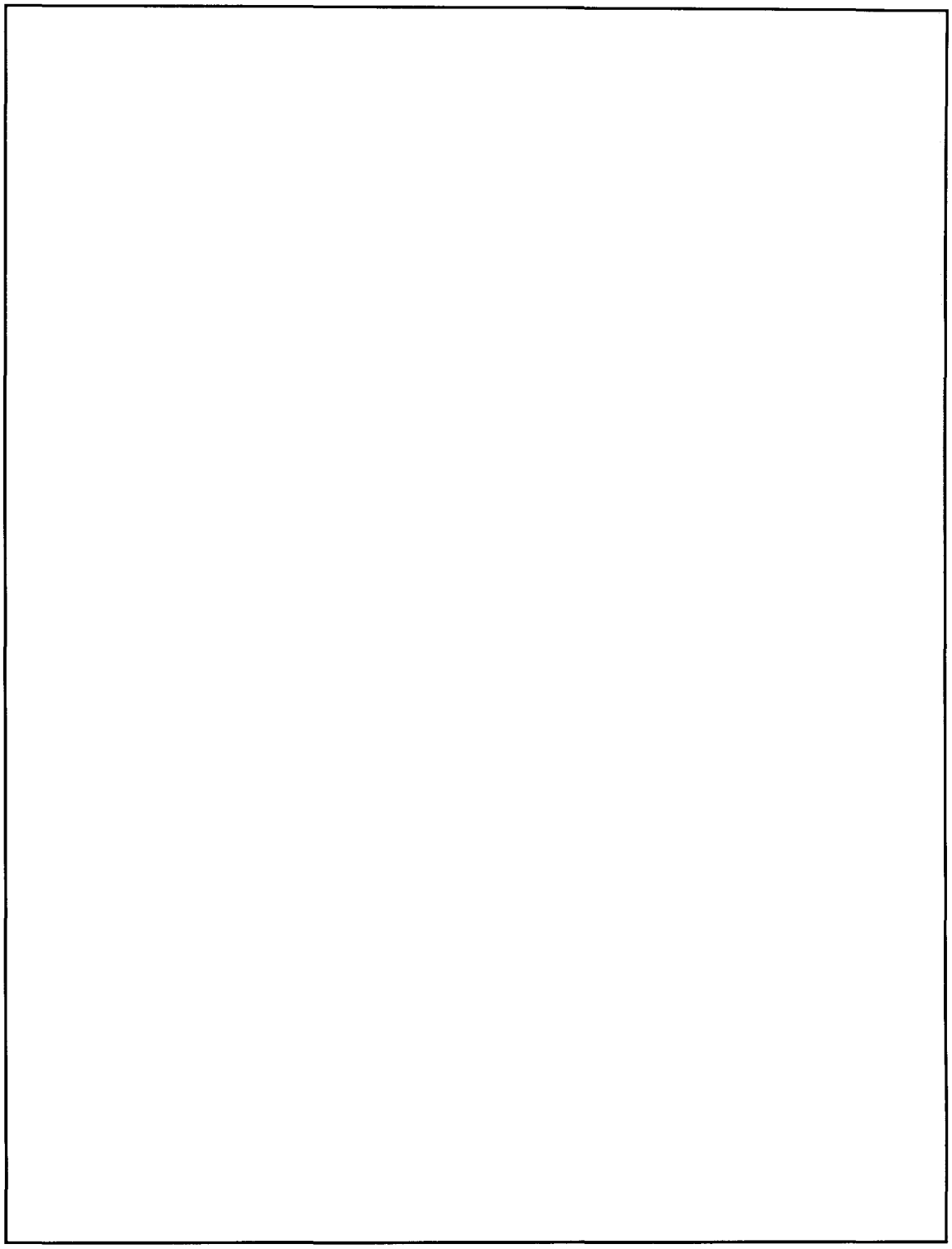


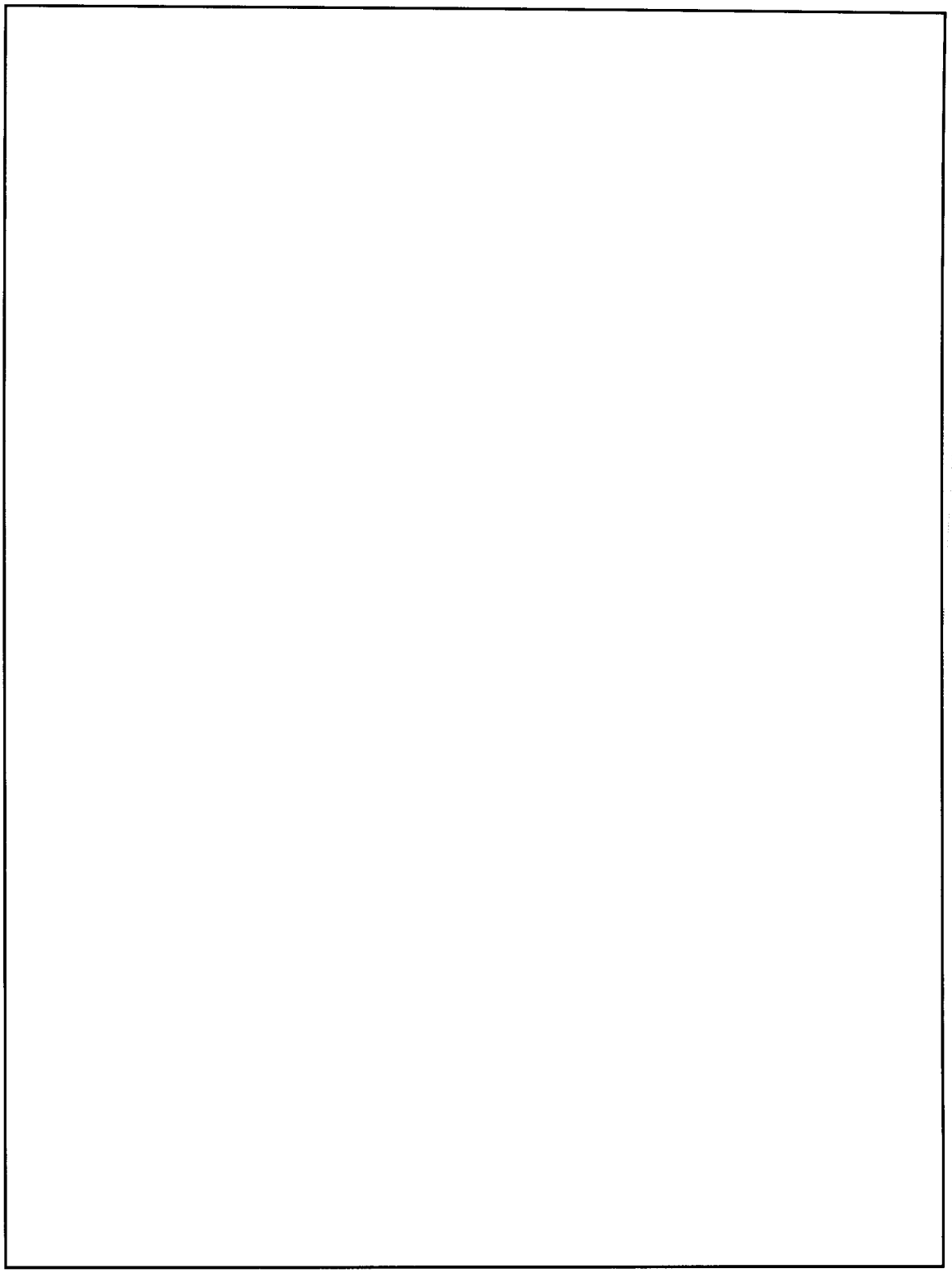








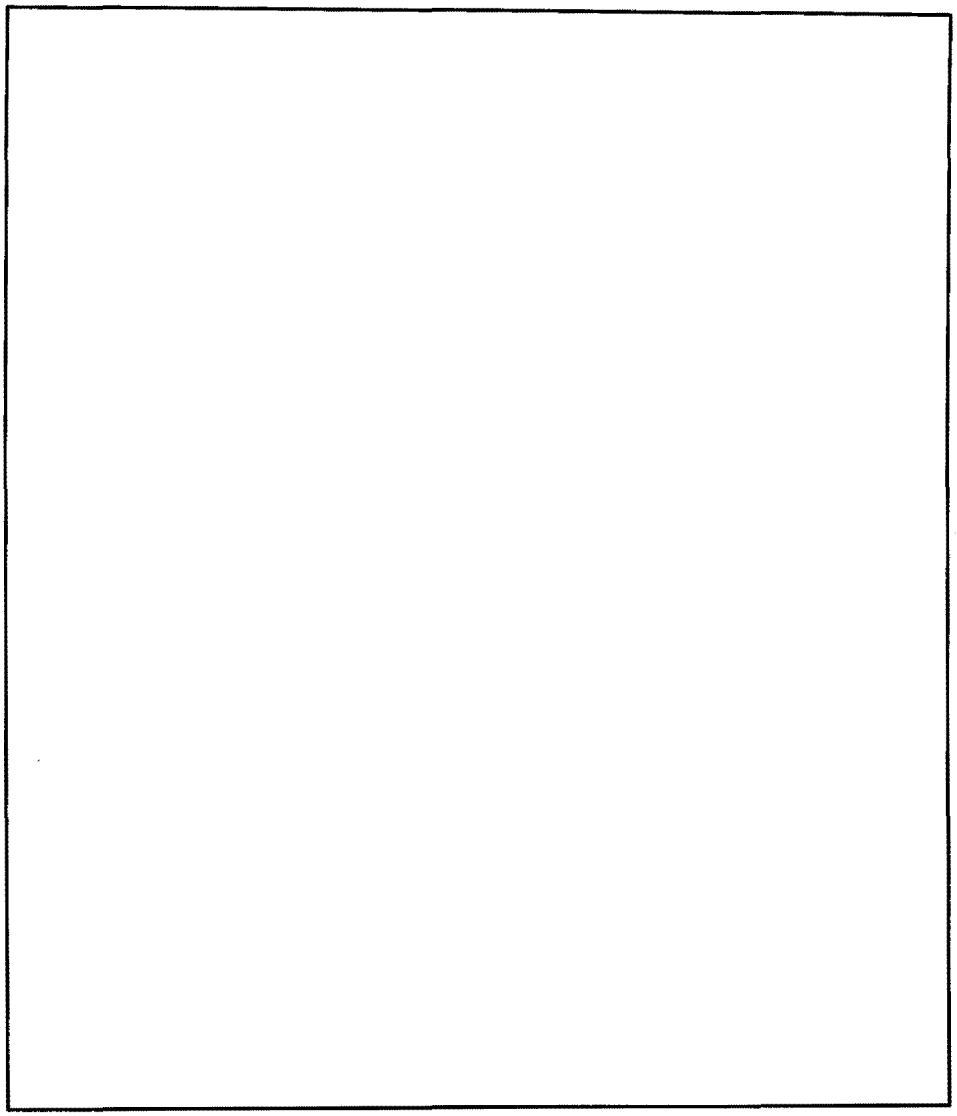




P.L. 86-36
EO 1.4.(c)

Acknowledgments

In recording the story of type [redacted] foremost recognition belongs to Mr. C. Garofalo (P1), who so capably directed the exploitation effort (as on every other [redacted] system) during the first year. Recognition also belongs to the many other dedicated members of the [redacted] Task Group, including analysts from P1, A61, and the former A2. I took over the task group at the end of the first year, after the initial trauma was past and the system was well on its way to recovery.



Area Studies and Their Place in Traffic Analysis

[redacted] P.L. 86-36

The area study of a target country and its foreign influences provides essential support to the traffic analyst in developing a knowledge of existing communications and in selecting methods for the exploitation of these communications. Area studies include a broad and diversified range of factors influential in communications development.

Initially one should become familiar with the physical terrain of a country. If there an outlet to the sea? If so, what communications serve the area? If not, is the country dependent upon another area to import and export material? Is transportation limited to natural means such as rivers and narrow roads, or are there adequate transportation facilities by which movement within the country can be accomplished? Is the area mountainous, thereby interrupting long-range communication, or is the land basically flat, aiding in long-range contact? What is the climate like? Is it extremely hot or cold? Is the weather a factor in the method used for communications, or does it have little effect?

In Africa an important developmental element is the European colonial power that ruled the area prior to independence. Each power imported its own communications equipment and trained its subjects in its own methods. Whether the colonial power was Britain, France, Belgium, Portugal, or Spain made a considerable difference in the procedures introduced and the level of sophistication achieved. The influence of the colonial power can be seen not only in the communications but in many other aspects of the developing countries. Of significance also is the present-day rapprochement between the independent country and its colonizer, in the type of aid agreements and the dependence of the new country.

The level of the communications is also dependent in part upon the education level of the technicians. Areas of low educational opportunities cannot be expected to employ sophisticated operating procedures. However, it has been noted that each year they become more advanced.

The administrative structure of a country is an especially valuable factor in the understanding and exploitation of the communications structure. If facilities are limited, it is to be expected that they will be placed where they are most needed. Frequently different organizations employ the same set of facilities for communication purposes. A normal pattern in Africa is to have the control station located in the capital city of the country with the outstations in the provincial capitals and any subordinate stations located within the area encompassed by the province. A knowledge of the administrative structure greatly facilitates the reconstruction of these networks. Along the same lines, a basic understanding of the organization of the police and military in each country is particularly useful.

Having acquired a basic understanding of the rudimentary background of a country, it is most helpful to have a knowledge of the attitudes of the people. This enables a traffic analyst to understand why various acts are performed and to anticipate the possible outcomes of any given events. To understand the people of a region, one must closely examine their historical background. What are their social patterns? How have they evolved and what part do these play in the daily life of the people? What are the religious beliefs and how strongly do they influence the people? Is the population, on the whole, stable, or are the people inclined to rise up easily against control? While these factors may not be readily discernible in countries of a high level of sophistication, they play an increasingly important role in the developing counties.

The political make-up of a country also is a gauge in the development of communications. Is the government popularly elected? Do tribal or party affiliations play important roles? Is the government a military dictatorship? How susceptible is the civilian government to a coup d'état by the military or some other factor? What is the party structure? Is the country ruled by a one-party government? Is the government corrupt, and what are the chances for subversive activity? If subversive elements exist in the country, what is their background? Are they communist-inspired, or is their raison d'être one that can be more easily remedied?

Bordering countries should be studied on the basis of not only their colonizer but also their relationship with the country of primary interest. If dissident elements exist, are they receiving support from a neighboring country? Is the country interested in the downfall of the government of its neighbor? Are there mutual defense pacts or customs unions between the areas? Often the relationship of a country with its neighbors is a determining factor for the structure of its communications. Is it necessary for the country to use transportation facilities of its neighbors? This aspect may involve the development of a communications link between the two countries.

The level of the country's economy and stability indicators should be studied. Are the large concerns operated by the nationals of the country or by foreign technicians? Do the companies have their own communications? Are they within the country only, or do they have a link with the colonizer? If foreign nationals operate the industry, is this a cause for unrest? What is the commercial importance of the country's products on the world market? Do fluctuating prices play an important role in the economic stability of the country? Does the country have important mineral resources so that it might be considered a prize in the East-West struggle? Is there no industry and is the economy dependent upon primary produce for its revenues?

Another area of importance in considering methods of exploitation is the language employed. In the African countries, one of the most secure mechanisms is the use of indigenous languages and dialects for sending messages. This is of importance to the traffic analyst in the area of station locations and military unit locations. An unknown language, like an unsolved cipher system, can place a handicap on the traffic analyst.

Only a few of the many aspects of area studies have been discussed in the foregoing pages. However, it should be readily apparent that area studies play a vital role in traffic analysis.

The 1970s

The Reality of Communications Changes

[redacted] P.L. 86-36

All analysts and managers of analytic efforts must constantly face both the possibility of a communications change on their targets and the consequences of such a change. The term "communications change" frequently causes unnecessary apprehension – the change does not inevitably signal adverse consequences on target identification, maintenance of continuity, and production of SIGINT. Many changes (introduction of new callsigns, frequencies, etc.) on most targets are routine; they occur regularly and are only slight hindrances to the proficient analyst. On the other hand, some communications changes are *not* routine and do have an adverse effect on SIGINT production. They can result in reduction, or even total loss, of capability to identify and maintain continuity on target communications nets and the specific associated terminals. The latter type of communications change is the subject of this article.

* * * * * * *

Changes that might affect exploitation capability will vary greatly for different targets, depending on the extent of current exploitation and on the complexity of the newly introduced operational procedures. However, knowledge of the relationship between various communications features can greatly assist in prediction of future operational usage. Some features that should be considered follow:

[redacted] P.L. 86-36 E.O. 1.4.(c)

3. *Sudden versus gradual change*: Many changes (e.g., newly allocated frequencies) can be implemented immediately upon receipt. Other changes require "live" testing and extensive operator training and orientation. The following changes, for example, would probably require an extended period for implementation:

a. *Introduction of a more sophisticated mode of communications*: Equipment procurement is usually limited, and testing and training are required before the new system becomes operational.

b. *Use of a new Morse cut number system*: Operator training is obviously required prior to full implementation.

c. *Introduction of abbreviated language for chatter:* The nationwide replacement of English by abbreviated [redacted] as the vehicle for operator chatter is an example of a change requiring extensive operator training. P.L. 86-36 E.O. 1.4.(c)

Some indicators of an impending communications change are

1. Temporary extension of the normal period of use of existing SOI materials;

2. Limited testing of new procedures on existing links/nets or on supplementary communications;

3. Direct references in chatter to new procedures. Such references could consist of anything from a casual implication to a statement of the effective date and type of new SOI materials;

4. Trends toward standardization or diversification, whichever is applicable;

5. Use of or references to more sophisticated modes of communication.

****

Although the ability to predict impending communications changes is a distinct advantage, recovery of continuity on target communications is greatly expedited by contingency planning that defines actions to be taken following introduction of new SOI materials. Contingency planning in preparation for subsequent analytic recovery must be realistic and flexible. Consideration should be given to the following factors:

1. *Timely field station reporting of deviations from the norm*: As the mission of most collection sites is limited in scope, this reporting permits higher echelon to make an early assessment of the overall extent of the communications change, to advise all elements concerned, and to issue necessary instructions.

2. *Target recognition/identification*: Even though such things as callsign and frequency usage have changed, the best source of target recognition/identification is the operator who has copied the target in the past and who will probably recognize it in the future. Operator identifications should be considered valid unless disproved. These identifications should be provided, in a format usable for traffic identification, to other field sites that are tasked with similar targets and that are likewise encountering difficulty in isolation and identification of mission targets. Thus, time will not be wasted in copying communications that are another site's mission.

3. *Establishing procedures for early continuous follow-up collection on potentially mission-associated communications*: Although these communications may not be

identified beyond nationality, establishing procedures for early collection will prove most advantageous.

4. *Determining possible methods of attack as a means of associating homogeneous intercept and performing follow-on analysis*: In making this determination, we must ask, "What would we do if the old tried and proven analytic techniques and aids were no longer available?" A definitive answer to this question will probably not be found, but alternate approaches can be devised. For example, if callsigns cannot be exploited, related intercept can often be associated on the basis of [redacted] features. These features may, therefore, need examination very early after a communications change. P.L. 86-36 E.O. 1.4.(c)

5. *Once the possible methods of attack have been determined, developing detailed procedures for quick implementation*: These procedures include issuing instructions to be followed in the event of a communications change, outlining processing (preferably in conjunction with a flow chart), and devising the machine software that would be needed for machine processing. Processing of data after an extensive communications change does not require completely new procedures, although some alternation or expansion of existing standard procedures will probably be necessary. Maximum retention of established procedures, which are already well known to all operating elements, will cause minimum confusion following a communications change and will aid in early recovery.

6. *Maintaining continuous documentation on all special processing or analytic actions taken and the type, extent, and data of actual changes in target SOI*: This documentation will aid in keeping all elements currently informed and in preparing for later SOI changes.

****

If this article succeeds in stimulating more realistic planning for future communications changes, deterioration of SIGINT production after such changes will be minimal.

A Note about Organizing T/A Problems

P.L. 86-36

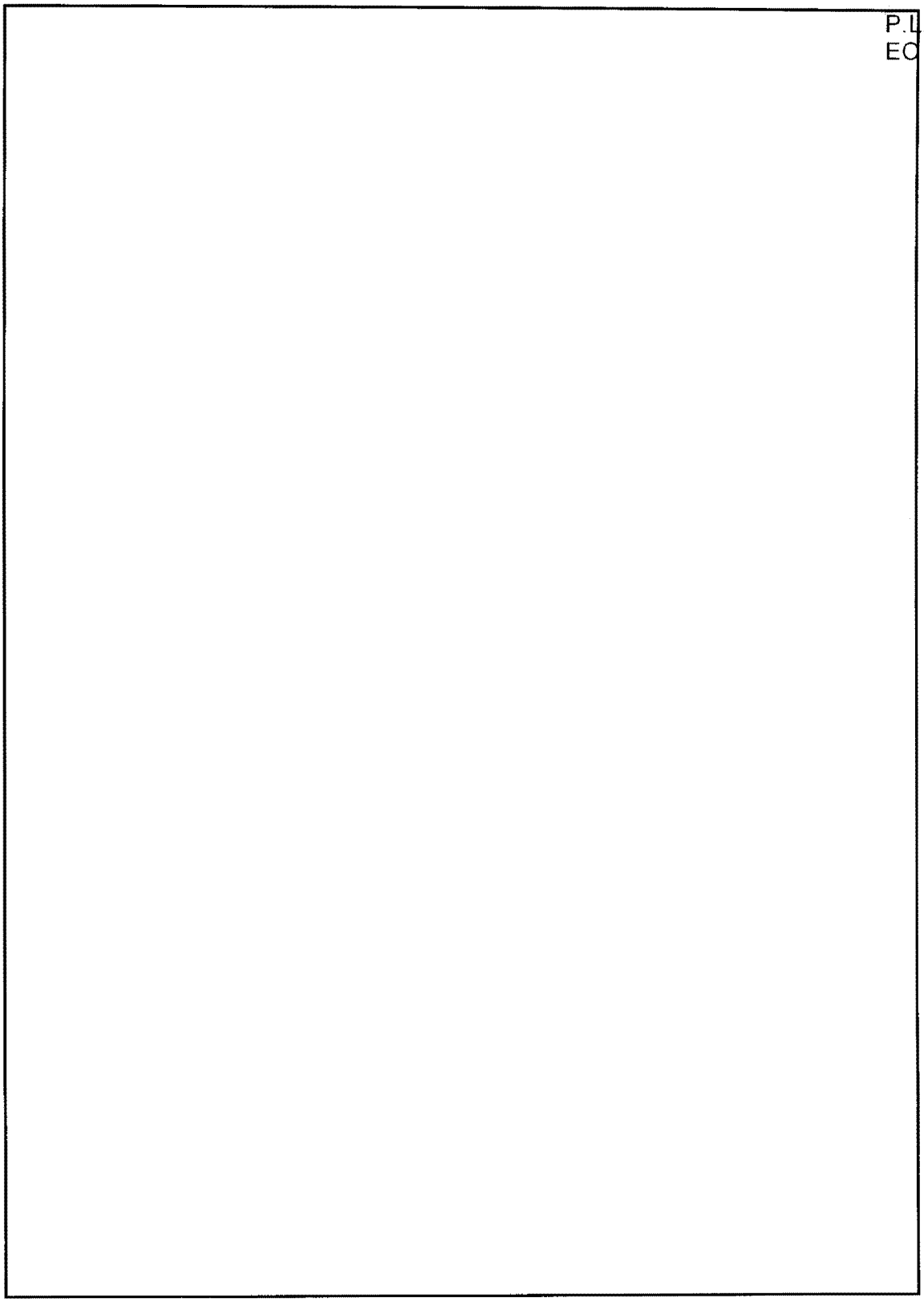
The ancients (Greeks, I think) believed that there was a central and fundamental Truth that underlay all worldly things and that man's goal should be the discovery of that Truth. In my salad days, as I wrestled with questions about how to organize a T/A effort, it seemed to me that there ought to be some basic fundamental T/A System; given that System, it ought to be possible to organize any T/A problem correctly.

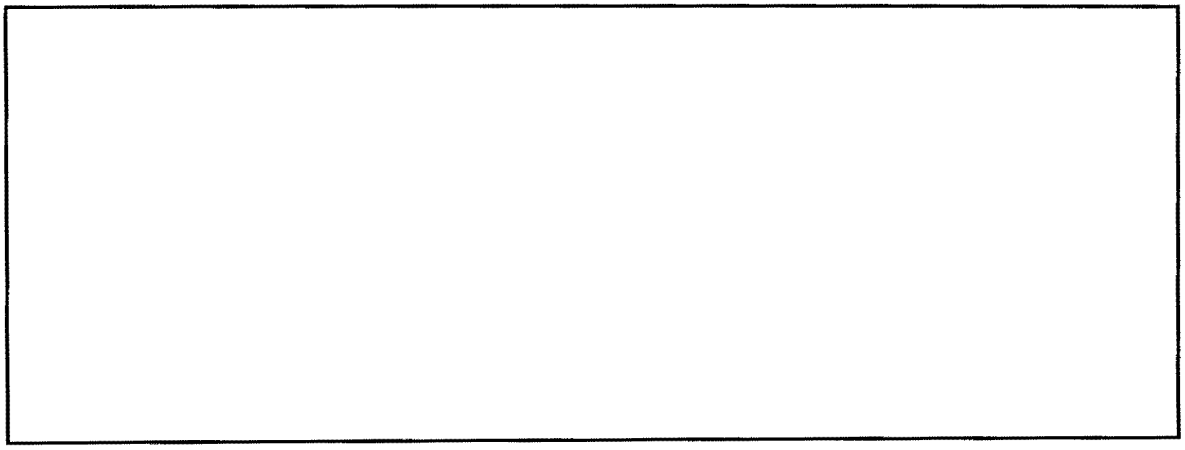
As my arteries have begun to harden, my beliefs about these questions have shifted. It now seems to me that the most effective organizations (T/A and others) have been those that concentrated less upon adherence to some discovered Truth and more on defense against catastrophic failures. Consider all of the possibilities (in order of likelihood, if you wish) that could wipe out the average T/A shop: many-fold increase in traffic, major comm change, loss of key personnel, comms outage, destruction of database, etc. Organizations that can survive are those designed to adapt and adjust – to roll with the punch. Those that can't adjust go quickly into imbalance and overload, and major surgery (reorganization and restaffing) is necessary.

The principal difference between these two viewpoints is in their levels of complexity. The central Truth idea is really a two-body problem: if you can measure where you think you are and where you think the center of Truth is, then you can form some notion about whether you are heading toward your goal or away from it. However, the catastrophe defense idea is more of a multibody problem – strengthening your defense against one possibility often weakens your possible response to others, and some balance is clearly necessary.

Unlimited defense against all possible contingencies is, of course, impossible without unlimited resources. The scariest part of this notion, however, is not that defenses must be limited; it is rather (as any computer programmer will tell you) that none of us is smart enough to think of all the bad things that can possibly happen. Surprises do come along, and it is, I suppose, the continuing possibility of the unexpected that keeps this business interesting.

P.L. 86-36
EO 1.4.(c)





Traffic Analysis Mechanization Forum

OPENING ADDRESS BY MAJOR GENERAL JOHN E. MORRISON, ADP

Good Morning, Ladies and Gentlemen, and representatives of the Service Cryptologic Agencies.

I see a man in the back there, [redacted], who reminds me of a story I tell frequently – but Charlie is rarely around to hear it. I joined the cryptology business in February 1942, when the Signals Intelligence Service was holding up in the Munition Building on Constitution Avenue – Charlie was my crypt instructor, using the orange handbook written by Billy Friedman. Charlie and I are still around, hustling at the old stand. Charlie has stayed in the business consistently through the years. And, lest I travel under false colors, let me say that half of my career has been in communications and half in the signal intelligence business, starting as far back as 1942 in the SIS, which later became the Army Security Agency. P.L. 86-36

I'm glad to welcome the SCA [Service Cryptologic Agency] people here – I see some old friends from the field, old friends from PROD, and I see number of people I do not recognize, who, I assume, are from the PROD organization.

I've looked at your three-day schedule; it's an exciting schedule, but I don't know how you'll ever get through it. But from a topical viewpoint there is a great deal of interest in this particular schedule. It will provide us all a common insight, I think, into the kinds of problems we are confronted with today, and most particularly how do we get a bigger bang out of the traffic analysis discipline?

Now we all know that CA is, I guess, the queen of the disciplines and has been for some time. It carries with it a mystique that permits its acceptability, its respectability, in almost any circle – even in uninformed circles. Also when you get into telemetry analysis, people understand that; and signals analysis, people understand that; but this TA business – what can you get out of TA?

What do you get out of TA? We've made a living out of TA!

We've done an awful lot of magnificent things in an ongoing war – a real war in Southeast Asia! That's what we get out of TA! We've made a living out of it.

We handle a tremendous volume of information in the computer center, and I guess because of the diagnostic problems, and the probability problems, and all those things that go on in connection with cryptanalysis, one might say that the lion's share of the electronic data processing capabilities in the basement of this building is devoted to cryptanalysis. When I'm making a "beg bug" lecture on the subject of what we do in PROD – I usually "whomp up" this comparison – we have general purpose computers and we have special purpose computers, and we use our special-purpose computers 90 percent of the time in

cryptanalysis, and we use our general-purpose computers 60 percent of the time in cryptanalysis.

The point is that we spend a lot of time on CA, and the bulk of the residual, the residue of capability, is devoted to the TA discipline – a discipline that has worked so well for us, yet we've got to get more out of it. We must be more imaginative and we must mechanize. In these days with the kind of peril we live in – with all kinds of synchronous crypto devices now available, people wring their hands and express great concern that pretty soon all external info is going to be denied and won't that be a shame. And we're going to be out of the TA business. And these are the same kind of people who said in 1955 "won't it be a shame when all the manual Morse is going in ten years" – I just don't believe that TA people are going to be put out of business. I think we have yet to realize our maximum capability, and it's the challenge of attempting to realize an enhanced capability that I leave with you today in this forum. I ask you to share with each other a common understanding of the importance of TA as it evolves, as we reflect upon it, as the various speakers who have been selected to talk to you provide you with their appreciation. It's going to be tough to cover your agenda, but there's no doubt in my mind that at the end of the three days there will be an appreciation – a real feel for TA as we look at it today and a challenge that must be perceived. I hope that we are energized in our thinking, and I hope we leave here with a new dedication to do something more by way of mechanizing and getting a bigger bang out of that particular discipline from which we have gotten so much pay dirt in the past and that promises to do even more for us in the future.

I welcome you all again – I'm delighted that you were able to take the time to join each other here. I think you do us all valuable service.

Again to our SCA conferees – glad to have you aboard. George, without further ado I'm going to turn the meeting over to you. Thank you – Good to see you all.

Introduction to Traffic Analysis Mechanization

ROBERT S. BENJAMIN

INTRODUCTION

Our purpose this morning is to set up a logical frame of reference for the many presentations on traffic analysis mechanization that will be following in this three-day symposium. We hope to provide an overview of traffic analysis and of mechanization as it relates to traffic analysis.

Mechanization in traffic analysis goes way back, well before computers. When we first got into the cryptologic business in cryptanalysis and later in traffic analysis, in early 1943, we encountered our first pile of "IBM Runs," as they were called then, at Arlington Hall Station. When we examined them, we found that the large pile of prints consisted of headings and preambles of Japanese Army, Navy, and Air Force traffic, sorted by various parts of the message heading. Most analysts were not using the runs, but a few of us who tried to look up things found them immensely useful in net reconstruction and in analysis of routing systems.

I will be acting as an "observer" this morning, a spokesman for many of my colleagues to whom I am indebted for the ideas I will be setting forth.

THE GOAL IS INTELLIGENCE

Traffic analysis - all SIGINT, for that matter - must begin with intelligence requirements. The SIGINT process is sometimes shown as a cycle, somewhat like Sherman Kent's "Intelligence Cycle," which appeared in one of his books. In the case of SIGINT, it goes: *requirements* – leading to *collection* – to *analysis* – producing *intelligence information* – which becomes *intelligence* – leading to more or slightly different *requirements*, and so on. To put it another way, in traffic analysis, we react and respond to requirements from intelligence consumers and must never lose track of this fact. Despite the intrinsic interest of what we do, the goal is intelligence.

Recently, I was reading S.I. Hayakawa's book *Language in Thought and Action* in which he made a distinction between "maps" and "territories." His general point was that in human discourse and in semantics, humans sometimes become confused between the "real world" (or territories) and the way we represent the real world, using symbols, names, etc. (the "maps"). This has inspired the attached diagram, figure 1, as one way to visualize the traffic analysis process. In TA, we build models of other's communications, study these models, and draw inferences from them. This chart may help us to visualize the general process. In figure 1, the top half of the chart (above the line) represents the real world. The bottom half represents how we see it in SIGINT, which we have called the

"SIGINT Models." The top of our chart is the territory; the bottom half is the map. The left hand half of the chart represents the SIGINT target, and the right is communications. Consider for a moment – the target, whoever he is, whatever he is up to, exists somewhere in the world. He communicates because of *need*; his communications represent a model of his organization. We intercept his communications, reconstruct his nets, and have a model of his communications. Basing our study and observations upon these communications, we build a model of his activities and intentions and report these in SIGINT end product. The *goal* of traffic analysis – of all SIGINT, for that matter – is to produce valid intelligence about the target.

DEFINITIONS

What is traffic analysis? There have been many definitions over the years, and a rather widely used short one now current is this:

> "Traffic analysis is that branch of cryptology which assembles information about communications networks by studying the elements of transmissions which are external to message texts."

One could go on to point out that the traffic analyst also may study some parts of a text itself – for example, discriminants, indicators; plaintext messages, short messages such as Air Defense "proforma" messages, and so on – and that he may make extensive use of non-

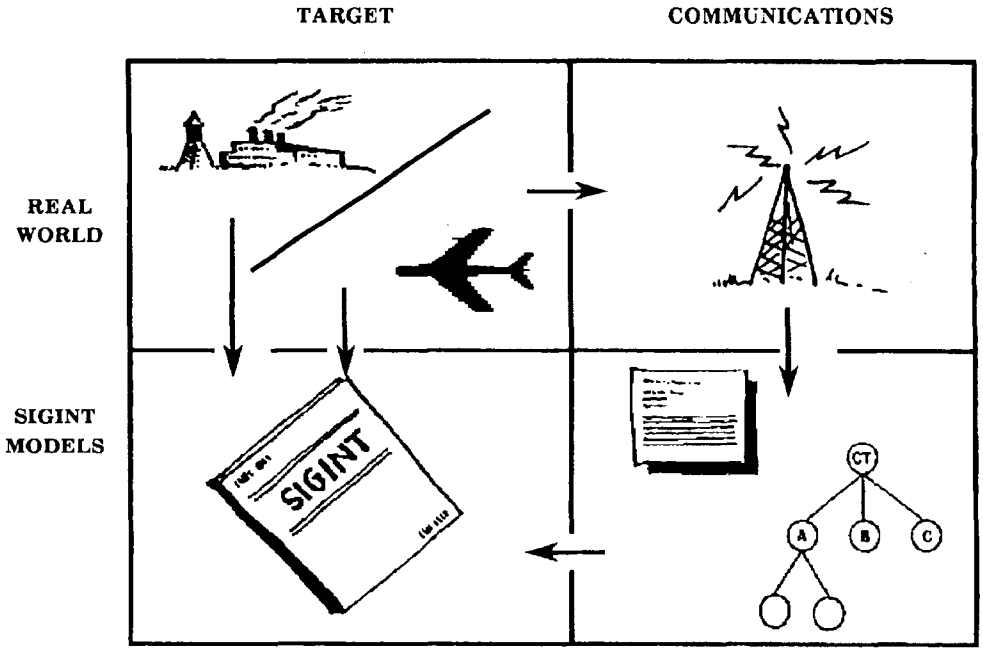


Fig. 1.

SIGINT information (collateral) to draw his conclusions. Traffic analysis has one or a combination of goals: to help SIGINT collection, to assist cryptanalysis, to improve intelligence information, and to assist the COMSEC effort.

DATA AND INFORMATION

In SIGINT, we are in the process of converting *data* ("that which is given") into information ("meaningful data"). These two terms are relative – in the total SIGINT process flow, this transformation takes place dozens and dozens of times between antenna (collection) and the point at which we issue end product.

Let us consider the traffic analytic process. As shown in the accompanying chart (see fig. 2), the analyst takes data and analyzes them. The analytic process consists essentially of making certain *observations* (counting, noting occurrences, measuring, etc.), coupled with making *inferences* based on the observations (extrapolating from the observations, drawing conclusions that are not explicit in the data, etc.).

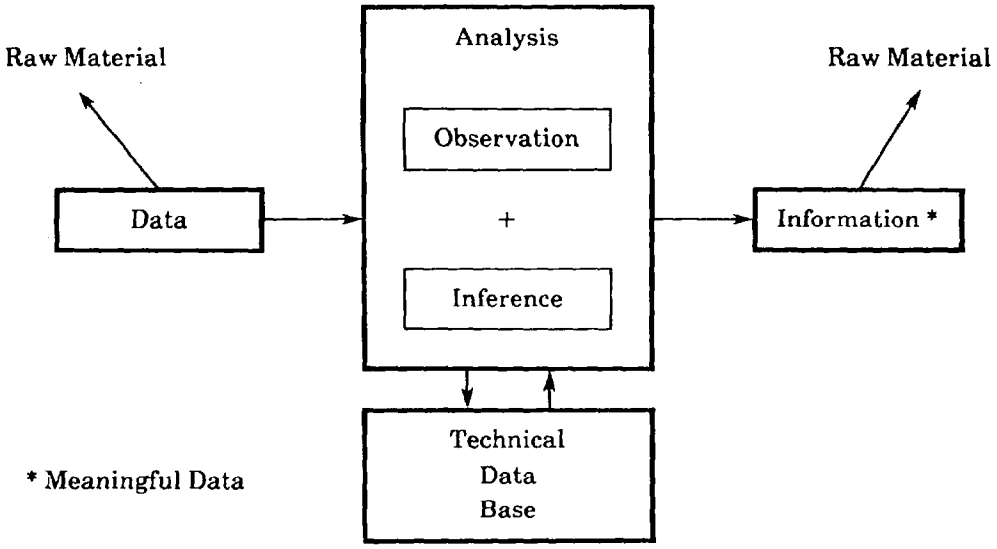


Fig. 2. The traffic analytic process

The analyst typically interacts with a technical database in this process of observing and drawing inferences. We are using the term "database" here to mean any files and records that an analyst has access to – card files, incoming hard copy of semiprocessed reports, ranging up to various computer-based files on magnetic tape, or even (in rare cases) files he can access on line with a computer.

Based on his analysis, the analyst produces information, leading to end product, which goes to consumers in the intelligence community. Much of the information may be fed back into the "technical database" to expand it and refine it.

Based on his analysis, the analyst produces information, leading to end product, which goes to consumers in the intelligence community. Much of the information may be fed back into the "technical database" to expand it and refine it.

THE TRAFFIC ANALYSIS CYCLE

Still another way of looking at traffic analysis to give us a better understanding of what happens is to consider what we shall refer to as the "traffic analysis cycle," patterned after the SIGINT cycle referred to earlier. Some persons have referred unkindly to this as the "Texan's map of traffic analysis." As you see in the accompanying chart (fig. 3), we

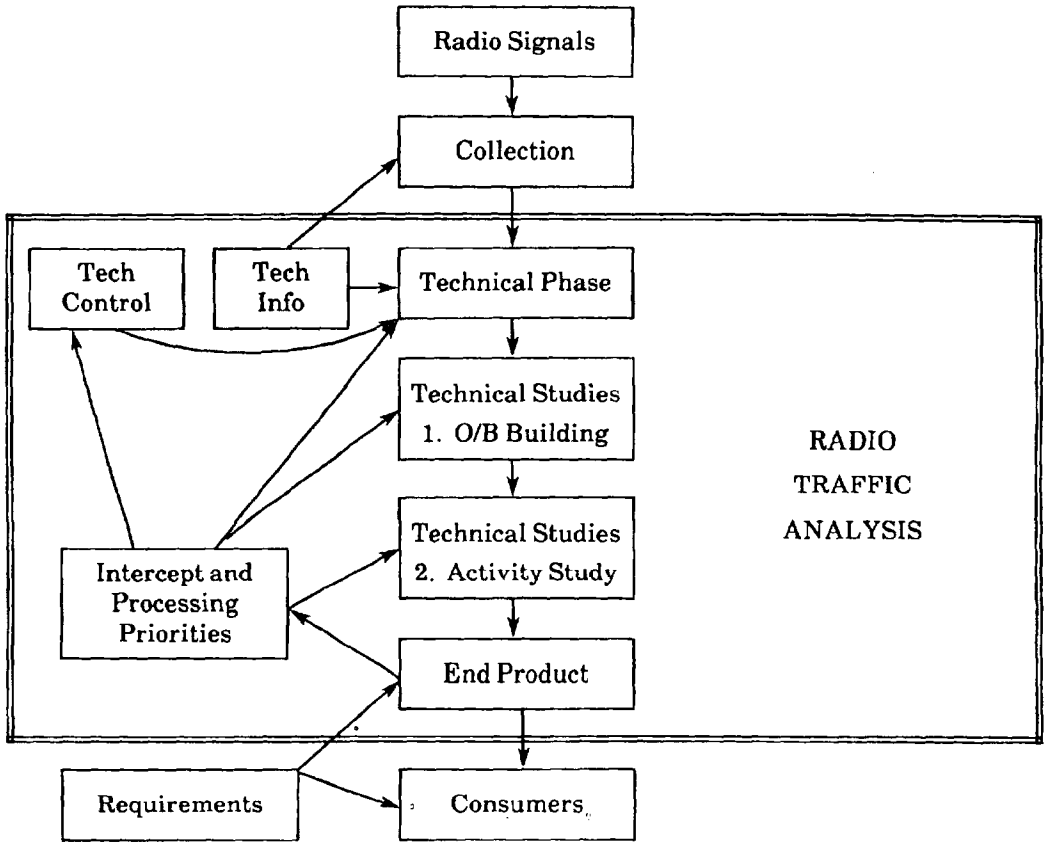


Fig. 3. The traffic analysis cycle

have set up a list of functional processes that constitute traffic analysis irrespective of echelon, things that go on between the antenna and the passing of product to consumers. In reaction to intelligence requirements, *radio signals* are *collected*, and the traffic analyst performs certain steps in a *technical phase* – things like traffic identification, net reconstruction, establishing net continuity, and drafting and issuing technical reports. These reports and cables provide a feedback flow of technical support to the intercept source. The next effort we will refer to as *technical studies (order of battle building)*. This consists of determining locations of radio stations and units, determining what organizations or types of units are involved, relationships between units, and the like.

Almost concurrently, the analyst carries on what we call here technical studies (activity study), looking into what is actually happening on the framework that is the order of battle. He looks for indications of things happening or about to happen (a whole talk could be given about the kinds of things that constitute SIGINT indicators): he studies activity generally; he establishes a formalized or general idea of what is normal; looks for phenomena or exceptions to the norms he has set; and he tries to interpret or explain these phenomena in terms of what is actually or probably happening to the target itself. We will return later to the idea of exceptions when we discuss mechanization. The analyst seeks to produce *end product* – I cannot emphasize enough that the goal of traffic analysis is producing SIGINT; all else is peripheral to that goal. The analyst should and often does produce product based upon his findings using non-SIGINT information as necessary, or he may furnish his findings to special research analysts, who may fuse the findings of several analysts with ELINT, cryptanalytic results, and with other non-SIGINT results to produce a comprehensive study.

Product is passed to consumers, completing the cycle. Feedback loops exist in our cycle, and our discussion is not complete unless we consider them. Requirements are passed from consumers to those in cryptology concerned with product matters. Based upon these considerations, all efforts represented by other parts of the traffic analysis cycle are constantly being readjusted – emphasized or deemphasized in terms of intercept and processing priorities. Technical control of the collection effort is being exercised in continuing response to these constantly adjusting priorities.

This, then, is the world of traffic analysis, working closely with other cryptologic specialists in the common goal of covering *data* to *information* to *intelligence*.

MECHANIZATION AND SYSTEMS

We would like to shift gears at this point and talk more about mechanization of traffic analysis, to establish a few logical bridges between the computer field and the traffic analysis field. First, a definition or so is in order. What is "mechanization"? It is generally agreed that *mechanization* means a process or system having an optimum mix of men and machines. The term *automation*, on the other hand, implies a system with no direct manual intervention, self-regulation within the system, and automatic "feedback"

loops. There are few examples of true "automation" in SIGINT (unless one takes a small piece of a system or a program); strictly speaking, by and large we are using much mechanization, little automation.

It may help to think of three types of "systems" that interact in any SIGINT process using machines (we will use the words "computer" and "machine" loosely and interchangeably). One must have *hardware systems* (the computers themselves, their tape drives, and communications linking them). There also are *software systems* (which, strictly speaking, are the programming systems that are available to a programmer when he begins to program for a particular application or problem). More important for us in this symposium, there are *cryptologic application systems* – programs and assemblages of equipments and programs that serve the traffic analyst, the special research analyst (formerly called the SIGINT research analyst), and the cryptanalyst. Consideration of these professions and of data banks that serve them leads us to a small digression in our train of thought.

OVERLAPS OF TA WITH OTHER SIGINT SPECIALTIES

Our cryptologic professions, and the techniques implied by them in SIGINT, complement each other to a remarkable extent. In fact, a person in any of our professions – i.e., Cryptanalyst, Traffic Analyst, Special Research Analyst, Signal Analyst, Collection Specialist, and so on – should know the rudiments of the other professions.

This overlap has some very interesting professional and cryptologic training applications. The reason I mention it today is that it has an important bearing on mechanization. We should not mechanize things in isolation without considering related problems. The cryptologic database interacts in dynamic ways. The need for interactions of data between large organizations – A, B, and G – and between analysts of different breeds, dictates applications systems designed to permit such interactions of the data, cross studies, and the like. When such matters are not considered, we may have two, three, four, or more databases containing essentially the same data in different, incompatible forms. The *standards* implications of what we are saying should be apparent, both at the *data element* level and at the format level. We shall have a few more words later on formats.

SOME TRAFFIC ANALYSIS MECHANIZATION IDEAS

At this point, I would like to toss out a number of ideas and terms. Most machine help to traffic analysis today still consists of *batch* processing, much like the so-called "IBM Runs" of Japanese traffic of almost thirty years ago that I mentioned earlier. We are getting more and more sophisticated, I suppose, but it is still "batch" processing – daily, weekly, monthly, etc. There is some *on-line processing* going on. Here, I mean processing where material is coming in on a signal line from the field, is going directly into a

computer without being handled manually, and some processing is being done to it before people see it. [redacted] will be discussing some on-line applications of this type. Also, on-line can refer to on-line inquiries at a console station connected to a computer; our capabilities in that direction are growing slowly but surely. I do not mean to convey the impression that on-line processing is necessarily preferable to batch processing; each has its place and will continue to have its place, dependent upon the nature of each particular TA problem.

We referred earlier to data standards. The Department of Defense is pushing very hard in the area of data standards (and in hardware, software, and media standards, for that matter). We at NSA must consider these Defense-wide standards seriously, but because of the special problems we run into in cryptology, we are not able to use them "as is" very frequently. The comptroller and personnel organizations (who have more occasion to deal with DoD people and whose data banks interact to a greater degree) are able to use these DoD standards directly to a much greater extent. Without defining the terms rigorously, let me say that data standards are of three types of things: Data Elements (classes of data), Data Items (things that appear in these classes), and Data Codes (short abbreviated codes for either elements or items, to be used in a data bank or descriptions). Collectively, these are referred to as *Data Features* Although some find even the idea of data standards distressing and distasteful, let me underline their importance. We simply cannot build large, useful data banks without seriously building and using standards. Dr. [redacted] will be having some comments on the need for standards and the special problems that the overlapping and competing of national and international standards organizations create for NSA and cryptology.

In the business world, managers have found that they cannot possibly look at all the data relating to their particular concern – whether it is running a production organization, supervising a sales force, or whatever. To make it possible to control an operation effectively, a technique called *management by exception* is being applied effectively. Rather than having a huge pile of material presented to him in the morning for study, the manager using "exception" techniques will specify that he is interested, say, only in the information relating to the top three and the bottom three salesmen's records for the previous period; or he may set certain upper and lower thresholds, or "norms," and call for production and sales figures only for the departments and employees who exceeded or fell behind the norms. Computers are superbly equipped to provide reports answering such questions.

The same idea has always been used in manual traffic analysis, and we will be seeing sharply increased use of "analysis by exception" techniques by machine in the future. To use the technique, a traffic analyst studies his material, establishes norms for events and occurrences, and asks for a machine search to find deviations from these norms. Output provided him shows these deviations (or exceptions); he studies them and draws appropriate conclusions. He may have to readjust norms as time goes on, since what is "normal" changes in time. New norms would be reintroduced in the system for all subsequent processing until a new adjustment is necessary. It goes without saying that

exceptions to the norms are quite likely to contain the "goodies" that will result in end product of value to consumers – thresholds must be so designed that this will be the case.

Without getting too deeply into the subjects, I would like now to discuss *algorithmic* versus *heuristic* problem solving. An algorithm is any definite, specific procedure or formula that, when certain data are put into it, and the procedure is followed, yields certain answers that are always the same. Simple arithmetic problems, algebra, and so on, are examples. Algorithms need *not* be numerical – the machine world abounds with examples dealing with all kinds of data. Heuristic problems, on the other hand, are those that are loosely structured or are so new that approaches must be discovered. Heuristic methods may be "rule of thumb" approaches, may seem to use "intuition," and may be probabilistic (at least not deterministic); one does not necessarily get the same answer, or any answer, to a particular problem. Chess, checkers, and various board games fall into the class of heuristic problems; so does intelligence gathering, and especially so does traffic analysis. Whereas most problems of an algorithmic nature can be readily programmed to be handled by computers, heuristic approaches are much more difficult. Some progress has been made in recent years in preparing "heuristic programs" for computers, and it is hoped that there will be a spillover into our field. Some of the things that speakers will be discussing these next few days have "heuristic" features – watch for them.

THE TRAFFIC ANALYSIS MECHANIZATION PROCESS

I would like to take a look at traffic analysis mechanization in several ways. Essentially, in TA mechanization, we are manipulating *sets* of data. Today's youngsters who are learning about sets in school will probably be better traffic analysts than we were – at least they will have the benefit of some theory relating to ideas that we have been using but had not had formalized for us.

I would like to consider TA mechanization trends over the years in terms of the traditional INPUT - PROCESSING - OUTPUT breakdown. I shall mention some dates – please regard them as approximate. They are based largely on my recollections. Communications developments play a most important part throughout. What is really happening is that TA mechanization has gone global; not only are we eliminating or reducing key punching, carrying punched cards across the room, and so on, but are doing it on a worldwide scale.

INPUT

Input developments have kept pace with industry developments and have often led them. From the early 40s until 1965, TA data were punched from hard copy traffic onto punched cards or punched paper tape, introducing errors and delays. Electrically transmitted traffic and summaries were recorded on punched paper tape for later machine processing. You will be hearing about some significant improvements in the area of input

– AG-22 intercept typewriters (to be replaced in the future by the Improved AG-22 Typewriter System, or IATS), and FLEXSCOP (Flexible SIGINT Collection Position, incorporating a CP-818 computer). These devices and systems solve many but not all of our input problems.

Improved communications are giving us a path that is increasingly direct from intercept antenna to computer at NSA, with a minimum of manual intervention; at least that is the goal. CRITICOMM has been serving as an interim system, and the high-speed data link project termed STRAWHAT is now coming to fruition. Magnetic tape communications terminal devices in C Group (Projects MESHER and MUSSER) are parts of the antenna-to-computer system.

FORMATS

Trends in analytic formats have been similarly marked by distinct improvements. By formats here I mean methods of preparing and forwarding data for higher echelon processing, either machine or manual.

From the early 40s until 1951, the message heading itself was the format (in slightly edited form). Even during this period, there was some experimentation going on with direct machine input of electrically forwarded material. In 1943, a group of young GIs were sent to USM-2, Petaluma, California, for just such a project. We edited material for poking and electrical forwarding; the traffic was to be converted automatically to punched paper tape at the Arlington Hall Station end of a cross-country circuit. The tape was then to be converted to punched cards for subsequent EAM processing. It was not until later years that I discovered that errors on the cross-country circuit were so great that the material was not useful without substantial reediting and repunching; this experience accounts for much of my past skepticism about communications lashups.

In 1951, the "signalled log digest" (or LOGEX), the first true electrically forwarded analytic summary, was begun. [redacted] P.L. 86-36 EO 1.4.(d) The concept of forwarding the results of each echelon's analysis to the next higher echelon so that analysts could start from that point was born here. The signalled log digests were really a slightly altered version of hand logs, forwarded by signal, even producing a space on the teletype print for analysts to draw a diagram, based on the "verbalized diagram" in the message. This early signalled material was neither intended nor suited for direct input into machines.

In the late 1950s, *MATSUM-type formats* were begun. These were similar to the signalled log digests but contained fielded data intended for subsequent EAM (punched card) processing. The Army Security Agency (ASA) in Europe pioneered this effort, and

NSA picked up the idea – the time and the situation were ready for the advance. Many similar formats for electrical forwarding were created and used over the years.

About 1967, *modular-type formats* began to appear. The best examples are the STRUM (Standard Technical Report Using Modules) and the FF STRUM (Fixed Field STRUM). As most of you know, the STRUM of a particular type is made up like a recipe, with whatever modules are necessary for the particular problem. I strongly believe in the modular approach and think that it is proving itself in practice. STRUMs contain some fielded information, but also have flagged and tagged information in the various modules.

Beginning in the late 1960s, *machine-generated reports* produced by field computers from AG-22 tapes started appearing. The first were the TRAPEZE project, [redacted] More recently, a version of the ELFAIR, a [redacted] has been computer generated and forwarded. There are undoubtedly others that we have not named. P.L. 86-36 E.O. 1.4.(c)

COMPUTERS TO THE FIELD

Ten years ago it was unthinkable to send computers to the field, but George Vergine, always about ten years ahead of his time; was suggesting sending out computers for field processing purposes. About 1964, [redacted] wrote a paper strongly recommending the IBM 1401 as the ideal field computer and headed up an early effort to develop programs for field use. Today we have many, many computers at our intercept sites, working with collection, doing conversion, editing, manipulating data, performing product-related tasks, and so on. P.L. 86-36

PROCESSING

A few words about the kinds of processing we have done using computers are in order.

In the early 1940s, in fact until the mid-50s, it was mostly sort and list of message externals. I would like to reemphasize that the sort and list is still the workhorse of our business, despite all the fancy kinds of processing being done or tried.

By the mid-1950s, callsigns were being handled by computer, keys were being decrypted, and some early work on DF plotting had been done.

Programs to produce analytic *summaries* were first started in the mid-1950s. The computer began giving us totals, groupings of data, without giving us back all the input data. This was perhaps the real beginning of TA data reduction by computer.

More fancy things are being tried and have been proved workable. [redacted] will be telling you about the "Traffic Analysis Processing System" (TAPS), which includes some quite advanced ideas. Such things as net reconstruction, net continuities, and various recoveries are being done by computer in special instances; you will also be

hearing about some examples of *alarm systems* based on thresholds and exception reporting.

OUTPUT

The nature of output for the benefit of TA and SIGINT generally is sharply changing. Data links work both ways and provide us the capability of moving output directly to the field for their use.

We have already referred to conventional sorts and lists as typical computer "printouts." Matrix output, in which data are displayed at the intersections of row and column coordinates, has been around for about ten years now and is being used in a number of problems to advantage. Matrices are particularly good for displaying TA data summaries.

Computer graphics, which include the whole area of X-Y plotters and cathode-ray tube output devices (producing so-called "soft copy"), are undergoing a surge in popularity right now and show great promise for even further TA applications. Some such devices display only "alphanumeric" data, and others show either characters or lines, which can make possible the display of graphs, non-Roman characters, and even net diagrams.

Map overlays are an excellent example of such an application. I believe that Mr. [redacted] will be showing you an example of an Airborne Radio Direction Finding (ARDF) map overlay, which illustrates both the idea of computer graphics and of exception reporting. The analyst is presented with an overlay showing *only* DF fixes that are within a radius of twenty-five miles of key South Vietnamese cities. P.L. 86-36

The list of types of output to serve the traffic analyst could go on and on. Some examples that deserve mention are *updated databases*, the generation and *preparation of reports* for reproduction, and the *preparation of messages* for electrical forwarding.

To round out the picture, and to keep everyone honest, I would like to touch on some of the classic *problems* and advantages that people are encountering in TA mechanization.

PROBLEMS IN MECHANIZATION OF SIGINT

Some of the problems we are going to mention have changed somewhat since we first compiled this list a few years back. Some are much greater than they formerly were, and others have practically disappeared. Problems that might be cited are

a. Objections to mechanization, as such

b. Need for a back-up capability

c. Problems in the data

1. Changes in the database
2. Garbles and corruption ("garbage in, garbage out")
3. Volumes of material (now often cited as an advantage, because of input breakthroughs)
4. Data preparation problems
5. Diversity of analytic problems

d. Problems in defining logic

e. Problems in getting at the data in storage

f. People problems (carelessness and human errors in programming, data conversion, or data preparation)

g. Problems with "systems" (some systems are truly too large; others should be designed to interact but are not; the standards problem, etc.)

h. Hardware problems ("down time"; computers in the field experience environmental difficulties, etc.)

i. Delays in getting results (this is really a matter of relative priority of problems)

REASONS FOR THE MECHANIZATION OF SIGINT

Despite all the problems just cited, there are a number of overwhelming reasons why mechanization must be considered, and why for many problems it is already an indispensable part of the processing effort.

a. Business vs SIGINT reasons (timeliness is more important in the case of SIGINT; cost may be an object, but the costs may be far greater not to use mechanization)

b. Timeliness

c. Accuracy (there is accumulating evidence that the use of AG-22s may increase the accuracy of input into our machine processes)

d. Mechanization of target communications methods

e. High volumes of raw data

f. Derivation of new information from large information banks

g. Processing of solved SIGINT systems

h. Research into unknown and changed systems

i. Larger look at data relationships (through information retrieval systems)

SOME CLOSING THOUGHTS ON TA MECHANIZATION

We had a serious communications gap between traffic analysts and computer people a few years back. Now, enough people have crossed the fences in each direction that things are greatly improved; there is increased understanding on both sides of the fence.

The integrity of data in machine files is a matter of concern. Somehow, we must preserve the total context of transmissions and provide an "audit trail" through machine analysis, so that we can always find out how certain conclusions were reached and what was actually transmitted in the first place. Also, the need for the simple inclusion of *validities* in machine records is a matter of concern. Things are seldom certain, but when we do not show a degree of validity, we imply that they are.

A final word on standards. I am not sure that completely "standard formats" are the right goal, although I am a staunch believer in modular formats, with many modules, appropriate for problems X, Y, and Z.

The slowness in developing workable data standards may or may not be our most serious single bottleneck in the whole area of mechanization. We must move more rapidly in standardizing data features – how we express things, irrespective of formats. Databases and retrieval systems demand this. There needs to be a more considered attempt to interweave A, B, and G Group processing systems. In fact, each office has not one but many processing systems. The key to what I am saying lies in the use of effective data standards, I believe, not in the creation of a large "system."

In conclusion, the future of TA mechanization looks bright. I can foresee the continued preparation of manually prepared modular-type formats for a long, long time in the future, but on a reduced scale. I believe that machine-produced summaries based on AG-22 output have a great future, but I would like to emphasize three things:

a. In using AG-22s in this manner, we are essentially moving the point of analysis from one place to another; with communications improving, we can do this.

b. We must make it possible for the analyst to get back to the total take, in some manner, if there is the need to do so.

c. An adequate "alternate system" or path must be provided to ensure that vital information, technical feedback, and intelligence can continue to flow in the event that data links are down. The use of modular-type formats as an alternate, backup procedure for all AG-22 installations in probably the best answer to this concern; this implies the continued need for some analysts at field sites.

I hope that I have sounded neither too pessimistic nor too optimistic today. There are a lot of very real problems emerging in TA mechanization – high error rates on summaries, humidity and dust interfering with operations, machine breakdown, escalating costs, and so on, but on the whole, we are moving ahead.

I am looking forward to hearing what the other speakers have to say and to further forums of this type in the future. Thank you.

Automation of a TA Process

TIM MURPHY

[redacted]

What few people realize is that the workload associated with the Southeast Asian (SEA) problems did not decrease as U.S. forces withdrew from Vietnam and as B3 (previously B6) underwent successive personnel reductions. In fact, the amount of SEA communications intercepted and processed at NSA was still peaking in 1975 when the South Vietnamese government fell. [redacted]

P.L. 86-36
EO 1.4.(c)

Traffic analysts have borne a proportionate share of the decrements incurred by B3, yet there has been virtually no drop in target communications. Analysts have been assigned larger case loads and have assumed responsibility for collection management; yet, in my view, the quality of analysis has improved, and the analysts, in general, are not overworked. There is little doubt that technical support to field stations has improved significantly.

The automation of a large segment of the SEA traffic-analytic processes has been the key not only to high-quality analysis but also to our ability to do the job better over the years with fewer people. Fortunately, during the early stages of U.S. involvement in Vietnam, managers with the Traffic Analytic Support Division for the Vietnamese problem took an enlightened view toward mechanization. With help from some of the Agency's leading traffic analysts and a cadre of highly qualified data-systems personnel, the first steps toward an automated traffic-analytic process were taken.

[redacted] At the same time, we began a major effort to mechanize our analytic findings and create a single processing system. In addition to transmitting our analytic findings to field sites, we also used their data to create identification dictionaries that became the heart of our match-ident process. [redacted]

[redacted]

P.L. B6886636
E.O. 1.4 (c)(c)

Of equal importance to these contributions was that the methods the experts used and the approaches they took to the TA task rubbed off on many of the junior analysts, with outstanding support first from C5 and later from B42, continued this trend toward automation, always striving to relieve analysts of most of the repetitive TA tasks and to permit more time for actual analysis. Among their major contributions were

- the creation of a single analytic database – the Southeast Asian Case File (SEACF)

[redacted]

In addition, the availability of on-line access to our database in recent years through the COPE terminal has led to many analyst-initiated special programs that have greatly expanded the analysts' capacity for research. I should also point out that field stations tasked against SEA targets have also taken many initiatives toward automation.

SEA MACHINE DATABASES, PROCESSES, AND RESOURCES

SEACF

Perhaps the most significant single step toward reducing the workload of SEA traffic analysts was the creation of the Southeast Asian Case File (SEACF). The SEACF not only resulted in highly efficient database management, but also permitted many follow-on processes that greatly reduced the workload of SEA traffic analysis.

Many of the processes introduced during the early stages of the Vietnam War to mechanize the TA process required the establishment of databases to support them. As those processes expanded, the number of databases expanded to the point where analytic time saved was being spent on database maintenance. A review of those databases revealed that there were a large number of common fields of information but comparatively few unique fields. In effect, we were multiplying our file-maintenance workload and making ourselves vulnerable to contradictions between identical data items in different databases. The major databases that had to be maintained prior to the implementation of SEACF were

[redacted]

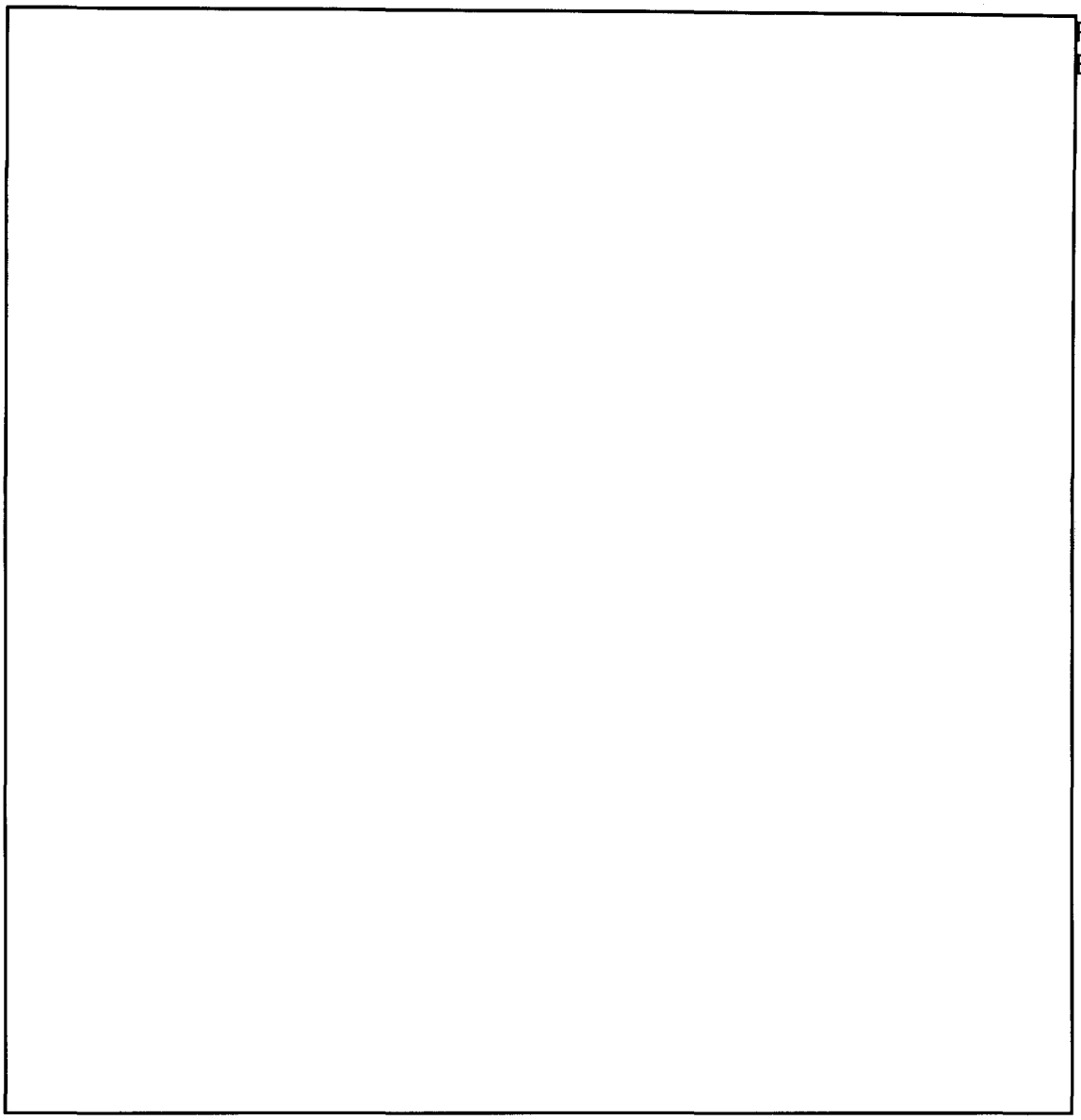
[redacted]

P.L. 86-36
E.O. 13526 1.4(c)

The SEACF consolidated all these data elements into a single database, thus eliminating the requirement to maintain those multiple databases. Since its establishment, the SEACF has been expanded to include data elements that support both cryptanalytic and collection-management functions.

As now constituted, the SEACF consists of eight basic data records which analysts use to provide permanent maintenance of the communication and crypt characteristics of a given target, identification and location data on that target, and collection-management data.

[redacted]



P.L. 86-36
E.O. 13526 1.4(c)

It was inefficient and time-consuming for analysts to collate all these varied inputs, yet very necessary from an analytic standpoint. Hence they were eventually collated by machine as part of our daily process, and our activity database is now a composite of all primary-source technical inputs.

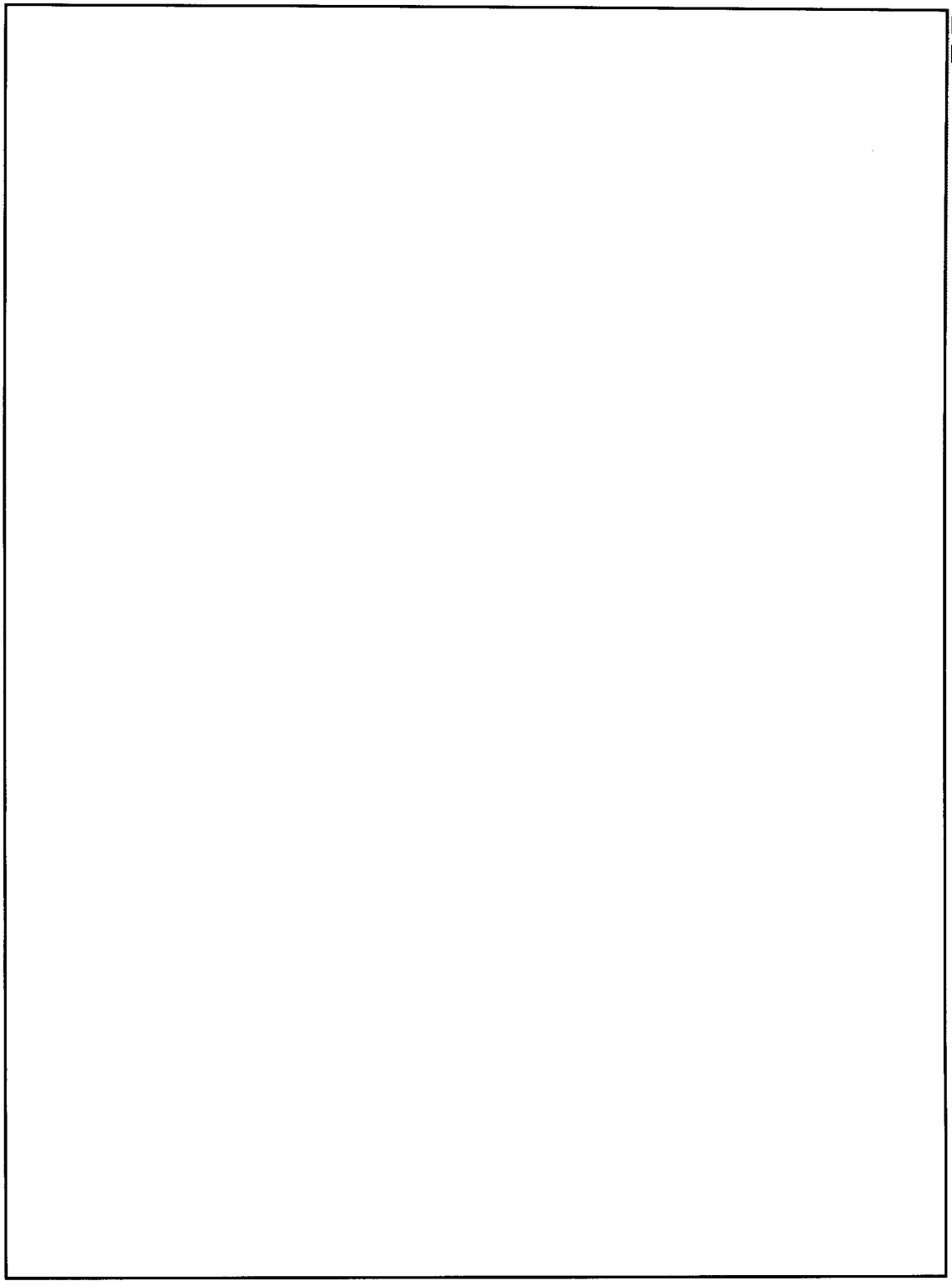
IATS [redacted]

Another major step in automating both the traffic-analytic and the traffic-forwarding processes was the implementation of IATS. The user routine developed for SEA communications copied on IATS or AG-22 intercept positions [redacted]

P.L. 86-36
EO 1.4.(c)

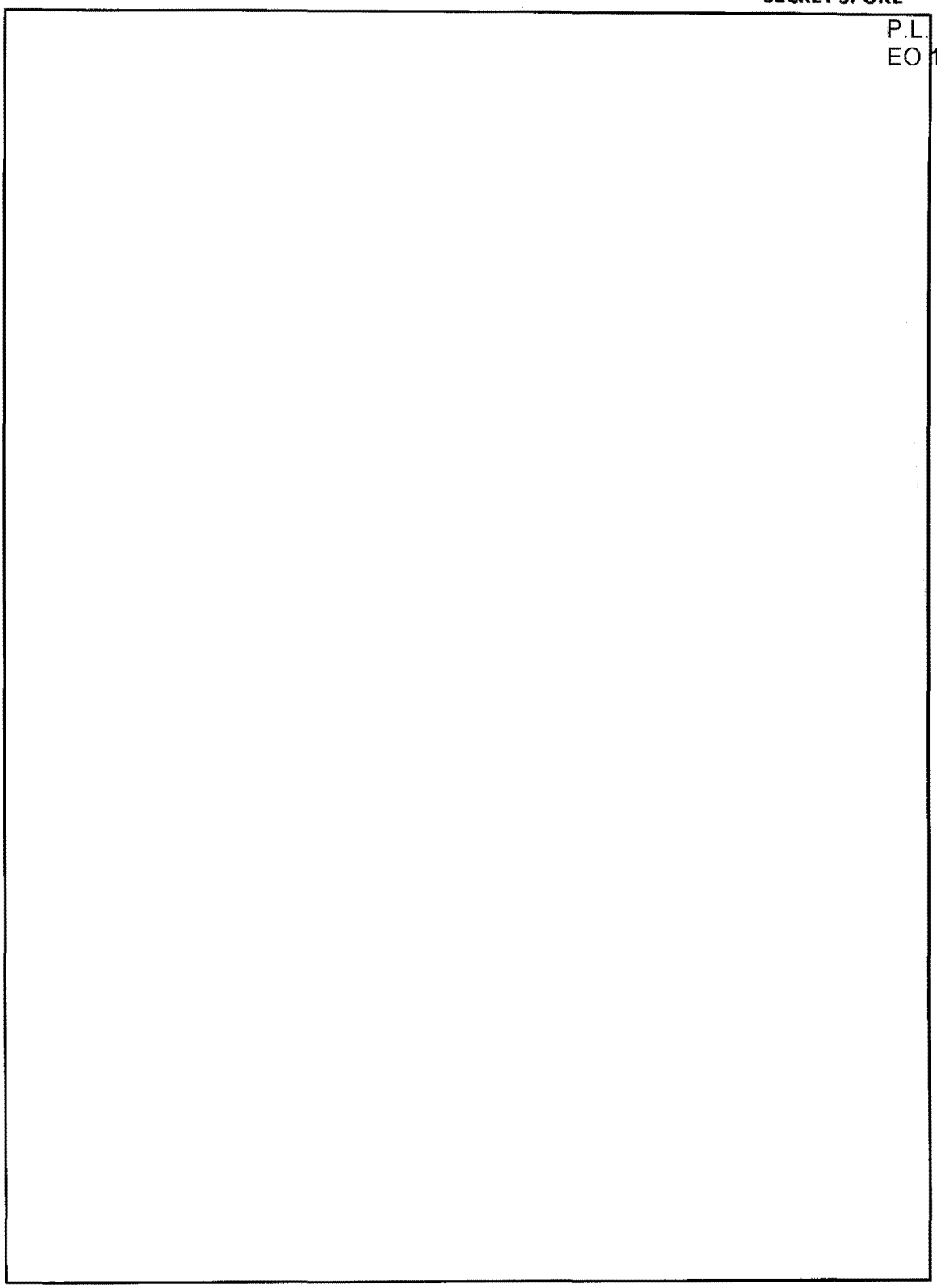
This program reduced by countless hours the task of the SEA development analyst. To a large degree, the analyst has been able to rely on the machine to isolate new continuities and then concentrate his or her efforts on identifying that continuity to region or function. The number of analysts tasked against the development problem was reduced from forty-five to ten between 1972 and the spring of 1975 with no adverse effect on the mission. Much of the credit goes to the SEADEV process.

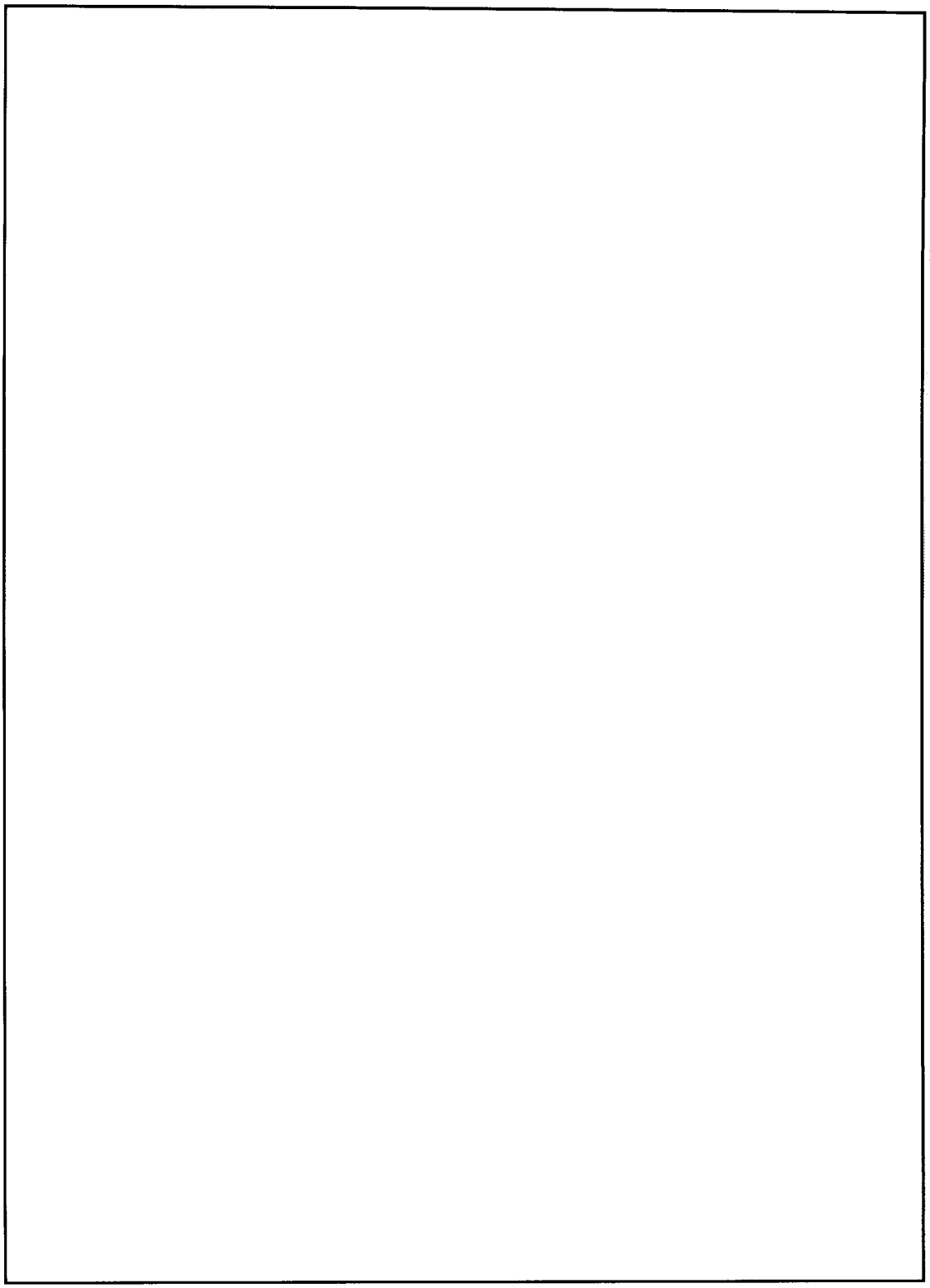
[redacted]



P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)





P.L. 86-36
EO 1.4.(c)

P.L. 86-36
EO 1.4.(c)

IMPACT OF AUTOMATION

In summary it can be said that the impact of automation on the SEA problem has significantly reduced the number of analysts required to do the job. The caliber of analysts required has increased, however, since their primary remaining function is pure analysis or, to use another term, "thinking." Many of the crutches that have kept analysts busy over the years (e.g., logging, sorting traffic) are gone.

To function effectively, SEA analysts must have an understanding of their databases and of how machines can be used to manipulate the data they contain. Imagination is currently a key asset since much of what can be imagined in terms of analytic approaches is now feasible. There is an increased demand for the traffic analyst/programmer. Knowledge of the SPECOL retrieval language is becoming a highly desirable attribute of the SEA traffic analyst. In short, the impact of TA mechanization needs "a few good analysts."

How Clean Does a Database Need to Be?

[redacted] P.L. 86-36

One of the first things one learns about computers is that they require a much higher order of accuracy in the material they manipulate than do comparable "human" processes. One learns to pay an extra measure of tribute in the form of added proofreading or other forms of quality control, so that the input is "clean" enough for the computer to handle.

After a while, as the novelty wears off, it sometimes occurs to one that not all of the data need to be so awfully clean. If we expect to sort or retrieve on a particular field or data element, then that field or data element should be clean and garble-free; but if a neighboring item is never (well – almost never) used as a control for sorting and retrieving, then it only needs to be as garble-free as *people* need. Quite clearly, if only half of your data elements really *need* quality control, then some of that manpower now spent scrubbing each little data element might be diverted to other tasks.

It is possible to imagine categorizing data elements as "first order" if they need to be "computer clean," and as "second order" if they need to be only "people clean." P.L. 86-36 EO 1.4.(c)

In this day of great monolithic databases, however, the use of varying quality levels can cause troubles, however laudable their manpower savings may be. A story "from life" will illustrate.

Some years ago, during the Vietnam War, we found ourselves receiving two streams of electrical material from the sites in the field, and both streams were used to feed computer processes [redacted]

The second was a cryptanalytic stream. A [redacted]

The specific details of these processes belong to another story (or series of stories). The point here is that there came a time when there was an operational need to identify which messages [redacted] It should have been easy. Neither system was new, and both had been working for quite a while with

reasonable success. (Success is a relative term; there were always problems, sometimes earthshaking problems, but by and large, the systems did work.)

[redacted]

It took a while to find out why, but after a time the answer became clear. Evidently the people at the sites, knowingly or unknowingly, practiced different levels of quality control on the various data elements [redacted]

All of which suggests several thoughts.

Garble rates can often be determined, at least approximately, by machine. Certainly differential garble rates can be (Field 1 has more or fewer garbles per thousand than Field 2). If databases that now exist were measured to show which data elements were "cleanest" and which were "dirtiest" (perhaps arrayed in a sort of quality hierarchy),

- the unwary might be warned off using the database for sorting or controlling on the wrong (dirtiest) data elements;
- hit thresholds might have to be lowered when dealing with "dirty" elements, even at the expense of wading through more "garbage" output;
- managers might better understand the manpower costs of various control strategies; but also
- we might decide that great monolithic databases are not always the answer when one must work with a variety of data sources having widely different notions of which items are "important."

The Hand Is Not Quicker Than the Eye

P.L. 86-36

[redacted]

Many years ago I was told that "a good analyst" does his own logging, counting, and tallying. While at first I admit I thought I was being set up to do all the menial labor (my son calls it "the donkey work"), it wasn't long before I saw that the senior people around me *did* do their own logs, and counts, and tallies – not always, but much of the time.

I can remember more than one callsign problem when the callsigns had been extracted (by hand) from some sort of generating matrix and inscribed (again, by hand) into pages. Often the markers of the pages would begin in an attempt to be very "random," but boredom and inattentiveness quickly set in and both processes, extraction and inscription, slowly became more orderly and regular. Near the end, as fatigue set in, the processes became virtually mechanical. Such "handwriting" patterns – top to bottom, left to right – are sometimes so strong that one can convert pages from arbitrary to true base on this feature alone. On a problem like this, one can deal with the problem on a statistical basis – one can even convince one's statistically/mathematically minded friends of the truth of one's solution – but the acid test is to sit down with pencil and cross-section paper and, by hand, duplicate the process, callsign by callsign. If your solution is right, you see it and you'll *feel* it intuitively.

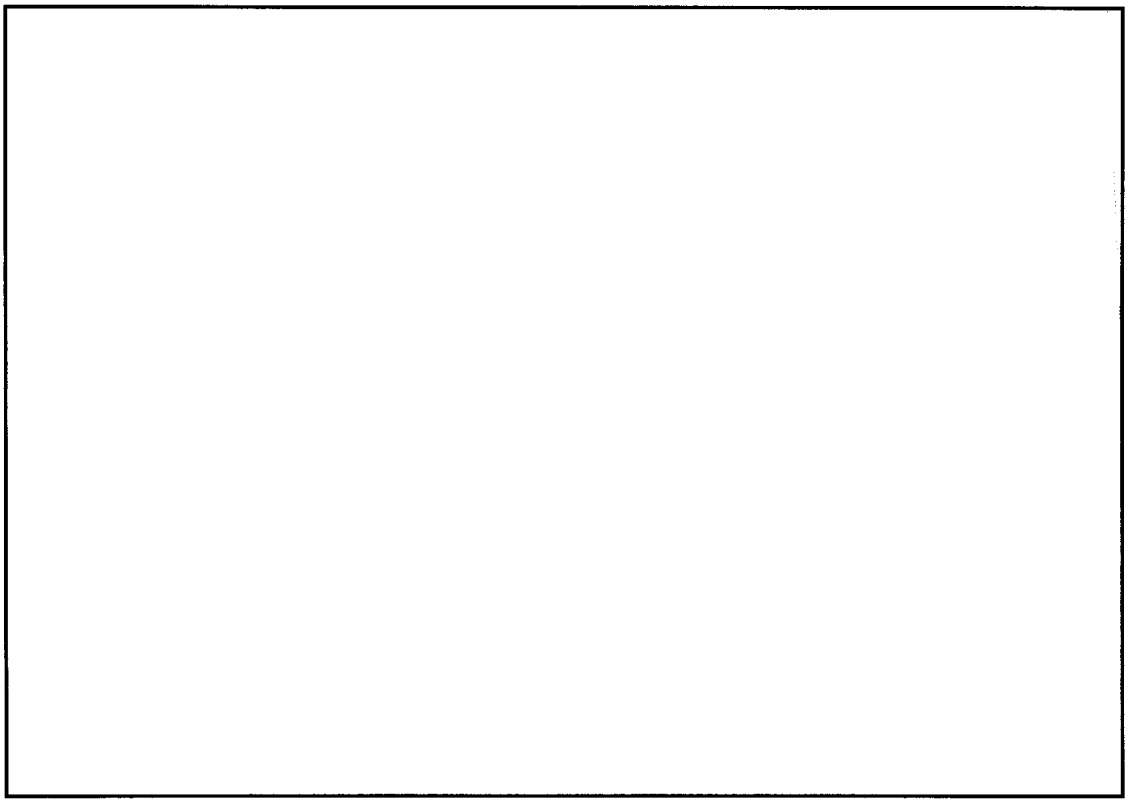
In both of these processes, we gain analytic insight by doing it ourselves. Logging brings us into contact – a kind of slow-motion contact – with the material we are studying. I don't know about you, but I know that I have *discovered* more things while logging, or counting, or tallying, or some other donkey work than I have while sitting there looking at the results of the logging/counting/tallying. Especially the discoveries that were unexpected – outside the range of what I *thought* I was going to find. In the extraction/inscription kind of problem, the insight comes as my hand follows the hand of the enemy signal officer. Why did he stop just there? What made him jump over (or away from) that callsign?

Nowadays we are told that the computers are going to do all things for us. But what happens to that intimate contact with the material when the original traffic – if you can call it that anymore – is deep inside a computer somewhere and all you've got to look at is some computer output? Well, some of us still find a way to do some hand-logging. And not just because we can't get responsive software support (that's a subject for a separate article). We *want* to log! It helps us touch the material. It's like buying a piece of land and not being satisfied with topographic charts – you have to go out and walk all over it. Then you begin to *know* the land.

P.L. 86-36
EO 1.4.(c)

I have always had the notion that someday interactive computers with *screens* might begin to meet this "touching" need of the analysts. [redacted]

~~CONFIDENTIAL~~



Has anybody done this sort of thing or ever seen it done? If it works, I'd sure like to stop all this logging!

The Lost Indicator

DR. RALPH W. JOLLENSTEN

INTRODUCTION

The purpose of this talk is to describe the type of questions that arise when a math problem is encountered in TA. Although some would argue that the problem discussed here is not strictly a TA problem, the underlying general principles are the same as those for a purely TA problem in which math is needed.

PROBLEM

A certain country has been sending military traffic in five-digit groups, using the fifth group (A5) of the message text as the indicator group according to the following rule:

Air traffic – the digits of the group sum to 23.

Army traffic – the digits of the group sum to 24.

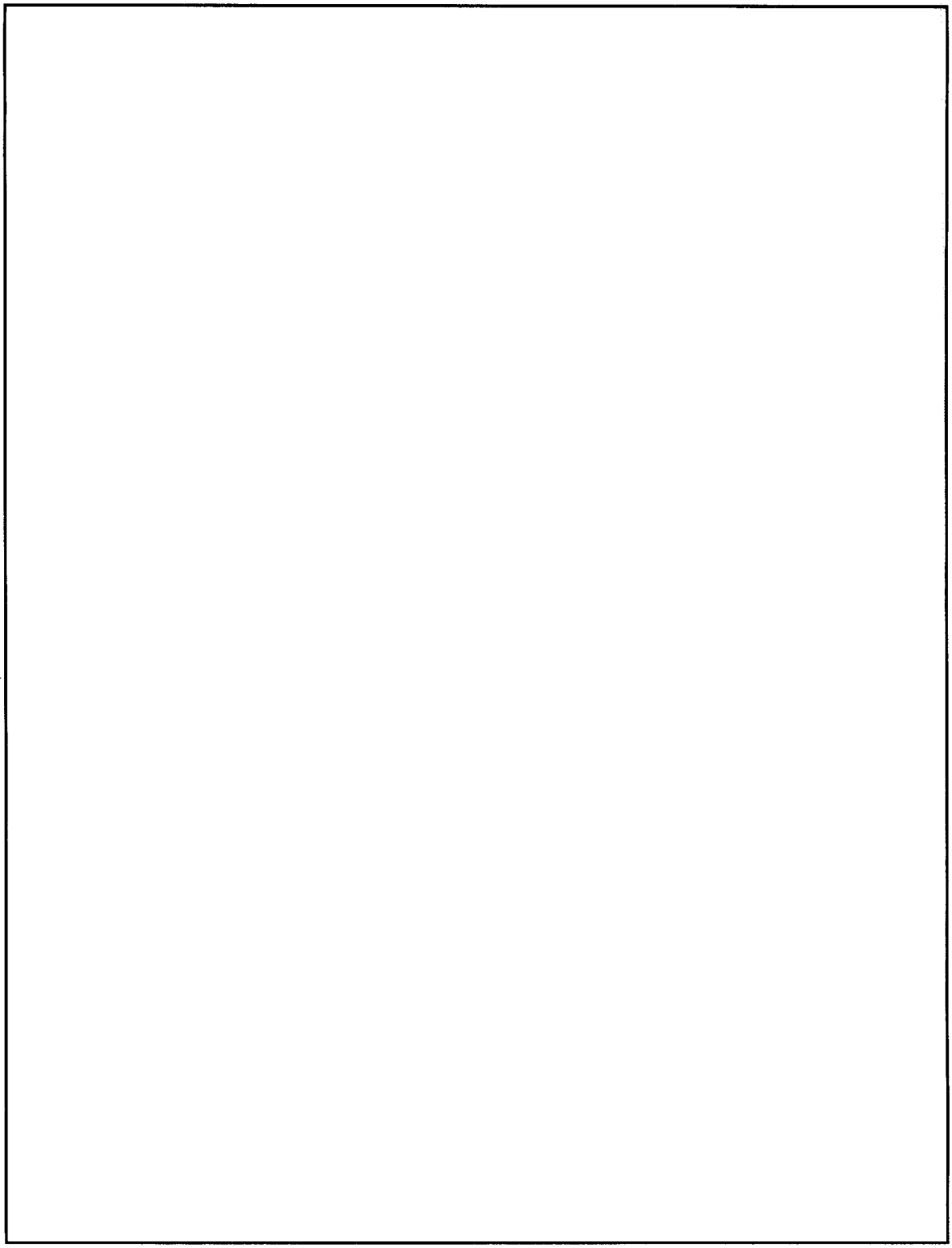
Navy traffic – the digits of the group sum to 25.

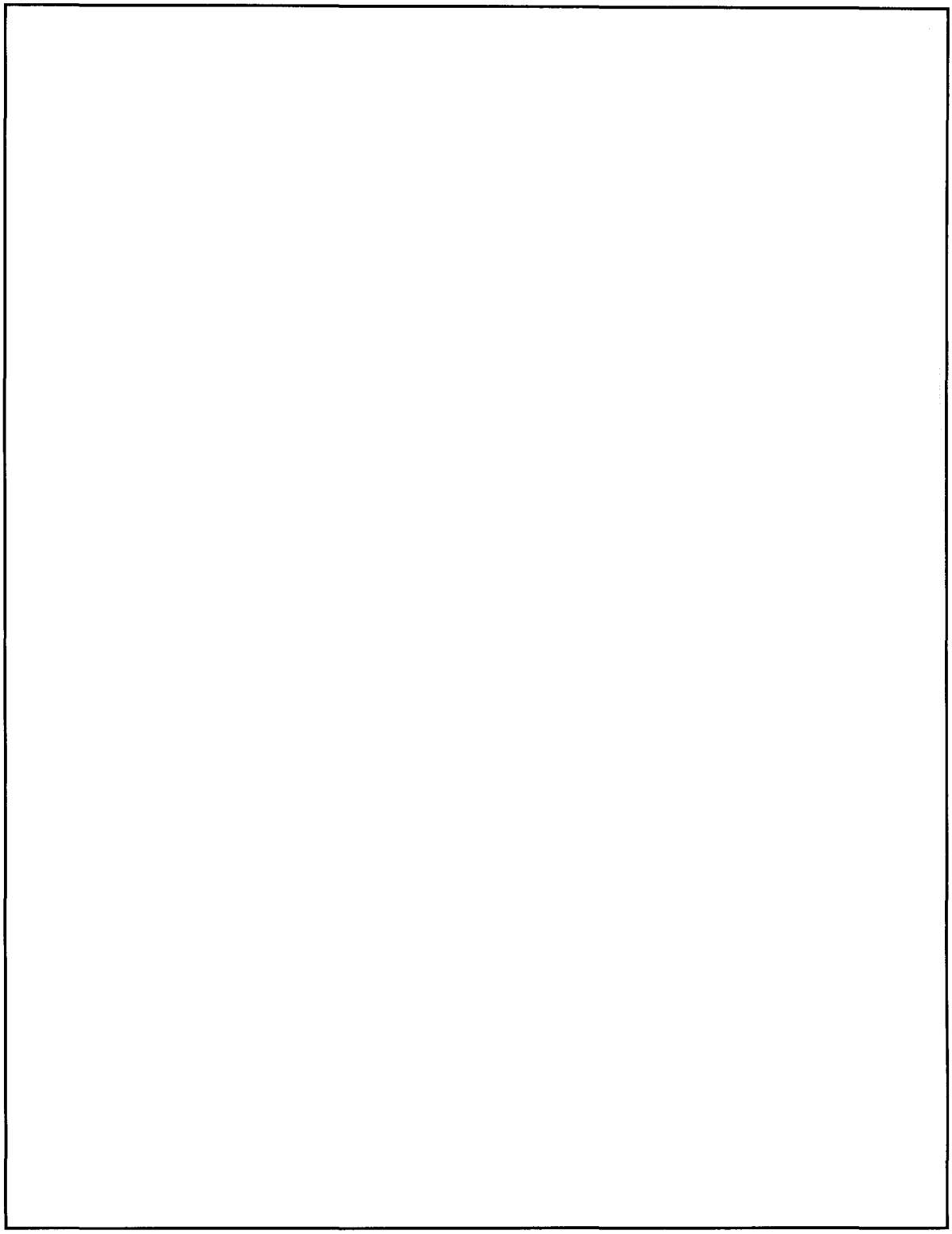
The military traffic is mixed in with other traffic having the same externals, except that the A5 position of the nonmilitary traffic exhibits no detectable bias. Obviously, the indicator characteristic is useful in differentiating between military and nonmilitary traffic.

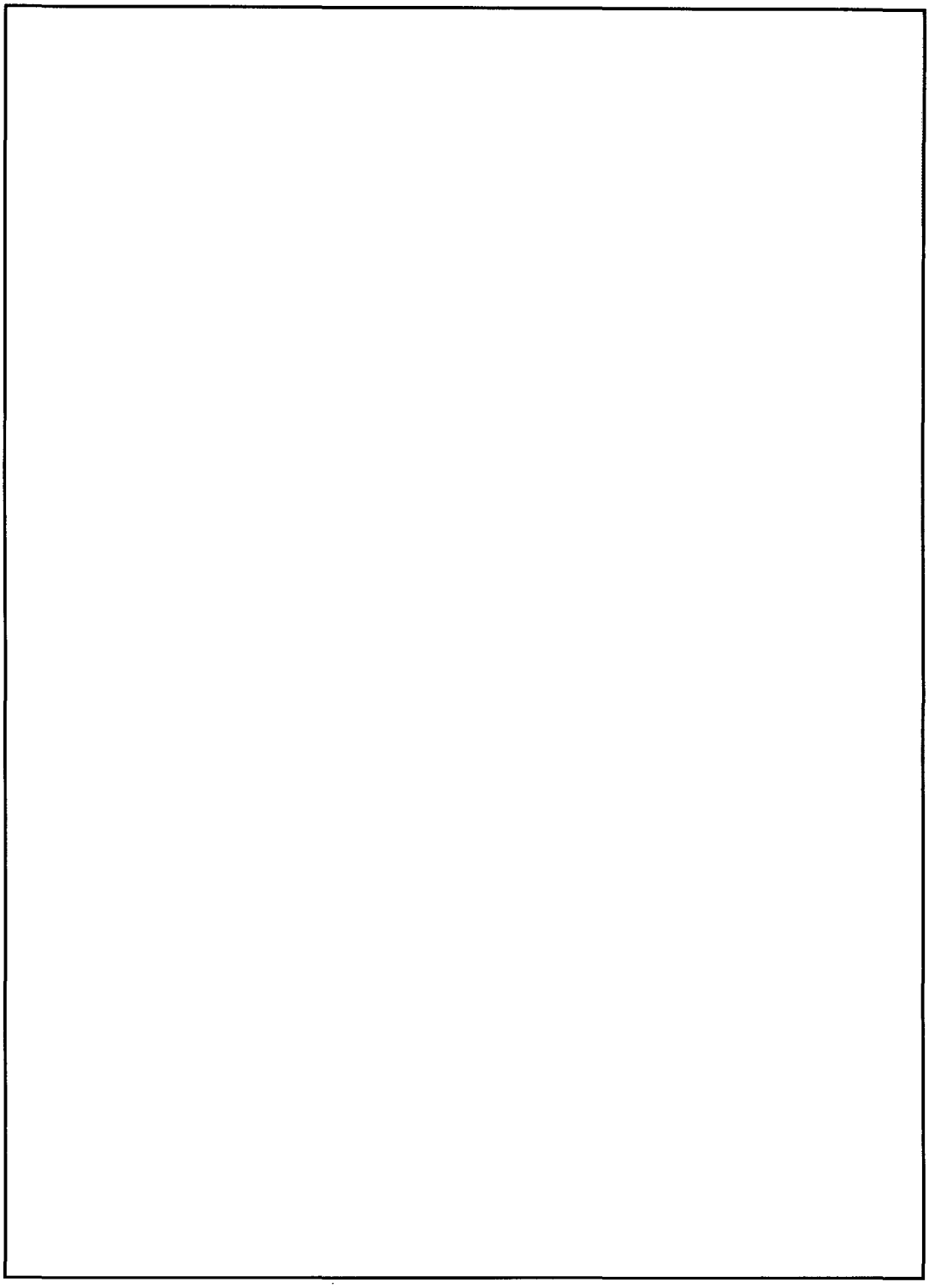
Suddenly, on the first of the month, the indicator disappears from the A5 position of the military traffic. *What happened to the indicator group*? Did it move to another position, or has an additive been applied to it?

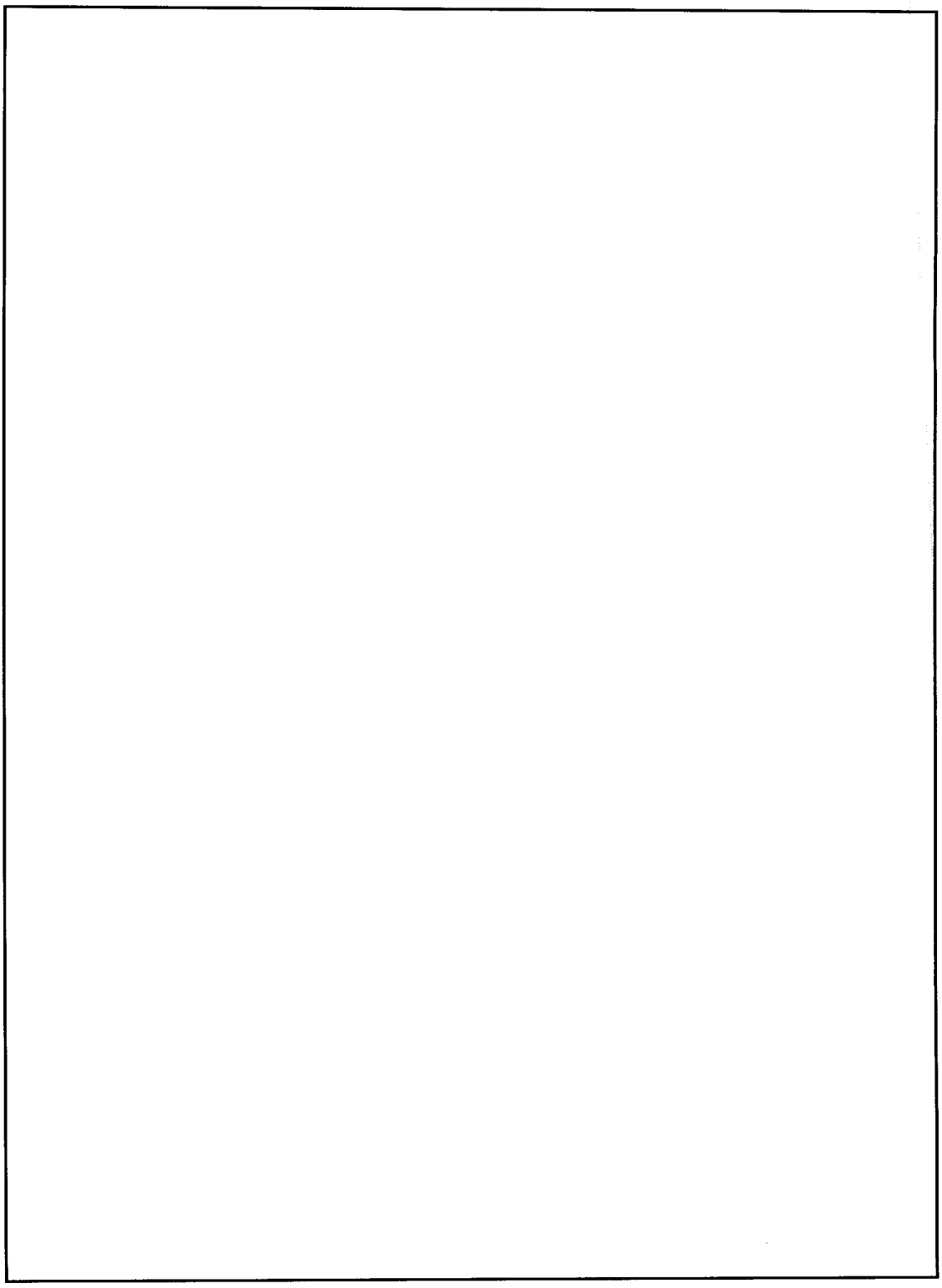
SOLUTION

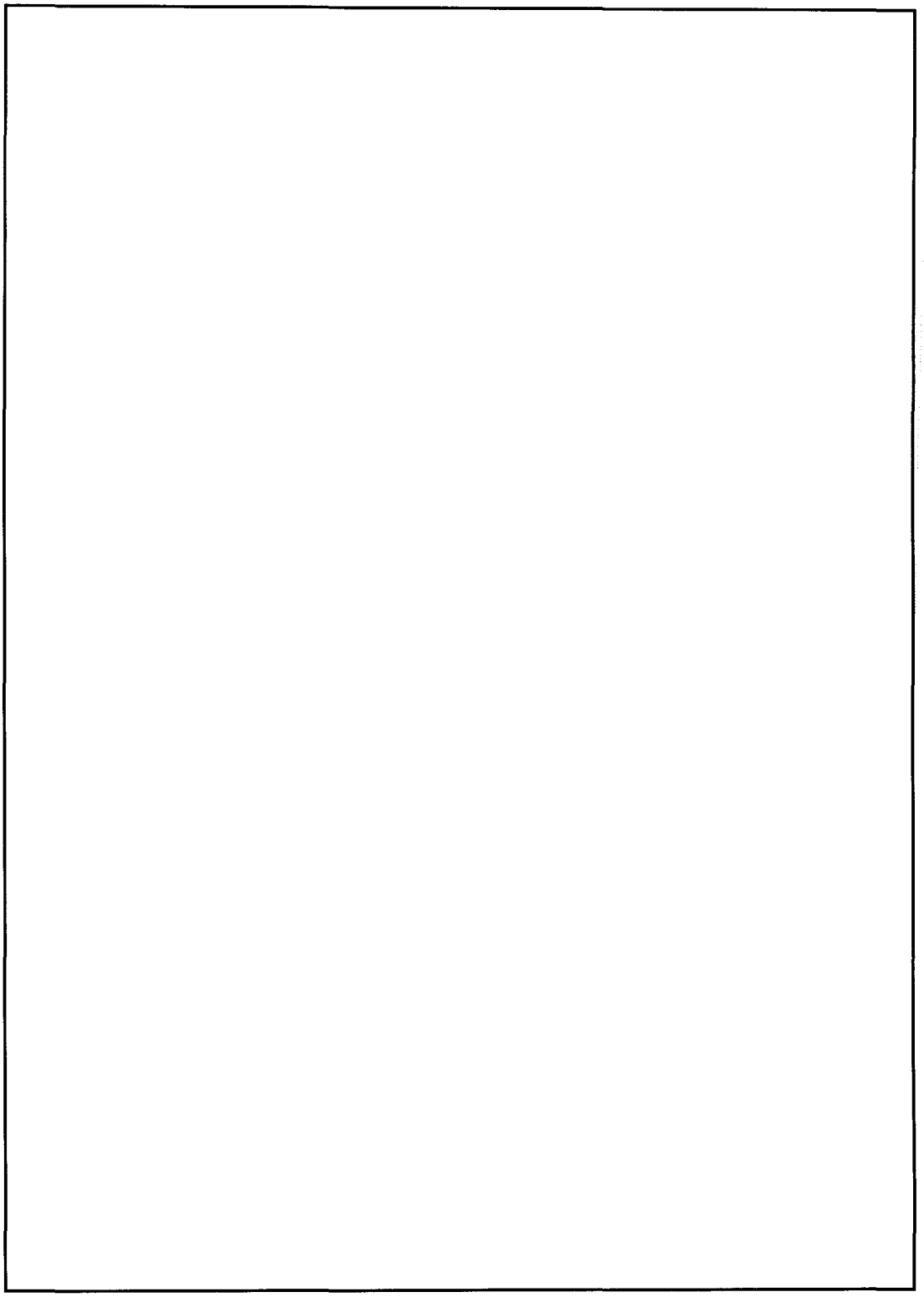
The analyst needs a method for diagnosing what has happened. To begin with, he decides to check positions A1 through A10, inclusive, to see if any of these positions exhibit any characteristics that would favor the hypothesis that the old-type indicator is present there. He has 200 messages to work with. Since he is not sure that they are all military, he doesn't know the distribution of the groups in each particular position of the messages. Some of the groups in a particular position may have causal sums while the rest do not. However, he feels sure that if the indicator is not present, the groups are distributed as if the digits of each group were equally likely. Therefore, he sets out to find or calculate the distribution of the sums of five-digit groups when each digit is equally likely.

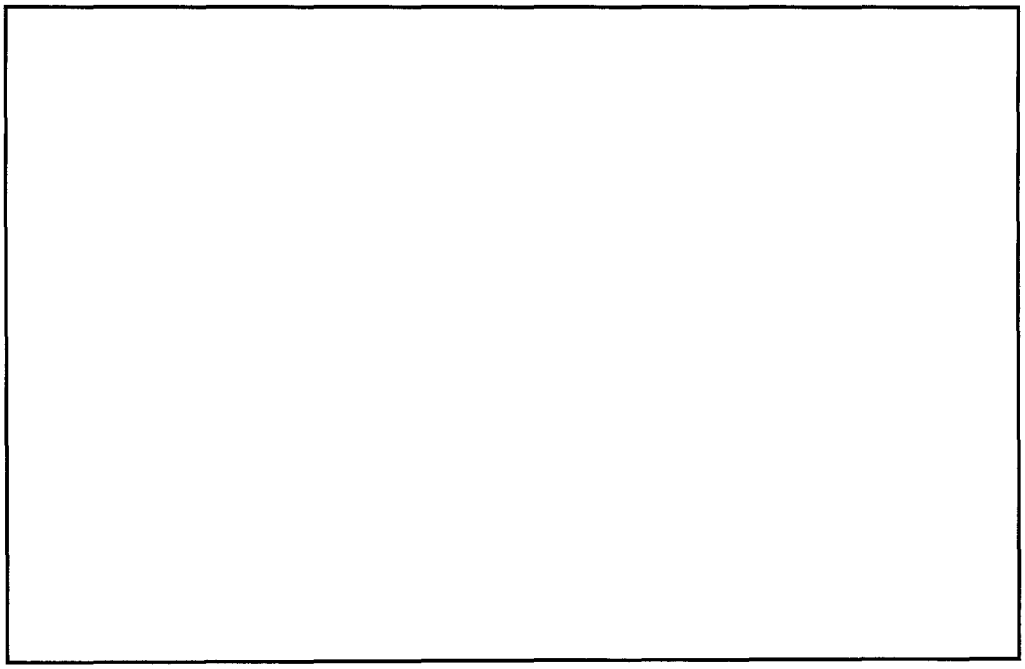












Applications of Set Theory to Traffic Analysis

[redacted] P.L. 86-36

The purpose of this presentation is to show an approach to traffic analysis that uses set theory concepts and terminology. For this purpose, we have created a hypothetical problem designed to represent some aspects that could be reflected in a real problem. Although the following example is limited to callsign analysis, a similar approach could be used to analyze frequencies, practice traffic systems, or other data.

The hypothetical problem involves the country of Transylvania, which is divided into seven military regions labeled A through G. The callsigns used in Transylvanian communications are derived from a fifteen-page callsign system. Each page is a ten-by-ten matrix of 100 callsigns with each callsign appearing only once in the system. Further, let us assume that each military region can use callsigns from three different pages as follows:

AREA	CALLSIGN PAGES
A	01, 08, 04
B	02, 09, 05
C	03, 10, 06
D	04, 11, 07
E	05, 12, 03
F	06, 13, 01
G	07, 14, 02

A "set" is defined as a collection of well-defined objects; given any object, one can determine whether that object belongs or does not belong to a given set, i.e., whether it is an element of the set. To illustrate a callsign set, we use a Venn diagram as shown in figure 1.

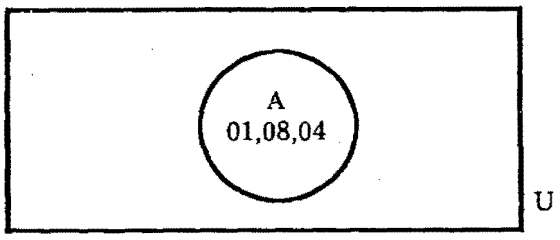


Fig. 1

The set "U," represented by the above rectangle, is the universal or complete set of callsigns in the Transylvanian system. In general, the universal set refers to the entire collection of objects being considered. The circle labeled "A" represents the set of callsigns from pages 01, 08 and 04, which are available for use on the internal communications of Military Region "A." Thus, all callsigns on pages 01, 04 and 08 are elements of the set of callsigns used by region A.

The union of two sets can be illustrated by the shaded area in figure 2.

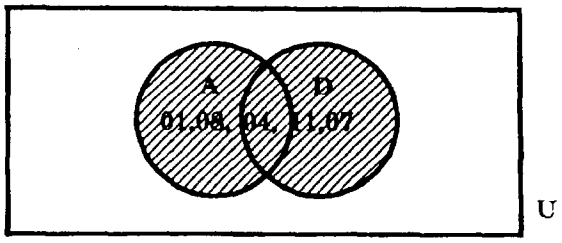


Fig. 2

We define the "union" of two sets A and D, denoted A∪D, as the collection of all elements that belong to either the set A or the set D, or both. The above example represents the union of the callsign sets used by Transylvanian Regions A and D, i.e., all callsigns in pages 01, 04, 07, 08, and 11.

The "intersection" of two sets can be illustrated by the shaded area of the Venn diagram in figure 3.

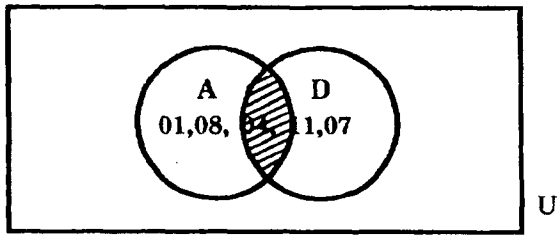


Fig. 3

We define the "intersection" of two sets A and D, denoted A∩D, as the set of all elements that belong both to A and to D. In this example, only callsigns from page 04 are available for use by both Military Regions A and D. Therefore, A-D is the set of callsigns on page 04. Suppose an unidentified radio group represents communications for elements of either Region A or D. Three possibilities exist:

- If at least some of the callsigns used are taken from either pages 01 and/or 08, then the radio group is in Region A.
- If at least some of the callsigns used are taken from either pages 11 and/or 07, then the radio group is in Region D.
- If all the callsigns used are extracted from page 04, then the radio group may be located in either Region A or D.

Two sets are said to be "disjoint" if they have no elements in common. For example, in figure 4 it can be seen that the communications of Region A will not use callsigns available to Region B and vice versa. This callsign set relationship gives a firm basis for the differentiation between communications of these regions.

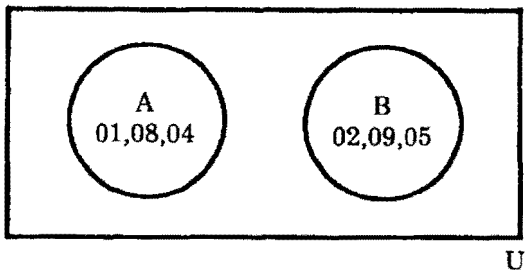


Fig. 4

In order to gain more insight and understanding of the communications of an entire country, it may be helpful to represent the technical data under consideration as sets in a Venn diagram. For our example, see the Venn diagram in figure 5.

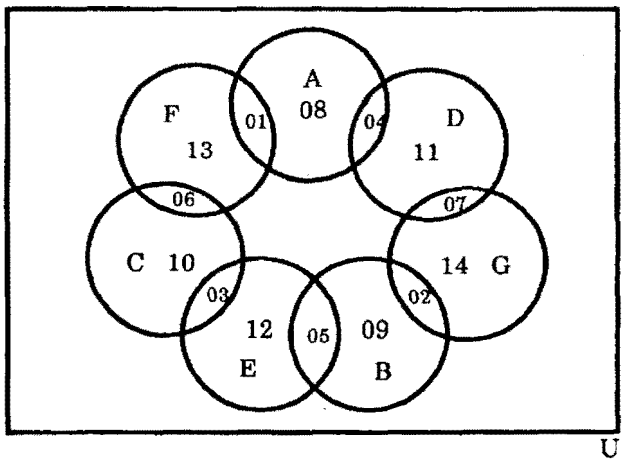


Fig. 5

AREA	CALLSIGN PAGES
A	01,08,04
B	02,09,05
C	03,10,06
D	04,11,07
E	05,12,03
F	06,13,01
G	07,14,02

From this Venn diagram, we can see that callsigns from pages 08 through 14 are unique to areas A through G, respectively. Consequently, these callsign pages can be used as a basis for identification of the area of communications. Since each of the callsign pages 01 through 07 is used by two different military regions, use of callsigns from these pages would reduce the problems of identification to one of two military regions. Further, callsign duplication, as shown in the above Venn diagram, may exist because of the

geographical separation of a military region by a natural barrier such as a mountain range, sea, or another country.

In conclusion, the analysis of technical data using set concepts is a systematic approach that may result in more understanding of the communications under study.

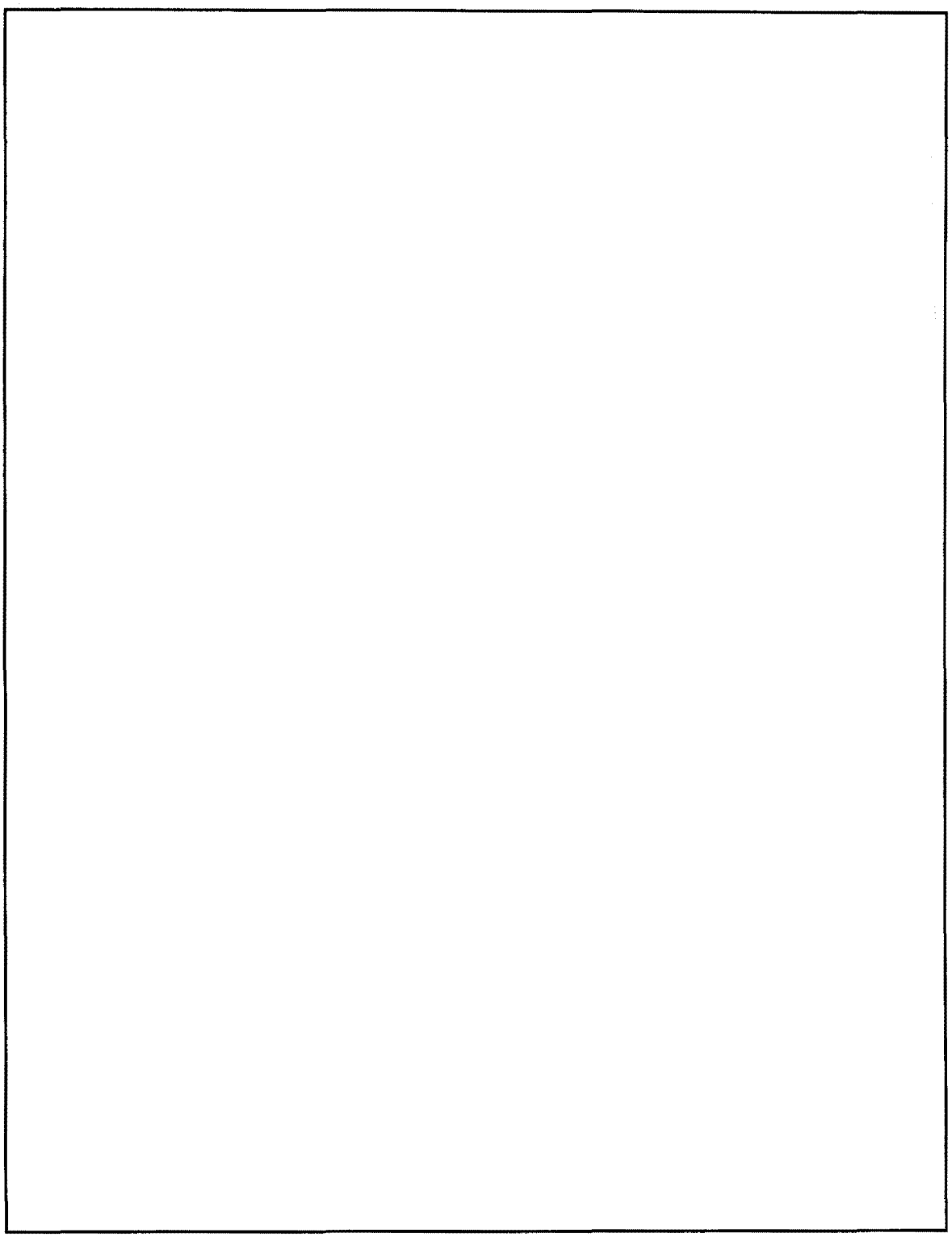
TA, CA, LOGIC, MATH: Where Do They Intersect?

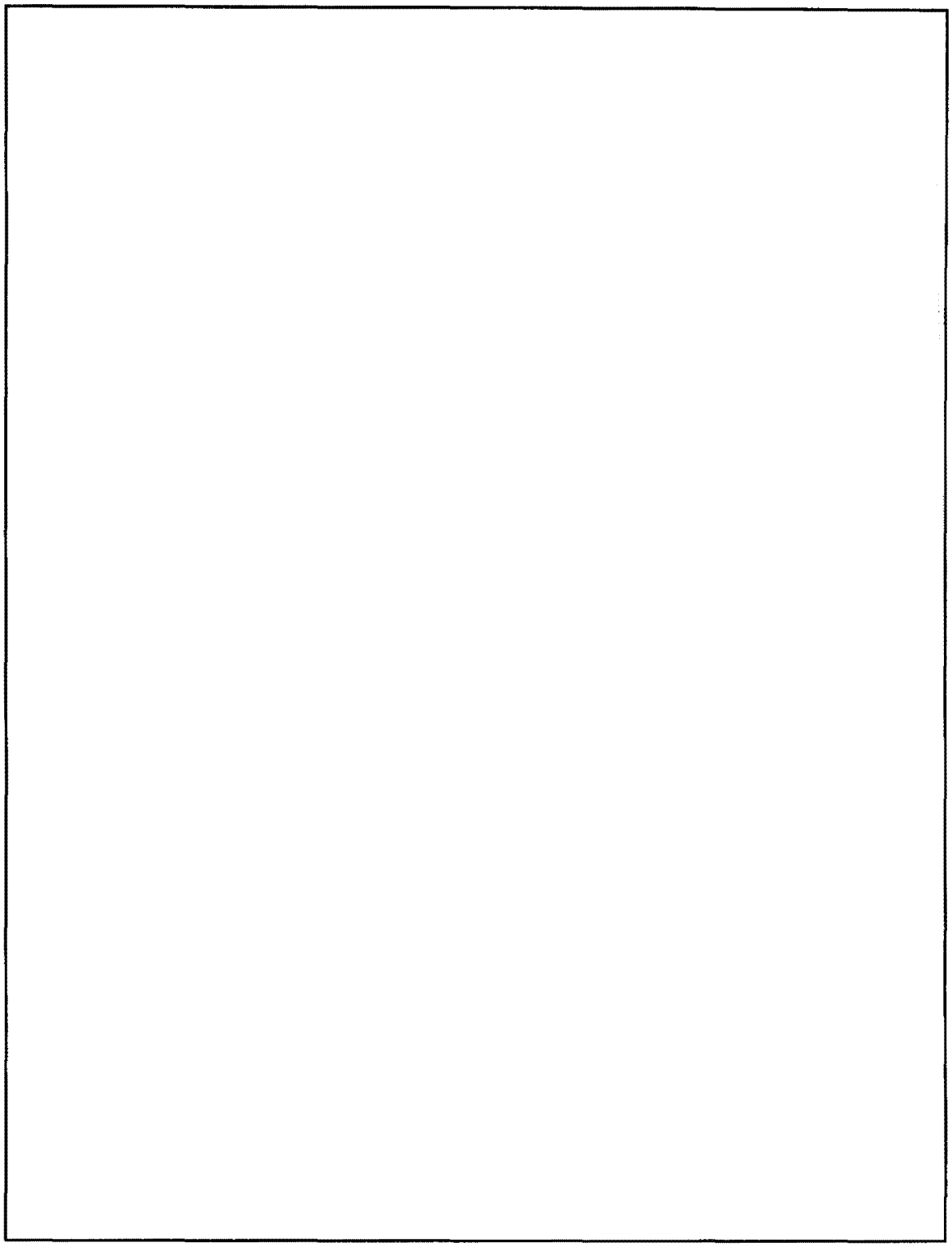
P.L. 86-36

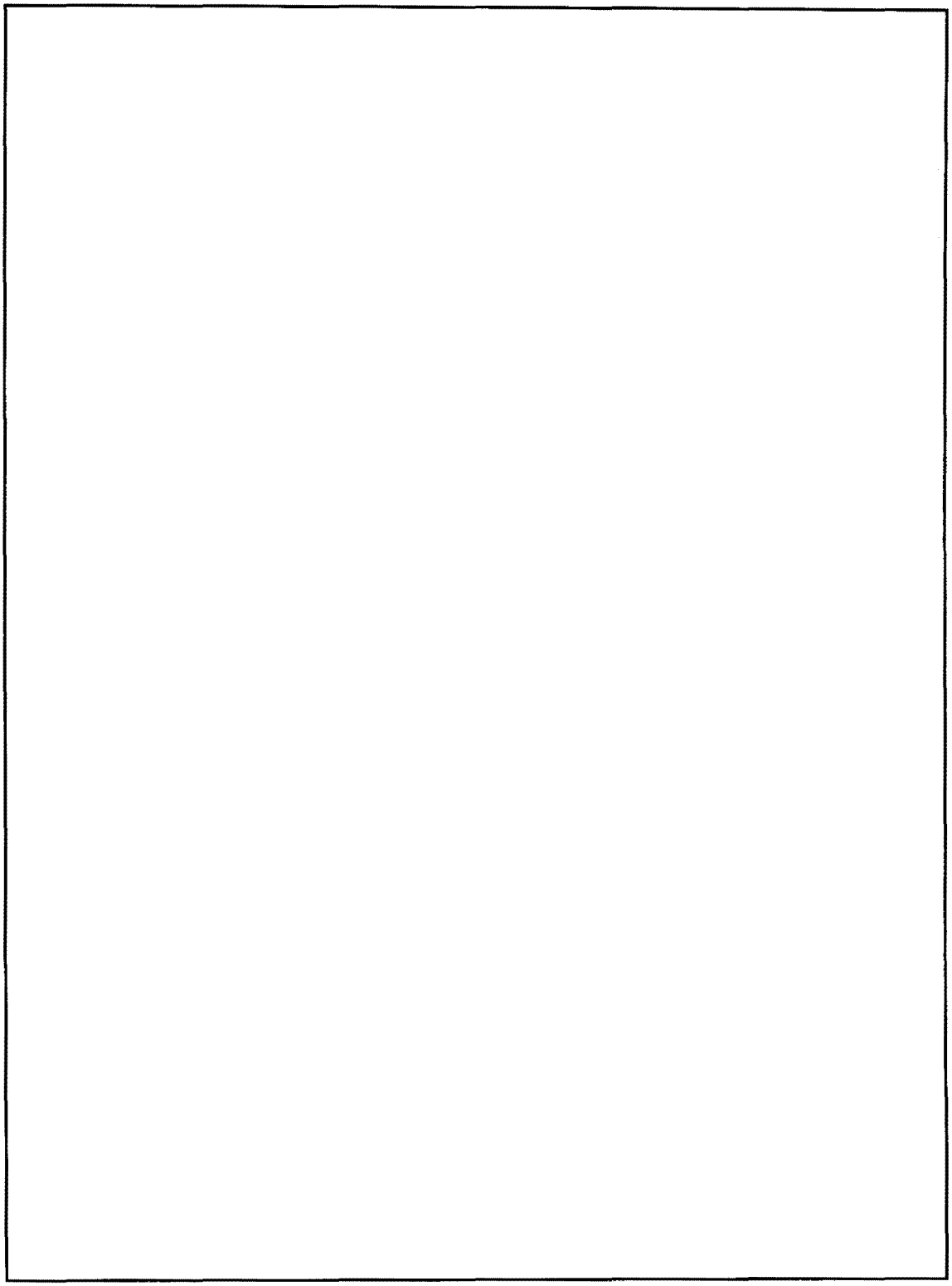
[redacted]

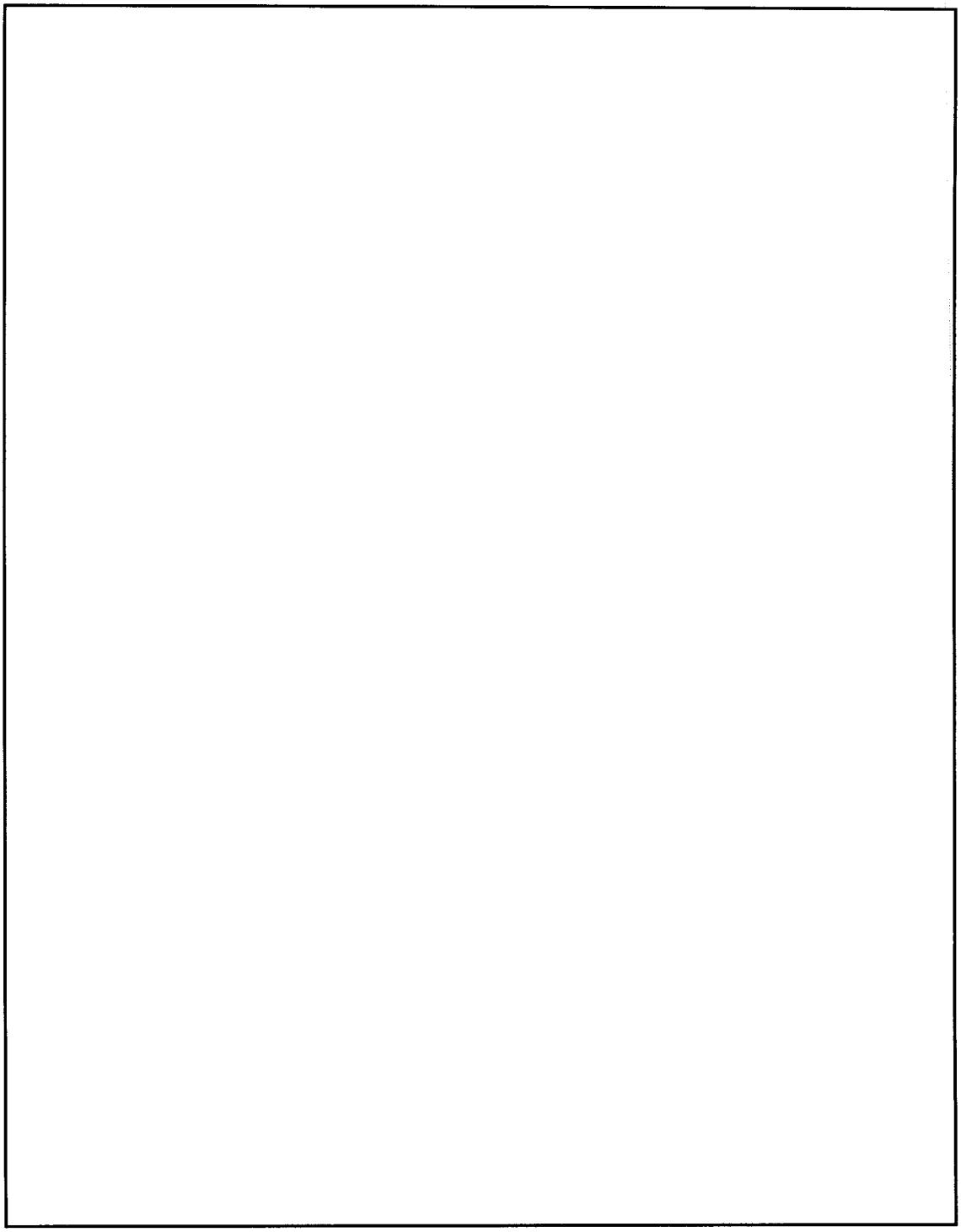
[redacted]

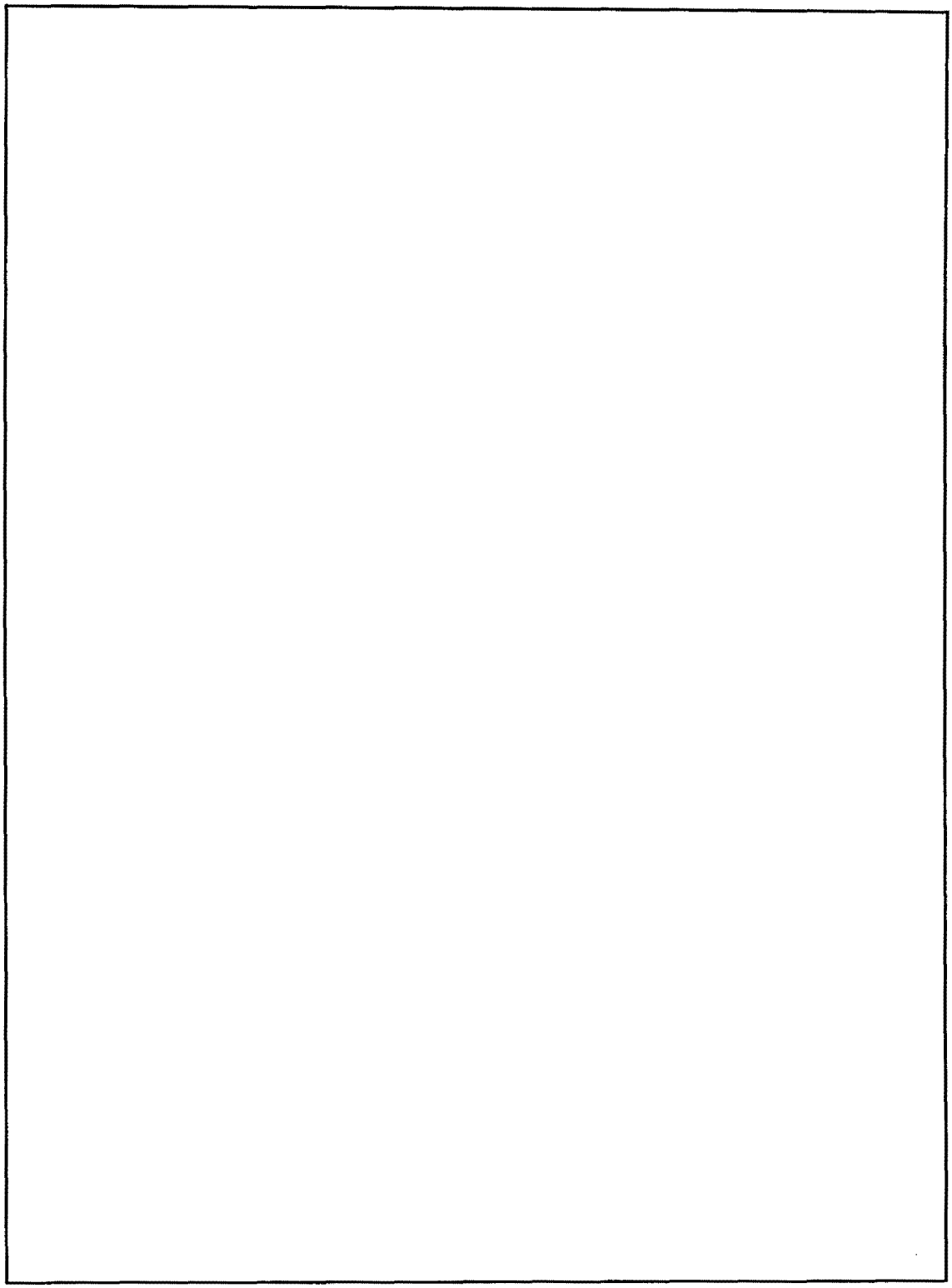
P.L. 86-36
EO 1.4(c)

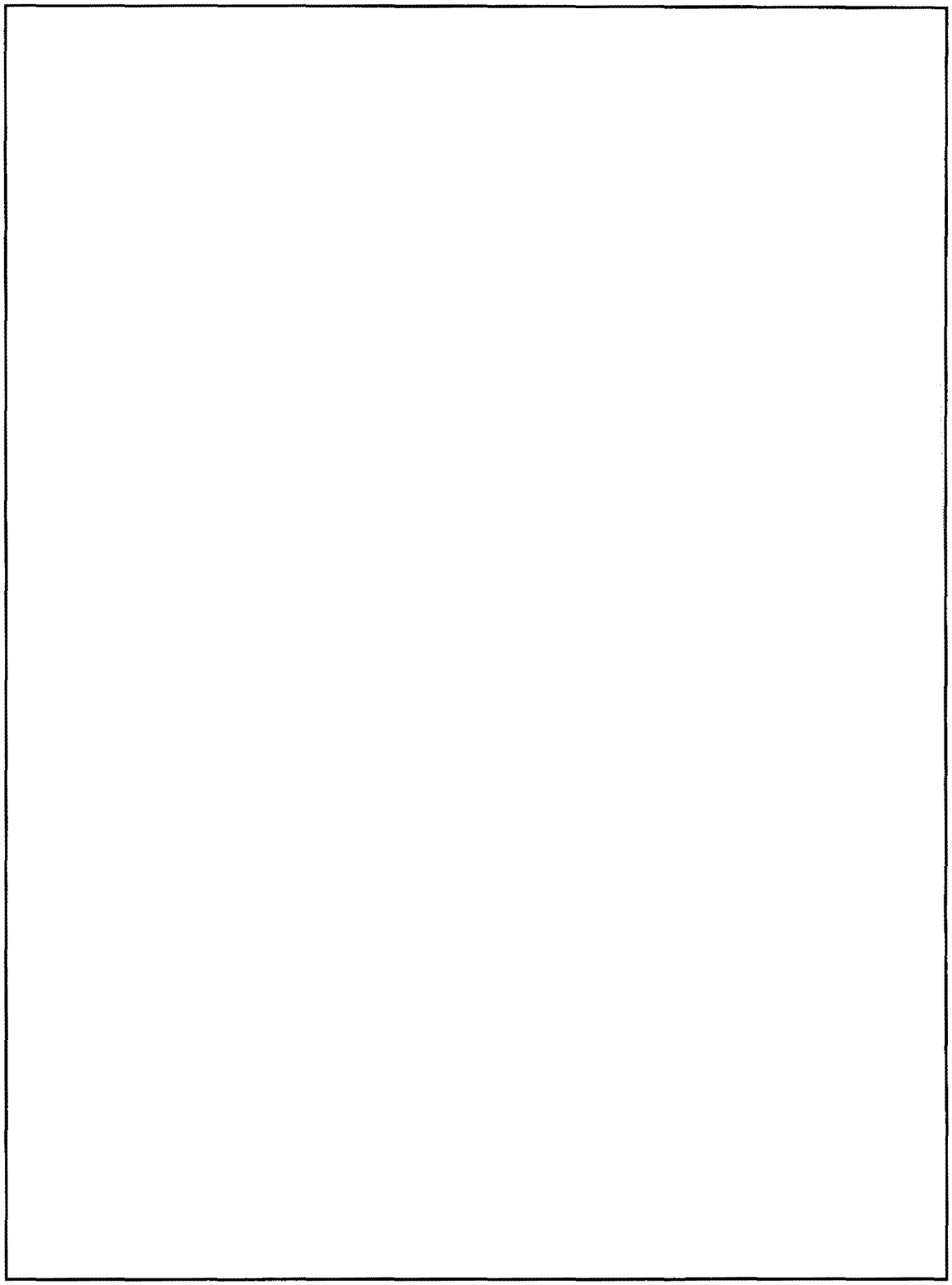


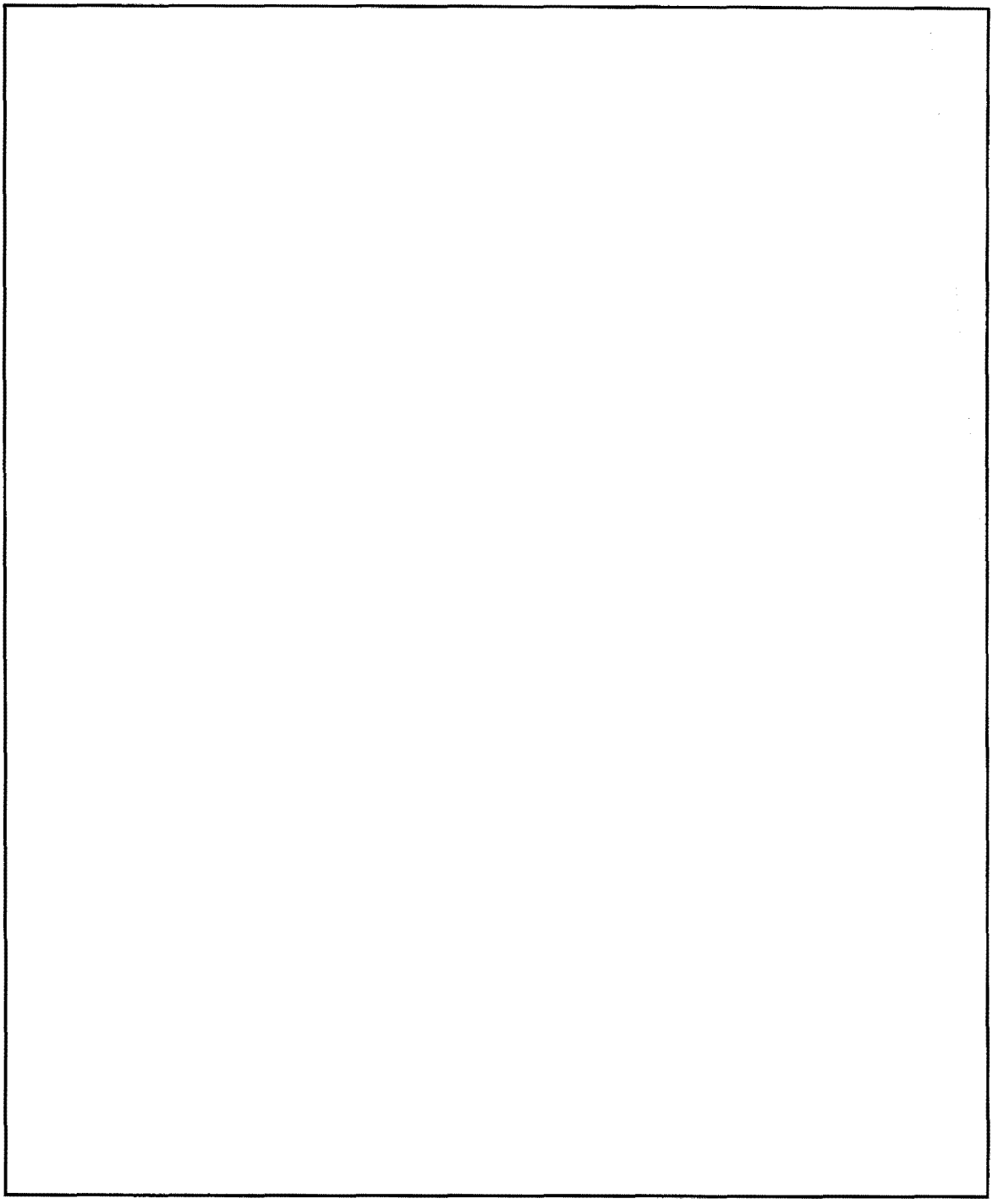


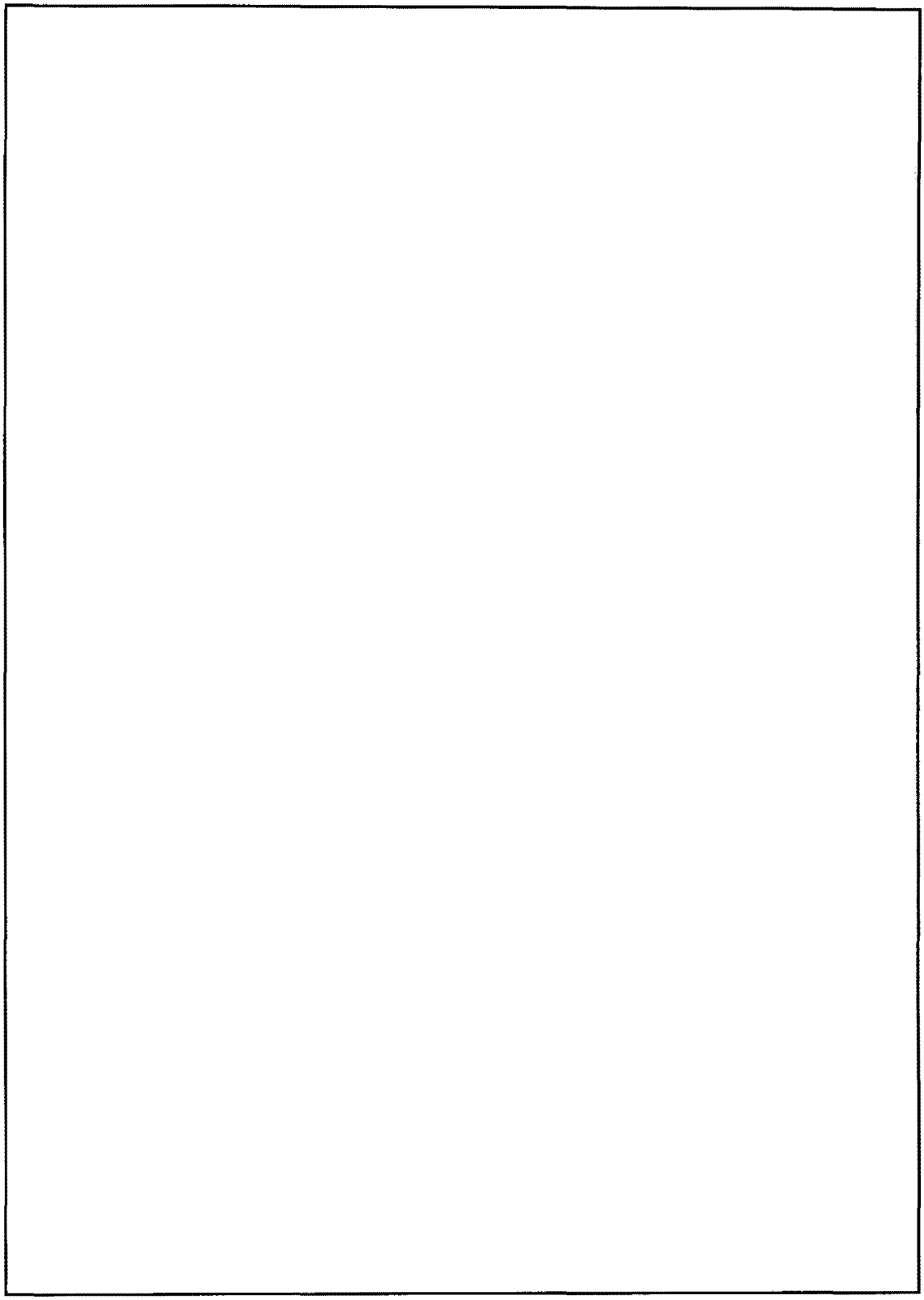


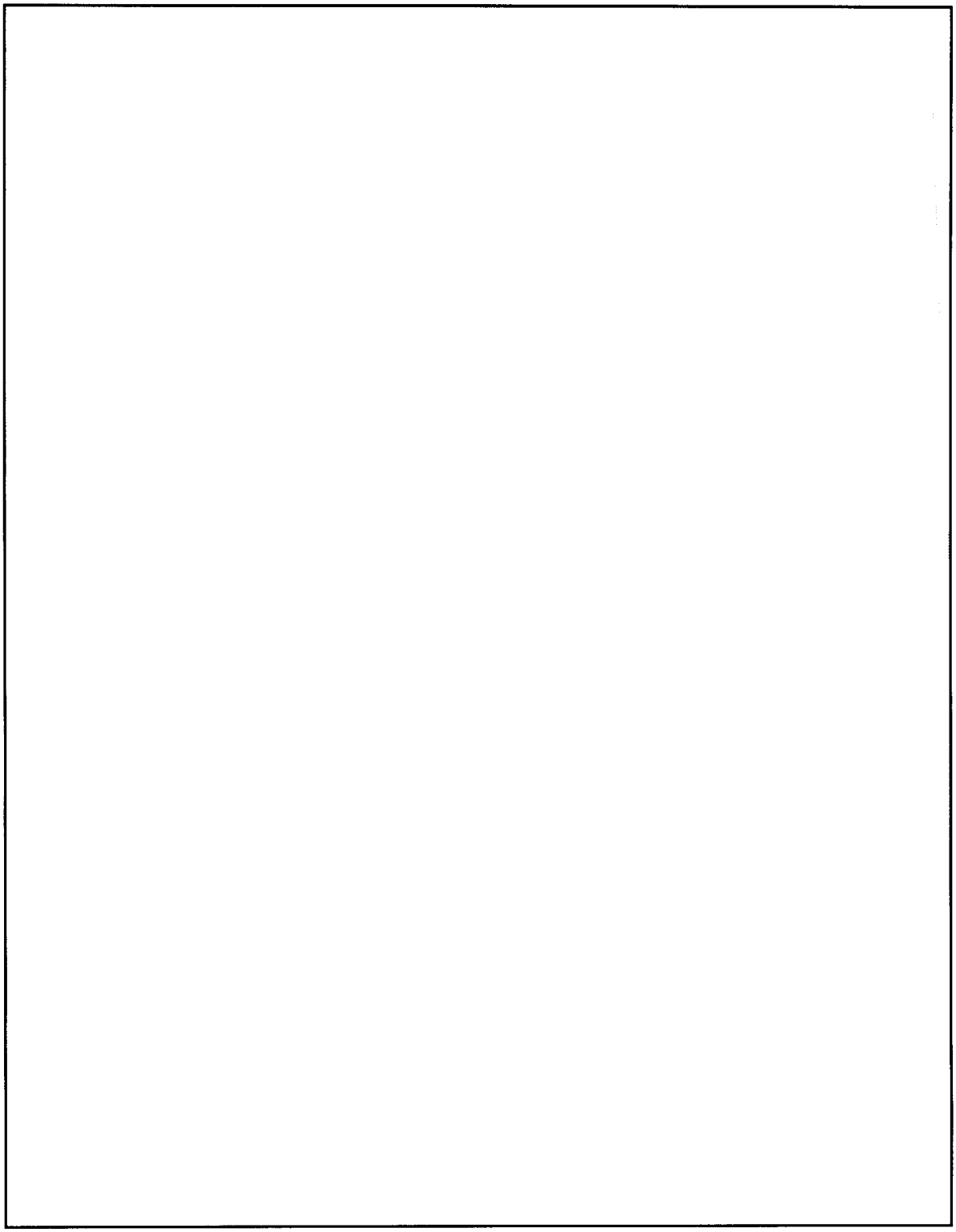


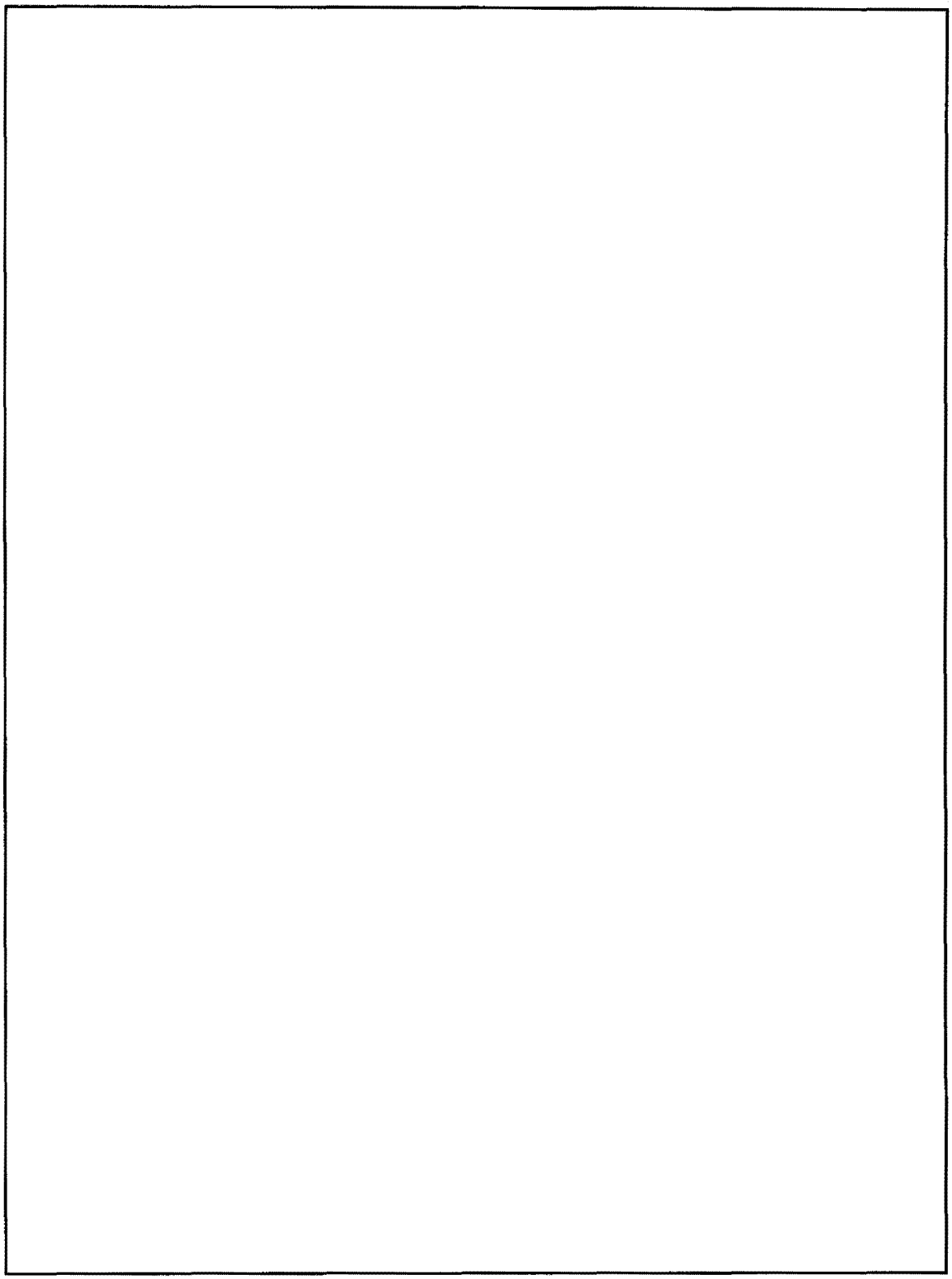


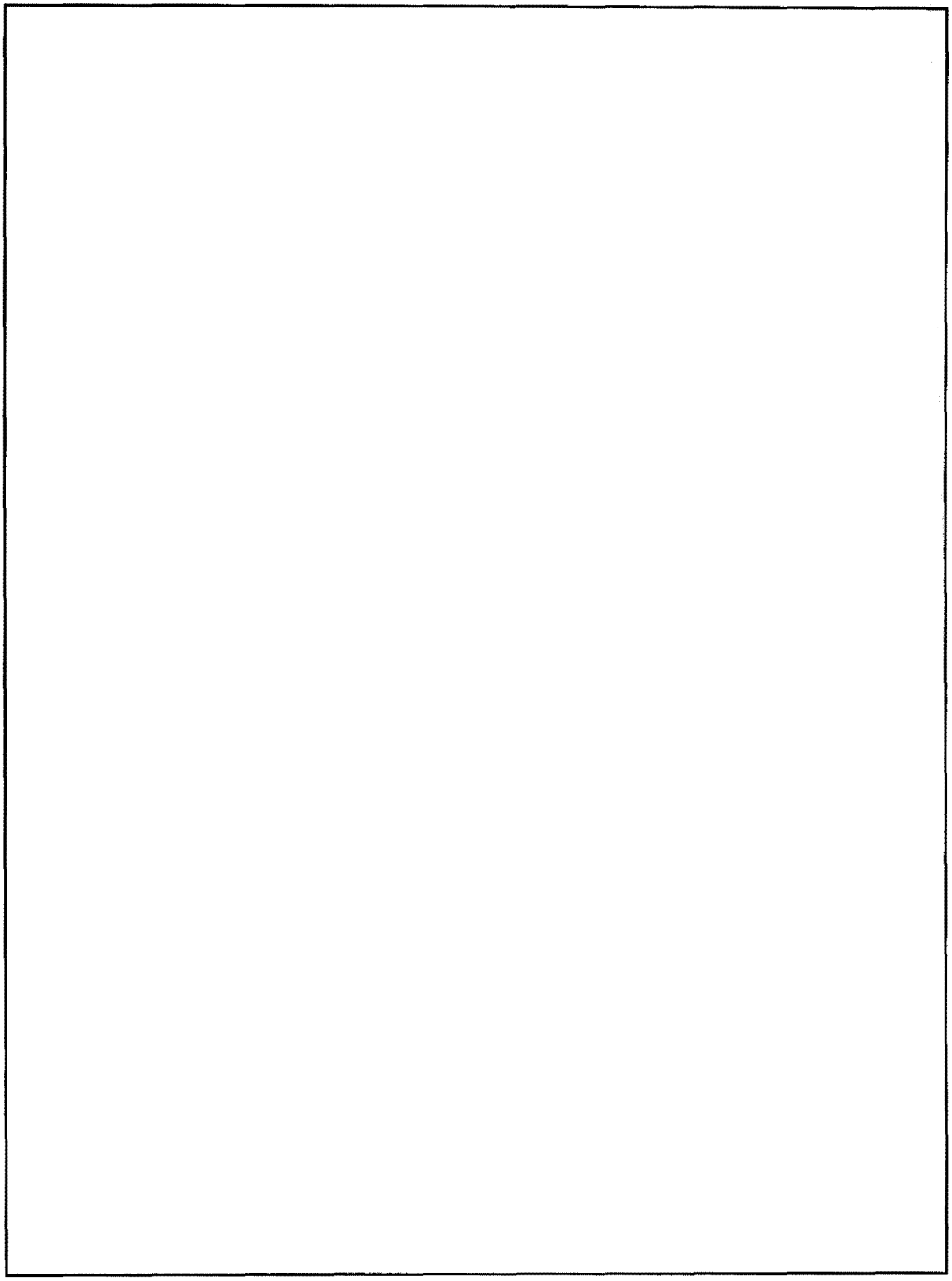


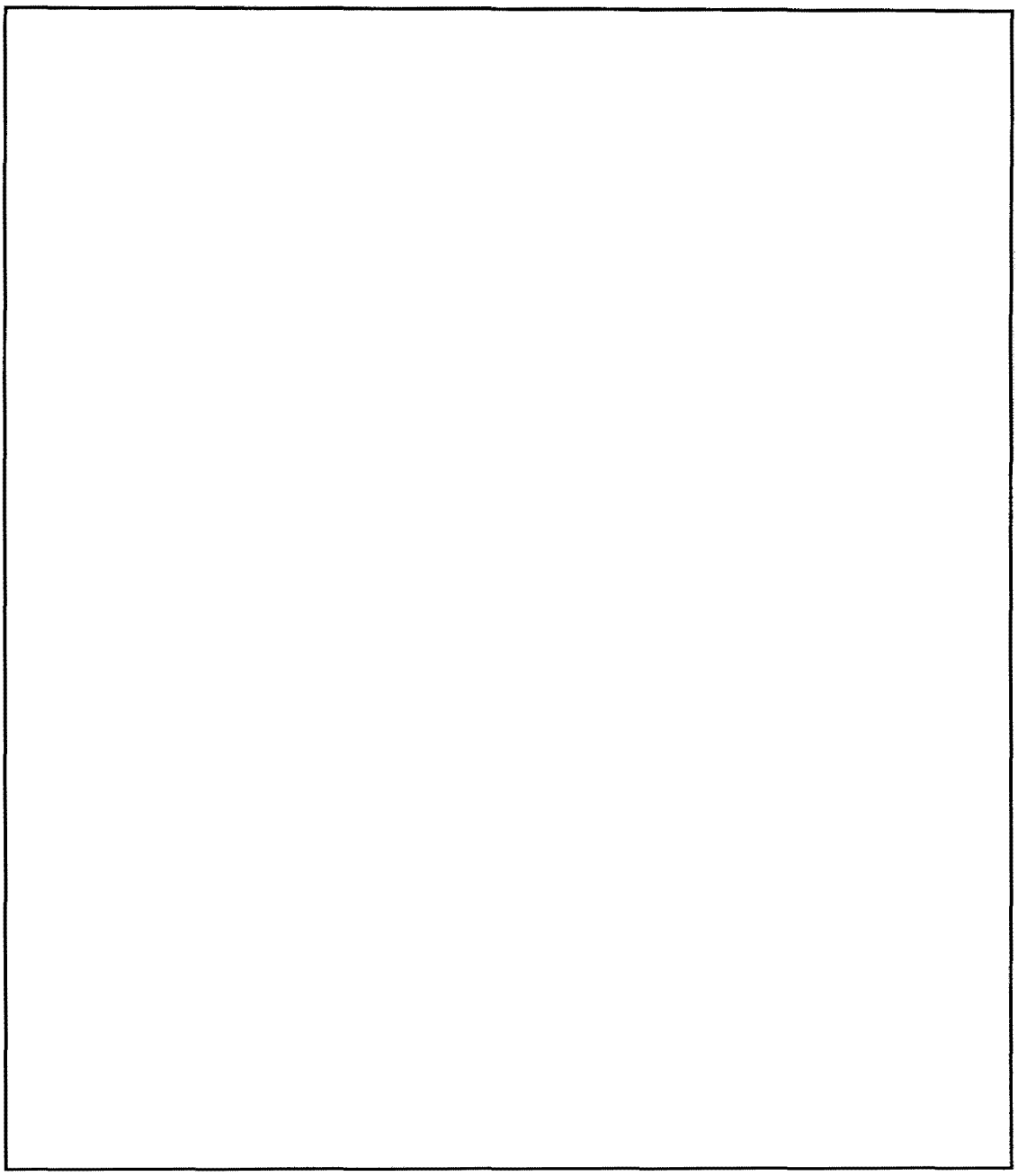


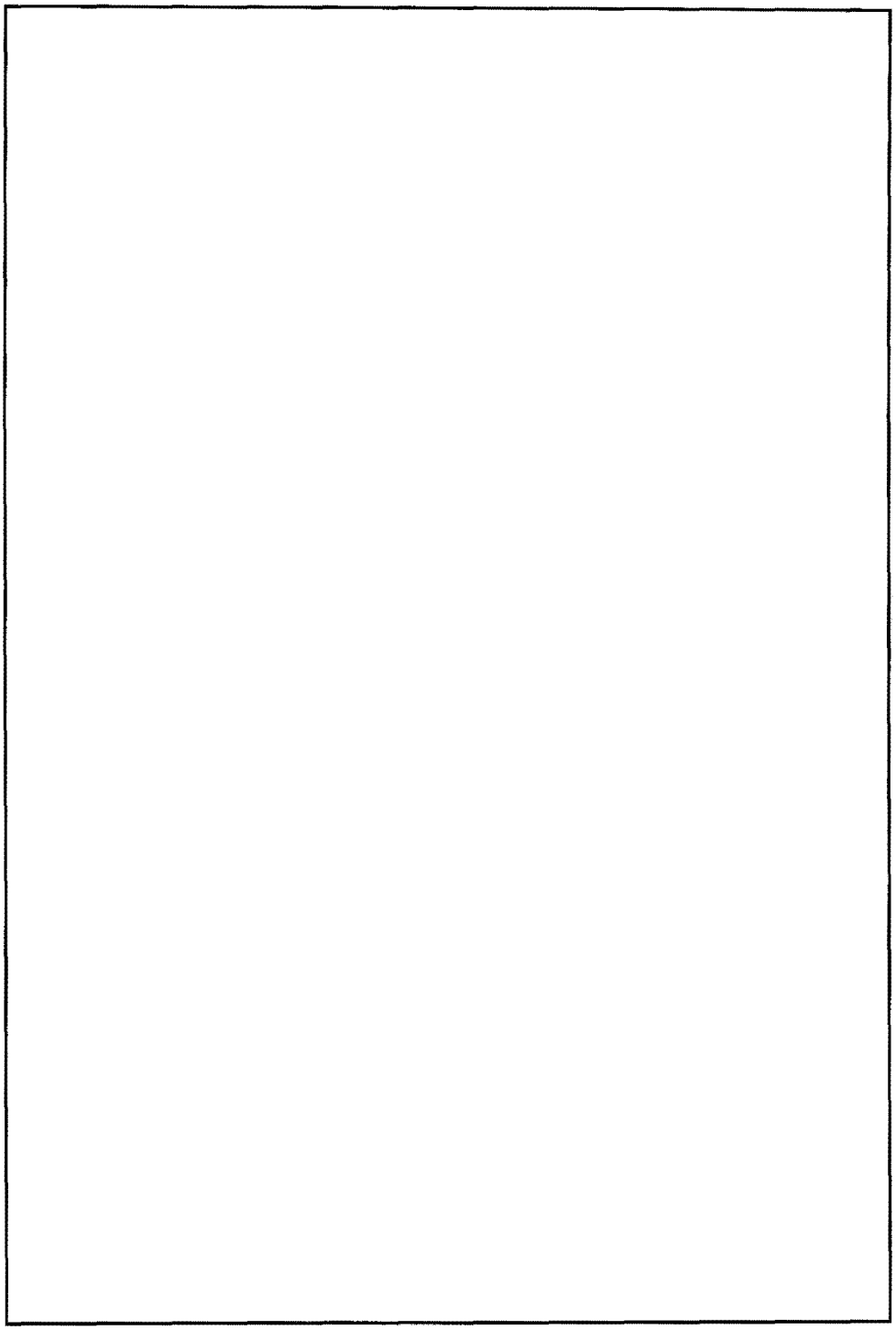


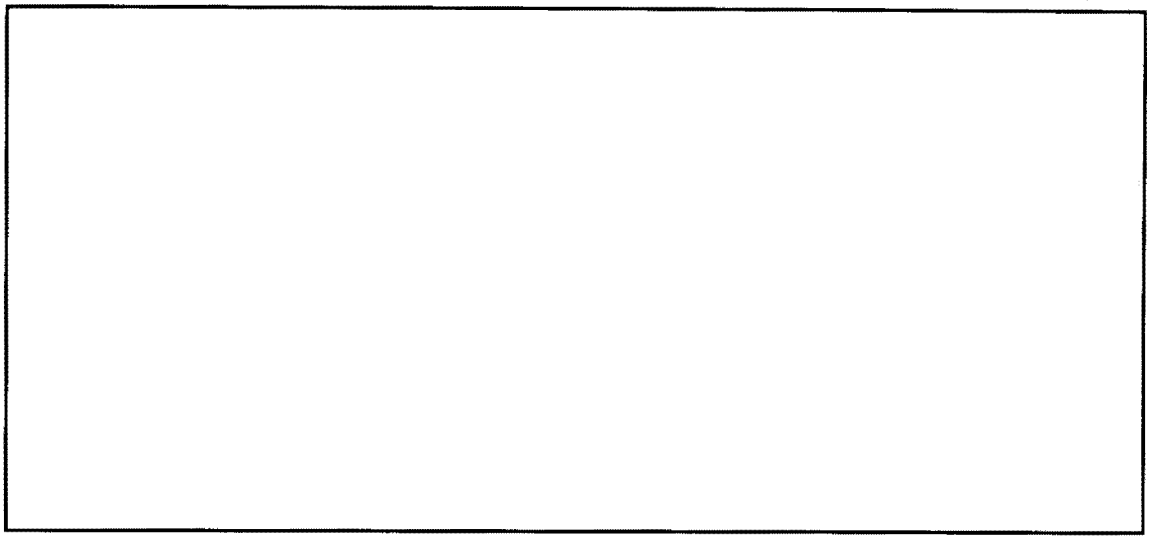












These two examples show how TA crosses many disciplines; it is fluid, unstable in many ways and allows for wide ranges of different techniques and types of systems. Particularly, I have found math to be a very necessary tool in the diagnosis of crypto/TA problems. But perhaps we traffic analysts have neglected to record these applications of math. We have used the concepts of set theory, or VENN diagrams and the like, in research on callsign systems, procedure systems or radio frequency plans throughout all phases of TA discipline. We may, however, have called it by another name. Therefore the query: are we introducing new techniques or new names?

SUMMARY OF PANEL DISCUSSION

The panel discussion held at the close of the two-day symposium attempted to answer the question "where do we go from here?" The consensus was that traffic analysts are, generally speaking, becoming increasingly aware of a need for mathematical expertise and that mathematicians are on the threshold of discovering another field they can support. Most participants in the symposium agreed that they had arrived at a new awareness.

Ideas as to what further actions could be taken following the symposium were summarized during the panel discussion as follows:

a. Mathematical training for traffic analysts

b. Exposure of some mathematicians to TA problems and TA work areas

c. Establishment of a register of mathematicians and traffic analysts and their respective skills

d. Establishment of idea-exchange groups where problems may be described and analytic approaches recommended

e. Documentation of TA-math uses, ideas and developments

f. Development of multidisciplined analysts

g. Establishment of a focal-point (s) for TA-math ideas and problems

Let's Not Lose Our Skills

[redacted] P.L. 86-36

One thing a middle-level supervisor in the Production organization realizes very quickly is that good traffic analysts are hard to find. Those traffic analysts with a skill in a specialized area such as frequency and callsign recovery are scarce. [redacted] P.L. 86-36 EO 1.4.(c)

As indicated in the A/DDO memorandum, the underlying causes for this decrease in traffic analysts are the rapid change to automated methods of collecting and producing SIGINT, and the personnel limits imposed on the size of the NSA work force. Since NSA cannot hire personnel to fill shortages in critical skills, the traditional skills have been reduced to accommodate increases in linguists, signals conversion personnel, collection technicians, and data systems analysts and programmers. As a result, we are creating a static pool of traffic analysts, retarding the development of our analytic talent and altering the career-progression patterns of the traffic analytic work force. It is these effects that I wish to discuss.

The end of the Vietnam War, the subsequent tightening of purse strings and the resultant reductions in traffic analytic spaces altered the availability of traffic analysts. By limiting the hiring of new traffic analysts and not replacing those lost by attrition, the size of the analytic career field was set [redacted] The immediate effects were minimal since the number of traffic analytic jobs was also decreasing, with the reduction of many of the timely requirements for information on Southeast Asia. Also helping to offset any immediate effects were the great strides made in mechanizing the traffic analytic processes during the Vietnam War. Efficiencies had been created and a degree of timeliness using methods of intelligence production never before possible had become routine.

The long-range effects probably will not be apparent until the late 1980s, but some symptoms are already beginning to appear. Our traffic analytic work force is getting old. Most of the younger analysts were hired during the 1960s and are now GG-11s or higher. Most basic traffic analytic work is now done by the military, either at the field sites or at NSA. No substantial group of young analysts at the lower grades is available for the future. The most aggressive analysts have already moved into management positions to further their careers. To aggravate what is rapidly becoming a bad situation, we have retarded the development of the younger traffic analyst. In the earlier growth days of our agency, a traffic analyst could grow in a specific target area, become recognized as an expert, and advance in grade and responsibility within his chosen career field. Today, the aggressive young analyst soon recognizes that his future is not in the technical side of the

traffic analytic business. To advance and achieve a modicum of success, he must move into management or to one of the critical-shortage skills. Consequently, we deplete our analytic talent base, and few people are left to form a nucleus for the future.

Those who are left usually have a sincere desire to remain in the technical side of the intelligence production business. Even those people are prodded by management to move into the more critical areas of data systems or linguistics. Since chances of promotion are mathematically better in these skills, many of the remaining talented young people do indeed transfer.

Those who remain face a slower career progression since the money provided for the special considerations given to the critical career areas reduced the total sum that would normally be equally divided among all those eligible for promotion. This means the traffic analyst must face stiffer competition for the promotions that are available, and ultimately his chances to achieve a position of leadership within the Agency are diminished.

As a result, probably in the near future, we are going to be faced with a severe analytic shortage similar to that which we now have with linguists. A more serious consequence will be the loss of analytic skills that can be learned only by years of experience. Specialists will be nonexistent, and major analytic recoveries will suffer. Although these problems can be alleviated to a degree by hiring from the SCAs and by programs such as the intern program, these are not immediate solutions. Unlike the data systems and, to a certain extent, the linguistic fields, our colleges and universities are not graduating many traffic analysts. It is a career field where experience is the best teacher.

To avoid future shortages, we should begin hiring some Traffic Analytic Technicians right now. These technicians could be hired out of high school at the GG-2 level and put through a program similar to that used for training linguists. Given the proper incentives, training, and experience, these people would be ready to take over the analytic work load in about ten years. If we fail to act now, we will have to react later, when our chances of success are fewer. Traffic analytic skills helped make our agency what it is today. Let's keep it that way.

P.L. 86-36

[While [redacted] *article was being prepared for publication, it was shown to* [redacted] *Chief, Traffic Analysis, Office of Techniques and Standards, and he was asked if he would like to add any comments. He has submitted the following addendum. Ed.]*

We could *also* hire ex-military traffic analysts, as we have in the past. This has the advantage that each "recruit" already knows what TA is, likes doing TA, and wants to make a career of it. That cannot be said of high school hires, and one must therefore expect a higher rate of "drop-out" than would apply to those already trained and experienced in TA (ex-military).

There must, of course, be some disadvantages to hiring ex-military traffic analysts. Otherwise, an agency as smart as we are would already be doing it.

LETTER TO THE EDITOR

~~(FOUO)~~ One of the advantages of being associated with a program such as the Traffic Analysis Intern program is the opportunity to watch the big picture develop. For three years I watched the traffic analysis career field being continually rescued from threats to its survival that came from whatever managerial wonders happened to be exerting influence at the time.

~~(FOUO)~~ While specific to the TA experience, these remarks point out the crucial aspects of organizational life: organization, corporations, or whatever, are really people. Hiding behind the various bureaucratic identities cannot disguise this reality. The "health" of the people affects the organization's. When people stop caring, growing, and producing, the organization ossifies and eventually fails.

~~(FOUO)~~ Personal career and organizational development are intimately linked. This agency has taken vital steps to facilitate career development, thereby assuring its future. This month's Career Development activities are a celebration of this process – in the past, present, and future – and its meaning for us and the Agency.

ROBERT HANYOK

AND FROM AN OVERSEAS READER . . .

P.L. 86-36

To the Editor, *Cryptolog*:

~~(S-CCO)~~ [redacted] article, "Let's Not Lose our TA Skills," (*Cryptolog*, March 1979), made an untimely appearance here [redacted] The week before it arrived, several of the people here, due to return to NSA in the near future, had attended reassimilation briefings, during which the overstrength skills problem was not only raised but also given as a rationale for the reassignment of some to a different career field. Some of the moves were in the out-of-TA direction! It's easy enough to fall out of touch when headquarters is an ocean away, but it's even easier to be confused by the apparent contradiction between the M3 view of TA as an overage skill, and the view shared by [redacted] that TA is a field with an impending shortage crisis. Perhaps some of the fifty-odd traffic analysts now in excess could be used to head off the coming shortage. The concern about the effect of transfers out of TA and the lack of new blood is shared by many. This feeling was expressed here recently by visiting managers, who stated a need for analytic talent to work in the rapidly expanding world of multichannel communications.

P.L. 86-36
EO 1.4.(c)

(U) What all of this may boil down to is the ever-present problem of individuals holding the title but not doing the analytic job, and the apparent inability of management to cope with this issue. *Good* traffic analysts are hard to find, and so may be talent in other

overstrength skills; the key may be quality vs. quantity, another problem that's always with us. If nothing else, [redacted] article may make some managers realize that skill balance by the numbers is not an end-to-all-your-troubles elixir for reducing the work force, and that talent returning from overseas should not be regarded as a magic ingredient for such a brew.

KATHY BJORKLUND

Letters To The Editor

Last month Cryptolog *printed a letter from Kathy Bjorklund in which she wondered why the view of traffic analysts as a vanishing breed, which has been expressed in* Cryptolog *by various people, is at such variance with the M3 view of TA personnel as an overstrength category.*

To the Editor, *Cryptolog*:

(U) Since you were kind enough to ask me for a comment on Kathy Bjorklund's letter, I felt obligated to break out [redacted] article, to which she referred. There are several hot spots in those two items and one that rises from them.

(U) First, *Cryptolog* has traditionally been an open forum, and I would not change that. But we who write for it from time to time are obligated to do some homework before we present opinions that aren't defensible. Or, maybe it's time to label fact and opinion so that readers can sort them out.

P.L. 86-36

(U) For Kathy, here are a couple of facts. While your briefing on reassimilation and career field overages was probably conducted by personnel or administrative people, they are not the ones who made the decision that TA is an overage field. As your Chief of Personnel Services, [redacted] could have told you, M3 is part of Management Services (DDM), and it is a support or service organization that attempts to meet *requirements established by other Key Components*. In this case, it was Operations (DDO) telling M3 that there were overages in the TA field and shortages in the language field; it was DDO telling M3 to initiate the needed personnel actions, e.g., reassignments and hiring. Can you imagine the confusion if M3 went about willy-nilly hiring and reassigning people against no known requirement?

(U) Another fact is that George's article is mostly opinion. Now he has as much right as anyone else to have and express those opinions, but he knows he will get some arguments. For example, we not only lost good analysts when some TAs moved into management – we also gained some bad managers, although that's not a problem peculiar to the field of TA.

(U) But by and large, I doubt that you could find anyone who has to pick up the tab in billets or skills balances who would say we have any current or near future shortage of traffic analysts, or of TA technicians to fill the vacancies that will some day exist in the analyst ranks.

(U) Comparing real and present shortages in the language and computer arenas to "maybe" shortages ten years down the pike may not be a fair analogy. The computer and language shortfalls are there because we have added jobs or lived with vacant positions. In the field of TA that has not been, and is not now, the case.

(U) Since most of our TA overages are at the technician level, I'm not sure I understand George's suggestion that we hire more technicians. But my not understanding is irrelevant – we aren't going to hire against a nonrequirement, at least not if I understand the way things work.

(U) Back to Kathy's letter for a final comment on her last statement: "...talent returning from overseas should not be regarded as a magic ingredient for such a brew." Given our selection processes, increased promotion points, and preferential treatment in assignments upon return for field people, I am a bit surprised that you believe there is an *intentional* negative attitude toward returning field people. And my opinion is that DDO, DDM, DDR, DDT and DDF would be equally surprised.

(U) Regards to you, Kathy. Congratulations to you, George. And, Dave, whenever you want an opposing view on almost any subject, please give me a call.

DAN BUCKLEY

To the Editor, *Cryptolog*:

(U) I read Kathy Bjorklund's letter with a feeling of depression – because what she says is all too true. The bodies-and-slots, or bean-counting, approach to personnel assignments is not one that is conducive to the continued development of the technical work force of the Agency.

~~(C)~~ During the skills requirement forecast of 1973, the career panels were asked various questions on personnel development covering the period FY74 through FY79. Questions such as the following were asked:

- What effect will new or emerging technology and modernization of cryptologic operations have on the skills under the purview of your career panel?
- Do you anticipate a need for developing multiskilled specialist, and if so, which skills or combinations of skills will be required?
- Will the need for specific skills (TA, CA, etc.) decline or increase?

(U) I don't know what happened to the results of this poll, since current personnel planning does not seem to reflect them, but rather continues to be based on projections of the current work force: How many people do we have in such-and-such COSC? Well, then, if we have that many, and if we are getting the work done, then that must be the right number. So let's just straightline that number for the next four fiscal years. Obviously, this approach is the basis for faulty TDs, since it makes no allowance for any shifts in requirements brought about by shifts in targets or other considerations.

~~(C)~~ Let's see how this works. At the moment Traffic Analysis is carried as an overstrength skill in A Group. The TACP [Traffic Analysis Career Panel] has two interns due to graduate this month. On the basis of their backgrounds, experience, the panel's recommendations and their own preferences, these interns should be assigned to A2. But

the thought of placing them in an overstrength element is enough to give the bureaucrats heartburn.

~~(C)~~ The placement of overseas returnees is similar. P41 attempts to assign personnel holding A Group overage skills to B, G, V or W; only a few of this year's returnees have been assigned to A.

~~(C)~~ In short, P41 and M3 will almost always stand in the way of any assignment to an overstrength element. I have accused P41 of approving TA intern placements using the bean-counter approach. They deny this vehemently yet state in writing, in a memo to Chief, M3:

[redacted] P.L. 86-36 E.O. 1.4(c)

A fair share – by the numbers!

(U) [redacted], quoted by Ms. Bjorklund in her letter, are correct: the number of traffic analysts is dwindling. Part of this is attributable to the reasons cited above. Another rank-thinning factor is age. Almost twenty percent of the people in COSC 1411, Traffic Analyst, are over fifty years of age; less than two percent are under thirty.

(U) What is the solution? As I see it, it is twofold. An immediate measure would be some directed assignments. This would include the identification of personnel holding a given COSC in an overstrength area, but not performing that function, and making appropriate readjustments, such as transfer, retraining or reclassification. It would also include the placing of overseas returnees in areas where their skills are most needed, even where they might be a temporary overstrength condition.

P.L. 86-36

(U) For the longer term we must nurture the TA intern hire, insuring that we have at least six to ten coming in each year, and placing them in the work force where they will produce for the Agency regardless of numbers or quotas.

~~(C)~~ Let me quote from an old-time member of the TA corps:

> How long does it take to build a professional traffic analyst from zero? If it takes, say, five years, then we are betting that whatever the situation is today, it will be the same five years from now. And what we are betting with is the Agency's reputation for adapting to fast-breaking changes in the world situation.

~~(C)~~ The TA intern program can and does build a professional traffic-analyst/reporter from zero with a very solid understanding of the interrelationships of the other cryptologic disciplines. The annual hiring of a few bright people – recent college graduates as well as former military analysts – should solve the problem of being able to find good traffic analytic talent in the future.

[redacted]
Executive, TACP

To The Editor, *Cryptolog*:

(U) Having had long, and often passionate, discussions with both Mr. Buckley and Mr. [redacted] on the subject of Traffic Analysis "overages," I was surprised to see that both gentlemen missed several important points (see Letters to the Editor, *Cryptolog*, July 1979). P.L. 86-36

(U) First, I think (please note, opinion) there are a fair number of individuals who hold TA COSCs who are not doing TA work. One example: a branch chief is a manager, not an analyst, yet the analytic COSC is often held.

(U) Second, quality is not an element included in the "bean-counter" approach; it's the number of bodies bearing the title that are counted. The fact that one quarter of the bodies may be doing three quarters of the work does not enter in.

~~(C)~~ Third, we seem desperately intent on trying to "professionalize" (read, certify) ever-increasing numbers of people in overage fields. The problem with this is twofold:

- What is the purpose of creating many more professionals than we have professional billets? What is the purpose of allowing second certifications in overage fields?

- Why are we tutoring professional aspirants? Individuals of professional quality will, like cream, rise to the top by dint of personal study and research. They will do so simply because it is in their nature to excel, not because they were pushed, prodded or carried through the test. (Please note that "top" refers to one's ability to perform, not to one's promotion record.)

~~(C-CCO)~~ I agree with [redacted] – we *are* losing our TA skills (See *Cryptolog*, March 1979). It is evident in the simple fact that many case analysts do not log intercept in such a manner as to see a simple rota. It is reinforced by the fact that on our professionalization exam the net reconstruction section is pre-logged and fairly easy. The difficult section is the crypto-TA part, and few traffic analysts are charged with this type of responsibility in their daily jobs.

(U) Suggested solutions for eliminating the overage and upgrading the quality are fairly simple. Ensure that only those doing traffic analysis carry that COSC; let's start calling managers managers. Next, devise a weighting system so that a manager can state for the TD that he needs three topflight TAs, or five average, or ten below-average (or some combination thereof) to accomplish his mission. And, finally, if we feel compelled to tutor someone, let's begin by tutoring those most in need so that they may become proficient in their current jobs.

(U) Years ago achieving professionalization was akin to winning a place among the elite. Today is simply a means of proving oneself average. Elitism is not only dead, but is scorned as well.

(U) Let's put the emphasis back on the quality of our human resources.

[redacted]

Simplicity in Color

C. GAROFALO

The conduct of crypto-TA studies involves the requirement to differentiate between qualitative levels or categories, and the use of a simple color scheme facilitates such differentiations. Any color scheme to be used in an analytic effort of large volume must be

- simple in nature,
- skillfully chosen, and
- systematically applied.

An analysis of the various colors available was made to determine which are practical and most suitable for the task. My experience has demonstrated that six different colors are most practical. These are black, green, red, blue, purple, and brown.

- Black – carbon (number 2) medium degree of hardness and density, suitable for both erasure* and longevity properties.
- Green – is the weakest, that is, of lightest density. All of the other colors under consideration superimpose on green quite readily.
- Red and Blue – are of equal boldness; either can be easily superimposed on both black and green.
- Purple – a bolder color that can also be produced by a superimposition of red on blue or blue on red.
- Brown – is considered to be the boldest of all colors as well as the most exclusive and conclusive.

Colors manufactured by different commercial firms vary drastically in hardness, density, and coloration; it is desirable, therefore, that having started with a particular brand to continue with that brand and not intermix brands to ensure that distinctiveness and clarity are maintained.

A color ladder may be displayed graphically as follows:

Color	Level
BROWN	5
PURPLE	4
BLUE	3
RED	2
BLACK	1
GREEN	0

* For Black erasures, a medium hard rubber erasure is adequate. For color erasures, best results are obtained with a typewriter eraser.

Another way to express the levels of the color ladder is by these definitions:

- Brown – The ultimate in degree of trueness, not to be questioned. May also represent captured, compromised information or its equivalent.
- Purple – High in degree of reliability; may be used as a substitute or companion for brown where special conditions of clarity or distinction are vital to the problem. Primarily useful as a final ordered and oriented intermediate enjoying the same general stature as brown.
- Blue – A relative base value having a significant bearing on the state of recovery.
- Red – A base of lesser value or no relativeness (completely arbitrary), a first step necessary in any endeavor.
- Black – To record or log information as it appears in its earliest or original form.
- Green – An envious color reserved completely for suspected garbles, projected or expected but unobserved values (not proven but highly suspected as being correct). Used to alter a meaning or information without obliterating the original (black) form.

Once a color scheme is established for a given problem, maintenance of color discipline is mandatory in order to achieve uninterrupted and unambiguous continuity. Discipline is also of great benefit to management in that it ensures that redistribution of analytic personnel can be effected with minimum disruption to the overall effort.

Postscript:

<u>Colors:</u>

Green	symbolized hope to the ancient Egyptians;
	in the Middle Ages was supposed to be good for the eyes;
	to the Mohammedan, a sacred color;
	in modern times has come to signify envy.
Purple	to the Tyrians and Romans, a purple robe or band of purple signified authority; became a symbol of majesty to the Romans.

The Impact of ARDF on Traffic Analysis

ALLEN L. GILBERT

The Vietnamese conflict and techniques for collection of signal intelligence developed and employed in that arena have profoundly influenced the traffic analytic approach to the Vietnamese Communist problem. One of the most effective techniques employed on a large scale in Vietnam has been Airborne Radio Direction Finding (ARDF). ARDF, in addition to revolutionizing the direct support of tactical units through timely and accurate locating of enemy units, has almost reversed the traffic analytic approach to maintaining continuity and developing new targets in some areas.

Traditionally, the traffic analyst is faced with the problem of reconstructing a communications complex through recovery of callsign and frequency systems, message externals, schedule activity and those rare compromises made by enemy communicators. This route usually requires close scrutiny and cataloging of the elements of intercept through an extended period of time, with the hope that a transmitter location will be compromised or that medium-range direction finding will suggest a location for the activity. ARDF provides a location [redacted] P.L. 86-36 EO 1.4.(c) The availability of ARDF on target transmitters considerably shortens the period of development for new activities and provides almost instant continuity on targets effecting communications changes.

In Vietnam, the concept of ARDF tasking provides coverage in all areas of hostile troop activity. [redacted] When aircraft are deployed to a target area daily, the recovery of the signal environment in the area builds rapidly.

Certainly, all other elements of traffic analysis must then come into play to establish case notations and identifications. ARDF alone does not solve the problem, but what an advantageous beginning it provides!

Barometer - Readers' Comments

Traffic Analysts: Write it Down Now!

In approaching a traffic analytic problem for which you have responsibility, have you ever wondered how any of the major callsign systems, procedure tables, address systems, or other complex phases of transmission security were solved, or what significant characteristics contributed to their solutions? It is highly unlikely that you could find a detailed written description of the analytic effort involved in any of these solutions, so you would have to go to the individual who had been most intimately concerned with it, the individual recognized as having had the responsibility for providing the technical direction toward the solution. He is *the* person who was confronted with the problem, recognized its difficulties, determined analytic approaches, made mistakes, went up blind alleys, made critical decisions, directed other analysts, and generally supervised the entire effort. Assuming that he is available, you could ask him to describe the entire process. There is a good chance, however, that because of passage of time or lack of thorough documentation, or both, he would find it difficult to reconstruct in detail the path and the thought processes that were followed in reaching the solution. Thus, valuable expert knowledge, which might be useful in the solution of current or future problems, would have perished.

How can the loss to posterity of expert knowledge in such a situation be avoided? Very simply, the analyst who is pursuing a specific problem should *keep daily notes* on his analytic activities, his thoughts, his approaches, his mistakes, his conclusions, etc., and then, upon arriving at a solution (or failing so to arrive), *prepare a detailed written record* from these notes. The record, to be of most value, should describe the entire effort from a strictly chronological viewpoint, so that the influence of hindsight might be avoided.

If this practice had been consistently followed in the past, the Agency would now have in permanent form a wealth of analytic expertise that led to past successes but that is now unfortunately past accurate recall. The practice should be followed by every analyst who is pursuing a specific problem, whether it is large or small: he cannot predict where his efforts may lead, and he may be making an important contribution to the overall body of traffic analytic knowledge.

[redacted]

P.L. 86-36

How Many Angels Can Stand on the Head of a Case Notation?

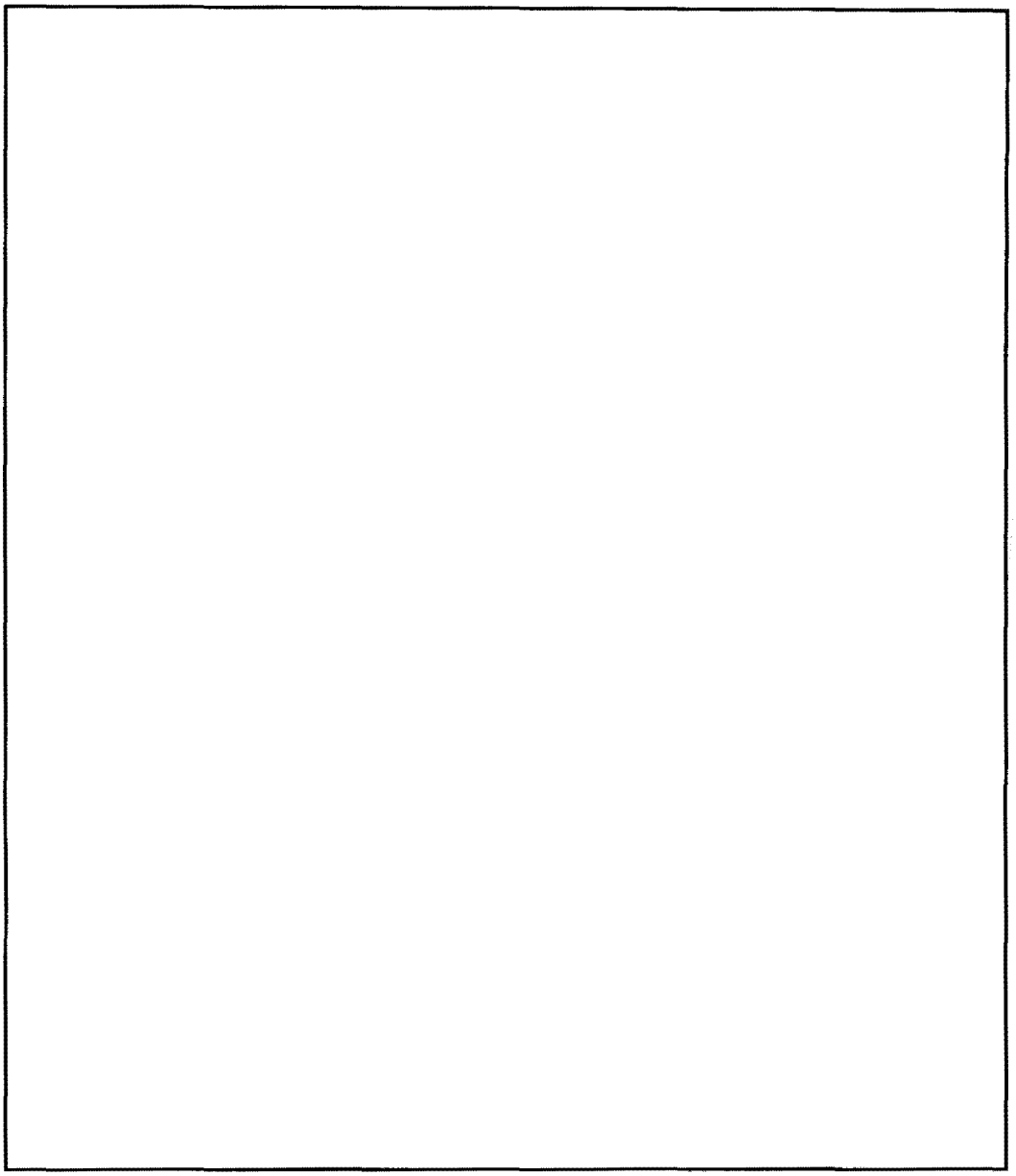
P.L. 86-36

[redacted]

~~(S-CCO)~~ Most persons can recognize a case notation as such, even though formats differ. Few can *explain* one unless it is one worked with daily. This is because notations contain over fifty categories of information, and each of these has sub-items ranging from four or five up to about 800. In short, there must be over two thousand coded meanings. How can this happen? In addition to the unstandardized [redacted] P.L. 86-36 [redacted] notations, the digits of the so-called "serial" are actually used as codes, singly or in combination, for the various categories shown below. Sometimes a given digit may have two meanings within a given notation. Also, the information selected for representation varies from target to target, from trigraphic source to trigraphic source, and even within the latter. E.O. 1.4.(c)

Some of the Information Contained in Case Notations

[redacted]



The 1980s and Beyond

Traffic Analysis: A Current Perspective

CW2 JAMES HOPPER, USAFS

P.L. 86-36
E.O. 1.4. (c)

~~(C)~~ Traffic analysis (TA) today is beset by a variety of problems affecting the analyst, not the least of which is a lack of understanding concerning the separate functions which comprise traffic analysis. Contrary to popular definition, the traffic analysis field of today encompasses much more than the mere analysis of communications externals. Traffic analysis consists of six separate functions:

- Collection Management
- Collection Support
- Processing
- Analysis
- Reporting
- Evaluation

These are intended to be mutually supportive of each other. However, because both managers and analysts lack understanding of the interrelationship that exists between and among these functions, they all too often are performed at cross purposes, with one function inadvertently affecting the success (or failure) in a follow-on activity. In these days of meager collection and analytic resources, it is imperative that an understanding of the relationship bonding the six functions of traffic analysis be fostered at all levels to ensure the complete and proper use of these resources.

~~(C)~~ To function effectively in the traffic analysis world of today, the traffic analyst must have a rudimentary knowledge of several areas in addition to communications externals. Among these areas are

Collection Management, including the Collection Objective Performance Evaluation Systems (COPES) and its follow-on, Collection Evaluation System (CES) statistical reporting;

Collection Support, including knowledge of working aids available to assist in collection and identification duties, as well as of target characteristics that can support both current and future collection operations;

Processing, including Automated Data Processing (ADP) routines available to assist in manipulating the intercepted data for subsequent analysis;

Analysis, including sufficient knowledge of the various traffic analysis techniques and target characteristics that develop information to satisfy consumer requirements;

Reporting, including the criteria and appropriate reporting vehicle for providing information to satisfy consumer requirements;

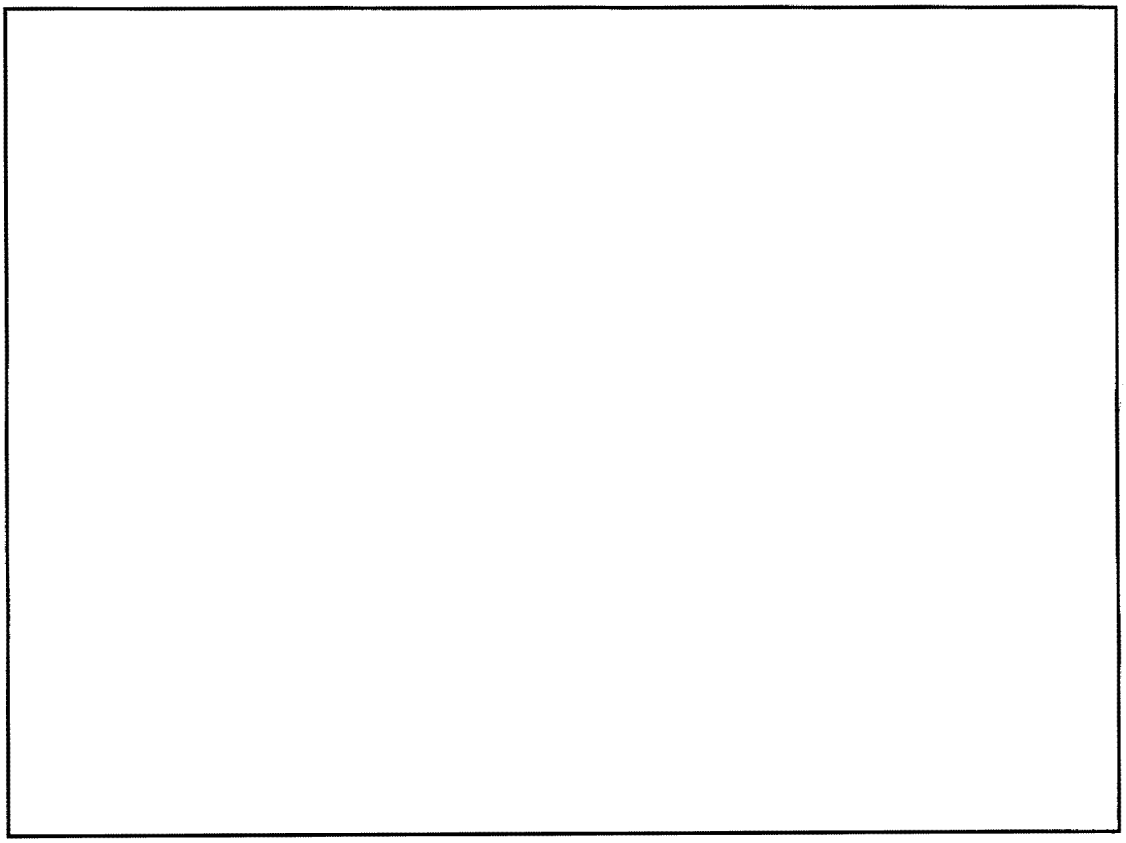
Evaluation, including the techniques available to constantly monitor and compare tasked and acquired collection so as to redirect these resources to areas of the target's communications that are susceptible to exploitation; and

Perspective, including a thorough knowledge of the target's order-of-battle (OB) structure that underlies the target's communications, as well as a thorough understanding of the target's past history from which to view changes in the target's communication habits.

A lack of knowledge in any one of these areas can ensure failure in attaining the ultimate goal of consumer satisfaction. Additionally, an incorrect managerial emphasis on any one function over another will also ensure failure in attaining this ultimate goal.

COLLECTION MANAGEMENT

(U) The first function to be encountered by the traffic analyst is Collection Management. It is at this point that the consumer's requirement is translated into specific collection tasking to acquire the needed information.



P.L. 86-36
E.O. 1.4.(c)

[redacted]

COLLECTION SUPPORT

Once the tasking is accurately developed and transmitted to the field site, the next function, collection support, determines the success or failure of a field element in satisfying its tasked requirements.

P.L. 86-36
EO 1.4.(c)

[redacted]

(U) At the local level, field site managers usually are faced with a decision of where to use their most talented personnel; an effective collection support element or an effective analysis and reporting effort. Unfortunately, all too often the choice is for the A & R effort because of the high visibility of analytic breakthroughs and consistent product reporting.

(U) This decision on the part of the field manager leaves the collection support effort with poorly trained analysts, generally those with the least experience in TA duties. These individuals are then placed in the fast-paced environment of the collection floor, an environment that breeds confusion and is the least likely place to learn the functions of traffic analysis.

(U) In addition to the assignment of poorly training personnel at the local level, at the national headquarters level technical support material is seldom provided in a manner that facilitates its use in the field. Most often this material is seldom provided in a bulk manner, which dictates tedious manipulation in the field to extract desired information. Yet this same manipulation is often performed with the national headquarters on a daily basis through various computer routines but is not made available to field sites. Thus, while a steady and voluminous stream of technical support material is provided to the field element, it is seldom provided so that the field can easily use it, and it is often too unwieldy to be used on the collection floor, with all its hectic activity.

[redacted]

Of these, the misidentification rate should be of the greatest concern since it dramatically impacts on the processing, analysis, reporting, and evaluation functions that follow the collection support function. A poor case (notation) identification rate in the collection support function means that all case identifications received for processing must be verified to ensure that the correct notation is applied, a time-consuming process for an individual already strapped for time in performing his or her other processing duties. Failure to verify the correct identification on all cases can have disastrous effects

- on processing, necessitating complete revisions of case history records;
- on analysis, which attributes incorrect technical operating characteristics to the wrong case;
- on reporting, which provides false information to the consumer; and
- on evaluation, which attributes tasking satisfaction to the wrong target.

To ensure the most effective collection support effort possible, field managers must develop an operational system that exposes all elements of the assigned analytical work force to both collection support duties and desk analysis duties. Ideally, such a system, which rotates the individuals between these two worlds, will ultimately increase the expertise levels available in both areas. Likewise, at the national level all methods of developing collection support material for field elements must be closely scrutinized to ensure that a minimum of manipulation is required on site to use the data.

PROCESSING

~~(C)~~ The next function of traffic analysis, processing, often assumes a life of its own. From the analyst's standpoint, processing (or, to use a more common term, "logging") quickly becomes associated with drudgery. The fact that processing is accomplished merely in order to organize intercepted data for subsequent analysis is quickly forgotten. Processing then becomes a mindless transfer of data from one medium, the raw intercept, to another medium, the casebook or database. Further, this attitude quickly leads to overlooked items of significance that otherwise would require immediate analytic or reporting attention.

(U) From the manager's standpoint, however, processing quickly becomes the key productivity measurement because of the statistical data available from database maintenance inputs. Since the underlying desire is for an accurate database from which to extract material for subsequent analysis, and from which to drive any automatic collection support vehicles that emanate from the database, the manager's concern becomes one of concern over database maintenance accuracy and volume. Unfortunately, this concern for accuracy normally translates into a concern over the correct formatting of the input rather than over the validity of the information itself. Likewise, the volume concern translates into a meaningless "body count" that is used to spur further productivity.

P.L.86-36
E.O. 1.4.(c)(c)

poses should be deleted from existing requirements. For example, the processing of voluminous message serialization data should not be imposed on the affected analyst if no one intends to perform a study of this aspect of the target's communications. The processing requirements should be continually geared to the voids of the target's communications that need to be exploited, and not to those characteristics that are commonplace and seldom change, as these voids are reduced through exploitation.

ANALYSIS

[redacted] underlying military force must be the first priority of the traffic analyst. Only through such mastery can an analyst understand the communications facing him or detect changes in those communications that can be attributed to something reportable. In addition to ensuring that the analysts are knowledgeable of the structure of the military force, managers at all levels must ensure that the analytic studies to be undertaken first have the potential of either satisfying established reporting criteria or developing material that will aid collection support activities. All other studies, no matter how well-intentioned, are merely a waste of an analyst's valuable time.

P.L. 86-36
E.O. 1.4.(c)(c)

REPORTING

(U) The reporting function is the sum total of how well the earlier functions were conducted. If these earlier functions were conducted in a shoddy manner, they normally will culminate in an inaccurate report that bears little relationship to the consumer's initial stated requirement. Conversely, if these earlier functions were conducted in an orderly manner so that each function supported the following one, the report will probably satisfy the consumer's request. In addition to satisfying the consumer's request, the analyst must also concern himself or herself about using the proper format for the information to be used in the report. Poorly formatted reports, while factually correct, convey a sense of disorganization that can color the credibility placed on the information by the recipient.

[redacted]

(U) Both of these rationalizations have effectively downgraded the opportunities available to the traffic analyst to participate in the reporting function, the only function which at present is directly keyed to reporting criteria that match the consumers' requirements. By reducing the analysts' participation in this function, we also reduce their ability to ensure that the previous functions remain directed towards the ultimate

goal of consumer satisfaction. Managers at all levels must emphasize the development and maintenance of effective and imaginative reporting programs that challenge the analysts' skills to ensure that that reporting function does not become divorced from all that has preceded it.

EVALUATION

[redacted]

P.L. 86-36
EO 1.4.(c)

(U) Through their involvement in the evaluation process, traffic analysts are well placed to redirect collection resources to exploitable areas - or at least to areas that have not been satisfied through past intercept - of the target's communications. Unfortunately, the evaluation process is normally either not performed at all, or it keys on indicators that, when viewed alone, fail to provide an accurate reflection of the productivity of the resource.

[redacted]

(U) As should be apparent, the traffic analyst of today is faced with a variety of functions. However, all of these functions are tied together by a thread of continuity relating to the final goal of consumer satisfaction. If these functions are not kept in their proper relationship to each other, either through analyst neglect or improper managerial emphasis, it will be difficult - if not impossible - to achieve a cohesive operational mission

that satisfies consumer requirements. Only through mutually supporting functions, as originally envisioned, can our scarce collection and analytic resources be used to their fullest extent. In other words, perhaps a return to the basics may be in order for the traffic analyst of today!

There's a New World Coming - Are You Ready?

P.L. 86-36

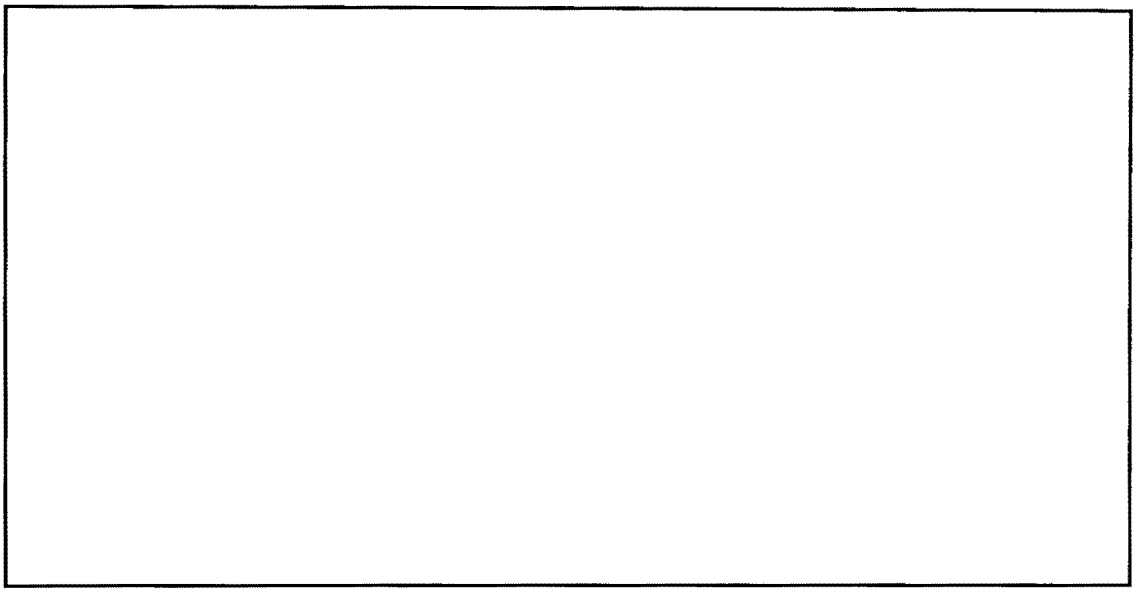
[redacted]

P.L. 86-36
EO 1.4.(c)

(U) Analyst response to a changing environment is an area that has piqued my interest for a number of years. This interest has become especially pronounced in the last four or five years, largely as the result of the increase in the variety and number of automated processes that have become available, my involvement in a number of long-term research projects, and the prospects of newer and more sophisticated machine-based analytic techniques. As a consequence, I have given much thought to the effects that this increased automation will have on the analyst and to what we, as an organization, can do to respond to the challenges and opportunities that will arise.

(U) If we are to accurately assess how the analyst of the future will react to the increased automation of the analytic process, it is necessary to know the analyst of today. This is logical, since the majority of tomorrow's analysts are already on board and active in the analytic field. It also becomes essential to define the functions of the analyst since all personnel who carry the title "analyst" are not analysts by the strictest definition of the word. For convenience and easy reference, I have divided these "analysts" into three categories that I've labeled, for lack of any better terms, "loggers," "case analysts" and "research analysts."

[redacted]



(U) The changes expected as we become more and more automated will alter the methods and procedures currently used in the analytic areas. This will have a profound effect on our operations, but to an even greater extent it will modify the lifestyle and environment of each of the three types of analysts I've defined. Each will be affected in a different way depending on the analyst's perception of analysis, his personality and his ability to adapt.

(U) Once the machine takes over the simple data manipulation and recording functions, the "logger" will become, to a great extent, obsolete. His routine will be upset and his workaday world completely disrupted. He will no longer have his logging to fill his day. He won't know what to do and he'll be completely lost. For those currently having trouble isolating the "loggers" in their outfits, they'll then be very easy to spot. Just look for those people sitting with a blank stare on their faces and for those making nervous movements at their desks as they anxiously try to find something to do. Eventually their names will appear on the list of those who are abusing their sick leave. The real "logger" will never recover from automation. He's lost his place in life. His day-to-day world will have been destroyed, and he simply won't know what to do. For many it will be too late to start over. Others will lack the initiative, while for still others, it's nothing more than a lack of talent. The world will have passed them by. They, of course, will not be to blame. It'll be the machines' fault, or management's fault, or maybe just the breaks of the game.

(U) In reality, the "logger" has always been a clerk with a professional job title and a professional paycheck. He was created by the system, and, with the advent of new automated techniques, will be destroyed by the system. Some will be salvaged. Some "loggers" will regroup, retrain and regain a place, perhaps at the "case analyst" level. Those that can't make the transition will have to be purged since the cost of automated systems will call for a decrease in personnel expenditures.

(U) The "case analyst" will survive and thrive in the new automation. He really never did care for the logging and data maintenance functions associated with his job; therefore, he'll adjust. He'll reorder his priorities and use the additional time now available for the development and analysis that he never could quite get around to under the old semiautomated method of operation. His productivity will increase, and more technical data on his targets will result. The ultimate gain will be the production of more intelligence information in satisfaction of our requirements. The "case analyst" will grow as a professional, honing his skills as he practices his trade, and in many instances will develop into a "research analyst."

(U) The "research analyst" will see few changes in his method of operation as a result of this new automation. He'll have to deal with new databases, new retrieval programs and new equipment, but his daily routine will remain pretty much the same as it is now. He will generally review the same types and amounts of material and work on the same types of projects. He should see some improvements in accuracy and completeness as a result of the elimination of the "logger" and the automation and resultant upgrade of the databases. He will be able to spend less time on the verification and data gathering phases of his assigned tasks and thereby be able to complete more assignments in a shorter time. This will allow a more efficient use of the limited number of "case analysts" and permit us to achieve maximum benefit from their talents. Automation will also improve the morale of the "research analyst" since he will be able to function almost entirely in his primary capacity.

(U) The benefit of this increased automation is readily apparent. The talent of our people can be used to the fullest, with dull, repetitive tasks reduced or eliminated. The timeliness, accuracy and quality of our product will increase. Personnel not working at their prescribed levels can be eliminated, with a resultant savings of money. All of this is, of course, predicated on manageable machine systems that will function as designed. Since our track record for the development of such systems is not impressive, let's hope that we have learned from experience, and not attempt to reap benefits before we have proven follow-on systems.

In Pursuit of: Faster Horses, Younger Women, Older Whiskey, and More Money

P.L. 86-36

[redacted]

(U) For the past two years I have been involved with a project that has given me more in terms of psychic income and pure excitement than perhaps any work-related activity that I remember. When you feel this good about something, it seems natural to want to tell everyone else and share the excitement. It's sort of a "look what I found" feeling. Of course, when you feel excited about something, it is difficult to know whether you have something worth saying and can remain objective about it. Nothing makes you feel quite as foolish as discovering the wheel only to find out that you were the only one who didn't have one all along.

(U) I've followed – from a distance – the articles, letters, and symposia decrying the diminishing number of analysts, the dilution of the career field, and the increasing work load. I really have nothing to add to the body of literature that has grown around those themes. I would like to note that some reasonably intelligent people have advanced them. Conversely, some reasonably intelligent people made the decisions that led to the described conditions.

(U) Having resisted the urge to vent my excitement on paper for this long, I thought I had it under control. Actually, I have been writing this piece all along. Part of my control mechanism was simply typing my thoughts on the screen and then hitting the delete button. That may happen to this version, and you will be spared once again. I'll tell you what "set me off" this time a bit later. First, let me tell you what I've been so enamored with.

(U) I'm a traffic analyst. Several years ago I began to work for the person I respect most in that field and share in the development of what has come to be called a Traffic Analysis Workbench System. Whatever comes of that effort, I'll always be grateful for being included.

~~(FOUO)~~ The idea is a relatively simple one: In terms of technology, the TA field is, and has always been, behind the power curve. Regardless of what high-powered machines exist, and in spite of the fact that some extremely sophisticated machine applications have been designed for analytic purposes, the analyst is still behind. There are several reasons this situation exists. However, it is primarily because analysts are directly dependent upon their machine support personnel. A few have managed (mostly out of frustration) to learn one computer system or another and support themselves. The problem with this is, if they were any good at it, they were usually lost from the field.

~~(C)~~ It's time the analyst was given some help–not to catch up to technology, just to keep from getting further behind. Given the costing cycle, the procurement cycle, and the installation cycle, I'm convinced that catching up is not possible. *Not possible*! The concept of a TA workbench involves installing a terminal on the analyst's desk. Read that again! *On the analyst's desk*. Not down the hall in a "machine room," not in a corner of the basement, and not around the corner where it "won't bother anyone" – *on the analyst's desk, the one he sits at.*

[redacted]

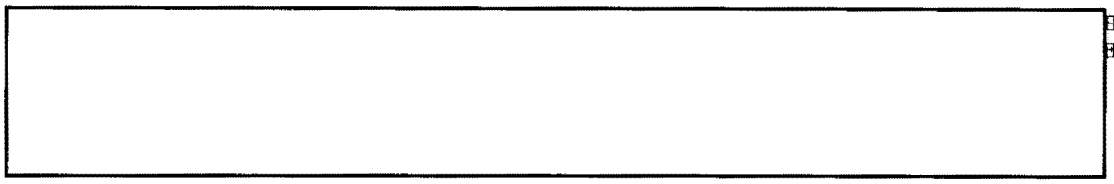
This puts the analyst in a position to access the major databases, where the daily traffic, as well as the technical working aids, resides (hides is a better word). With the terminals on their desks, analysts will have constant access to their material and perhaps approach the paperless environment.

~~(FOUO)~~ Under the umbrella called PINSETTER, we have been proceeding along a development path that will hopefully lead to the kind of help the analyst needs. Because the most precious computer resource is the programmer, the analyst must be released from depending on him for every minor need. This is true for several reasons. First, the analyst needs to be able to access his data, process that data, and change those processes without having to write memos, generate specifications, write justifications, wait for software and then participate in debugging. Second, the programmer as a resource is too valuable to be tied up with changing sort specifications every time an analyst needs a different output. Last, the plain facts are that we have a terrible time retaining good programmers. No sooner do we develop a good working relationship with a top-notch programmer than he begins to understand something about an analyst's job; then along comes a better offer and he's gone.

(U) From a machine standpoint, meeting these goals requires a system that is easy to learn, flexible, and provides a reasonable response time. By "reasonable" I don't mean instantaneous. Most analysts can live with an execution time that is not measured in nanoseconds. Most of our work has taken place on a PDP-11/70 host using UNIX as the operating system. UNIX is a high-level language that was developed by Bell Laboratories. It meets the above criteria, and it is very forgiving to a klutz at the wheel.

~~(C)~~ We have found that most of the processes that a traffic analyst needs to be able to do can be accommodated with the UNIX package. Where it was found lacking or inefficient, the solution has been provided by a unique working relationship with a small group of highly talented programmers in T333.

[redacted]



(U) To digress for a moment, the realization that certain processes are simply too big for TSS applications is important to maintaining a proper perspective. This determination must be made, and large "number crunching" must be performed where the processes are most efficiently handled. However, the process can often be executed where most efficient and the results passed to where they can be best used, on the TSS. I might add, in two years of handling TA processing, it has been necessary to "send out" only one job for actual execution on a "big" machine. Of course, many of our extracts from major databases are "preprocessed," prior to transfer, to make them more TSS friendly. But I discount this, since it is largely "invisible" to the requester.

~~(FOUO)~~ If the solution were apt to provide a useful " UNIX-extension," we would request T333 help. The results have been the most rewarding part of this experience: generalized UNIX-like utilities that solve analytic processing problems. The big plus? *Anyone* who knows a little UNIX can use them. On the other hand, if the solution appeared to be problem specific, we would attack the problem with our own resources. The results of these efforts have proven equally rewarding. Based on our own experience and some operational testing in analytic elements of A3, B2, B5, G6, and G9, I'm not sure if a more effective analytic tool than UNIX could have been designed if that had been Bell's intent. This leads to a philosophical difference in user support design.

~~(FOUO)~~ There is a mask-and-menu school of thought that holds to the belief that the user should be led through the processing cycle by the software. A menu is presented with a few options to select from and a mask provided through which to make alterations. These M&Ms believe it is best to protect the user from the complexities of the system and protect the system from the klutz at the wheel. It has a place. I would look to this area for the type of handling necessary for, perhaps, TEXTA updates.

(U) Another approach is to provide the user with the modules necessary to manipulate the data, a high-level language to package the modules, and the ability to communicate with other users and peripherals such as high-quality printers: basically, a sort of Procedural Applications Language that is not unique to traffic analysis. Perhaps a Universal Procedural Applications Language approach. The user is free to design personal processes and, more importantly, *change* those processes at will. Users are not dependent upon the programmer for every minor modification, routines do not have to be recompiled after each change, and the results of the changes are immediate. I believe UNIX meets this challenge.

(U) The M&M approach keeps the analyst (or user) dependent upon the programmer for modifications, thus preserving the problem of too much demand being placed on a resource that is already overtaxed. The solution to the demand for software packages has

all too often been the letting of contracting, at considerable expense, to develop processes that a few analysts, skilled in a handler like UNIX, might be able to get along without.

(U) If our own resources were concentrated in a manner conducive to the development of generalized handlers (a Universal Procedural Applications Language), and perhaps a bit of that contract money concentrated into rewarding the good programmers we have left, we might be able to come up with better analysts and better programmers. As a by-product, we might be able to handle the workload with the number of analysts we have and do a better job of it.

(U) So, what was it that set me off this time? A few days ago, while demonstrating a few system capabilities to a potential user, I was walking through the steps of a UNIX shell file (merely a collection of UNIX commands that execute sequentially and perform some process) and he asked me if I "wrote this program." The words startled me. Wrote a "program"? Me? I'm a traffic analyst, I can't "program." My rather bumbling answer was something to the effect that this is really not a program, just a collection of instructions to perform a certain process on this computer. After he left I put the shell on the screen and read it a few times. By gosh, a few years ago I would have called that mess a program myself. It "looks" like a program. It "acts" like a program. And my extemporaneous answer wasn't too bad a definition of a program.

~~(C-CCO)~~ I had to pause and reflect a bit. I put that shell together in about five minutes. What does it do?

[redacted]

Based on past experience in trying to get a process to do a select of this nature, and going through the "channels" to get it, this "quickie" shell seems fairly powerful.

[redacted]

(U) I think I've found a faster horse, I probably couldn't keep up with younger women anyway, and I'd rather have a cold beer than older whiskey, so if anyone knows someone looking for a "programmer," I'll settle for two of four.

Computerizing Traffic Analysis (U)

[redacted] P.L. 86-36

This paper was presented at the November 1982 meeting of CISI.

The traffic analyst finds himself turning to data systems because he often has mountains of data to examine, because the people who receive TA results usually want their information very rapidly, and because almost all the data the traffic analyst wants to see are already inside a computer somewhere.

(U) Most traffic analysts who try to look at data systems develop a kind of schizophrenia. On the one hand, the TA data that come in today have to be processed and analyzed today because there will be another batch of data coming in tomorrow. This means that the traffic analyst has to use today's data system to handle today's data. On the other hand, it does seem to us traffic analysts that data systems people would much rather talk about tomorrow's system – the one that isn't here yet, the one that won't have all these glitches and problems that today's system has.

(U) The traffic analyst who is in the trenches on a current operational problem would easily trade all the glowing promises of some brighter tomorrow for a quick fix on some of the glitches in today's system that will keep him from bleeding to death right now. That isn't my subject today - I really want to talk about the future. But as I thought about standing up here in front of all you data systems people, I couldn't resist putting in a plug for the working traffic analyst; he needs your help, both today *and* tomorrow.

THE PROLOGUE IS PAST

(U) I might be well to begin with a little history, or at least history as I remember it. My first recollection of what we now call data systems was a lot of eighty-column cards and a card sorter. That was about thirty-five years ago. Watching those cards go through that sorter was rather hypnotic. The possibilities seemed limitless then - if we could only find a cheap and easy way to get the data onto the cards. I think the equipment was called Electronic Accounting Machines (EAM), and the people who supported the traffic analysts were called Methods Analysts (in the 1940s and early 50s).

(U) Since our data consisted of a matrix with eighty columns and many rows (one row for each card), our output consisted of that same matrix with its columns and rows transposed in some way. Later, we added the ability to look up words or strings in a dictionary and insert the result back into the matrix.

(U) Many years and computer systems later, in the mid-1960s, this was still the primary data systems support to traffic analysts: a transposed matrix (now often wider

than eighty columns) with a dictionary lookup. There were attempts to go beyond this. Most of the things we tried were made to fit one specific problem and never developed into general TA tools. We developed ponderous, monolithic record formats whose structure provided a special place for each variety of data we thought we would find in the traffic. What I remember most vividly are long, soporific meetings where all we ever seemed to talk about was what *format* the data were going to be in. We spent untold amounts of energy and resources getting all of our data *into* these unyielding, user-murky systems, and there were often little energy and resources left over to develop any user-friendly *output*.

(U) The result of this, in many areas, was that the output received by the traffic analyst was not much more than his original raw traffic, transposed both horizontally and vertically, and with some information added through dictionary lookup processes.

A LONG THIN MATRIX

The form in which the output was delivered to the analyst was often decreed by someone remote from the analyst - someone who never had to actually live with the output - and it was rarely if ever changed to fit the current needs of the local problem or individual analyst.

(U) It is still possible, even today, to see analysts sitting down with computer output and handlogging data from that computer output onto a form for their own personal use. In at least two areas, one might then see that same handwritten log being used a little later to punch cards for further computer processing!

WHAT IS THE TRAFFIC ANALYST TRYING TO DO?

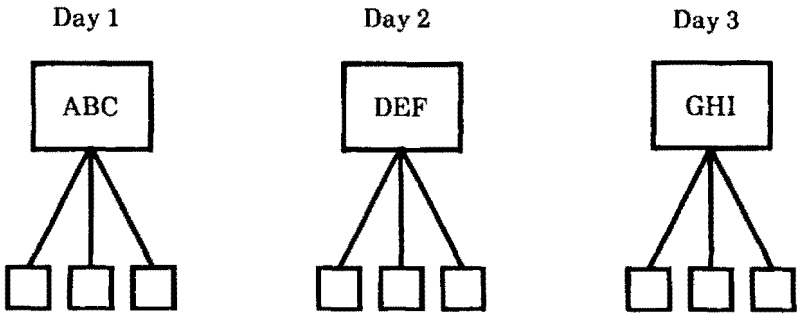
(U) The traffic analyst is trying to draw a picture of his communications target. He usually wants this picture to show how his target looks when it is operating normally. Once he knows what his target's normal behavior is, then he is in a position to detect variations, and report them to intelligence consumers.

CONTINUITY

(U) Traffic analysts are usually looking for something they call continuity. When faced with a target that has daily-changing callsigns, the traffic analyst seeks to learn which of today's callsigns matches what callsign used yesterday.

If I can say that the station that used callsign ABC on the first day is the same station that used callsign DEF on the second, then I can say that DEF (on the 2nd day) is continuity of ABC (on the 1st). On the third day, if I can say that GHI was used by that

same station, then I can add GHI (on day 3) as another link in a growing chain of continuity. Many of our TA targets do change their callsigns, frequencies, addresses, and other features on a regular basis. They do it to make collection and identification more difficult, and it is the job of the traffic analyst to defeat these changes by the development of continuity.



CONTINUITY

Date:	1	2	3	4
STN 1:	ABC	DEF	GHI	...
STN 2:	...	...		
...	...			

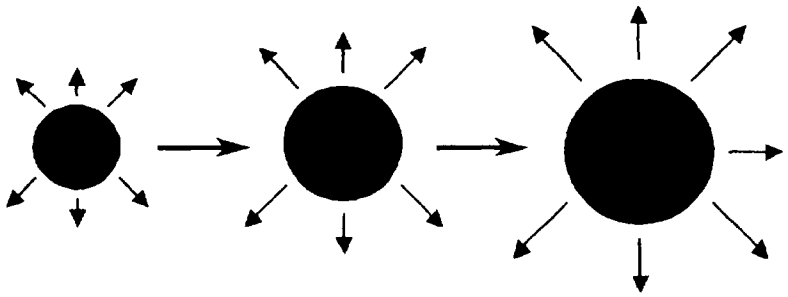
TWO KINDS OF TRAFFIC ANALYSIS

(U) There are two forms of traffic analysis on most problems: development and maintenance. To borrow an example from cryptanalysis, the attack against a cipher system often goes through two phases:

- first, diagnosing and recovering of the general cipher system, and
- second, exploiting and processing the recovered system, which often involves solving daily keys or settings.

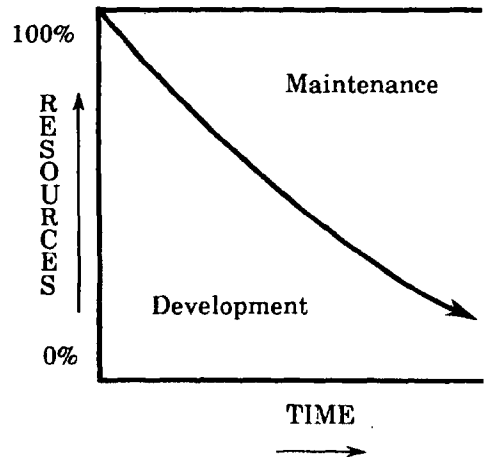
So too, in traffic analysis, one can consider that there is a development (or recovery) phase and a maintenance (or exploitation) phase, which may or may not include product reporting. However, in traffic analysis, the two phases often occur at the same time.

(U) In some ways, the traffic analysis process resembles a spreading oil blot. Out on the edges, new target territory is being conquered; new target communications structures are being discovered and cataloged; new methods of identifying and distinguishing various communications are being developed. But back in the central part of the oil blot, the territories previously conquered must be kept track of; the continuity of target communications structures previously recovered must be maintained.



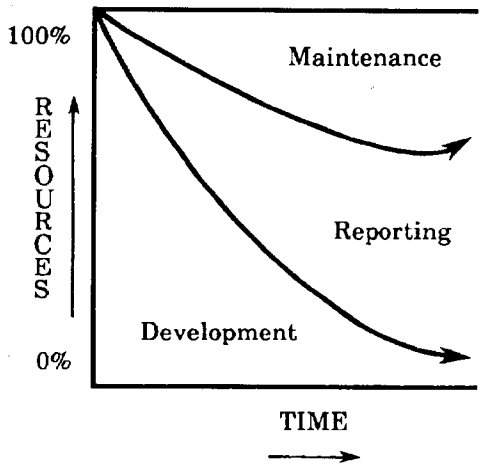
Recovery – outer edges
Maintenance – center

Oil Blot



(U) The more territory one conquers, the thinner the center of the oil blot becomes. The more communications structures one recovers, the more continuities there are that now must be kept track of. As the maintenance effort grows, it will use more of the available resources, draining them away from the recovery part of the effort, and at some point it will have absorbed enough of the resources so that a point of "no growth" is reached and, for all practical purposes, recovery of new structures stops. If expansion doesn't stop, the center of the oil blot will break; if development doesn't stop, the maintenance effort will fall behind and begin to lose track of continuities, which will then have to be discovered and developed all over again. This tension over resources between maintenance and development is similar to the one between software maintenance and software development.

(U) Sometimes the personality of the manager plays a part in just where this point of "no growth" takes place. Some managers are more at home in the settled, stable atmosphere of the center, where things don't change much from day to day. These



managers tend to concentrate their attention on building a smooth-running system at the center, and may put a larger proportion of their resources into that area, so that the "no growth" point is reached more quickly. Other managers thrive in the rough and tumble frontier atmosphere out on the edges of the problem, where each day is likely to bring some new and different challenge. These managers tend to concentrate their attention on the recovery effort, sometimes at the expense of the more humdrum maintenance.

REPORTING

(U) Some traffic analysis problems have a lot of potential for reporting - for providing the intelligence consumer with a blow-by-blow account of what the target is going. Targets that involve ships and aircraft often have this potential because they move around from place to place, and the analysts often find much of their time taken up with reporting which ships and aircraft were active today, in what areas and performing what missions. Where this reporting potential is high, it tends to draw off resources from both development and maintenance. Managers whose problems have a strong reporting emphasis (especially time-sensitive reporting) will generally try to pull resources from development rather than from maintenance, because losing the continuities means losing the raw material for the reporting effort. Losing the development effort is generally seen as the lesser of two evils.

(U) As an aside, I should say here that the reporting side of traffic analysis is generally well ahead of the technical side in the use of computers. Since my primary interest in this paper is the working-level traffic analyst, I will be concentrating on the technical side, and I do not propose to discuss the reporting aspects of TA except as they touch on the technical side.

(U) From the standpoint of the two kinds of traffic analysis - development and maintenance - we can express the general goals in the following ways:

TA DEVELOPMENT GOALS

(U) We rarely collect or analyze all of the communications of any given target. We are almost always working on a sample of the target. At any given time, there is some residue of the target that we do not maintain continuity on, and bits and pieces of that residue find their way into our unidentified or search pile - the file of incoming traffic that looks as if it belongs to our target but doesn't exactly fit any of our known continuities. Development TA concentrates on that pile, trying to dig out new target nets and continuities. This unidentified pile is almost like "background noise": it is always there, whether we talk about it or not. If we are still growing (if the oil blot is still expanding), then our development goal is to dig more of the target out of the unidentified pile. If we have reached the "no growth" point, then our development goal is to be able to recognize and develop any new communications that the target might put on the air - communications that ought to stand out against the "normal noise" in the unidentified pile.

TA MAINTENANCE GOALS

(U) During the maintenance phase, we want to be able to hang on to the continuity that we have already recovered. We want to do this

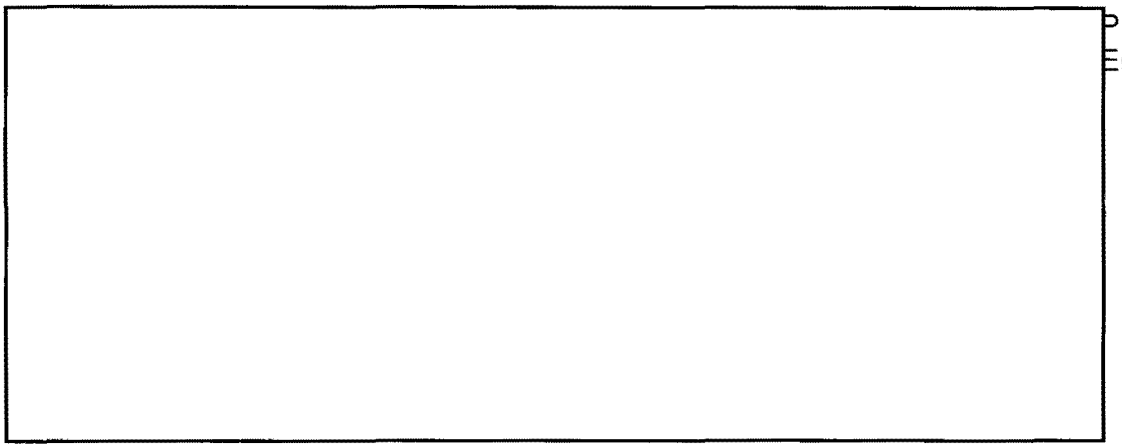
- to support whatever analysis efforts are currently engaged on the target (such as cryptanalysis, language, reporting, etc.), and
- to support whatever collection effort is working against the target.

(U) To do the first support requirement properly, we need to be able to correctly distinguish and identify each of our continuities as the traffic arrives at the point of analysis, i.e., *after* it has been collected. However, to do the second support requirement properly, we need to be able to tell the collector *before* he collects the target, what the target is going to look like and what the target is likely to do. If we can tell the collector what callsigns the target will use, what frequency he will use, what time of the day he will come up, and what he is likely to do when he does come up, then we have satisfied our goals for maintenance traffic analysis. On some problems, we are fortunate in being able to do this on a regular basis. On others, we spend the first few hours of the day (or callsign period) scurrying about to recover new keys and then, for the remainder of the day (or period), we can project what the collector will encounter in the way of callsigns, etc.

HOW CAN COMPUTER POWER BE APPLIED TO THE TA PROBLEM?

~~(S-CCO)~~ In order to consider how the power of the modern computer might be applied to traffic analysis, we need to look at the model of TA that emerges from these two phases: development TA and maintenance TA. Although I have described them as if they were distinct and separate, they really ought to be thought of as a conjugate pair, because they tend to occur together on most problems. It is also possible for certain problems to be best

described as a hybrid of these two forms: during the war in Vietnam, one out of every three pieces of intercepted traffic was unidentified, largely because of the rapidly changing nature of the target. The point I want to leave with you today is that any attempt to provide the traffic analyst, either here in this building or anywhere in the world, with a Traffic Analysis Workbench System must reckon with the fact that the problem he is working will always be some mixture of these two forms of traffic analysis. We also need to consider that a TA problem can quickly change from one form to the other.



P.L. 86-36
E.O. 1.4.(c)

~~(C)~~ We decided to see if we couldn't find a way for computers to help us with the more stable maintenance problem. I remember spending several weeks laying out the logic and processes on the problem. And I remember being told, at the end of the project, that there wasn't nearly enough memory available to do what I needed.

	MAINTENANCE	DEVELOPMENT
Problem type:	slowly changing	rapidly changing
	bookkeeping	pattern searching
	"Anything changed?"	What's new?"
How dynamic?	slowly changing	rapidly changing
Foreknowledge:	high	low
State of solution	solved	unsolved
Control:	semiautomatic	hands-on
Interaction:	human-efficient	human-intensive
Techniques:	target specific	human specific
	knowledge-based?	"mix-n-match"
Worst case:	"below the salt"	start from scratch

A COMPARISON OF TWO FORMS OF TA

(U) Let's look at these two forms of TA a little more closely. How do they compare when we look at them from the viewpoint of providing today's (and tomorrow's) traffic

analyst with a computer support tool kit, while using a terminal workstation in an NSA worldwide networking environment?

(U) In development TA (the garrison communications in our example), we have a bookkeeping problem,

- where the emphasis is clearly on keeping track of a lot of known continuities;
- where we expect the changes in the target characteristics to be relatively modest;
- where the technical means of keeping up with the target (i.e., callsign and frequency systems, address tables, etc.) are largely solved or understood; and
- where we have good prospects of being able to project the appearance and behavior of the target from day to day.

(U) In development TA (the training communications in our example), we have a pattern-searching problem,

- where the emphasis is on sifting through masses of low-yield ore, looking for something that forms a continuity;
- where the next success may look nothing like the last one; and
- where the chances of finding that needle in the haystack may depend as much on the personality of the searcher as on the content of the haystack.

If we can't *keep* continuities (i.e., are not *able* to), then the target stays in the development phase, no matter how much we know about it. Someone once said that TA continuities take either 95 percent of our resources or 5 percent. That number may not be right, but the idea is. Being able to keep track of the continuities is the key to whether the problem is development or maintenance in nature. A daily-changing callsign system *looks* to us as if it is rapidly changing if we haven't solved the system, but once the system is solved, we then perceive it to be slowly changing. It is a matter of viewpoint.

(U) In maintenance TA, we work largely with what the target gives us. A package of techniques to grapple with a callsign system may work well enough on a problem where the callsigns are the key to our keeping track of continuity, but may be almost useless on another problem where the callsign system isn't solved and we must rely on other things, such as serial numbers or addresses.

(U) In development TA, on the other hand, a particular technique may pull one new structure out of the search pile and then never again find anything. The development analyst may need to continually devise new attacks and new methods; to him, the search pile is a featureless mass, and it is his job to sort out the various pieces and find ways to distinguish one piece from another with some reliability.

(U) The maintenance TA problem probably needs a package that will

- look over the incoming material for the day;

- make reasonable guesses about continuities (including garbles);
- flash a warning light at the traffic analyst when things look *very* wrong or when it is confused by something; and
- provide a clean and readable summary of its results to the analyst for review.

It ought to keep up with both short-term and long-term trends, and should be especially attentive about "missing persons," portions of the target which haven't been seen for a while.

(U) The development TA problem, on the other hand, needs a tool kit that will provide the analyst with a range of diagnostic, computational, and pattern-searching techniques that can be brought to bear on the problem, in whatever mix the analyst needs at the moment.

WORST CASE

(U) I have shown what might be called the "worst case" for each of these forms of traffic analysis.

(U) In maintenance TA, one sometimes finds that a problem must somehow be worked, but that it has no real resources and not enough clout to get any. Now, in the best of all worlds, where everything is done right and for the right reasons, such problems should not exist. If a problem is worth working on at all, it is worth the resources needed to get the job done. However, in the real world, those problems that are "below the salt" will be working with whatever support they can beg, borrow, or scrounge. Proving a general package for such problems would pay for itself a hundredfold in the first few years. At the minimum, the package needs to be able to "ring an alarm bell" when the target starts to disappear, or becomes more active, or changes in some other way.

~~(S-CCO)~~ In development TA, the worst case might be the situation where nothing is known. That is not as uncommon as some people might think. [redacted] P.L. 86-36 E.O. 1.4.(c)(c) When we pull together an analysis effort for a sudden war or brushfire, the analysts are usually drawn from other problems around the building; it would be nice if they didn't have to add "learning a new system" to all the other problems they will face on the new target. Therefore, the tool kit for such situations must be quite general and all-purpose.

TWO SYSTEMS OR ONE?

(U) What I have been describing so far may sound like two different systems, but what I am proposing is one system, with two parts. I have already said that these two phases or aspects of TA occur together, and I should add that on more than one problem, they are frequently done by the same people. New continuities are recovered by the development

TA process, and then handed over to the maintenance TA effort to be kept track of. Information is often derived by the maintenance effort that will help the development effort. What the traffic analyst needs is one system that has enough flexibility for him to move whichever way his TA problem takes him. It would also be useful if the language we use is one that isn't going to change every few years because some equipment in the basement is being upgraded.

PINSETTER

(U) Several years ago, we began to work on the concept of a Traffic Analysis Workbench System, with the covername PINSETTER. Some of what I have described here comes out of that experience. PINSETTER has been described elsewhere, so I will not spend time on it here. However, I will share with you some of my personal conclusions about PINSETTER, especially those which seem to be pertinent to the future.

(U) There are aspects of traffic analysis that resemble word processing, and a good screen editor seems to go a long way toward putting the analyst in contact with his traffic, letting him rearrange it and touch up the rough edges and garbles the way he (the owner) wants them. It lets him look at the data *before* he decides what processing to apply to them. It also puts him in a good position to generate reports about his problem, especially the technical reports with technical data embedded in narrative text.

(U) A good tool kit, similar to UNIX and the PINSETTER extensions, is invaluable in providing the traffic analyst with the ability to tailor-make his own flexible processes for large scale manipulation of his traffic.

(U) Many of the practical results of PINSETTER results that found their way into daily applications on specific targets were not limited to traffic analysis. It became a regular occurrence to hear people from other cryptologic disciplines tell us that much of the UNIX/PINSETTER package for traffic analysts was what they needed, too.

PROBLEMS THAT NEED SOLVING

(U) Among the many problems that need to be solved, I would like to mention two. Both of these are areas that are critical to the future TA Workbench System.

ARCHIVES

(U) Some of our continuities form chains that stretch back to the end of World War II. One of the things that data systems people don't like to hear is that we need storage for data whose lifetime must be measured in years, and perhaps decades. Some years ago, there came a time when all of our incoming data went solely into the computers in the basement. It was the culmination of the dreams of a number of people: to take the raw traffic away from the analyst! I don't challenge that decision. It is history. But I must say

that on many TA problems around the Agency, there are no good records on our *known continuities* from that date forward, unless there were analysts still keeping some sort of hand records. The philosophy on most computer hosts is that any records not accessed within some period (usually a year or less) are taken off the system.

(U) Even if the data are put onto tape, the medium will deteriorate. Once on tape, the data are "out of sight and out of mind." The software understands that data will sooner or later disappear or be "improved." Nevertheless, the analysts on that problem are still responsible for that period of time, and may still have to field questions about their targets for that time period. So far, we have dodged this bullet, but sooner or later we will have to face the need for long-term archives.

INFREQUENT USE OF PROCESSES

(U) The second problem involves the question of software that is only infrequently used. For example, suppose that one of our larger targets has a major communications change every five or six years. The effect of this change is so great that it interrupts intelligence reporting on that target until the new communications structures are understood and recovered. Each time the change occurs, an intensive effort is therefore mounted to recover our continuities in the shortest possible time.

(U) In the old days, when the special effort was over, everything was bundled up and packed away for retrieval when the next change came along. But how do we handle this now that we have modern data systems support? After five or six years, how much of the software is still useful? Chances are that the database has been changed, as well as the host on which it resides.

(U) Another example might be the diagnostic techniques to attack a particular kind of callsign system. Once the system in question is solved, how should we preserve the software so that it doesn't need to be reinvented the next time such a system is encountered? Suppose we don't find a similar system for five, or six, or even ten years?

CONCLUSION

(U) I don't offer either my observations or my experiences as criticisms, but rather as areas of traffic analysis support which need to be solved. I have tried to avoid mentioning specific hardware or software, except as examples. A man named Bob Biles taught me long ago that users should never tell computer people what equipment to use.

(U) Perhaps traffic analysis has lagged behind other cryptologic disciplines in making full use of modern data systems. But that is changing, thanks to the patience, ingenuity, and hard work of many of you here today. I still keep a supply of pencils around, and I still have a pencil sharpener on my desk - but I have noticed that I don't really use them very much anymore.

Traffic Analysis: Specialty Without Portfolio

[redacted]

P.L. 86-36

Editor's Note: This is an address given by [redacted] the A2 Senior Analyst, at the 1980 symposium of the Communications Analysis Association; it is based on his extensive experience on the Soviet military problem.

In addition to cryptanalysis, which I do not intend to deal with in this discussion, communications intelligence has always involved two primary, overlapping but distinct, tasks with respect to target analysis:

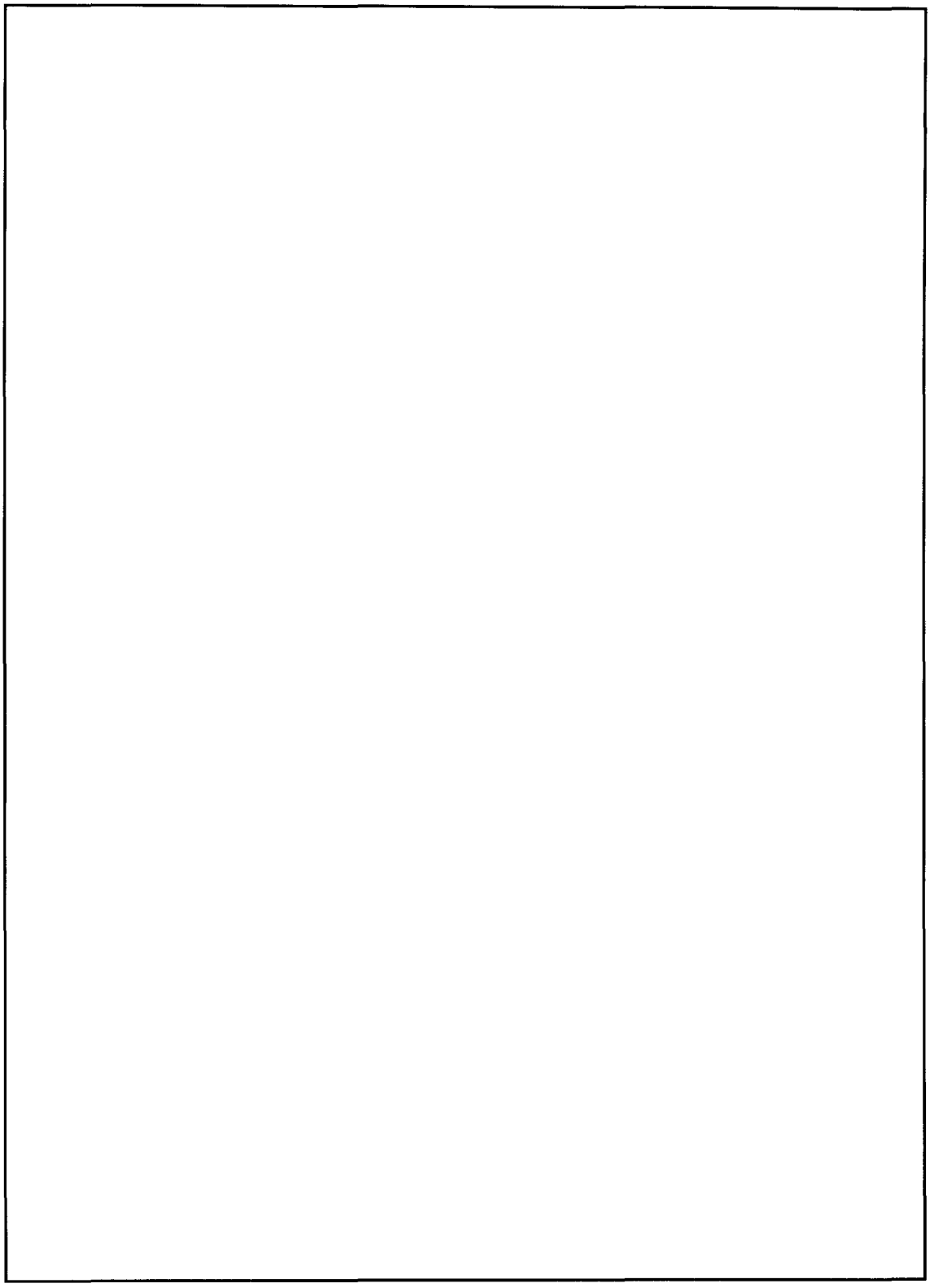
- ordering and understanding target communications structure and procedures– commonly referred to as *traffic analysis*, and
- describing target organizations, activities, intentions and trends – known as *intelligence analysis* or *special research analysis*.

The major overlaps of the two disciplines are in their contribution to target organization, or order of battle, and command and control.

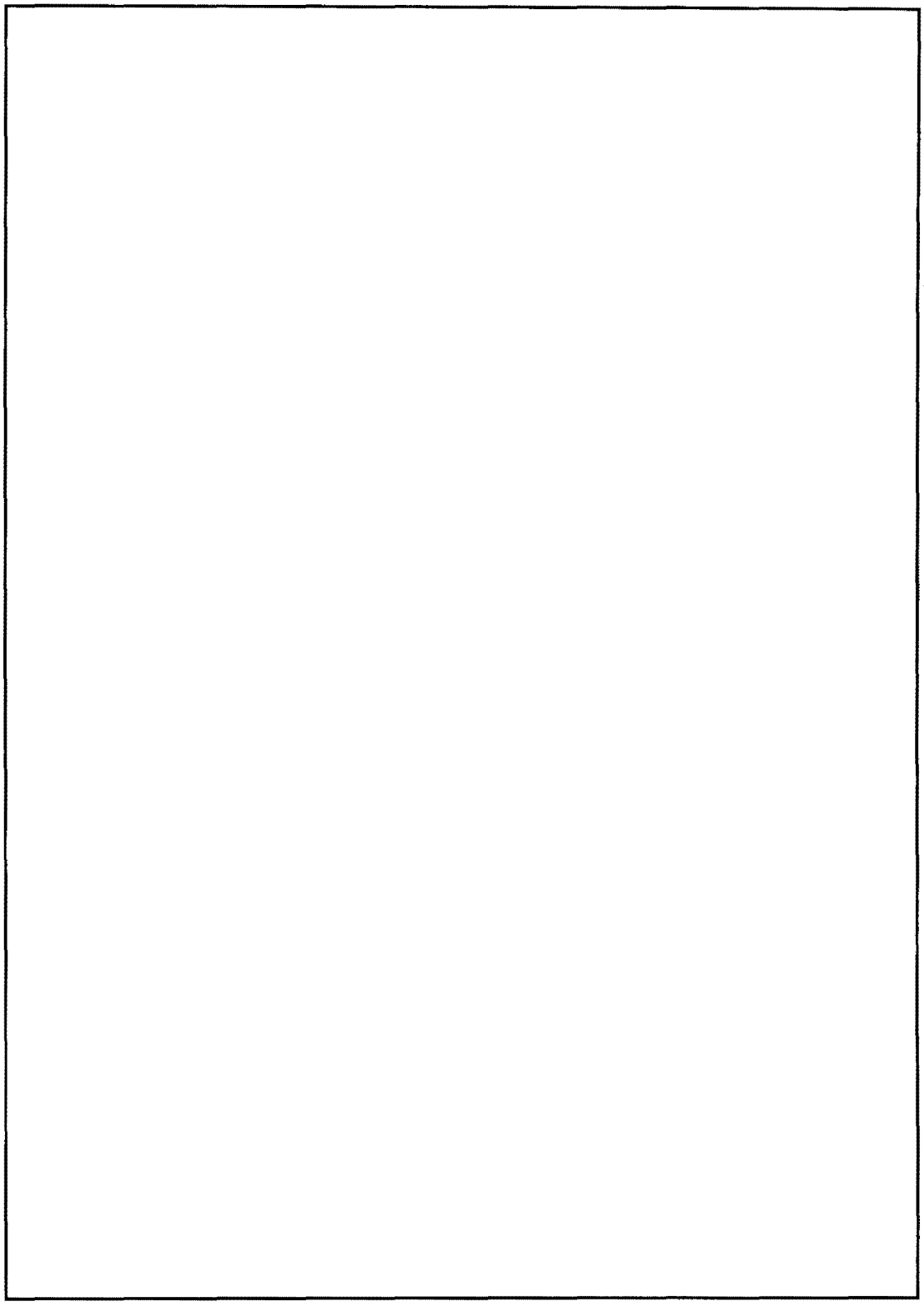
Of these two skills, only the latter one, intelligence analysis, has been effectively accommodated in the NSA career structure. Traffic analysis, in terms of its application, is largely regarded as a skill to employ if time and resources permit, which means that it is basically nonfunctioning in many important areas. In career terms, it has been essentially inaccessible to representative numbers of people, being an apprentice slot that must be abdicated by those with more than modest ambitions.

[redacted]

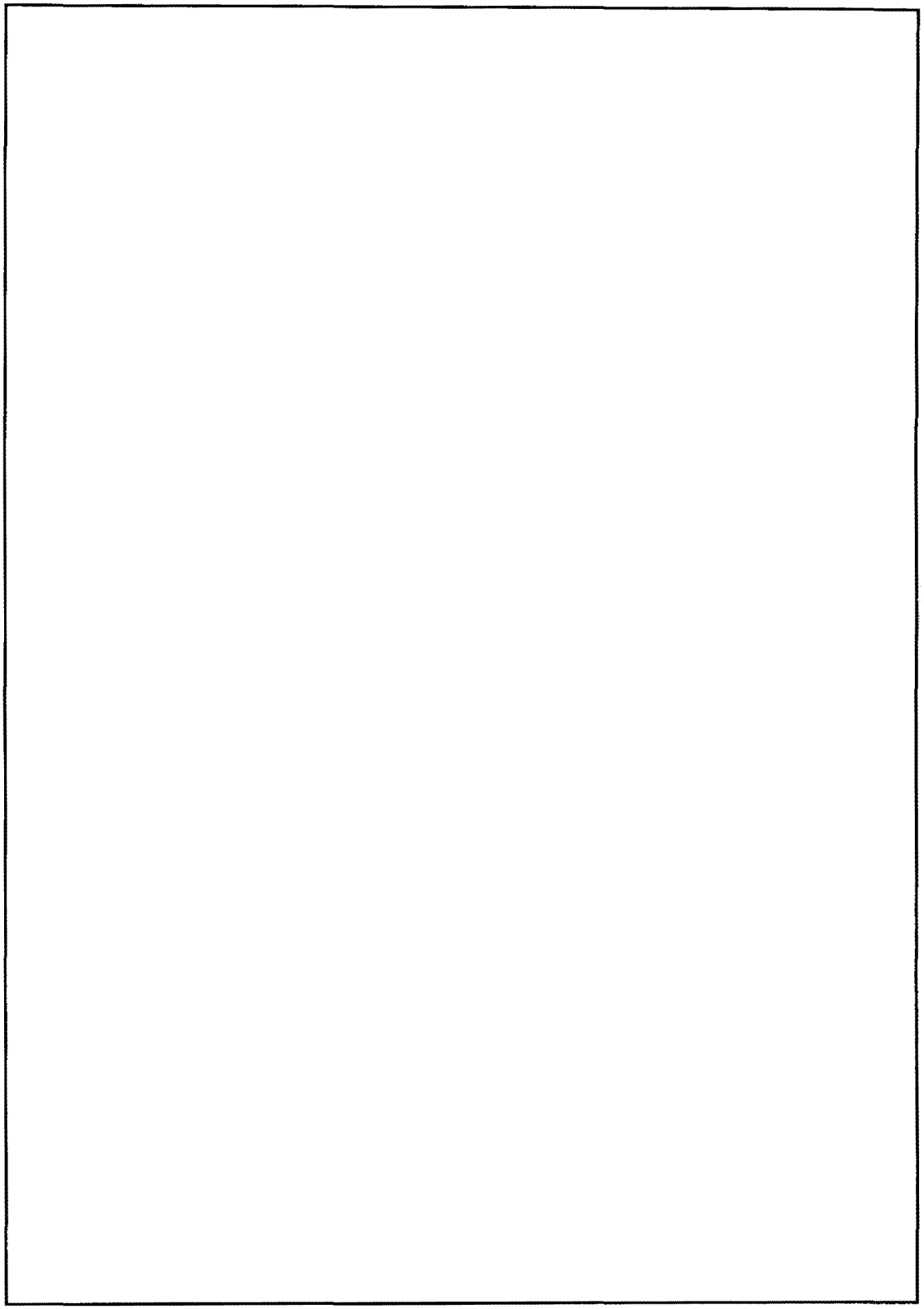
P.L 86-36
E.O. 1.4.(c)(c)



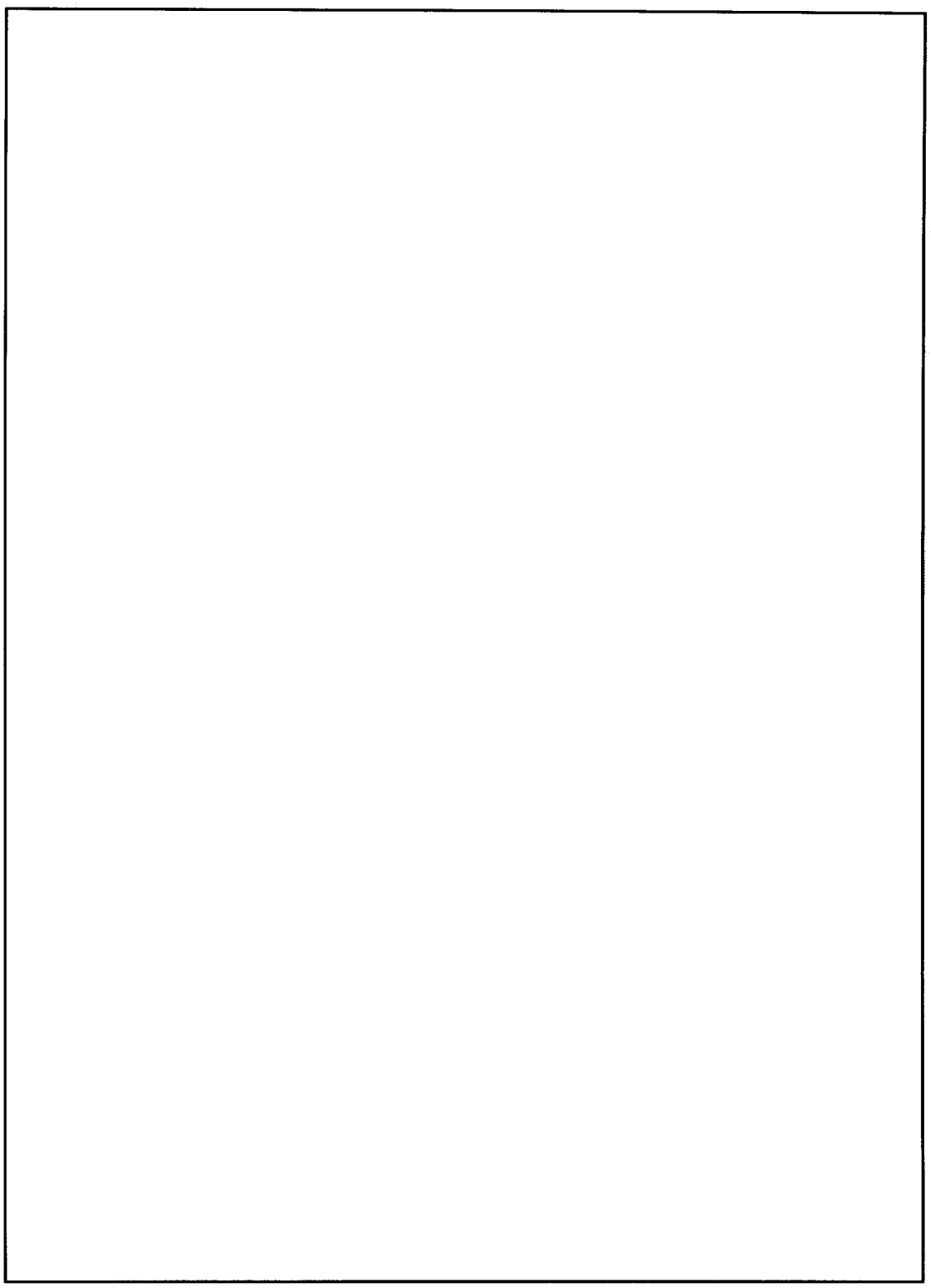
P.L. 86-36
EO 1.4.(c)



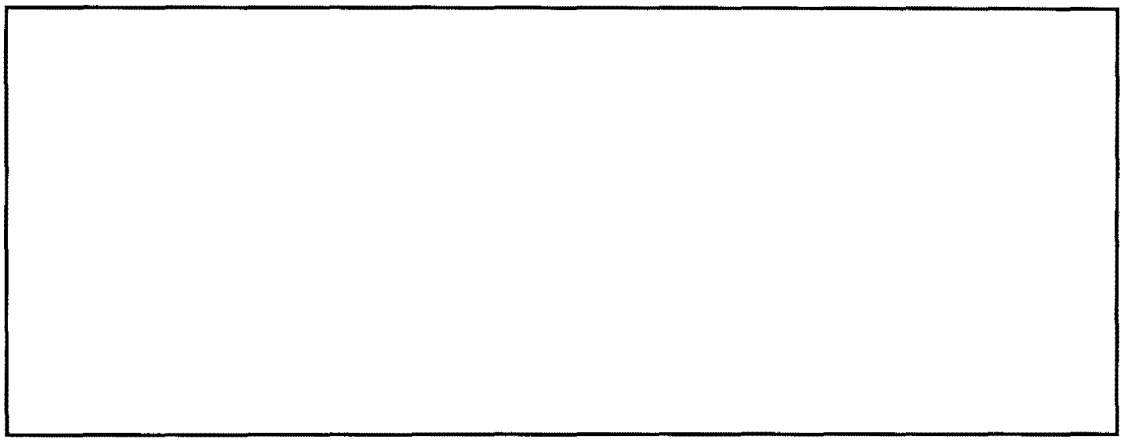
P.L. 86-36
EO 1.4.(c)



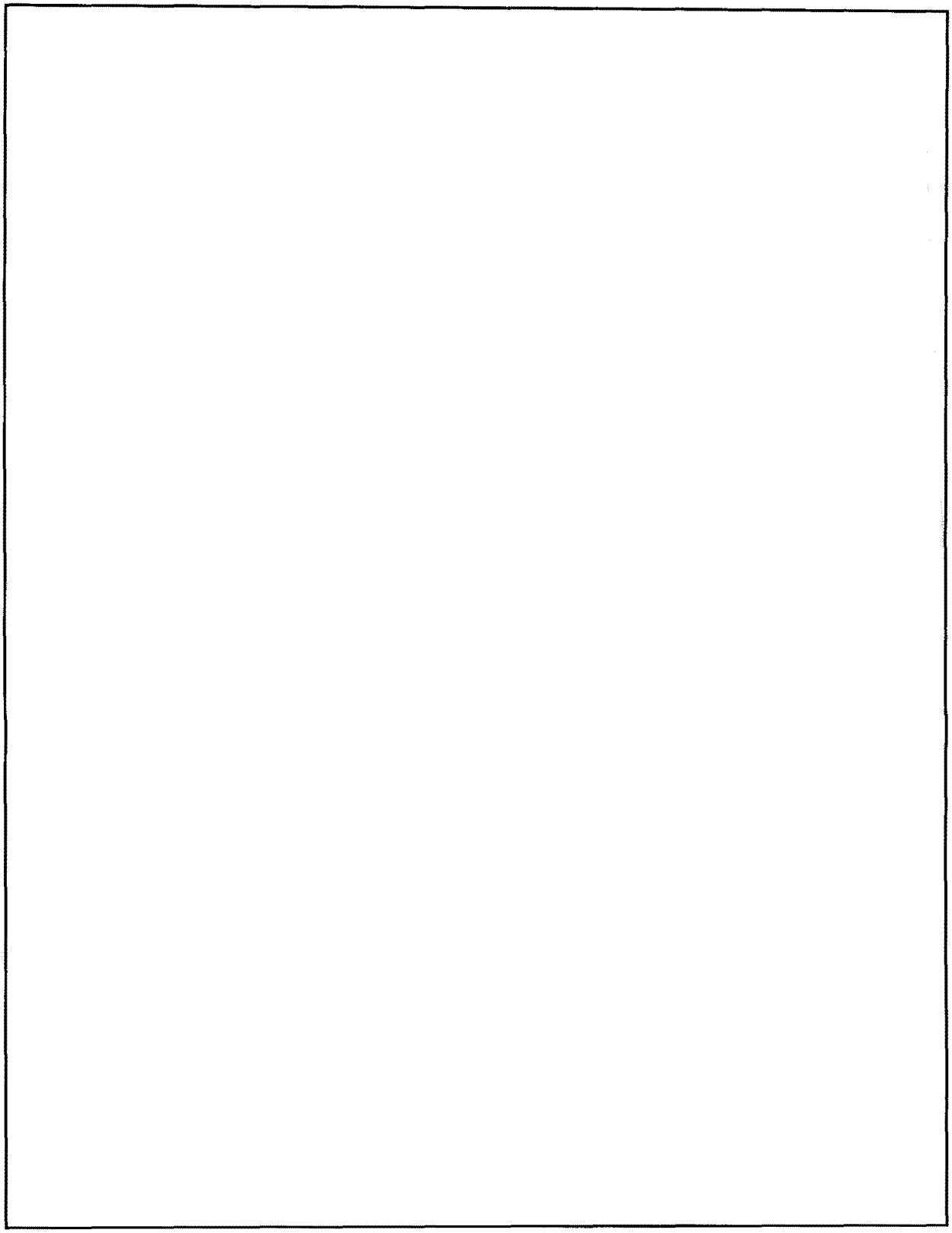
P.L. 86-36
EO 1.4.(c)

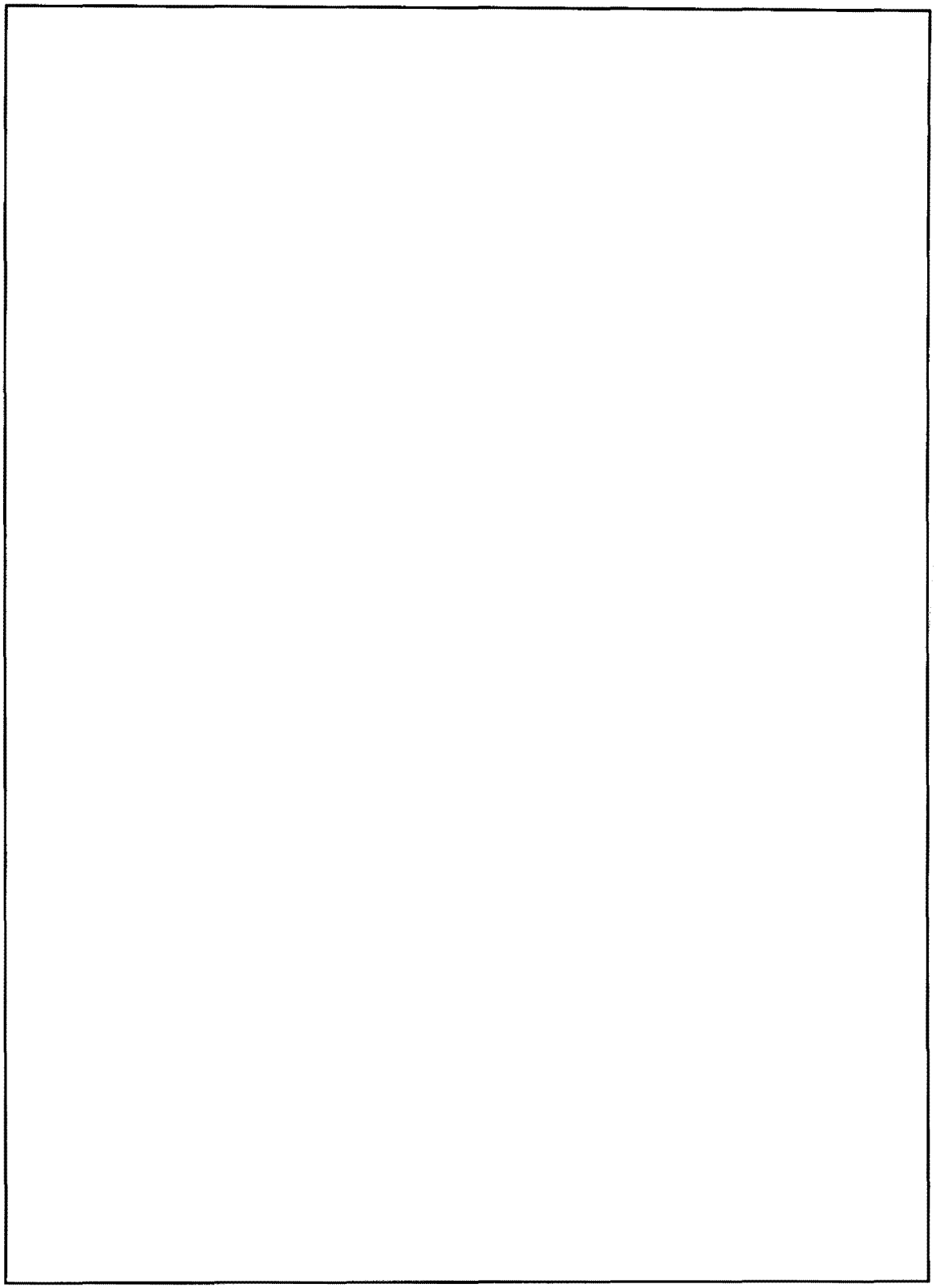


P.L. 86-36
EO 1.4.(c)

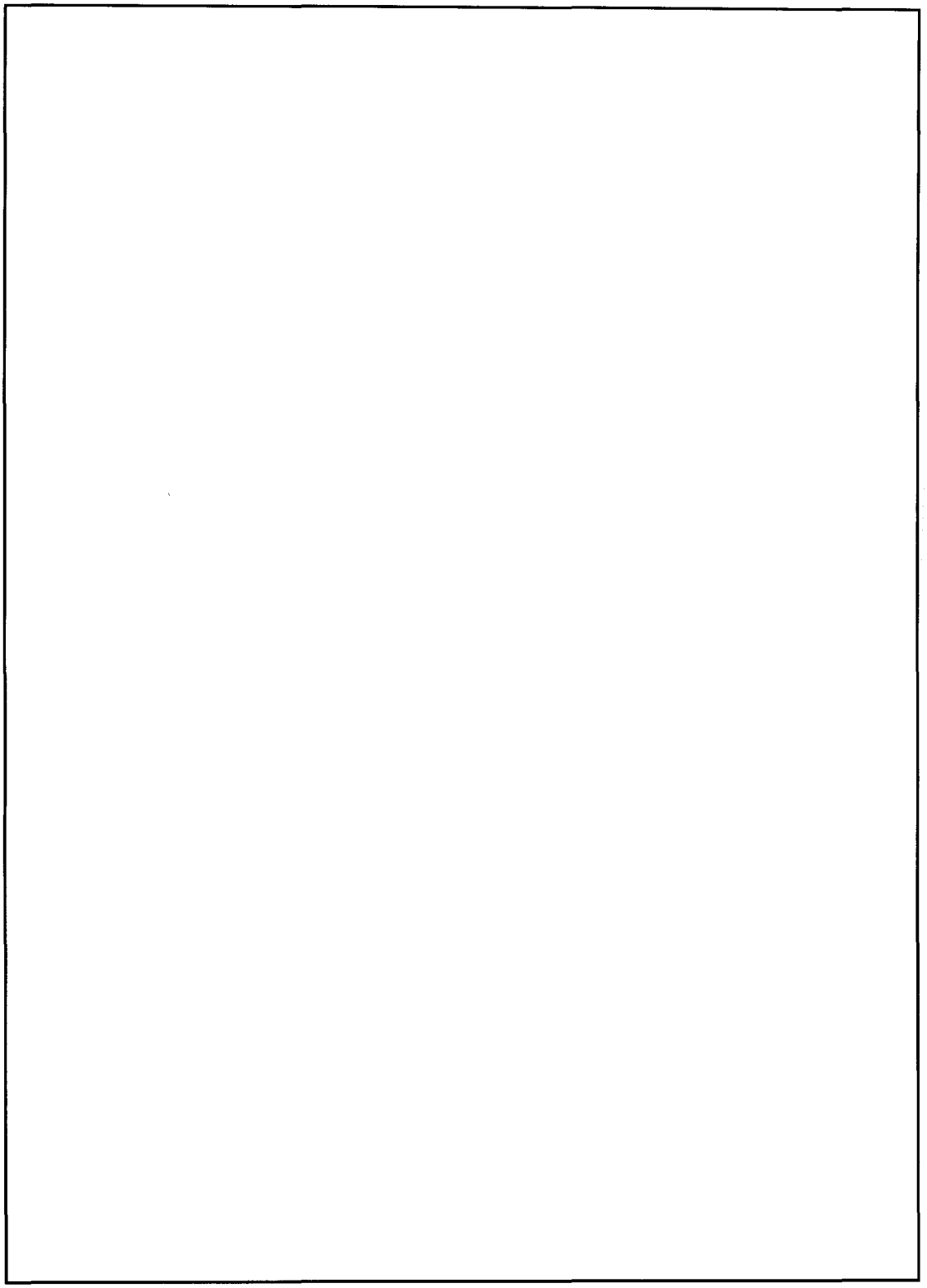


P.L. 86-36
EO 1.4.(c)

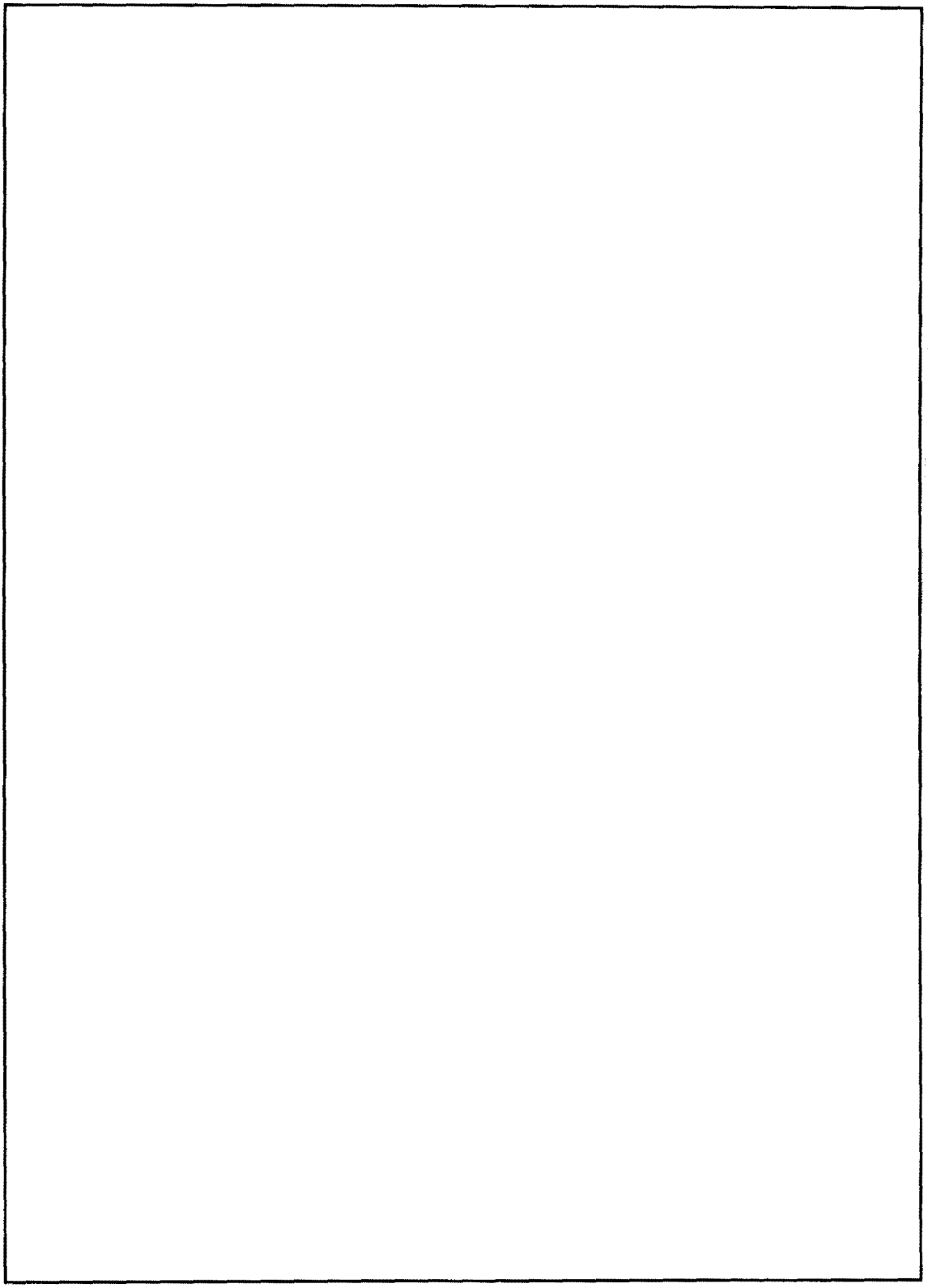


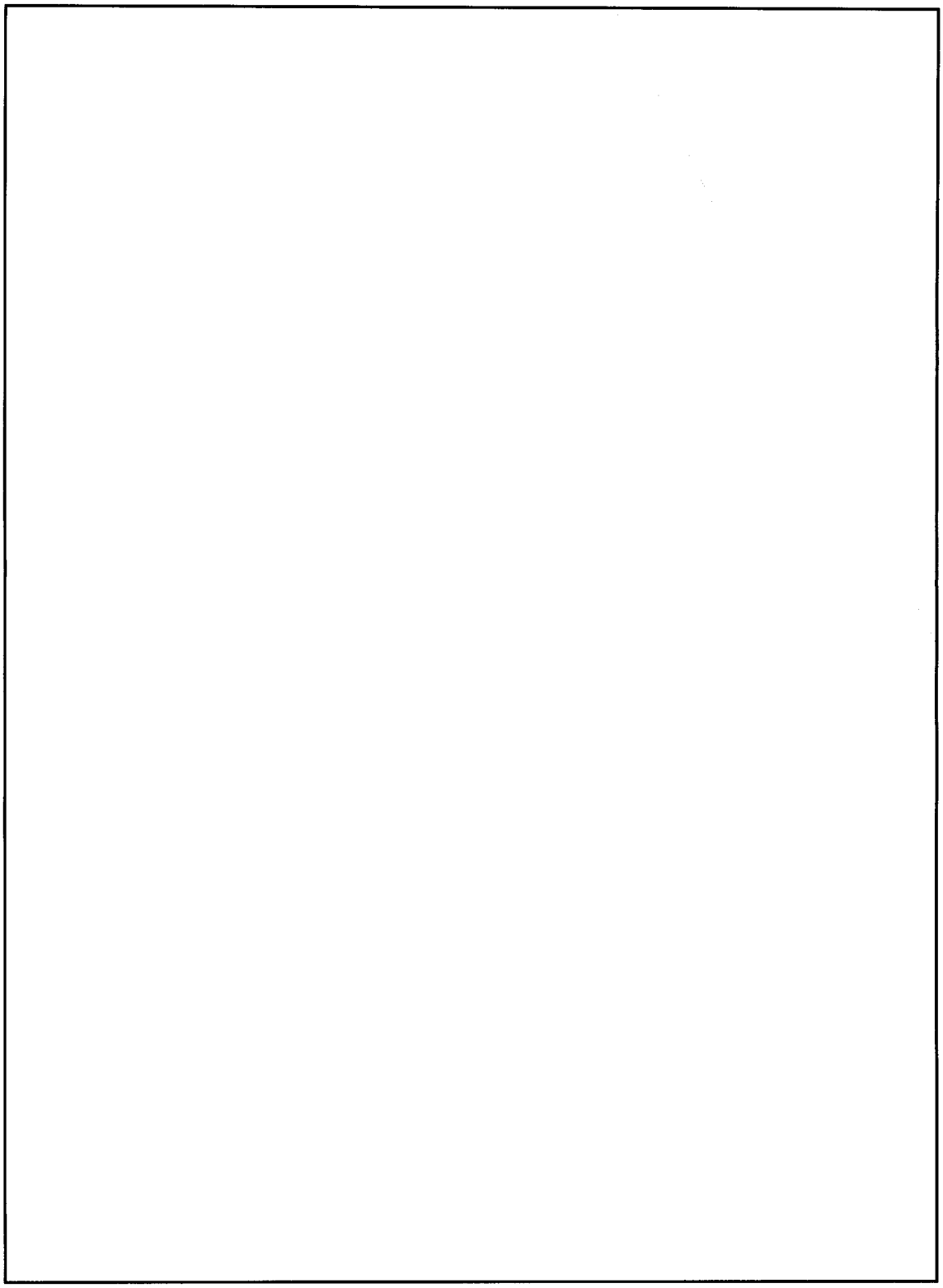


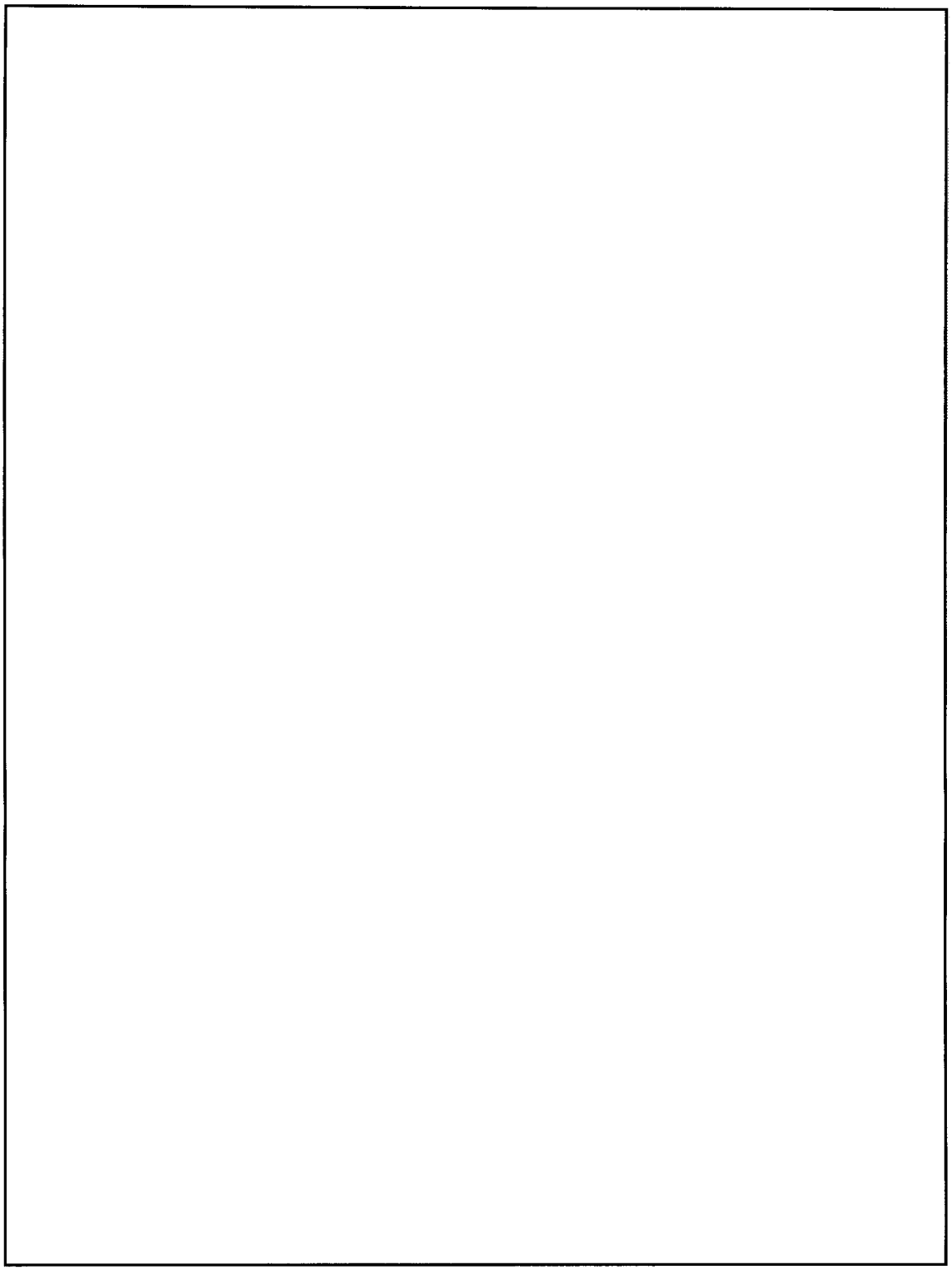
PRLL 886386
EIEO 144(c)
EIEO 144(d)

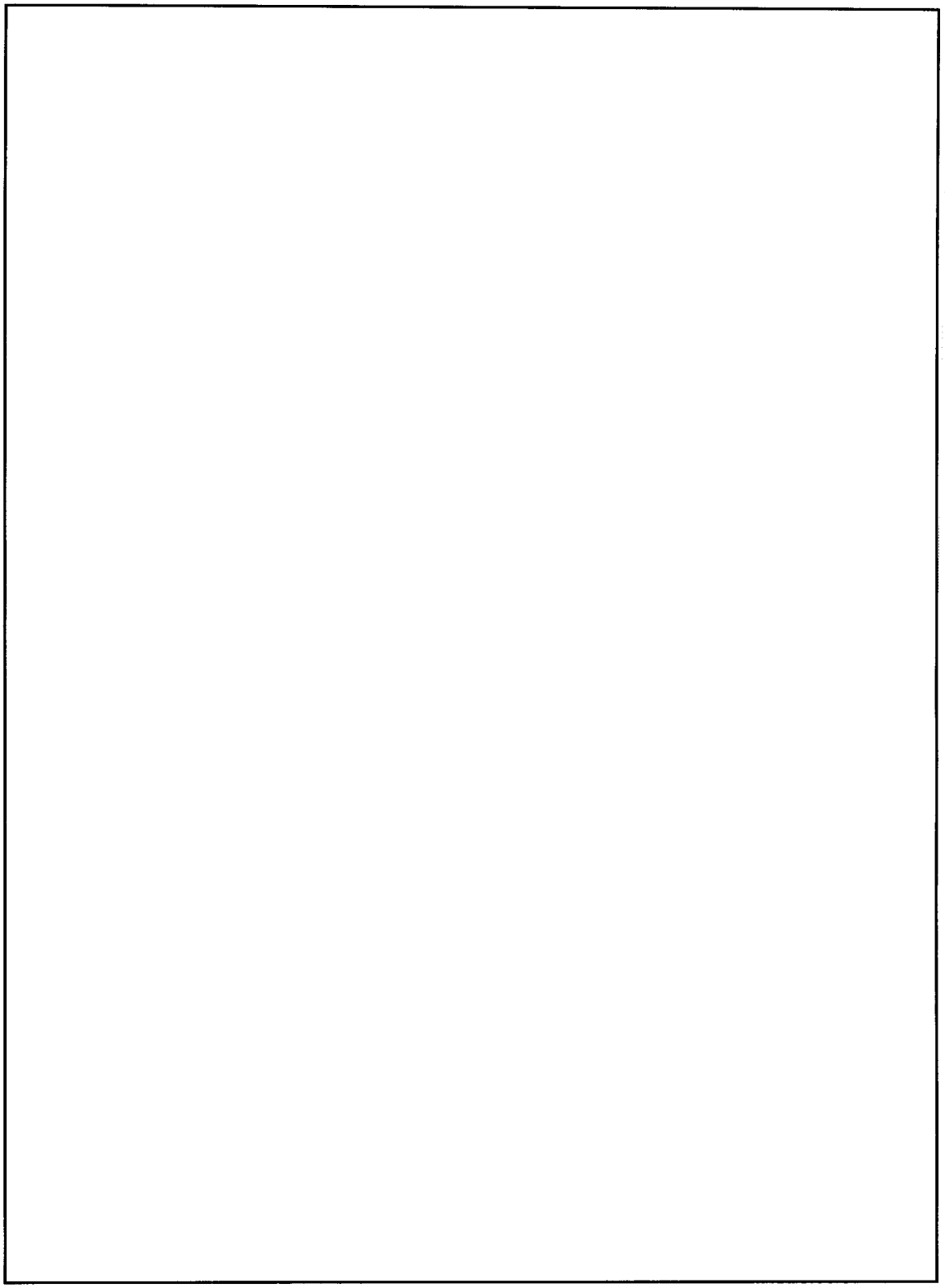


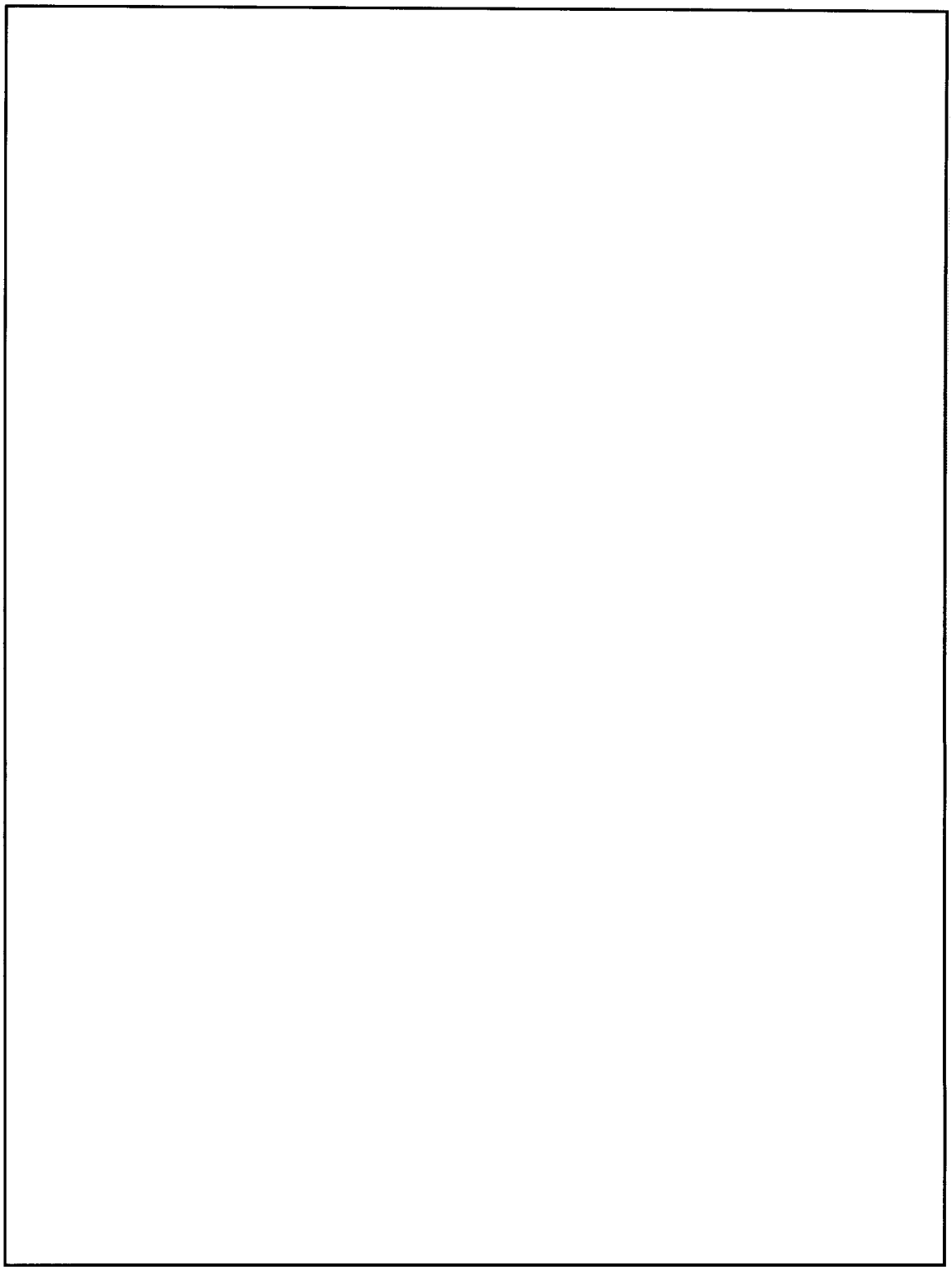
PRLL 886366
EECI 144(c)

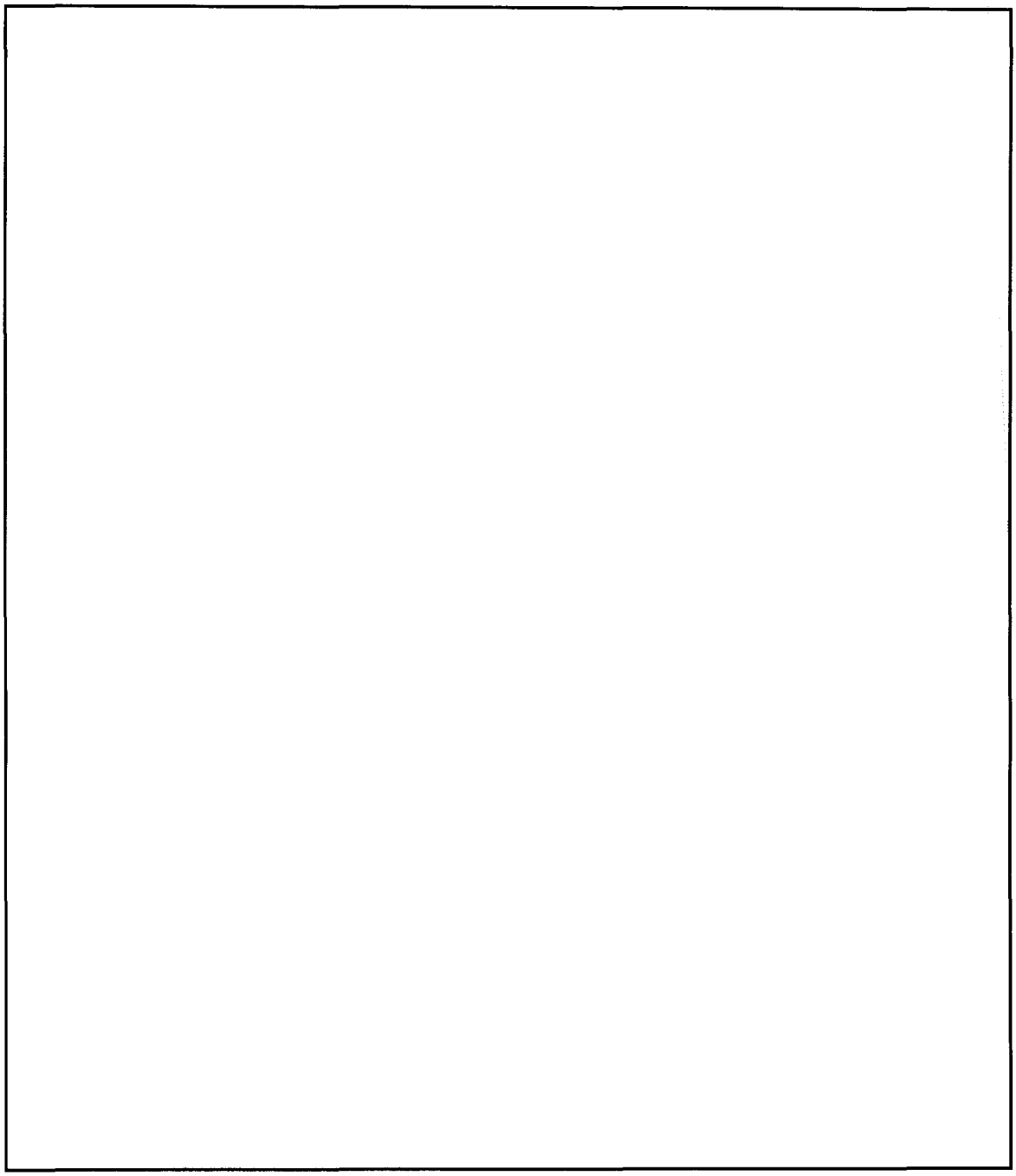




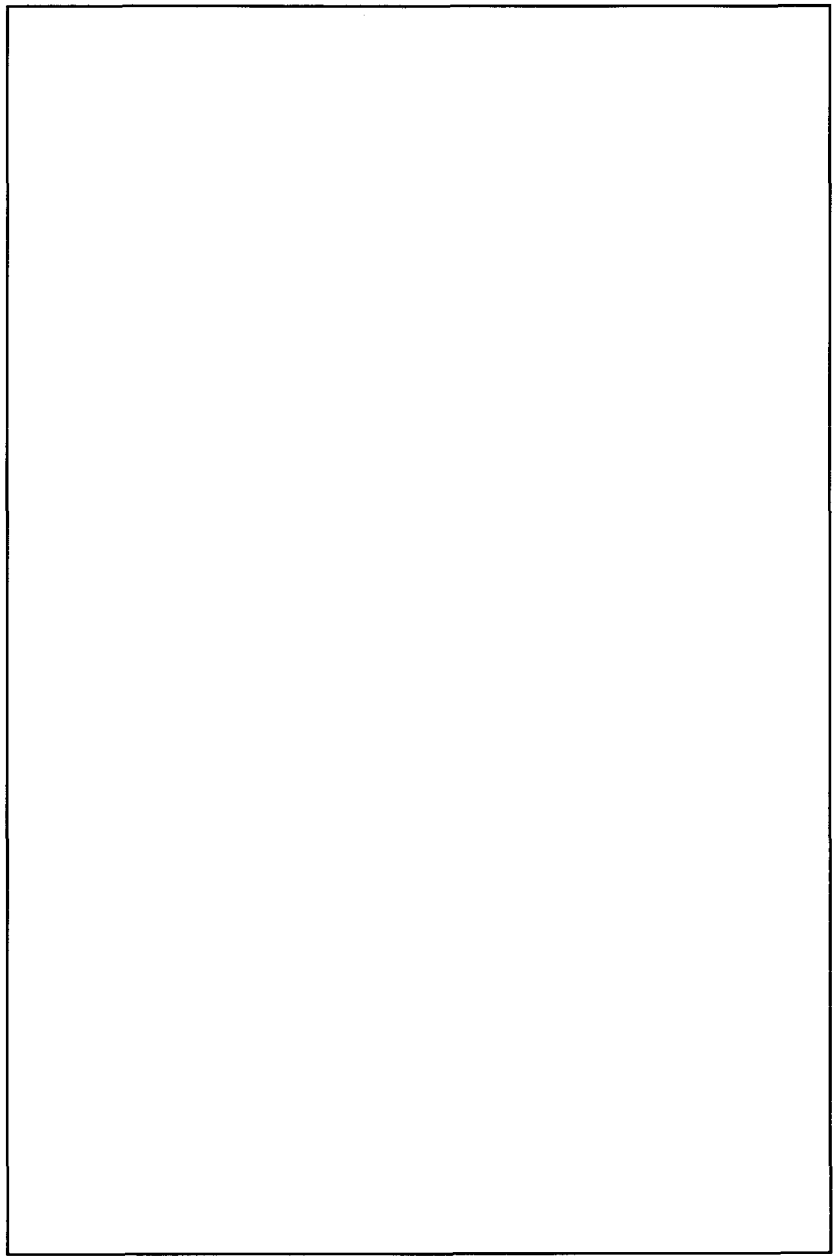


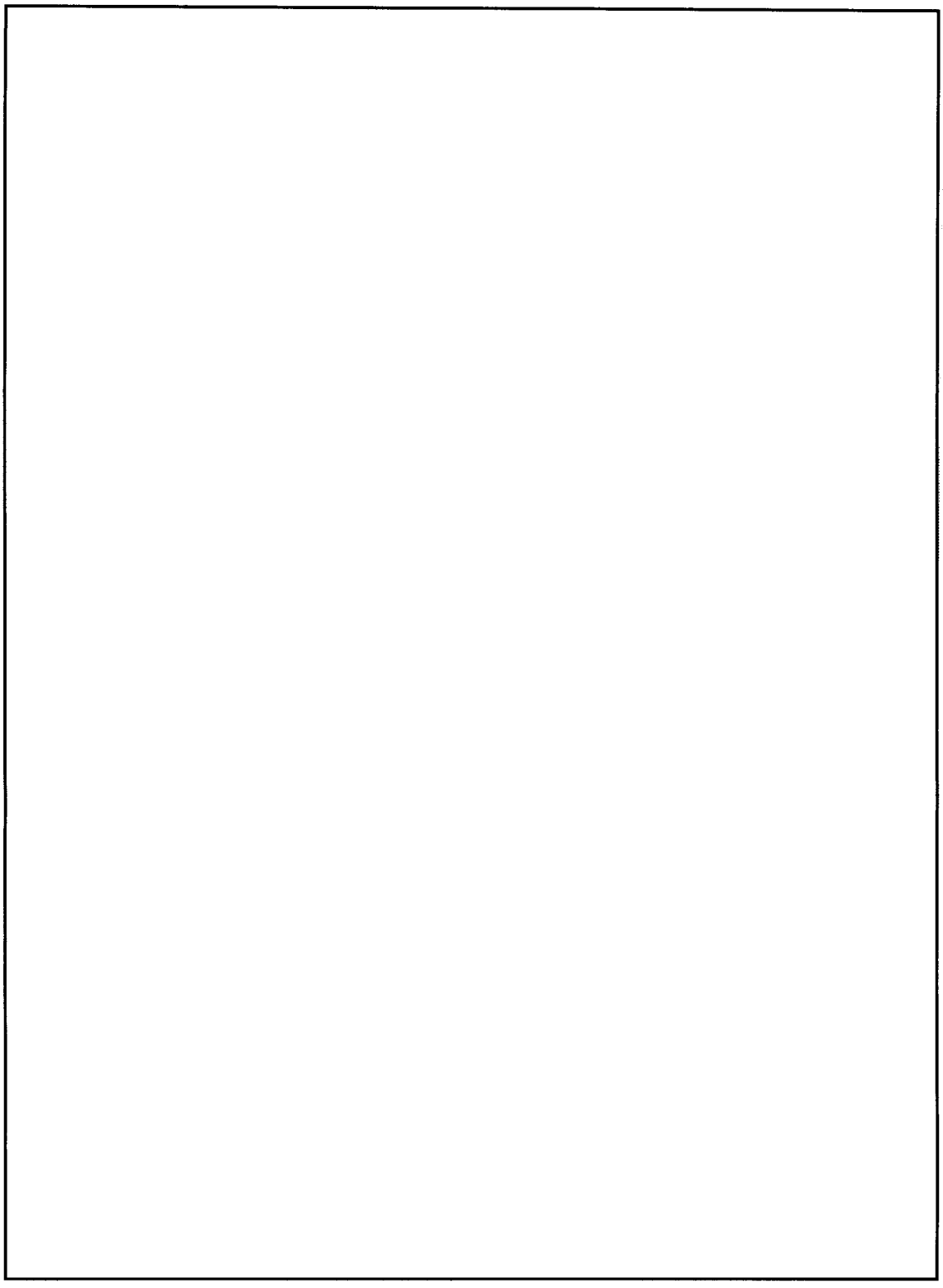


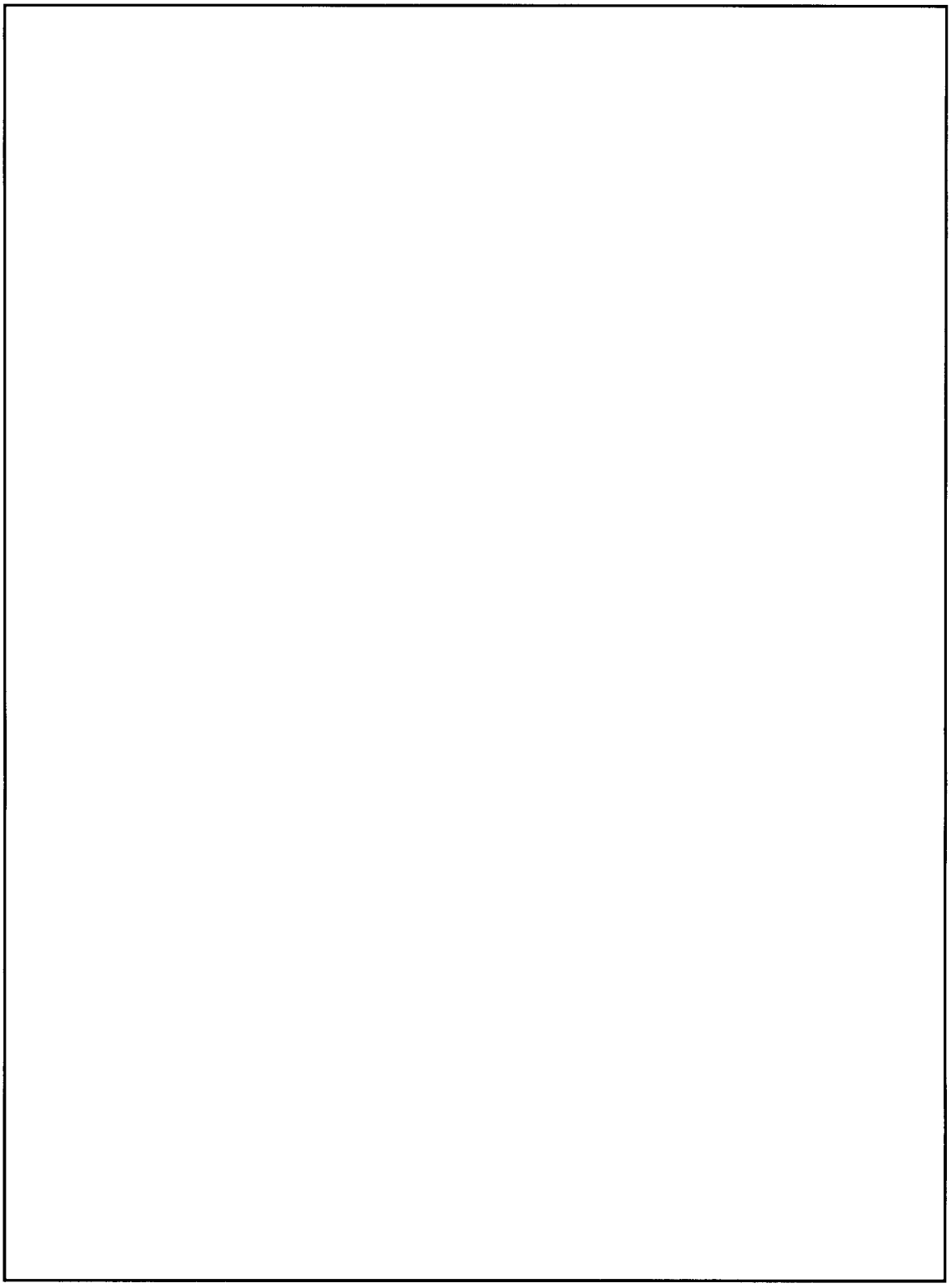


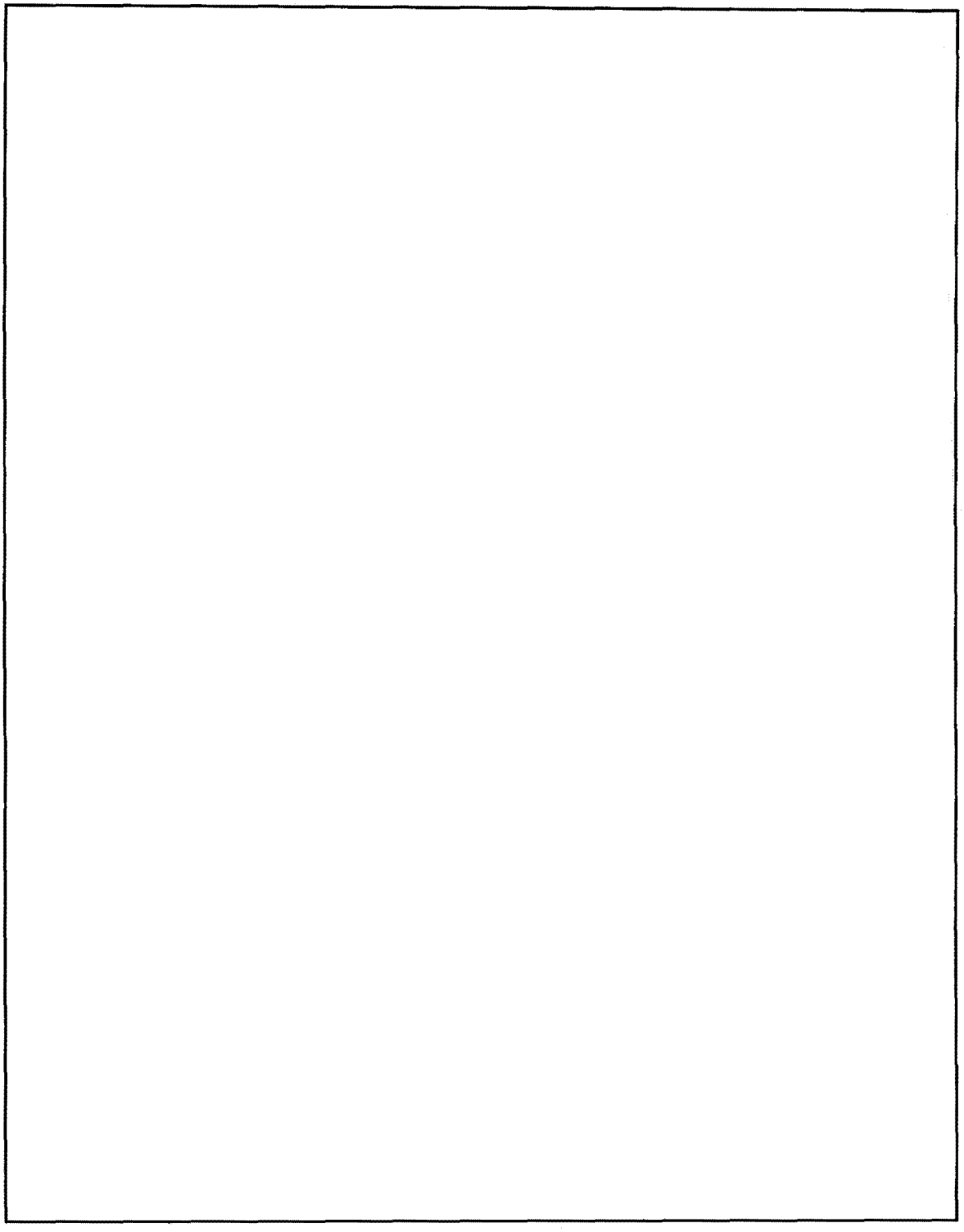


P.L. 86-36
EO 1.4.(c)

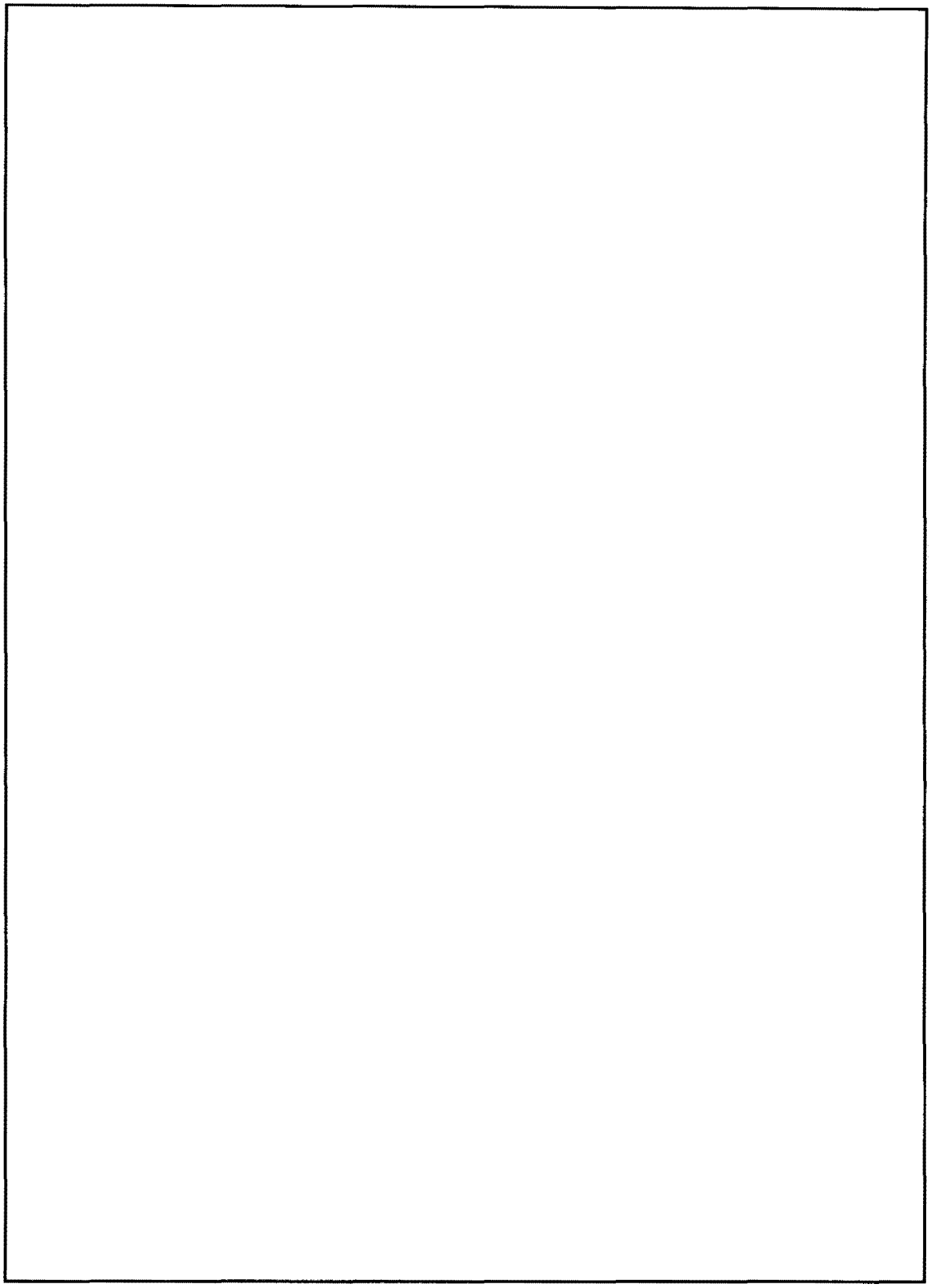


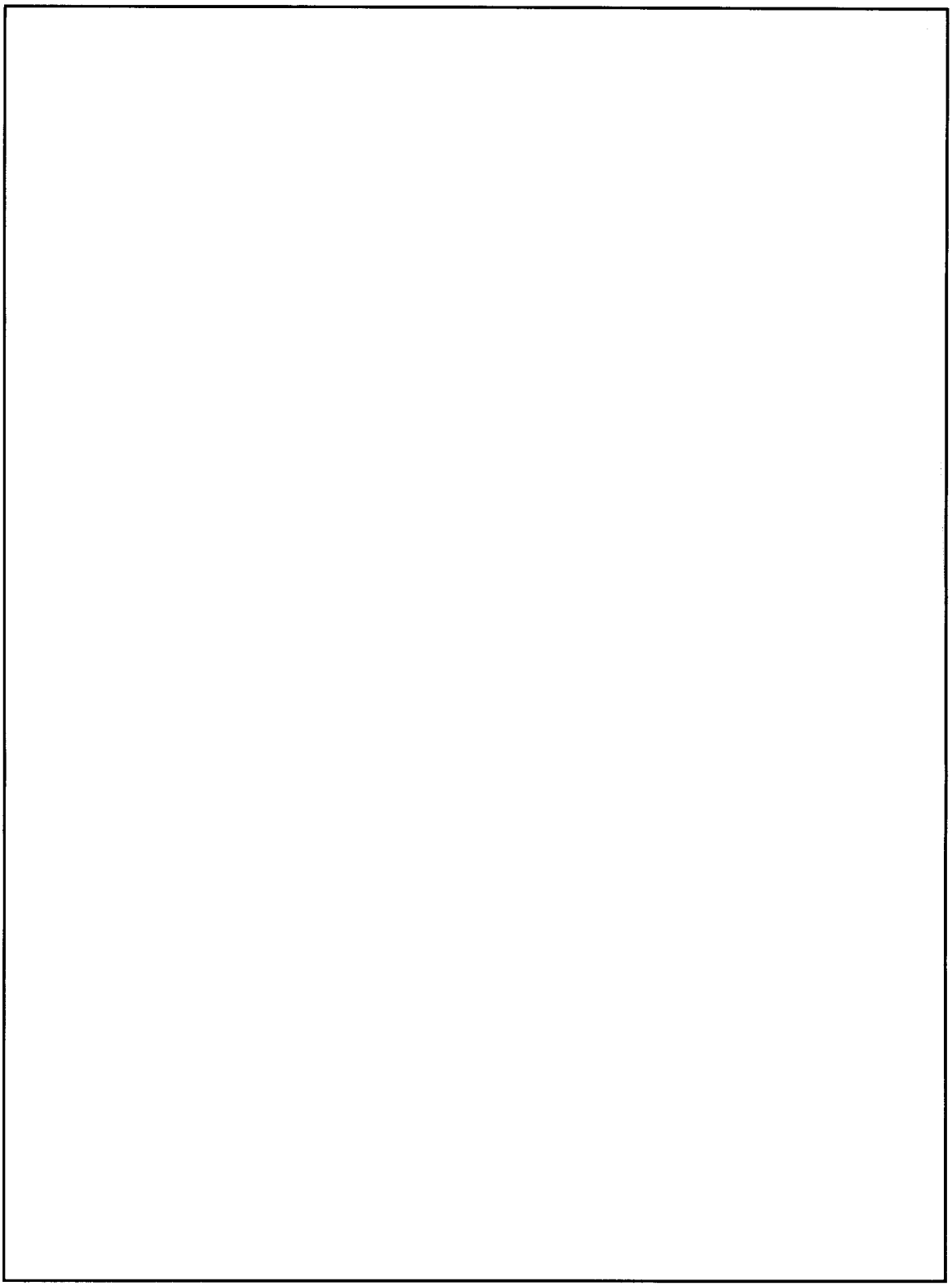


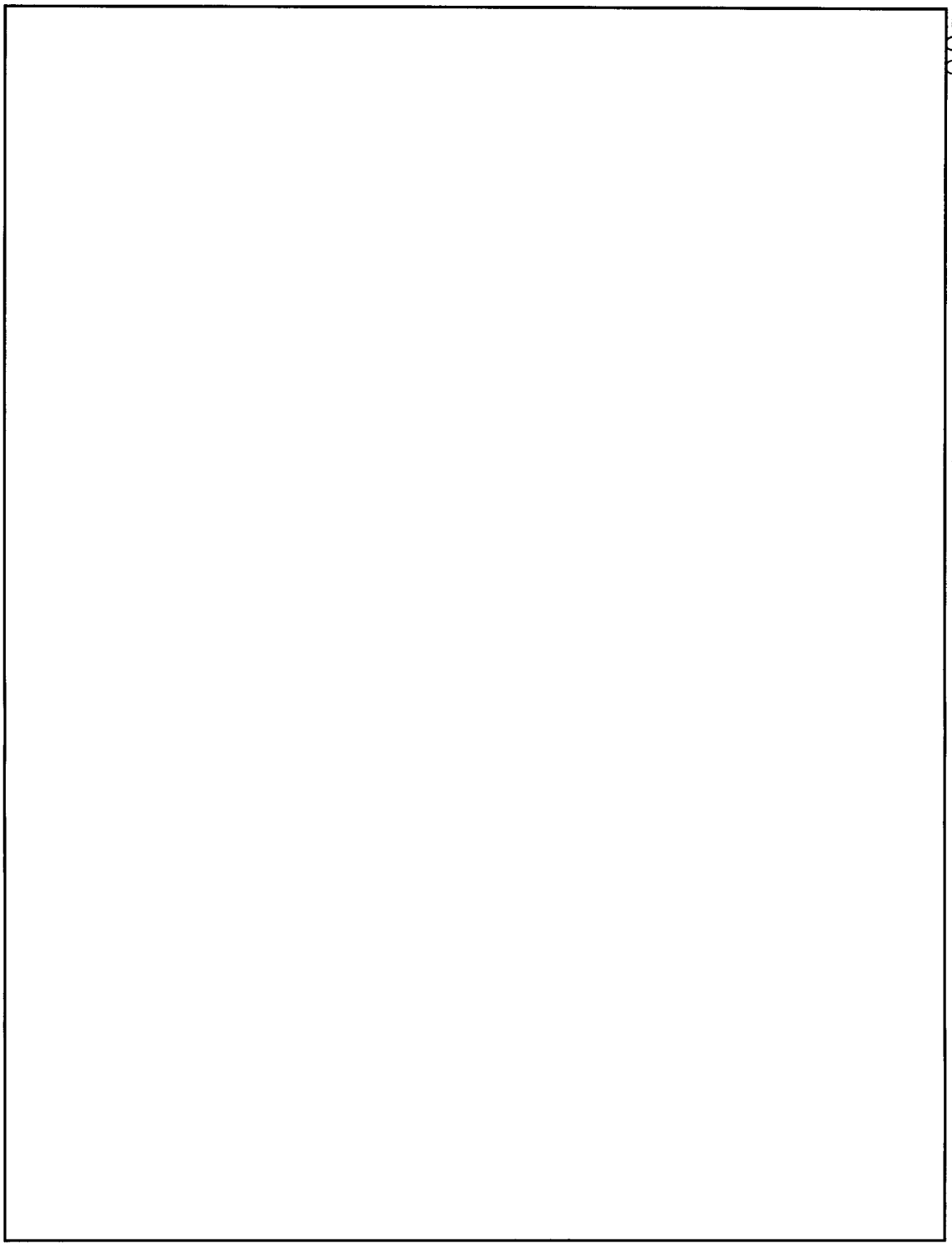




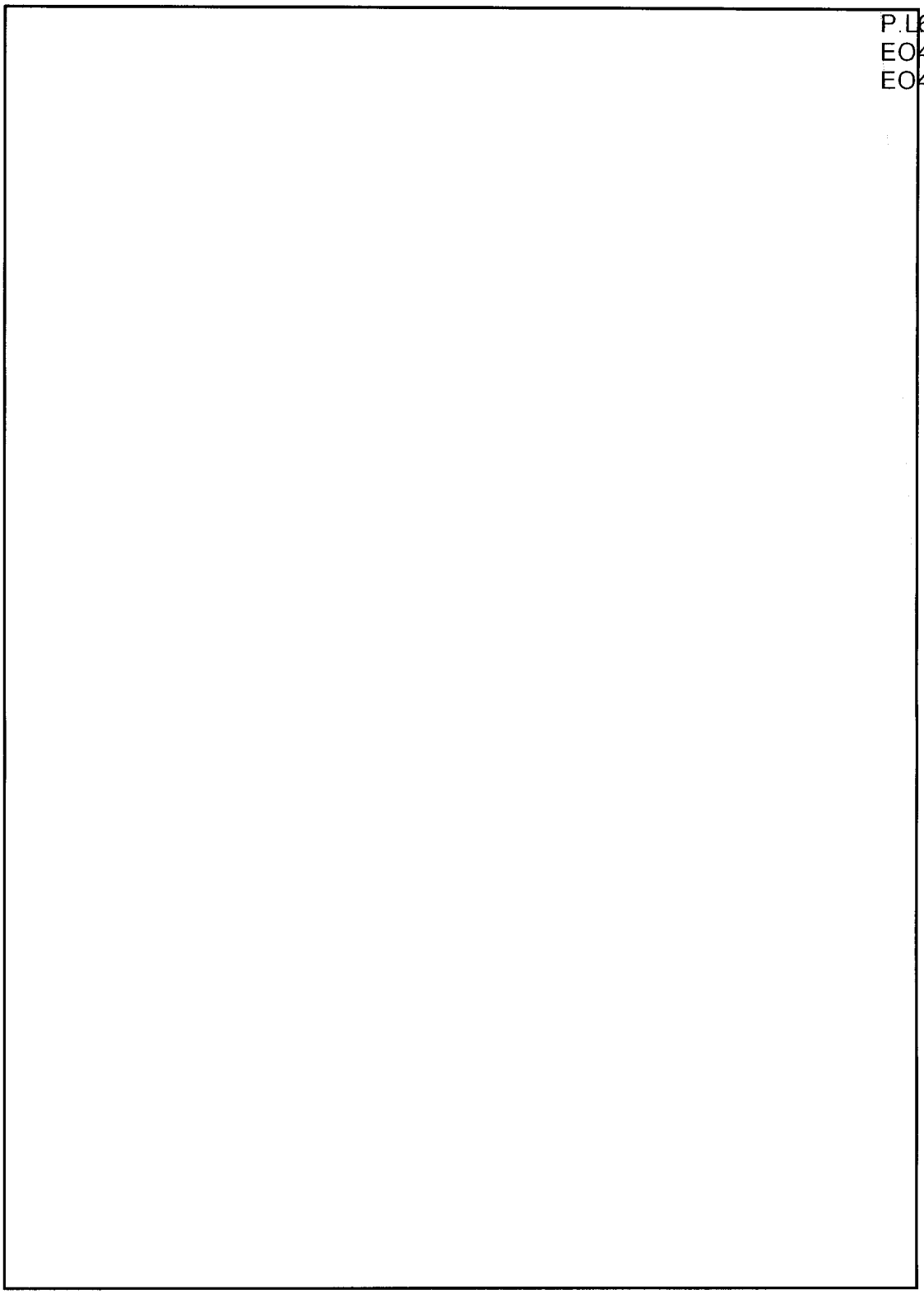
~~SECRET SPOKE~~





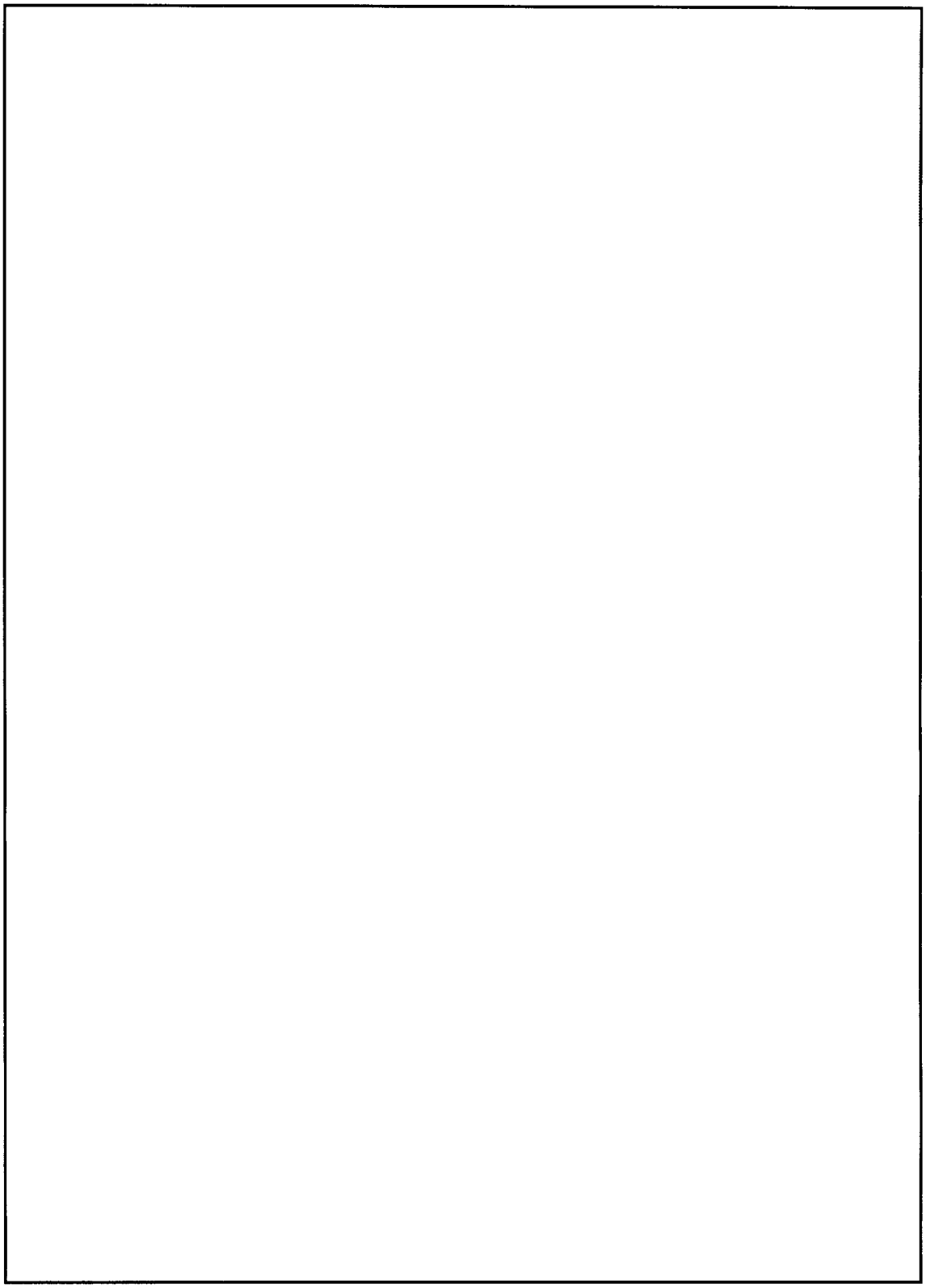


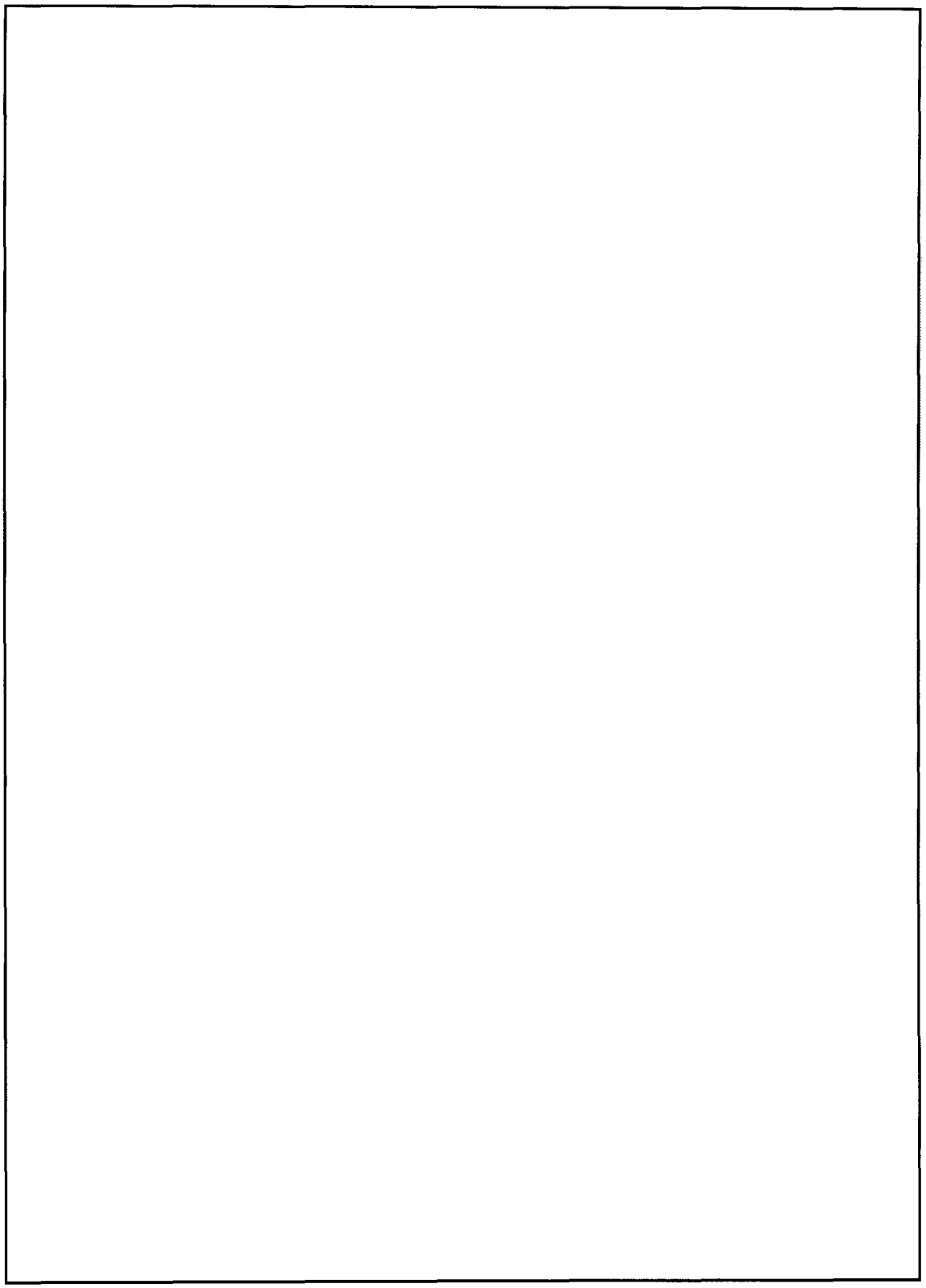
L.R86-36
E.O.1.4.(c)
E.O.1.4.(d)



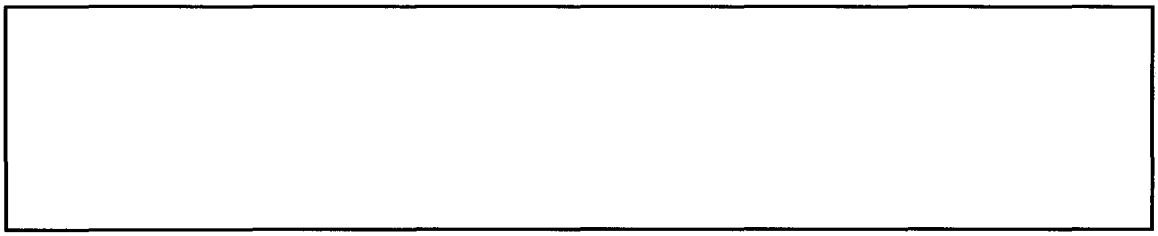
P.L. 86-36
EO 1.4(c)
EO 1.4(d)

~~SECRET SPOKE~~





~~SECRET SPOKE~~



The Future of Traffic Analysis

P.L. 86-36

[redacted]

It is a pleasure to be here and to be asked to think about the future of TA. That's a subject I've been thinking about, in one way or another, for most of my adult life.

I would like to begin by making some predictions about TA twenty years from today. I found a crystal ball and was going to set it up here on the podium for these predictions. However, the guy that owned it couldn't figure out why I wanted it, so I decided it wasn't worth the trouble.

Here are the predictions.

- *Twenty years from today, people outside the field will be telling us that TA has no future.*

Back in 1946 when I first started, people were quick to tell me that TA was a wartime skill, that it did a fair job during the war, but that it wouldn't be around very long in peacetime. In fact, I can remember not really wanting to be in the field of TA. I was convinced that CA was more interesting, and for a while I did my best to get out of TA so I could work in CA. (Later on, when I got my hands on some actual raw traffic and began to work with collectors, I found that TA was a lot more interesting than I thought.) And people have been predicting the demise of TA ever since. By now it's an old song, but I even hear it today. So it doesn't take much nerve to predict that we will still be hearing that song twenty years down the road.

- *The highest graded individual in the TA field will be a supergrade, or whatever they are calling them twenty years from now.*

This is another easy prediction. [redacted] got to be a supergrade as a Traffic Analyst, and so did I. I see no reason why other Traffic Analysts can't do the same. If anything, it ought to be a little easier for you, because the Agency is now more attentive to the technical track than it has been in times past.

- *Most of the daily front page news in the intelligence community will be provided by TA.*

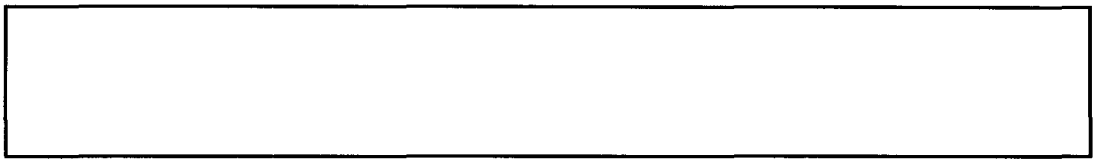
This is another easy one. We do it now. We have been doing it. It seems an easy projection to say that we will continue. We will still be relying on TA for much of our Information [*sic*] & Warning. There may be some new high-tech wrinkles in the I&W world twenty years from now, but TA has a good track record for reliability and consistency in this area. It is so simple for TA to "reach out and touch" targets to see if

~~FOR OFFICIAL USE ONLY~~

they are normal. Even if some good gadgetry comes along, the result will be some sort of partnership between the new techniques and the old reliable methods of TA.

- *We will still rely on TA for collection steerage.*

It is funny how often this is overlooked in day-to-day operations. And yet some TA shops could almost pay their own salaries in the savings from more efficient use of collection resources. Signals are getting more complex. Some of today's targets have a lot of money to spend and are modernizing faster than our collection system. All of this will require even *more* efficiency for collection steerage, and that's where TA has to come in.



FPLL.8866366
EO1144(c)

This hasn't changed for years, and probably won't over the next twenty. TA people are still "batching" traffic into homogeneous groups to prepare it for cryptanalytic attack. Ask your favorite cryppies if they would like this to continue. Once cryptanalysts experience good TA support, they become believers; they will ask for it again and again, because they know it helps them to do their own job well.

- *On Tuesday, the 24th of May, in the year 2005, someone will be heard to say, "My problem isn't a standard TA problem – we don't use callsigns."*

I think I first heard this about thirty-five years ago when I started working on a radioprinter problem. I really don't think there is a *standard* TA problem. What we have is one or two problems that are so large, we tend to think of them as standard. But they aren't. Traffic analysts have a large bag of tools, built up over the years. We keep adding to that bag of tools, but we don't throw old tools away. Lately, we've been added some computer tricks to our tool kit, and over the next twenty years, I suspect that other new tools will be developed. We need every tool we can get.

Art Levenson used to say that we were a bit like a man that has lost his wallet on a very dark street. We don't look for it where we think we lost it – in the dark. We look for it under the street light where we can see. We have to work with what the target gives us. And we use whatever tools are appropriate for the features the target gives us.

This leads me to my last prediction, one I hope does *not* come true:

- *Sometime during the next twenty years, your target, or the target you are most interested in, will have a major communications change.*

Maybe the target will find out what we use to exploit his communications, how we do our little magic tricks to produce TA results. Maybe they will have a spy, or maybe some public figure will slip and say too much, or maybe someone will go out and write another

dumb book. Whatever the reason, the target will change its system, perhaps at great cost and inconvenience.

First there will be panic and lot of running around. Then, after things settle down a bit, the traffic analysts will begin to take a look at what the target is giving us to work with. Then they will dip into that big old bag of TA tools and start building another processing system, a system that will feed the collectors, and the cryptanalysts, and the intelligence community. As they recover the new signal plan, what the traffic analysts find will be new, and maybe some of the tools they use will be new. But it will still be TA.

Valedictory of a Traffic Analyst

JOSEPH STARR

P.L. 86-36

(U) On August 1, 1985, I retired from the National Security Agency after almost forty years of cryptologic work, which included at one time or another most of the things NSA does in the fields of collection, analysis, and SIGINT reporting. I enjoyed every minute of it. I honestly don't believe I could have chosen a more enjoyable or rewarding career. If I had been born rich, I would have done traffic analysis for nothing; if I had been independently wealthy, I would have paid the Agency to let me do it. Hang with me for a few minutes of serious discussion about machine processing problems, and I'll share with you a few observations, comments, and recommendations that may contribute to your enjoyment of the profession and perhaps help you to avoid some of the pitfalls that beset the paths I wandered in.

(U) The most important question confronting the profession today is why, from a traffic analyst's viewpoint, data processing systems have not yet produced the Utopia we were led (or stampeded) to expect back in the early 1960s.

(U) In the January–March 1980 *Cryptolog*, [redacted] correctly sorts working analysts into three categories: loggers, case analysts and research analysts. He then predicts that automated processing techniques will permit us to eliminate the loggers, and assesses that the research analyst is the one with the bright future because he is concerned with the "why of analysis...driven by his desire to explain." But every analyst should be saying why, and George's prediction that the logger will become obsolete just hasn't happened, although it should have. Indeed, we now have a new generation of loggers who have even less understanding of traffic analysis than those who preceded them.

(U) After George discusses how analysts are going to have to adapt in order to be productive in a modern (machine-oriented) world, he puts his finger squarely on the major problem area, "manageable machine systems that will function as designed." And he goes on to point out, ". . . our track record for the development of such systems is not impressive."

(U) In the December 1981 *Cryptolog*, [redacted] published an article on machine processing that everyone who claims to be a traffic analyst should have read. Part of what Dale addressed was the problem with keeping competent programmers on the job, and how the traffic analyst could be freed from total dependence on the programmer.

(U) Traffic analysis is basically a very simple art if you are able to keep your mind loose so that you can recognize and exploit whatever the target gives you to work with. This is a fairly easy exercise intellectually, but it is much more difficult to structure your thought processes in order to design a machine processing system that will give you essentially the same versatility. Unfortunately, we have some managers and analysts who have produced processing systems and tried to make the target fit the processing

P.L. 86-36
EO 1.4.(c)

scheme, and I include in this category most of those procedures that were designed to replace a hand log kept by the analysts with a similar log prepared by the machine. The results were predictable. What we have now are logs prepared by machine that in many instances are inferior to those the analyst prepared by hand. And, without the benefit that accrued from working the traffic by hand, today's analyst has even less understanding of the data and may in fact be at a total loss to explain observed anomalies.

~~(C)~~ We can reverse this trend. We need to build on the good decisions we have made with regard to automating data processing for traffic analysis, and we must be willing to discard the bad decisions. What we really need to do now is to get on with developing an expert system that will process automatically all incoming traffic, compare what is observed to a dictionary of stated norms, and send appropriate alert messages to analysts and reporters on trouble spots.

(U) None of this should be difficult. Building and testing dictionaries will be tedious, but in the process of doing this, the analyst will be compelled to learn a great deal more about his cases than he now knows, and supervisors will be compelled to work with analysts to a much greater extent than is taking place now. When an expert-type system is in place and functional, one of the benefits will be that time will become available for a different and much more meaningful kind of on-the-job training.

~~(S-CCO)~~ We began exploring how to develop an expert system for processing just before I retired. I expect initial development to be slow, painful, and frustrating, but I do expect the system to "function as designed." What we must have to make it work is a sufficiently confident estimate of our analytic judgment and capabilities to tell the machine how to do *all* the dog work for us and then let it do the job. There can be no doubt as to our ability to make the right technical and reporting decisions based on the alert messages because each analyst must understand his responsibilities well enough to have described his case, net, and network norms to his analytic dictionaries.

(U) We will see vastly improved databases as a side benefit of this kind of processing. If the input data aren't good, the expert system is going to make noise; it will not permit any analyst to do a poor job on editing input data without sounding off.

(U) I am not persuaded that an expert system can be developed and implemented by evolution; probably the best (and certainly the quickest) way to effect such radical changes in the way traffic analysis is accomplished would be to select the right analysts and programmers, charge them with developing an expert system to do traffic analysis on a specific target, and set a deadline of perhaps a year hence for the initial job to be finished.

There should be no restrictions as to how the task is to be accomplished, and there should be no arbitrary limitations as to the techniques to be used (e.g., storage of norms for ordinary comparisons should not be made excessively difficult by the intricacies of an existing database).

(U) There is no question that the Agency will develop an expert system at some point in the future, if not for normal traffic analytic functions, then to provide rapid data evaluations for tactical support of military forces. I regret that I will not be here to see it.

(U) Here is the advice I promised earlier.

(U) Learn to be persuasive as well as informative in any presentation you make. The best ideas you have aren't worth much if you can't sell them. You cannot depend on decision makers to steer the right course because it is (or appears to you to be) the logical thing to do.

~~(FOUO)~~ Reporting the results of your analysis is part of your job. Learn what the intelligence requirements are for the target you are assigned and relate them directly and specifically to how you work your traffic. If you don't understand what it is that you are supposed to be getting out of the traffic and don't try to find out, you are still a logger, and that's all you're ever going to be.

(U) Avoid meetings. I am convinced that many people at the Agency really and truly believe that they are making progress as long as they are talking with each other regardless of whether anything is actually being done. I have attended some meetings where the only concrete thing accomplished was an agreement to meet again at some specified date in the future to discuss the same subject. And so help me, they all left happy.

(U) Don't take sinful pride in your own words. If the staff officer who reviews your message or report wants to change your words for his, don't be offended. Staff officers do serve a useful function. If you have treated them with respect in the past, they will often help you get out of trouble.

(U) I finished this article just as my NSA career came to an end. Reading it over, I find a line or two that may be mildly objectionable to one person or another. It was not my intention to offend anyone by my choice of words or by my comments, and if I have given offense, I apologize. This doesn't sound like me, but it does sound nice, and I think I'll leave it right there. Goodbye, good luck, God bless you all.

~~(S-CCO)~~ Upon joining the U.S. Navy (WAVES) in February 1943, Mrs. Filby trained in aerology at Lakehurst Naval Air Station. In the summer of 1944 she was stationed at the Naval Communications Annex (NCA), where she accepted an appointment as a civilian in May 1946 and served as an analyst, translator, reporter, and staff product and technical editor in the weather branch until 1958. This period included a tour with the [redacted] (1953–55). From 1958 until 1964, Mrs. Filby served as an analyst, cryptolinguist, and reporter in Soviet naval and merchant shipping problems. This period included assignment to the Military Cryptanalytics course (taught by Lambros Callimahos), a year-long Advanced Intensive Russian course, and the pilot SIGINT reporting course at the National Cryptologic School (NCS). She was instructor and developer of the NCS SIGINT reporting course (1964–83), organizer of a two-day seminar on SIGINT reporting including Second Parties (1978), and designer of the first SIGINT reporting course for the field (1982). Mrs. Filby was chief of the Intelligence Skills Division, Intelligence and Analysis Department (E4) at the National Cryptologic School (1983–86). She continued teaching and presented the field SIGINT reporting course in [redacted] In 1986 she was assigned as special assistant to the Dean, E4. She studied the status of SIGINT reporting throughout the Agency; developed a course on the National SIGINT Operations Center; and developed and managed seminars on SIGINT Users, Support to Military Operations, and Current Issues in SIGINT Reporting. In July 1991, Mrs. Filby was assigned to the Center for Cryptologic History. She has been president of the Crypto-Linguistic Association (1975-1976) and has received several awards: NCS Teacher of the Year (1970); the Meritorious Civilian Service Award (1972); and the CIA Sherman Kent Award for the most outstanding contribution to the literature of intelligence (first NSA winner, 1983).

FPLL 8663866
EO 1144(a)
EO 1144(d)

P.L. 86-36

SOURCES

[redacted] "How Many Angels Can Stand on the Head of a Case Notation?" *KEYWORD*, November 1972, 4.

Benjamin, Robert S. "Some Thoughts Concerning Traffic Analysis Mechanization." *NSA Technical Journal*, 1966, 97–101.

_____. "Introduction to Traffic Analysis Mechanization." Traffic Analysis Mechanization Forum, February 1971, Ref. S # 194,544, 4–22.

[redacted] "Applications of Set Theory to Traffic Analysis." Traffic Analysis-Mathematics Symposium, May 1973, Ref. S # 208,891, 202–205.

Bjorklund, Kathy. Letter on reassimilation of traffic analysts. *Cryptolog*, June 1979, 17.

[redacted] Letter on personnel assignments. *Cryptolog*, July 1979, 14–15.

Buckley, Dan. Letter on TA overages. *Cryptolog*, July 1979, 14.

[redacted] "Traffic Analysis on [redacted] Data Transmission Systems." *COMMAND*, October 1968.

[redacted] "Area Studies and Their Place in Traffic Analysis." *COMMAND*, October 1968, 14–16.

Delaney, James D. [redacted] *NSA Technical Journal*, Fall 1971, 91–106.

P.L. 86-36
E.O. 1144(g)

[redacted] *COMMAND*, March 1971, 31–52.

[redacted] "TA, CA, LOGIC, MATH – Where Do They Intersect? (TACALOMA)." Traffic Analysis-Mathematics Symposium, May 1973, Ref. S # 208, 891, 226–246.

_____. "Simplicity in Color." *Cryptolog*, February 1982, 24–25. (with title "Gary's Colors," *Cryptolog*, September 1974; *COMMAND*, October 1971.)

Gilbert, Allen L. "The Impact of ARDF on Traffic Analysis." *DRAGON SEEDS*, December 1971, 7–8.

[redacted] "Maybe It's Related to the Phases of the Moon." *DRAGON SEEDS*, June 1972, 5–12.

Hanyok, Robert J. Letter on TA career field. *Cryptolog*, May, 1985, 10.

Hooper, James P. "Traffic Analysis: A Current Perspective." *Cryptolog*, June 1984, 1–4.

P.L. 86-36
EO 1.4.(c)

[redacted] ~~(S-CCO)~~. *Cryptologic Quarterly*, Spring 1991, 87–105

[redacted] "Traffic Analysis: Write it Down Now." *COMMAND*, February 1974, 31.

P.L. 86-36

Jollensten, Ralph E. "The Lost Indicator." Traffic Analysis-Mathematics Symposium, May 1973, Ref. S # 208,991, 106–116.

[redacted] "Traffic Analysis: Specialty Without Portfolio." *Cryptolog*, April–June 1981, 15–18.

Mason, Fred. "Cleaning the Augean Stables or How Much TA Can a Computer Do?" *NSA Technical Journal*, Summer 1968, 119–127.

_____. Letter on data queries. *COMMAND*, March 1969, 25.

_____. Letter on human confirmation of computer data. *COMMAND*, August 1970, 41.

Morrison, John E. Opening address, Traffic Analysis Mechanization Forum. February 1971, Ref. S # 194,544, 1–2.

Murphy, Tim. "Automation of a TA Process." *Cryptolog*, October 1975, 33–35.

[redacted] "Let's Not Lose Our TA Skills." *Cryptolog*, March 1979, 11–12.

_____. "There's a New World Coming – Are You Ready?" *Cryptolog*, January–March 1980, 1–2.

[redacted] "Traffic Analysis of the Future." *COMMAND*, October, 1968, 12–13.

_____. Letter on use of computers. *COMMAND*, August 1970, 40.

[redacted] "The Reality of Communications Changes." *DRAGON SEEDS*, June 1972, 13–16.

[redacted] "In Pursuit of Faster Horses, Younger Women, Old Whiskey, and More Money." *Cryptolog*, December 1981, 16–18.

[redacted] "Establishing Communications Norms." *COMMAND*, August 1969, 18–22.

Shaw, R. H. "What Good is Traffic Analysis?" *NSA Technical Journal*, Fall 1979, 68–73; from P1 Informal No. 10.

[redacted] Letter on TA overage. *Cryptolog*, August–September 1979, 17–18.

Starr, Joseph. "Valedictory of a Traffic Analyst." *Cryptolog*, June–August 1985, 9–10.

Stoffel, Wayne E. "Chatter Patterns: A Last Resort." *NSA Technical Journal*, October 1957, 63–75.

[redacted] "A Note About NR's." *COMMAND*, August 1969, 11–12. [redacted]

[redacted] "Recovery of a Vietnamese Communist Callsign System." *DRAGON SEEDS*, December 1971, 5–6.

[redacted] "A Note About Organizing T/A Problems." *COMMAND*, March 1974.

[redacted] "How Clean Does a Data Base Need to Be?" *Cryptolog*, January 1975.

[redacted] "Computerizing Traffic Analysis." *Cryptolog*, May 1983, 36–43.

[redacted] "The Hand Is Not Quicker than the Eye." *Cryptolog*, March, 1978, 9.

[redacted] *Cryptolog*, September 1978, 9. [redacted]

[redacted] "True Base: Two Tales." *Cryptolog*, May 1982, 15–19.

[redacted] "The Future of Traffic Analysis." *Cryptolog*, May 1983, 9–10.

P.L. 86-36

ADDITIONAL ARTICLES ON TRAFFIC ANALYSIS IN NSA SOURCES

[redacted] "Model 204 – The Analyst's Computer." *NSA Technical Journal*, Summer 1976, 65–75.

Benjamin, Robert S. "Overview of Mathematics Support to Traffic Analysis." Traffic Analysis-Mathematics Symposium, May 1973, Ref. S # 208,891, 3–17.

[redacted] " The Origination and Evolution of Radio Traffic Analysis, the World War I Era." *Cryptologic Quarterly*, Spring 1987.

_____. "The Origination and Evolution of Radio Traffic Analysis, the Period between the Wars." *Cryptologic Quarterly*, Fall–Winter 1987–88.

_____. "The Origination and Evolution of Radio Traffic Analysis, World War II." *Cryptologic Quarterly*, Winter 1989.

Cahill, Robert. ". . .Be Considered a Single Field?" *KEYWORD*, July 1973, 5.

Chiles, Gloria. "TA Draw." *COMMAND*, March 1971, 23–26.

Callimahos, Lambros D. "Introduction to Traffic Analysis." *NSA Technical Journal*, April 1958, 1–11.

P.L. 86-36
EO 1.4.(c)

[redacted] "The Cryptography of [redacted] Traffic Analysis-Mathematics Symposium, May 1973, Ref. S # 208,891, 59–71.

[redacted] "The Basic Probability Concepts and Their Applications to Traffic Analysis." unpublished article in TA library collection.

Dale, D. E. Letter on intelligence reporting. *COMMAND*, March 1971, 53.

[redacted] "Computer Aided Traffic Analysis in [redacted] Division." *Cryptolog*, October–November 1986, 1–8.

P.L. 86-36
EO 1.4.(c)
EO 1.4.(d)

Donym, Sue. "Second Sighting." *Cryptolog*, January 1979, 12.

[redacted] "Squares." Traffic Analysis-Mathematics Symposium, May 1973, Ref. S # 208,891, 93–104.

Gilbert, Allen L. "Mechanization for T/A Development." *DRAGON SEEDS*, September 1972, 14–15.

[redacted] "How the Traffic Analyst Can Help Others." unpublished article in TA library collection.

"The GOLD NUGGET Award for Excellence in Traffic Analysis." *Cryptologic Quarterly*, Winter 1989, xv–xviii.

[redacted] "Is There a Doctor in the House?" *Cryptolog*, September 1977, 9–10.

[redacted] "Can Traffic Analysis and Special Research....." *KEYWORD*, July 1973, 4.

[redacted] Jackson, William J. "TA Management Information System." Traffic Analysis Mechanization Forum, February 1971, Ref. S # 194,544, 213–224.

Jackson, William J. "TDB: The TEXTA Data Base." *Cryptolog*, August 1974, 4.

_____. "An Approach to Callsign Analysis." *Cryptolog*, December 1974, 7.

[redacted] "Net Reconstruction – A Basic Step in Traffic Analysis." *NSA Technical Journal*, July 1958, 31–45.

[redacted] "Collection-Support TA Is Not for Everyone." *Cryptolog*, February 1978, 7–8.

[redacted] "Go-Go Traffic Analysis." *COMMAND*, October 1968, 10–11.

[redacted] "AG-22: Where Do We Go Now?" *DRAGON SEEDS*, December 1972, 22–23.

[redacted] "Use of Displays in Traffic Analysis." Traffic Analysis Mechanization Forum, February 1971, Ref. S # 194,544, 72–82.

[redacted] "Collection Data Services Support to TA." Traffic Analysis Mechanization Forum, February 1971, Ref. S # 194,544, 40–46.

[redacted] "The Desk Analyst's Math." Traffic Analysis-Mathematics Symposium, May 1973, Ref. S # 208,891, 49–58.

[redacted] "TA Continuity." *COMMAND*, March 1969, 14–24.

_____. "Where Are You Going and How Do You Know?" *COMMAND*, August 1970, 35–39.

_____. Letter on intelligence in TA technical data, *COMMAND*, August 1970, 42.

_____. "Normal Reporting." *COMMAND*, March 1971, 28–30.

_____. Letter responding to comment on reporting. *COMMAND*, March 1971, 53.

_____. "Some Notes on TA Management." *COMMAND*, October 1971, 32–35.

_____. "After Continuity, What?" Traffic Analysis-Mathematics Symposium, May 1973, Ref. S # 208,891, 18–21.

_____. "Traffic Analysis of the Future." *Cryptolog*, June 1979, 10.

_____. TEXTA: What Is It? Where Is It Going?" *Cryptolog*, December 1981, 19–25.

Taylor, James W. "Traffic Analysis of the Present." *COMMAND*, August 1969, 13–15.

_____. "Traffic Analysis Processing System (TAPS)." Traffic Analysis Mechanization Forum, February 1971. Ref 194,544, 235–238.

Tiren, David J. "T/A Math Symposium Reviewed." *DRAGON SEEDS*, December 1972, 34–39.

[redacted] "NSA Traffic Analysis Overseas." unpublished article in TA library collection.

[redacted] "Practical Traffic Analysis from the Viewpoint of the Theory of Knowledge." manuscript in TA library collection.

This Page Is Intentionally Left Blank

Directorate of Intelligence

A Compendium of Analytic Tradecraft Notes

Volume I
(Notes 1-10)

Reprinted with a new Foreword by the Deputy Director for Intelligence

February 1997

Directorate of Intelligence

A Compendium of Analytic Tradecraft Notes

Volume I
(Notes 1-10)

Reprinted with a new Foreword by the Deputy Director for Intelligence

February 1997

Reverse Blank

Contents

		Page
Foreword		v
Summary		vii
Note 1	Addressing US Interests in DI Assessments	1
Note 2	Access and Credibility	5
Note 3	Articulation of Assumptions	9
Note 4	Outlook	13
Note 5	Facts and Sourcing	17
Note 6	Analytic Expertise	25
Note 7	Effective Summary	29
Note 8	Implementation Analysis	33
Note 9	Conclusions	37
Note 10	Tradecraft and Counterintelligence	41

A Compendium of Analytic Tradecraft Notes

Foreword by the Deputy Director for Intelligence

The core mission of the CIA's Directorate of Intelligence, which I head, has remained the same despite a decade rocked by profound changes in the world. As the analytical arm of the CIA, we seek to provide the most useful, high-quality analysis to US policymakers, lawmakers, warfighters, law enforcement officers, negotiators, and other officials responsible for protecting US national interests. Our analysis continues to draw from a wide range of sources—from newspapers to the most sensitive technical collection systems.

How we fulfill our mission, however, has changed dramatically. Intelligence analysts are challenged as never before to be creative and proactive in meeting intelligence needs. Long analytic papers largely focused on the Soviet threat worldwide that were the norm 10 years ago have given way to a combination of briefings and short but insightful written and multimedia products covering a broad range of regional and transnational issues.

Now more than ever, new products are tailored to the individual intelligence consumer's concerns. Our analysts put the highest premium on knowing what their consumers need.

The revolution in information technologies has improved our access to sources and our ability to quickly deliver intelligence. But it has also made our work more challenging as we are bombarded with information of varying quality, relevance, and depth.

To meet the challenge of political change and technological advances and take advantage of the opportunities they present, the Directorate of Intelligence has reexamined its core analytic "tradecraft" skills, updating them to reflect how we do our business. The word "tradecraft" comes from our colleagues in the clandestine service, who use it to embody the special skills and methods required to do their business. We have borrowed it to capture our special skills and methods.

We are making the *Compendium of Analytic Tradecraft Notes* available to scholars to shed light on how we support intelligence consumers. This release, although unusual for an intelligence agency, reflects our renewed commitment to reach out to academia and the public, as defined in the Directorate's new Strategic Plan.

Pursuit of expertise in analytic tradecraft is a central element of this plan. Our tradecraft enables analysts to provide "value-added" to consumers of intelligence by ensuring:

- Dedication to objectivity—tough-minded evaluation of information and explicit defense of judgments—which enhances our credibility with consumers dealing with complex and sensitive policy issues.

- Delivery of our products to the right people in time to be useful in their decisionmaking, and using feedback and tasking from them to drive the collection of the basic intelligence that we need to produce our analysis.

Analytic tradecraft skills also serve as "force multipliers," helping us provide top-quality analysis:

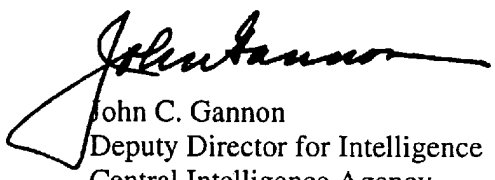
- The feedback our customers give us on our customized analysis clarifies for the analyst what questions most need answering.

- Employing rules for evaluating information and making judgments helps analysts manage the deluge of information, discern trends, and identify attempts at deception.

- Tradecraft standards can be used to iron out differences among experts who have complementary substantive specialties. Their interaction enhances teamwork, which allows the DI to be more productive.

The author of the *Tradecraft Notes* is Jack Davis, a retired CIA officer who has spent 40 years as practitioner, teacher, and critic of intelligence analysis. The *Notes* benefited from the foresight and sharp editorial pen of F. Douglas Whitehouse, Chief of the Directorate's Product Evaluation Staff, during 1994-96. Above all, they reflect the strong commitment to raising analytic standards begun by my predecessor, Douglas E. MacEachin, who served during 1993-95.

Requests for additional copies of *Tradecraft Notes* or copies of the Strategic Plan should be addressed to my Communications Chief, Jon Nowick, on (703) 874-3882. I also welcome your comments on this volume as my colleagues and I work to enhance the way we serve our nation.



John C. Gannon
Deputy Director for Intelligence
Central Intelligence Agency

Summary

Below is a brief characterization of each of the 10 Tradecraft Notes presented in this volume.

Note 1. Addressing US Interests in DI Assessments
PES launched the tradecraft series with a note on the various ways analysts can assure value added for their important clients in the world of policymakers, warfighters, and law enforcement officials:

- One tradecraft tip recommends converting general substantive issues into specific questions that key officials might raise in their preparations to decide on policy action.

- Analysts are encouraged either to organize their assessment around these questions or to make sure in some other way that the operational concerns of policy officials are well covered.

Note 2. Access and Credibility
Demonstrates how the nine evaluation criteria used by PES work together to enhance access to and credibility with the US officials who count most on the analyst's substantive agenda:

- The first challenge is to convince key consumers that the DI assessment is targeted to their concerns. Thus, the importance, for example, of *Addressing US Interests*, providing an *Effective Summary*, and assuring *Effective Use of Unique Intelligence*.

- The second challenge is to maintain credibility in an environment of uncertainty overseas and policy competition in Washington. Thus, the importance of rigorous attention to *Facts and Sourcing* and explicit *Articulation of Assumptions*.

Note 3. Articulation of Assumptions
US officials who must make their policy decisions amidst uncertainty about developments abroad are more likely to rely on DI assessments when the assumptions supporting the analysts' estimative judgments are made clear.

Tradecraft tips cover techniques for:

- Identification, challenge, and defense of *drivers* (key variables) and *linchpins* (assumption about the drivers) before analysts start to draft an assessment.

- Presenting the argumentation in textboxes, for example, when it is not appropriate to belabor the text with details that explicate the critical thinking underlying key judgments.

Note 4. Outlook
The outlook sections of DI assessments must address not only what analysts believe to be the most likely course of developments but also important alternative outcomes that could confront US officials:

- On issues vital to US security such as the military intentions of adversaries, analysts must help policymakers and warfighters engage in contingency planning by addressing alternative courses of developments, including plausible challenges that analysts believe are remote possibilities.

Note 5. Facts and Sourcing
What the analysts know and *how they know it* are central to their credibility not only with policy officials asked to rely on DI assessments for designing and taking action, but also with the managers who are asked to place the Directorate's authority behind the memorandum or briefing.

The two evaluation standards at play here—the handling of facts and of sourcing—were combined in one note that sets out guidelines for analysts and illustrates "best practices" for explicit and tough-minded depiction of information derived from reporting and research. For example:

- Be precise about what is known.

- Distinguish between reported information and analyst judgment.

- Take account of the possibility of deception.

Note 6. Analytic Expertise
Analytic expertise establishes the DI's authority to speak to an issue on which US national security interests are at stake. This note addresses the several facets of analytic expertise and provides tradecraft tips for effectively conveying authority in DI assessments.

The aspects covered include:

- In-depth substantive knowledge that clarifies complex issues.

- Skill in interpreting unique intelligence information.

- Deft organization of data in support of findings and judgments.

- Insight into the decisionmaking processes of US officials.

Note 7. Effective Summary
An effective summary makes the distinctive DI value added stand out for the intended consumers within constricted space limitations. For example:

- When the clients for a DI assessment are few in number and their priority interests regarding the issue at hand are well known, the analyst's job is to craft a summary that presents in a couple of lines of text the *what's new* and the *so what.*

- When an assessment is broadcast to a larger and more diffuse audience, to assure requisite attention, the summary has to convey evidence of the DI's distinctive expertise as well as key findings and judgments.

Note 8. Implementation Analysis
Implementation Analysis is one of the techniques for extending customized intelligence support to policymakers and action takers outlined in Note 1, *Addressing US Interests.* When the DI provides an assessment of tactical alternatives available to the United States for pursuing opportunities and averting dangers, the role of the analyst complements but is distinctive from the role of the policymaker:

Analysts—calling upon their expertise on foreign cultures—identify and evaluate alternatives for implementing objectives.

Policy officials first set the objectives and then make decisions about which tactics to adopt.

Note 9. Conclusions
Analysts must be precise in conveying their level of confidence in the conclusions of a DI assessment; that is, their findings based on organizing, evaluating, and interpreting all-source information:

- When analysts believe they have made their case after a careful scrubbing of ample information, they should state their conclusions boldly (regarding, for example, what has *increased, decreased,* or *taken on a pattern*).

- In contrast, when available information is susceptible to foreign deception operations and other sources of ambiguity, the analysts' reasonable doubts (for example, about *cause-and-effect relationships*) must be shared with the officials who may rely on DI assessments in taking policy action.

Note 10. Tradecraft and Counterintelligence
Guidelines for countering deception efforts to distort analysts' understanding of what is going on abroad build on the advice for rigorous evaluation of information contained in Notes 5 (*Facts and Sourcing*) and 9 (*Conclusions*).

For issues where analysts suspect the presence of deception and for all assessments on which policy officials may directly rely in making decisions on whether to take military or other action to defend US interests, we recommend a structured effort to validate the integrity of key information.

On these *suspect and sensitive issues*, we urge analysts to answer a blunt question:

- *How do you know you are not being deceived?*

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

March 1995

Note 1

Addressing US Interests in DI Assessments

This is the first of a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

The DI professional ethic requires that analysts provide direct support to policymakers' efforts to define and defend US national security interests. The standard is for DI products to convey distinctive value added that promotes feedback, tasking, and access generally. In many cases, this standard requires going beyond general relevance to US interests to customized assistance for identified policy officials who have the "action" on designing, implementing, or monitoring US policy on an individual issue.

The ultimate judges of the utility of DI products for the policymaking process are the officials who choose whether or not to rely on them. The opportunities for adding distinctive intelligence values are usually clear to DI analysts when policy officials ask for a study, memorandum, or briefing. These officials indicate what they expect to gain from their request: for example, specialized information, research findings, cause-and-effect analysis; cost-benefit assessment of tactical alternatives.

The challenge to address effectively US interests is greater when the initiative for launching a DI product comes largely from the intelligence side of the relationship. It is here that Agency monitors (such as the staffs of the congressional oversight committees) are most likely to raise questions about the policymaking utility of individual DI products.

How to proceed? Each analytic assignment represents a distinctive opportunity for providing support to policy officials and the policymaking process. That said, veteran analysts and managers have garnered from direct experience and feedback from policy officials that DI products are usually best directed to meet the needs of the user when they are either organized around or specifically highlight one or more of the following values:

- Opportunities and dangers for US interests, especially unexpected developments that may require a US reaction.
- Motives, objectives, strengths, and vulnerabilities of adversaries, allies, and other actors.
- Direct and indirect sources of US leverage on foreign players and issues.
- Tactical alternatives for advancing stated US policy goals.

Veteran analysts and managers also recommend the following *Tradecraft Tips* for increasing the utility of DI assessments for policymakers.

Getting Started

- *Think of the analyst's role as that of the objective or tough-minded expert for a policymaking team.* Much of the time, hands-on policy officials know the "story" or general pattern of events overseas regarding their priority accounts. What they need most from the intelligence analyst is organized information, including specialized intelligence, that clarifies the goals and motives as well as the strengths and weaknesses of adversaries, allies, and other foreign players.
- *Recognize that research and reporting are inputs or means to an end.* The output is customized support to help policy officials get their jobs done—usually planning for, taking, or monitoring an action. The goal is to convert substantive expertise into action-support analysis before conveying it to consumers.
- *Put a face as well as a name on the five to 10 policy officials who are the core customers on a country or functional account.* Analysts should study what these officials have written or said on important substantive issues and debrief policy staffers who work for core consumers, as well as anyone on the intelligence side of the river who knows their professional habits. The goal is to learn how key officials absorb information and reach judgments, as well as their current priority interests.

- *Target the policymakers' specific interest in a substantive issue.* To identify lines of analysis that provide value added, analysts should think through what they would want to know *if they were policymakers charged with leveraging an issue.* That done, in drafting an assessment or outlining a briefing, the analysts bring to bear the DI's collective substantive expertise, distinctive collection resources, and rigorous analytic tradecraft.

- *Be aware that consumers' needs may change as the policymaking process evolves.* Policy officials often are receptive to broad analytic treatments when an issue first emerges and they are in their long-range planning or goal-setting phase. But once the lines of US policy are set, their focus shifts to specifics about vulnerabilities, leverage, and other facets of policy implementation.

Special Tradecraft Challenges

- *Support the policymaking process without engaging in policymaking per se.* The "if, then" approach can facilitate close policy support without crossing the line to policy prescription. *If* the US policy goal is to get from A to B, *then* the analysts' research findings, all-source collection, and general expertise indicate the following opportunities for moving forward and dangers to be avoided.

- *Long-shot threats and opportunities.* Policy officials often have a strong interest in low-probability, high-impact dangers and objectives. DI analysis in support of policymaking in these circumstances should provide expert, tough-minded assessments that concentrate, not on *whether* an event is likely, but on *how* and *why* it might come about, including the leverage the United States has for constricting dangers and enhancing opportunities.

- *Pointing is not choosing.* Policy-support analysis at times requires the analyst to identify and clarify the vulnerabilities of adversaries and the sources of US leverage over allies and third parties as well as enemies. The responsibility and risk of choosing what actions to take remains with the policymaker.

- *The timeliness challenge.* When policy officials are engaged in managing day-to-day crises, they will use whatever information is available to them when a decision point comes. Rarely will they wait for intelligence analysis. To provide utility, intelligence updates and other analytic support must be delivered in time to meet decision and action deadlines.

Drafting and Self Review

- *Convert issues into questions.* One way to assure utility for policymakers is to organize an analytic effort around the known or presumed questions of key officials on the account. Whenever appropriate, use the questions as section headings, or otherwise make sure that the sections address the identified operational concerns of hands-on policy officials.

- *Use the "so-what" test.* In reviewing a first draft, analysts should evaluate the sections of the paper from the intended customers' point of view and ask—*so what?* Does the draft address specifically and effectively what key policymakers need to know to get *their* jobs done?

- *Or use the "action-support" test.* As an alternative test of the policy utility of a draft, analysts can list the five or so matters they personally would like to see clarified if they were directly responsible for managing US policy action. Next to each entry, list the paragraphs of the draft that provide *actionable* information or insight. Adjust the draft if key identified concerns are not addressed or if too many of the paragraphs are not directly related to specific concerns.

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

April 1995

Note 2

Access and Credibility

This is the second in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

The goal of enhancing the policy utility and analytic quality of DI papers and briefings is centered on efforts to promote analysts' access to and credibility with the US officials who count most in policymaking, warfighting, and law enforcement:

- The quest for access—and with it guidance, tasking, and feedback—is driven by the DI's determination to produce analysis for people, not publications.

- Commitment to credibility reflects the core professional value of presenting objective analysis to officials who often have a range of conflicting information and views on complex issues.

The two standards are complementary. Without credibility, analysts will lose their access to the hands-on policy and operational officials who need sound and reliable intelligence analysis to succeed in their professional missions. Without access, even unquestionably objective assessments do little to promote the effective use of intelligence by consumers.

As indicated below, the nine standards the Product Evaluation Staff uses to evaluate DI analytic performance reflect the importance of increasing access and protecting credibility:

- The first challenge for analysts is to make clear to key officials *what's in it for them* when asked to commit their most precious commodity—their time—to read or listen to a DI assessment. Thus, the need for analysts to address US interests effectively, provide value added via substantive expertise and special information, and summarize key points efficiently.

- The second challenge is to help key officials succeed in promoting US objectives by producing assessments that can be relied on for sound treatment of evidence, inference, and judgment.

Increasing Access

Addressing US Interests. The most important and demanding charge given to DI analysts is to assist US officials to fulfill their obligation to design, implement, and monitor national security policy. The highest standard is to structure DI assessments to underscore what officials need to know to get their jobs done (for example, about vulnerabilities and strengths of adversaries). When this is not practical, DI deliverables should contain a carefully crafted section that addresses implications, dangers, and opportunities with the role of US policymakers, warfighters, and law enforcement officials as *action officers* clearly in mind.

Sophistication of the Analysis/Depth of Research. Especially in broadly distributed and fully developed assessments, analysts have to convey their distinctive expertise on an issue. This demonstration of authority to speak to the issue should be based on some combination of research methodology, firsthand knowledge of country or subject, all-source data bases, closeness to collectors, and clear articulation of facts and assumptions—attributes that make a busy policymaker want to come back to the analyst for additional information and analysis.

Unique Intelligence Information. Especially in quick turnaround deliverables for small numbers of key officials, the analyst should make appropriate use of unique, at times highly classified, information that provides insights not otherwise available to well-informed officials. Policymakers and warfighters who have the action on key issues almost always have the clearances as well. At times they need assistance, however, in understanding the context and character of intelligence from clandestine collection and other special sources.

Effective Summary. The analyst's charge is to convey the distinctive values of the paper in the prescribed space. To maximize service to heavily engaged officials, the most important findings and judgments should be highlighted within a bare-bones depiction of the general context. Even more than in the main text, the summary should be made "actionable" via emphasis on US policy implications.

Maintaining Credibility

The Facts—Or What We Know. With emphasis on what is new, different, attention-worthy, a DI assessment should set out what the Directorate knows with sufficient confidence to warrant reliance by policymakers and warfighters in planning and executing US courses of action. When relevant, DI deliverables should also address what analysts do not know that could have significant consequences for the issue under consideration. If the paper notes intelligence gaps, it should, when appropriate, suggest collection strategies to fill the gaps.

Sources of the Facts—How We Know It. DI assessments have to depict the sources of information on which consumers are asked to rely within the general rules for using evidence. Direct evidence (for example, imagery and most intercepts) should be distinguished from testimonial evidence (for example, most clandestine and embassy reporting). On complex matters (for example, the attitudes and plans of foreign leaders) analysts should make explicit their levels of confidence in the evidence.

Conclusions. Assessments should enunciate the conclusory findings from the hard evidence (for example, well-documented events) in terms of trends, patterns, and precedents that underscore dangers or opportunities for US policymakers, warfighters, and law enforcement officials. When appropriate, the calculus that leads to the extension of the factual base to an actionable finding should be spelled out (for example, rules used to establish degrees of risk in dual-purpose technological transfers).

Clear Articulation of Assumptions. When analysts address uncertainty—matters that require interpretations and estimates that go well beyond the hard evidence—their argumentation must clarify the premises, suppositions, and other elements of critical thinking that underlie the judgments. For example, effective argumentation for consumers, who will often have their own strong opinions, requires the analyst to clarify not only degree of confidence in key assumptions but also the criticality of the latter to bottom-line judgments.

Outlook. The outlook sections of estimative assessments (for example, the likely course and impact of political, economic, and military developments in foreign countries) should identify the dynamics that will have the greatest impact on subsequent developments. In other words, what are the drivers that will determine the outcome, or what drivers would have to change to alter the outcome?

- The analyst's judgment on the most likely outcomes must follow clearly from the marshaling of evidence and articulation of assumptions.

- When the US stake is high and plausible alternative outcomes are judged to be in the range of, say, 20 percent or greater, outlook sections should also identify the factors at play that could lead to unexpected developments, signposts of change, and events that could trigger a major shift in direction (for example, assassination of a leader).

- On issues vital to US security (for example, military intentions of adversaries), analysts must help policymakers and warfighters engage in contingency planning by (1) addressing all factors at play that could influence subsequent events, (2) ranking their relative importance, and (3) relating them to a range of plausible outcomes, including alternatives analysts deem to be remote possibilities.

Reverse Blank

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

May 1995

Note 3

Articulation of Assumptions

This is the third in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

DI analysts are regularly tasked to assist policymakers, warfighters, and law enforcement officers in *managing the uncertainty* that complicates US efforts to deal with national security threats and opportunities. Many issues cannot be addressed with certainty—by analysts, by policy officials, or even by the foreign players involved. The pattern of political and economic developments in, say, a newly democratic country can depend on so many actors, institutional variables, and contingencies that the outlook cannot be predicted with high confidence. Estimating over an extended timeline or during a period of political or economic crisis increases the burden of uncertainty.

As a rule, the greater the degree of uncertainty attending an issue:

- The greater the analysts' reliance on judgment rather than evidence; thus the greater the likelihood of estimative error.
- The larger the prospect for divergent views about the outlook among analysts and concerned policy officials.
- The greater the need for sound reasoning and precise argumentation to align facts, assumptions, and judgments.

This tradecraft note on *Articulation of Assumptions* and the next note on *Outlook* will address the DI tradecraft for argumentation that sets the standard for helping consumers deal effectively with the uncertainty they face in planning for, taking, and monitoring US action.

By "argumentation" we mean the communication in an intelligence assessment of the structure of the analysts' critical thinking in support of the bottom-line judgments. Under the DI tradecraft standard, when policymakers, warfighters, and law enforcement officials are asked to rely on DI analysis, the reasoning that ties evidence, to assumption, to judgments must be:

- *Logical*—soundly reasoned.

- *Precise*—clearly stated.

- *Realistic*—attuned to the hazards of forecasting error.

Drivers and Linchpins

The DI tradecraft for the articulation of assumptions places emphasis on identifying the *drivers* or key variables—the uncertain factors that analysts judge most likely to determine the outcome of a complex situation. At times the economy is the key uncertain factor; at times the loyalty of the security forces; at times the leadership skills of a president or dictator. At times all three are judged to carry equal weight in driving future developments.

The analysts' working assumptions about the drivers are sometimes referred to as *linchpin assumptions* because these are the premises that hold the argument together and warrant the validity of the conclusion.

The following are hypothetical examples to illustrate the relationships of drivers, linchpin assumptions, and conclusions:

- The loyalty of the military is the key factor in determining Egyptian stability in the short term. The military probably will continue supporting the government. Therefore, the government is unlikely to be seriously threatened by opposition forces over the next year.

- Castro's skill in handling recurring antiregime incidents will largely determine the Cuban regime's staying power over the next several months. He probably will continue to diffuse antiregime pressures with a mix of carrots and sticks. Thus, a serious threat to regime stability is unlikely.

Linchpin assumptions are by definition debatable and subject to error. Thus, analysts must defend their judgments by marshaling supporting evidence and reasoning. For instance, in the Egyptian example, the analysts should offer convincing evidence for the assumption that "the military probably will continue supporting the government."

Moreover, on an important issue such as this, the inherent uncertainty has to be accounted for by addressing plausible alternative courses of development, a topic that will be covered in the Tradecraft Note on "Outlook." Here we present recommendations for refining and articulating the assumptions that support the analysts' bottom-line conclusions.

Tradecraft Tips

1. Each assessment represents a distinctive challenge in terms of how to set out the argumentation. As a rule of thumb, the more complex and controversial the issue, the more the analysts should make clear the sinews of the reasoning:

- For some papers, the assumptions can be adequately articulated in the course of the text.
- For others, a textbox may be needed to clarify the causal relationships.
- At times, the entire assessment should be organized to march step-by-step through the critical thinking.

2. Before starting to draft an assessment, analysts should open up the search for drivers, and not rely solely on what was determined to be the key factors in the last exercise. That is, they should put aside their previous conclusions and focus initially on the range and alignment of assumptions:

- For example, generate a list of all the important variables—factors that cannot be known with certainty that are palpably affecting the issue under study.
- Assess the relationships among these variables—search for hierarchies of importance and other linkages.
- At times, with the help of colleagues acting as *devil's advocates*, construct competing cases for selecting the drivers from among the host of variables.
- A useful question to ask to isolate the key variables is: *What factors would have to change to change your mind about the expected outcome?*

3. Also, analysts should open up the process of determining assumptions about the drivers:

- Before settling on the linchpin assumptions that will serve to underwrite the conclusions, assess the quality of the evidence. One test: How likely is new information to change your judgment of what is probable?
- Again with the help of colleagues, test the soundness of the supporting line of reasoning (the articulation of subordinate assumptions) that leads to the linchpin assumptions:

  —In the Egyptian example, the subordinate assumptions to the linchpin assumption that the military probably will continue to support the government could include judgments about the military's stake in secular government and antagonism toward the Islamic extremists.

- Also test key assumptions against any contrary judgments held by other informed observers. What hard evidence and inferential reasoning, for example, lead them to alternative interpretations?

4. Analysts should review their first draft against a tough standard:

- Could a consumer who was not reading all the traffic quickly identify and summarize the essential elements of the assessment's reasoning?

5. Some specific questions analysts should ask about the draft:

- Does the depicted hard evidence adequately explain the linchpin assumptions?

- Do the assumptions in turn adequately defend the bottom-line conclusions?

In Sum

DI analysts can speak with authority on substantively complex and politically controversial issues only through sound and precise argumentation. The more effectively drivers and assumptions are identified and defended, the greater the credibility of the bottom-line conclusions.

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

June 1995

Note 4

Outlook

This is the fourth in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

This Note on *Outlook* continues coverage of DI standards for helping policymakers, warfighters, and law enforcers manage uncertainty regarding threats to and opportunities for US security interests. (Please see Note 3, *Articulation of Assumptions.)*

The outlook sections of DI assessments must address not only what analysts believe to be the most likely course of development but also important alternative outcomes that could confront US officials. *This concern for the unlikely or unexpected* reflects an experience-based appreciation of (1) the fallibility of analytic judgment, (2) the special analytic requirements of US officials for addressing long-shot threats and opportunities, and (3) the adversarial character of the policymaking process.

The perils of analytic judgment include:

- Limitations in the evidence and in the analysts' understanding of complex issues that can lead to judgments structured around either the wrong drivers (key variables) or incorrect linchpin assumptions.

- The impact of essentially unpredictable events on sound analytic judgments; for example, changes in political stability caused by assassination of a president or the sudden advent of a charismatic opposition leader.

Policymakers and other consumers who carry the burden of executing US policy often have a different attitude than analysts toward unlikely events.

- Officials who are charged with advancing a long-shot objective may probably see a 20 percent likelihood of success as promising opening odds for arranging a negotiated settlement of a longstanding civil war or diverting an entrenched nuclear weapons program.

- Officials also require an understanding of unlikely developments to prepare contingency plans against low-probability, high-impact dangers (such as protecting Persian Gulf oil suppliers from another Iraqi military attack on Kuwait or an Iranian blockade of the Straits of Hormuz).

Finally, the outlook on important issues can be subject to deep-seated disagreements—among and between analysts, Administration officials, and congressmen—that generate suspicions about the objectivity of DI memoranda and briefings.

- At such times, DI credibility can depend more on explanation of why the outlook—for example, for Cuba after Castro or for Russia after the next election—cannot be predicted with high confidence than in an attempt to trivialize uncertainty by "just making the call."

General Rules

As indicated in previous Tradecraft Notes, each DI assessment represents a distinctive challenge to analysts on how to assure credibility with the consumers who count most in planning and executing US policy. The general rules that follow should weigh heavily as analysts choose the most appropriate approach.

1. In all cases, the analysts' judgment on the most likely outcomes must follow clearly from the marshaling of evidence and articulation of assumptions.

- The more complex and controversial the issue, the more analytic effort is required to ensure that drivers and linchpin assumptions are precisely stated and well defended.

2. When the US stake is high (for example, political stability of an important ally or adversary) and plausible alternative outcomes are judged to be in the range of for instance, 20 percent or greater, the outlook section should also structure these potentially important outcomes. Policymakers and other consumers should get enough understanding of these alternatives to decide whether to review contingency plans, ask for more evidence, or levy additional tasks on analysts.

Analysts should identify:

- *The factors at play that could lead to unexpected developments.* What alternative key variables could *drive* the outcome in a different direction (perhaps the economy, or growing corruption)? Or what plausible reversal of linchpin assumptions about correctly defined drivers could turn things around (perhaps the Egyptian military *will not* remain loyal to the Mubarak government)?

- *Signposts or indicators of change.* What intermediate developments would indicate that events may not be working out as originally expected? For example, such negative signposts for regime stability as the advent of coup plotting or capital flight.

- *Events that could trigger a major shift in direction.* What essentially unpredictable events could precipitate the unexpected outcome? For example, a crop failure, or a mishandled natural disaster, or anti-government demonstrations that get out of control.

3. On issues vital to US security (for example, military intentions of adversaries), analysts must help policymakers and warfighters engage in contingency planning by:

- Addressing all important factors at play that could influence subsequent events.

- Ranking their relative importance.

- Relating them to a range of plausible outcomes, including alternatives analysts deem to be remote possibilities against which policy planners may nonetheless decide to deploy resources.

Tradecraft Tips

1. Analysts should avoid unrealistic precision in citing odds. Weather forecasters may have sufficient data to determine that the chances of rain *are slightly better than even.* Analysts rarely have such luxury in assessing the political or economic outlook.

2. Also avoid phrases that compound unavoidable uncertainty with unnecessary confusion: for example, *real possibility, good chance.*

3. As a rule, use constructions that tie the outcome to the driver and linchpin assumptions, rather than flat predictions.

- *Castro is unlikely to be forced out of office over the next six months unless his security forces mishandle disturbances and trigger prolonged violent riots.*

4. To minimize misinterpretation when making important judgments, combine probabilistic phrases and rough numerical odds.

- *On balance, Castro is unlikely to be forced from office in the next six months (less than a one-in-five chance).*

5. To understand the often intense concern of hands-on policy officials about a 20 percent likelihood of a disastrous turn of events happening on their watch, analysts should consider whether they would voluntarily get on an airplane that had a one-in-five chance of crashing.

6. To deal rigorously with unlikely developments, analysts should switch their focus from *whether* something will happen to *how* it could happen. Some techniques for generating credible alternative scenarios by structuring the available evidence differently:

- *Who and What Counts.* Generate lists of the key individual and group players that can determine the outcome of an issue (for example, whether Egyptian politics will continue to simmer or will explode), and critically examine the factors most likely to determine their behavior (such as institutional loyalties, personal rivalries, family interests).

- *Thinking Backwards.* Start with the assumption that the targeted danger or opportunity has occurred. For example, revolutionary violence undermines the Castro government! Then generate one or more plausible "how-it-could-happen" scenarios, by postulating who would have to do what, when, how, and why.

- *Judgments Discarded.* List assumptions that fell by the wayside in reaching the bottom line. Regarding the judgment that the military will continue supporting the Egyptian government, for example, revisit any available data or supportive reasoning indicating such support may be weakening, for example, among junior officers.

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

July 1995

Note 5

Facts and Sourcing

This is the fifth in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

> *The present note is longer than those previously published because it addresses two closely related evaluation standards.*

The credibility of DI assessments with key consumers starts with the analyst's skill in organizing and evaluating the information presented in support of policymaking, warfighting, and law enforcement. Estimative judgments are also important, and at times essential for addressing complex and uncertain issues. But extensive feedback makes clear that US officials with hands-on responsibility for planning and executing policy take their first measure of DI analysts in terms of the judgment they exercise in providing actionable and reliable information:

- As a rule, then, the consumer's confidence in the analyst's estimative judgment comes only after he or she has established credentials for expert command over all-source information.

- Thus, while taking account of space limitations, analysts should err on the side of providing more rather than less relevant information.

This tradecraft note, on *Facts and Sourcing,* presents DI guidelines for depiction in memorandums and briefings of what the DI knows—that is, the character and source of its information. The guidelines will be illustrated by hypothetical examples of "best practices" for handling recurring challenges in characterizing information—for example, addressing the reported attitudes and intentions of foreign actors.

Definitions

DI analysts have a good track record in conveying what they know clearly and credibly to consumers of intelligence. What is undertaken here is codification of rules of thumb into general guidelines.

The following definitions are an attempt to promote standardized use of common terms and concepts relating to intelligence information.

Fact: Verified information; something known to exist or to have happened.

Information: The content of reports, research, and analytic reflection on an intelligence issue that helps analysts and their consumers evaluate the likelihood that something is factual and thereby reduces uncertainty.

Direct Information: Information relating to an intelligence issue under scrutiny the *details* of which can, as a rule, be considered factual, because of the nature of the source, the source's direct access to the information, and the concrete and readily verifiable character of the contents. For example:

- Special intelligence quoting what a foreign official said.
- Imagery providing a count of the number of ships at a pier.
- An event observed by a US Embassy officer.

Indirect Information: Information relating to an intelligence issue the details of which may or may not be factual, the doubt reflecting some combination of the source's questionable reliability, the source's lack of direct access, and the complex character of the contents. For example:

- What a third party told a reliable clandestine source a foreign official said.
- The count of ships at a pier as reported in a foreign government document.
- A US Embassy officer's report of an event based on local media accounts.
- Special intelligence citing what a foreign official believes.

Sourcing: Depiction of the manner in which information was obtained, in order to assist in evaluating the likelihood that the content is factual. A single report from a source or collection platform can contain both direct and indirect information.

Data: Organized information that provides context for evaluating the likelihood that a matter

under scrutiny is factual. The information can be either direct (a chronology of events based on observation by US Embassy officers) or indirect (a chronology based on reports provided by a liaison intelligence service.

These terms are illustrated by the following hypothetical example.

We believe country X has begun a major crackdown on the "Extremist Movement," which the government holds responsible for the campaign of terrorism over the past two years.

The Army has been ordered to support the police in cleaning out *Extremist* strongholds (*direct information*), according to special intelligence (*sourcing*). The President of X reportedly is using last week's attack on a shopping center in a working-class neighborhood to justify calling upon the Army to close down the terrorist campaign (*indirect information*), according to a reliable clandestine source (*sourcing*). The progovernment press reports (*sourcing*) the *Extremists* cannot match Army firepower and are taking high casualties (*indirect information*). A US Embassy observer reports (*sourcing*) seeing Army trucks deliver more than 100 prisoners, some badly wounded, to the Central Prison (*direct information*). According to country X police officials (*sourcing*), these were part of the 1,000 *Extremists* rounded up so far in the crackdown (*indirect information*). CIA's "Country X Terrorism Chronology" indicates this is the first time the Army has been used against the *Extremists* since the terrorism campaign began in 1993 (*data*).

Guidelines

Rule 1. Be precise about what is known.

With US interests, and at times lives, on the line, policymakers, warfighters, and law enforcement officials need to be informed precisely *what the all-source analysts know and how they know it*. In making decisions on whether and how to take action, it is important for them to know if the information is direct or indirect, and if and why the analysts have concluded it is factual.

Most key consumers of intelligence have learned to respect the complexity of the national security issues they are charged with managing and the frequent uncertainty about what is taking place and what lies ahead. DI analysts should write to their standard and not to that of the occasional consumer who *wants answers* no matter what the circumstances.

Thus, in the name of reliability, analysts should never exaggerate what is known. They should report any important gaps in information bearing on US decisionmaking and potential courses of action, as well as relevant information that seems to contradict the main flow of information.

Best Practices

- According to special intelligence, President X has canceled his planned trip to country Y. Imagery indicates no signs of the airport security procedures that usually are undertaken for a Presidential flight. The media in both countries, however, continue to report plans for the scheduled peace talks between the two countries.

- We have no direct information on President X's involvement in narcotics trade, despite persistent charges in the media by his political opponents that his reelection campaign is being financed with funds he obtained from his engagement in trafficking.

Analysts should be precise as well in sourcing information. The phrase, *According to the US Embassy*, for example, does not inform the reader whether the information is direct or indirect.

Best Practices

- US Embassy officers observed sparse crowds at several political rallies.

- In the opinion of a US Embassy official, political support for President X has increased in recent weeks.

Rule 2. Distinguish carefully between information and fact.

Analysts may have direct information on what a foreign leader said, for example, and responsibly conclude this as factual. But what that foreign leader believes, intends to do, and will do cannot be known to be true on the basis of a report on what he or she said.

Best Practices

- According to special intelligence, President X is telling confidants he will fire Prime Minister Y next week.

- President X is reported to be ready to fire Prime Minister Y, according to a reliable clandestine source.

Rule 3. Distinguish carefully between information and estimative judgment.

Analysts' estimative judgments, as indicated, are an important element in the process of supporting policymakers, warfighters, and law enforcement officials. As a rule, these judgments cannot rely solely on reported opinions of foreign players or clandestine sources.

They must be amply argued in terms of the entire body of available information and sound inferential reasoning.

Best Practices

- We believe recovery is under way in Country X. CIA's "Country X Economic Database" shows sustained improvement over the past three months in expanding production and exports and in containing inflation. According to a reliable clandestine source, the Finance Minister has stated that the economy has turned the corner toward recovery.

Also, care should be taken to avoid confusion over whether the DI analyst is making an estimative judgment or a source is expressing an opinion. Thus, the following formulation should be avoided: "Country X has turned the corner toward recovery, as indicated by a reliable clandestine source with access to the Finance Minister."

Best Practices

- According to a reliable clandestine source, the Finance Minister has stated that country X has turned the corner toward recovery.

Rule 4. Take account of substantive complexity.

The more complicated an issue (that is, the more inherently difficult it is to be certain on a matter), the greater the informational demands to establish that the matter under consideration is factual. The burden of proof for determining what foreign leaders or groups believe or intend to do, for example, is much greater than that required for determining what they have done or said. Again, analysts may properly make a conditional judgment about what a foreign leader intends to do. (*We believe country X is preparing to invade country Y.)* But only rarely can this be stated as verified or factual information. (*Country X will invade country Y.)*

Best Practices

- We believe country X is preparing to invade country Y. The deployment of military forces of country X along the border of country Y is consistent both with routine annual military exercises and with preparations for an invasion. Special intelligence, however, indicates two key generals have been called back from an important arms purchase mission abroad. A reliable clandestine source reports that two generals who oppose an invasion have been placed under house arrest. US Embassy officers report extensive civil defense drills and the closing of the national airport to civilian flights. According to a CIA database, these actions have not been undertaken in previous military exercises.

The mindsets of foreign leaders—their attitudes, for example—are also extremely difficult to verify, even with direct or firsthand information, and should rarely be stated as factual. When appropriate, mindset can be a subject for the analyst's estimative judgment.

Best Practices

- Multiple reliable clandestine sources report President X is optimistic about economic prospects.

- President X probably is optimistic about economic prospects. Multiple reliable clandestine sources report his recent upbeat statements. Moreover, recently released IMF statistics indicate a marked improvement in exports and worker productivity.

Rule 5. Take account of policy sensitivity.

As with substantively complex matters, the burden of proof is high on matters that are controversial among policymakers or politically sensitive between the administration and Congress. Directly stated, a solid informational base is needed to present as factual (rather than as the analysts' conditional judgment) something that will be seen by key consumers as *bad news.* As a rule, then, on controversial matters analysts should place emphasis on the relevant information, and not on estimative conclusions.

Best Practices

- Six international observers have described the large-scale election irregularities they monitored in country X, according to press reports. Special intelligence indicates progovernment activists introduced hundreds of bogus ballots into the vote count in three outlying districts. The usually cautious press in country X is reporting alleged eyewitness accounts of progovernment activists denying opposition supporters entry into voting places in several precincts. The legitimacy of the election is coming under increasing question on the part of foreign embassies, according to reliable clandestine sources and press reports.

Similarily, when addressing the behavior of a given country regarding treaties and agreements with the United States, DI analysts should place emphasis on reporting rather than interpretation. As a rule in these matters, *analysts monitor* (report relevant information), and *policymakers verify* (decide whether a violation of a treaty or an agreement has taken place).

Best Practices

- The following information relates to the recent behavior of country X regarding its pledge, under the US economic assistance agreement, to cease support of antigovernment guerrilla forces in country Y:

  —The President of country X told the US Ambassador that all official assistance had been terminated, although small-scale shipments of weapons by private groups that sympathize with the guerrillas' cause might still be taking place.

  —According to a reliable clandestine source, a senior assistant to the President of X has ordered the military to hide small shipments of weapons for the guerrillas in trucks engaged in normal cross-border trade.

  —Special intelligence indicates that a military mission from country X is to await further orders before purchasing abroad communications equipment requested by the guerrillas.

Rule 6. Take account of the possibility of deception.

Deception can be defined as the manipulation of information by a foreign government, group, or individual to get US intelligence analysts to reach an erroneous conclusion. Deception often works because it gives busy analysts what they are seeking—seemingly reliable information on which to base a conclusion.

Here is where the strength of the all-source analyst comes into play. One test for detecting and countering deception is to determine whether all the sources and collection platforms that should be reporting on a matter have indeed done so.

Databases, or organized information, also help. *Is the reported or observed information consistent, in all important details, with past patterns? Do intelligence services with an interest in the matter have a record of perpetrating deceptions?*

So does critical thinking. *Is the information consistent with the analysts' best judgments on the subject's interests, capabilities, and methods of operation?*

Best Practices

- President X assured the US Ambassador on Tuesday that all missile sites in his country had been dismantled, but imagery from last week shows no dismantling activity at the 29 missile sites listed in CIA's database.

- We have no direct information to support reports by a clandestine source with access to Colonel X that antigovernment military forces loyal to him are about to undertake a military coup. No other clandestine sources with military contacts are reporting advanced

coup planning or unusual movements of troops. Opposition political groups abroad report that they are unaware of any serious coup activity, according to multiple reliable clandestine sources. The government, therefore, could be running a deception operation involving Colonel X, to smoke out "disloyal" officers.

Rule 7. Use the term "evidence" sparingly.

This tradecraft note uses the term *information* as synonymous with the term *evidence* as it usually is employed in DI assessments. That is, both are used to refer to the content of reports and research that helps reduce the uncertainty surrounding a specific matter.

The US legal system, however, uses *evidence* in a more specialized manner—to refer to matters introduced in a court case and subject to proof and refutation by contending parties. Because the DI is increasingly providing assessments to support law enforcement officials and because even other kinds of assessments can be subpoenaed for possible use in a court case, analysts should avoid using the term *evidence* when *information* serves their purposes just as well. At times, characterization of the information is sufficient to make the analysts' point for the benefit of consumers.

Best Practices

- Information from special intelligence and clandestine reporting indicates that Justice Minister X has been involved in the narcotics trade.
- Special intelligence and clandestine reporting indicate that Justice Minister X has been involved in the narcotics trade.

Special Circumstances

This note has concentrated on general guidelines for depicting the character and source of the DI's information. The DI serves a broad range of audiences with varied needs and entitlements for intelligence support on a multiplicity of substantive issues. Thus, the special character of the subject matter, the delivery vehicle, or the audience can require exceptions to the rules posited above.

For example, either the limited clearances of the recipients of an assessment or a customer's request for an unclassified memorandum can require the analyst *to avoid precision* in depicting information and sources.

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

August 1995

Note 6

Analytic Expertise

This is the sixth in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

Analytic expertise establishes the DI's authority to speak to an issue on which US national security interests are at stake. Demonstration of expertise in DI assessments is thus needed to gain access to and credibility with the policymakers, warfighters, and law enforcement officials who carry the heaviest burden for US decision and action on national security issues.

As with all evaluation criteria addressed in these tradecraft notes, analysts have to tailor their demonstration of expertise in individual memorandums and briefings to the circumstances of each assignment. These include the degree of substantive complexity, the analytic requirements and timeline of the policymaking process, and whether the DI production unit already has established close ties to its key clients.

As a rule though, no DI product should be delivered without deliberate effort to make it stand out from the formidable competition including other intelligence providers, journalists, scholars, lobbyists, and various additional purveyors of information and judgment:

- Demonstration of in-depth substantive knowledge is usually the most important element in establishing the credentials for a DI product. To a large extent, the Directorate *is* what it knows and can bring to bear to reduce uncertainty on complex issues.

- Analytic expertise is also conveyed by (1) skill in accessing and interpreting clandestine and technically collected information, (2) deft organization of data in support of findings and judgments, (3) dealing effectively with longshot contingencies and with uncertainty generally, and (4) demonstrating insight into the decisionmaking processes of intelligence customers.

How much expertise needs to be demonstrated? Taking space and time limitations into account, the more the better. The DI not only has to stand out regarding the breadth and depth of its analytic expertise, it also has to convince its key customers that it can put this expertise to use for their benefit.

Again, the appropriate means through which to convey expertise varies with each analytic assignment. As a general test, we recommend that analysts read their first draft critically, to answer the following questions *as if they were posed by a policy official deciding whether to rely on the DI to meet the challenges on his or her agenda.*

- Do the analysts show in-depth knowledge of their subject—the history, civil culture, and other general contexts of the issue, as well as the latest reporting?
- Is there evidence that the analysts have "been there" or represent an analytic and operational team with members who have experience-based insights?
- Have the analysts brought to bear all the dimensions or disciplines that define the issue—political, economic, military, S&T?
- Have the analysts brought to bear all-source information and made a special effort to help the busy intelligence user grasp the key patterns revealed by the information?
- Do the timing and format reflect the analysts' sensitivity to the timeline, decision points, and underlying tensions (areas under debate) of the policymaking process?
- Do the analysts have an effective method or structure for arraying information and reducing uncertainty?
- Further on uncertainty, do the analysts help me think through complex challenges by making their key assumptions clear and dealing rigorously with alternative interpretations and outcomes?
- In sum, would I want to rely on DI analysts and pose followup tasking, to deal with the threats to, and opportunities for, US interests on my policy agenda?

Tradecraft Tips

Research papers are natural vehicles for effective display of analytic expertise. DI veterans, over the years, have devised an armory of measures for demonstrating hard-earned individual and collective expertise even in quick turnaround papers and within the space limitations for most DI deliverables. We list below some of these measures:

- *Evidence of previous research.* In a preface, footnote, textbox, or annex, list related finished intelligence on the subject at hand. Be sure to take a Directorate or team approach by citing the works of other production units.

- *Evidence of scholarship.* Often one footnote or textbox that indicates the breadth of the analysts' grasp helps to establish credentials. For example, citing a historical incident with either common or contrasting elements to the issue at hand.

- *Evidence of data bases.* Expertise can be demonstrated by a paragraph or textbox that presents a chronology, a series of quotes over time by a foreign leader, or a schematic representation of trends (terrorist incidents, inflation or economic growth rates, growth in military inventories, S&T milestones).

- *Evidence of ground truth.* At times it takes only a sentence or two to demonstrate special insight into key personalities, groups, and forces at work. Use your own feel for the ground truth or rely on your analytic teammates to work in some experience-based references. Examples could include references to local political humor, to the household commodities on which short supplies would be most likely to cause popular disgruntlement, or to the modus operandi of local intelligence and security forces.

- *Evidence of teamwork.* Put your professional support colleagues to work on your behalf to clarify a key point or to organize and display the information supporting a point—via annotated maps, imagery, and other graphics. Interviews with customers indicate that those who are heavily engaged on an issue particularly appreciate visual aids that help in keeping up with the fire hose of information.

- *Leadership analysis.* US leaders, naturally enough, tend to be interested in foreign leaders, especially their approach to making decisions, negotiating, and dealing with conflict. Addressing these matters in the text, a textbox, or an annex demonstrates both the breadth and depth of the DI's collective expertise.

- *Secrets.* Excessive classification should be avoided in assessments intended for a broad and general audience. But when a DI assessment is intended for the handful of officials fully engaged (and fully cleared) on an issue, contextual explanation of information from clandestine and technical sources conveys a sense of special expertise.

- *Mysteries.* Demonstrating skill in dealing with uncertainty is appreciated by the hands-on policy officials who have to decide which risks to cover. This includes making explicit the assumptions that drive the argumentation and taking account of low-probability, high-impact contingencies. Here, too, the coverage can be set aside in a textbox or annex, if the goal is to keep the main text lean.

- *The only game in town.* Understandably, policy officials believe that policymaking and implementation is the reason why intelligence exists, and not vice versa. Analysts should demonstrate—in a cover note, preface, or footnote, if not in the main text—that they are informed on the policy timeline and the key matters under debate. Indeed, few things call the DI's reputation into question more than an assessment that arrives after a decision has been made or that addresses in a conventional manner issues on which there already is both broad knowledge and consensus among policy officials.

- *Customized support.* When writing for a small number of officials, analysts can demonstrate by the issues they highlight that they know where their consumers are on their learning curve as well as their decision cycle.

Expertise in Support of the Intelligence Consumer

We end with an obvious caution. When the analysts know their clients' specific needs, demonstration of expertise is readily projected as a tool or means for providing value added. With larger assessments prepared for a broader audience, more care has to be taken to avoid excessive display of knowledge—that is, substantive expertise as an end in itself. Here is where investment in knowing the timelines of the policymaking process and the specific dangers and opportunities policy officials are dealing with comes into play.

September 1995

Note 7

Effective Summary

This is the seventh in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

The summary plays a key role in determining the kind of impact a DI report or memorandum will have on the policymaking process. Thus, within the allotted space, the summary has to make the distinctive DI value added stand out—whether consisting of special intelligence with immediate bearing on US security interests, important findings from the sifting of all-source information, or actionable judgments about pending threats and opportunities.

As with other criteria covered in this series of tradecraft notes, analysts have to tailor each summary to the circumstances of the individual assignment. One way or another, though, the analyst has to crystallize the DI expertise presented in the text in a manner that will seize the attention of the intended audience.

When the clients for the assessment are few in number and their priority interests regarding US policy and action agendas are well known to the DI, the analysts' job is to craft a summary that crisply presents the *what's new* and the *so what:*

- For example, in a Special Intelligence Report, the allotted "hook" of a couple of lines of text must be designed to assure the intelligence consumer that his or her time will be well spent in digesting the rest of the report.

When an assessment is broadcast to a larger and more diffuse audience, the analysts' challenge in determining the structure and content of the summary is greater. Usually, the two most important goals are:

- *To highlight the value added of the paper* against the contingency that busy readers will not get into the main text, especially the implications regarding threats to and opportunities for US interests.

- *To support these values with distinctive expertise* in order to motivate the "gatekeepers" to read the text and recommend that their principals survey sections targeted to help them advance their policy and action agendas.

To account for the diversity of the potential audience for broadcast assessments, other introductory sections can be put to use in flagging the full range of value added and DI expertise. In particular, an *introductory textbox*, placed immediately after the summary, can be used to meet the needs of specialized segments of the audience:

- For example, a depiction of the background or general context that would try the patience of the officials already directly engaged on a policy issue can be provided in a textbox to serve the needs of peripherally engaged intelligence consumers.

- Similarly, technical findings needed to meet the threshold of value added for a small, highly specialized portion of the intended audience can be placed in a textbox.

- And when depiction of policy implications on a controversial issue requires more space for balanced presentation than a summary can accommodate (for example, cost-benefit analysis of alternative courses of action), a textbox is an effective solution.

A *preface* is also a useful instrument, in longer and broadly distributed assessments, for supplementing the summary:

- Use it to explain to peripherally engaged readers the precise policy challenges the assessment seeks to clarify.

- Use it to augment DI credibility; for example, by listing prior publications on the issue at hand.

Tradecraft Tips

DI veterans offer the following experience-based tips for enhancing the effectiveness of summaries:

- *Conform the summary to the text and vice versa.* Often the process of squeezing all the values of the text into a summary paragraph or page sharpens the analyst's depiction of key variables (drivers), cause-and-effect relationships, and argumentation generally. Retrofit any new insights and values into the text.

- *Break up the typography.* Many readers interpret summaries with paragraph blocks that run solidly from margin to margin as a signal that the memorandum or report is "user unfriendly":

  —Use short paragraphs, bullets and subbullets, **bold face**, and *italics* to break up the space and to help the busy decisionmaker latch on quickly to the key information, relationships, and judgments.

- *Fit the writing style to audience and purpose.* When writing for a broad audience, including many policy officials with whom the production unit has only limited contact, top-quality exposition can help attract the readers' attention to the main text. When working in support of a single consumer, however, consider using a more informal style to speed his or her grasp of the value added:

  —One official reported that he did not have time for "whole sentences"—just for what it was the analyst wanted him to know.

- *Concentrate on the new and important.* Historical background and other setting of the context can be presented tersely or dispensed with altogether. Use the allotted space to concentrate on content that will make a difference to well-informed policymakers, warfighters, and law enforcement officers as they contend with their daily challenges:

  —This usually means policy implications. In effect, the summary is a vehicle for explaining why a busy policy official should spend time on a DI product.

  —Strive to make the summary *actionable*; that is, structure it to help a policy official get something started, stopped, or otherwise sorted out.

- *Role-play key members of the targeted audience.* Regarding what belongs in and what can be omitted from the summary: If you were a time-challenged policy official, what would you want to gain from spending five minutes or so with your assessment?

- *Make fewer points, but make them well.* If you have to choose between the quantity and quality of the points made in the summary, opt for the latter. This is particularly important when writing for a well-informed audience which has no need for a "tutorial" on the issue:

  —If the assessment makes a bottom-line predictive judgment, refer to the key assumptions and other essential elements of the argumentation.

  —If the assessment conveys important new findings, cover the reliability of the sourcing and the essence of the methodology.

Reverse Blank

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

October 1995

Note 8

Implementation Analysis

This is the eighth in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

This note discusses *Implementation Analysis*, one of the techniques for extending customized intelligence support to policymakers, law enforcement officials, and warfighters outlined in Note 1, *Addressing US Interests in DI Assessments.*

Implementation Analysis provides decisionmakers and action takers with an assessment of tactical alternatives for pursuing opportunities and averting dangers regarding established US policy goals. The role of the analyst complements but is distinctive from the role of the policymaker:

> *Analysts identify and evaluate alternatives for implementing objectives; policy officials first set the objective and then make the decisions about which tactics to adopt.*

Illustrative hypothetical cases of Implementation Analysis include:

- Identifying the major supply routes available to a military adversary and evaluating their logistic importance and vulnerability to US attack.
- Identifying the money-laundering techniques used by a major drug trafficker and evaluating their vulnerability to disruption and curtailment.
- Identifying and evaluating the economic vulnerabilities that could be exploited to leverage a foreign government to terminate development of a nuclear weapons capability.
- Identifying diplomatic, political, and economic initiatives that could be taken to shore up an unstable government the United States wishes to keep in office.
- Identifying and evaluating confidence-building measures either to draw military adversaries into negotiations or to restart stalled talks.

Why and When

Policy implementation regularly involves attempting to advance US interests under uncertain and often risky conditions. In these circumstances, policy officials recognize that US objectives can be difficult to achieve. Deterring rogue states from developing weapons of mass destruction and promoting democratic practice in polities with entrenched authoritarian traditions, for example, require overcoming deeply imbedded obstacles. Policy officials need support from intelligence analysts in identifying and assessing opportunities and dangers.

Intelligence analysts, through Implementation Analysis, can bring important value added to the policymakers' table:

- Expertise in understanding foreign cultures, including the risk analysis and negotiating styles of adversaries and allies.

- Findings on strengths and vulnerabilities of target countries and organizations, based on evaluation of all-source information.

- Detachment from departmental bureaucratic pressures and a commitment to objectivity in examining tactical alternatives.

Even when the analysts' inventory of alternatives largely mirrors that of policy officials, the latter benefit from exposure to the organized information and rigorous argumentation of the former.

In addition to its intrinsic value added, Implementation Analysis can also help the DI maintain effective policy ties on politically charged issues. When pursuit of US goals entails coping with multiple difficult challenges, heavily engaged policy officials do not appreciate a steady stream of DI assessments that reminds them (as well as congressional critics, for example) that they are working against long odds. Implementation Analysis sends the message that the intelligence team, although professionally committed to objectivity, is not indifferent to the challenges the policy team faces and will lend its expertise to help advance and protect US interests even under difficult circumstances.

In any case, analysts should place a premium on close lines of communication in delivering Implementation Analysis:

- As a rule, policy officials should *request* such customized support.

- Intelligence managers who are well connected to the officials doing the heavy lifting can, at times, advertise the capability and solicit a request.

The initial DI delivery of Implementation Analysis usually consists of a briefing or memorandum for one or a handful of principal policy officials. In recognition of the value added, the latter have in the past subsequently asked for:

- Regularly scheduled repeat briefings or memorandums.
- An increase in the circle of recipients.
- Incorporation of the analysis into policy planning documents.

Tradecraft Tips

Veteran analysts offer the following tradecraft tips for putting Implementation Analysis into practice:

- Redefining an intelligence issue in the policymakers' terms can be a useful first step for providing value added through Implementation Analysis. In other words, analysts shift focus from their normal quest for understanding *what's going on in country X* to the policymakers' quest for *doing something about what's going on in country X.* This requires:

  —Recognition of the policymakers' role as "action officers"—charged with getting things started or stopped among adversaries and allies overseas.

  —Recognition of the policy officials' propensity at times to take risk for gain. For example, policymakers may see a one-in-five chance of turning an unsatisfactory situation around as a sound investment of US prestige and their professional energies.

- Analysts also gain insight for adding value by concentrating on what it takes to achieve the operational goal (*think like a policy professional)* before turning to an objective survey of the ground truth (*execute like an intelligence professional*):

  —For example, if the objective of US policy is to leverage a foreign government or organization to reverse its course, analysts can first think of what developments could lead to that outcome and then make an inventory of the forces at play that could trigger such developments.

- The *If, Then* structure often can be used to relate US tactics to US goals, while reserving the DI's tough-minded analytic posture toward both—that is, without crossing the line between professional analytic support of the policymaking process and poliey prescription. For example:

  —*If* US policy calls for getting from point A to point B, *then* here are some gateways to consider and some cul-de-sacs to avoid.

  —*If* the US policy objective is to strengthen the forces for moderation in country X, *then* the following factors should be examined as potential catalysts for the desired development.

- Implementation Analysis often requires *divergent thinking*—the setting aside of attention to mainstream interpretations and the most likely outcome and focusing instead on the full range of plausible alternative interpretations and outcomes. Analytic techniques such as brainstorming, role playing, and "thinking backward" (examining the paths by which a low-probability event could occur) can help identify little-known forces at play that could effect a change in momentum:

  —When analysts are pessimistic about prospects for advancing US objectives, they can employ a variation of the Sherlock Holmes methodology for moving forward when there is no promising suspect in a murder case. *Provide policymakers with an assessment of the least unpromising tactical alternatives.*

  —DI analysts, in effect, are the scouts that provide information and insights to help the policymaker-coach develop the most sensible game plan, win or lose.

- In addition to knowledge of the ground truth, the value added of Implementation Analysis can depend on analysts' knowledge of US instruments for leveraging a situation (that is, the available *carrots and sticks*). Analysts are well advised to make an inventory of US means for executing foreign policy based on the study of policy documents and discussions with intelligence managers and contacts in policy agencies.

- The final step for Implementation Analysis is presentation of the results of the analytic process in ways that make it clear that professional analysts have been at work. Often the responsible policy officials will be more interested in *how analysts reached their evaluations of alternatives* than in the evaluations per se:

  —Presentation and ranking of alternatives via a matrix containing a rough cost-benefit analysis is a useful way to convey the analysts' underlying all-source findings and linchpin assumptions. At the same time, such a matrix focuses the DI effort on *analyzing alternatives*, while leaving the actual choosing to the policymakers.

- Because Implementation Analysis calls on distinctive and challenging tradecraft techniques, analysts should engage colleagues and managers early on in the process of defining the issue and selecting promising tactical alternatives to assess. This team approach will help tap into corporate expertise, as well as smooth the coordination and review processes.

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

December 1995

Note 9

Conclusions

This is the ninth in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting the standards into practice.

Conclusions—the analysts' findings based on organizing, evaluating, and interpreting the all-source information available on the issue at hand usually are the most important value added for key consumers of DI assessments. Because policymakers and action takers rely on DI assessments as they define and defend US interests, analysts must be precise in conveying the level of confidence in their conclusions, taking appropriate account of the prospect of deception and other sources of uncertainty.

Heavily engaged policy officials often receive directly much of the open-source and intelligence information available to DI analysts. But the policy officials need DI assistance in keeping track of the facts, fictions, and trivia. The important event has to be identified from among the ordinary, the underlying patterns have to be cobbled together from seemingly unrelated pieces of information, and the reliable sources have to be distinguished from the self-serving.

On complex national security issues the information available to the analysts rarely speaks for itself. Gaps and inconsistencies are the rule. This is where the DI analysts' expertise comes into play. When seasoned and skeptical DI analysts believe they have made their case by a careful scrubbing of ample all-source information, they should lean forward in making their conclusions precise and clear to the policy officials responsible for management of the issue. Analysts who have organized and evaluated their information are able to *conclude* with authority, for example:

- The latest information shows country "X's" expenditures on weapons-related technology *increased sharply* in 1995 after several years of little or no growth.

- DI data demonstrate that incidents of human rights violations in country "Y," as reported by international monitors and reliable clandestine sources, are *decreasing for the first time* since the military government took power in 1989.

- The DI database shows that terrorist incidents in country "Z" *are taking on a pattern* of attempting to intimidate the foreign business community.

- Examination of DI chronologies of the seven national elections since the restoration of civilian government in country "A" indicates that recent government use of armed thugs to break up opposition political rallies *is without precedent.*

- The *cause-and-effect relationship* between Premier "B's" political difficulties and his calling for military exercises to turn public attention to the "foreign threat" is by now well established.

DI assessments are particularly valuable to policy officials when the analytic findings are derived from the collective databases of a multidisciplinary team. Depiction of the political context for a foreign country's lax policy on narcotics controls, for example, or its financial and technological potential for pursuing a nuclear weapons program enables users of DI analysis to take a better measure of the potential risks and benefits of contemplated US policy initiatives.

In contrast, when available information is incomplete or susceptible to foreign deception operations and other sources of ambiguity, the analysts' reasonable doubts about, say, cause-and-effect relationships should be shared with the officials who may rely on DI assessments in taking policy actions.

Many of the issues that the DI tackles are inherently complex and thus shrouded by uncertainties. The analysts have a professional obligation—where warranted—to conclude that *they do not know*. In such instances, presentation of two or more plausible interpretations of the available information makes a more useful conclusion than a single unreliable one masked in vague language (for example, *a real possibility*).

Analysts should be particularly wary about projecting thin information as a DI conclusion. When, for example, analysts do not have a solid informational base and are relying on a small number of reports depicting an event as unprecedented or a pattern as well-established, they should attribute such conclusions to the source. Clandestine agents, foreign officials, and the local media may jump to conclusions. DI analysts should not.

In sum, the value added to policymakers, negotiators, warfighters, and law enforcement officials of conclusions in DI memorandums and briefings rests on:

- The solidity of the individual and collective DI expertise brought to bear through analysis of databases and other information.

- The precision analysts use in stating levels of confidence in their findings.

Tradecraft Tips

DI veterans offer the following recommendations for conveying conclusions effectively:

1. When analysts have reached firm conclusions on complex and especially controversial issues, take the time to present the data, to point to the relationships and other implications, and to state the conclusions forcefully. For example:

- The latest technically collected information, when combined with previous all-source reporting, indicates that country "X" has the means to conduct a weapons test within months, if not weeks.

2. Again, when an issue is complex and controversial, describe the credentials that lie behind the findings—in a textbox or footnote, if not in the main text. For example: depict the reliability of the sources of the information and other specific characteristics of a database; spell out the indicators used to determine diversion to military use of dual-purpose technology imports.

3. To minimize confusion when conveying a necessarily qualified conclusion, think of supplementing adverbial descriptors with a statement of rough numerical odds:

- On the basis of the well-documented effectiveness of "X's" intelligence service in penetrating previous plots and the poor security exhibited by the present conspirators, the President almost certainly knows about the impending coup attempt (roughly a 90-percent likelihood).

4. When the quality of available information requires either reserving judgment about conclusions or presenting multiple plausible interpretations, consider including a textbox or annex on information gaps and collection requirements.

5. When the text must be kept brief because of space limitations of a DI art form, the findings can be laid out in some detail in a textbox. This coverage can be useful both for those consumers who need a quick study into the issue and those with direct responsibility for decision and action who have an interest in taking precise account of what the DI knows.

6. Also use a textbox to explain any major shift in a DI conclusion from previous assessments or the basis for a contrasting conclusion held by other Intelligence Community analysts.

7. When appropriate, use chronologies, matrices, and other graphics to supplement the text in conveying complex trends and relationships. Even the best informed policy officials appreciate graphics that help them evaluate important information.

8. Conclusions are the bedrock foundation for estimative judgments in DI assessments that address future patterns of development. In papers that are divided between sections that set out the findings and those that make predictive judgments, analysts may find it useful to summarize the findings in a textbox immediately preceding the estimative portion. This helps clarify the argument for the critical reader. It can also help analysts audit their own logic trail.

Directorate of Intelligence

Notes on Analytic Tradecraft

Product Evaluation Staff

December 1995

Note 10

Tradecraft and Counterintelligence

This is the 10th in a series of Product Evaluation Staff notes to clarify the standards used for evaluating DI assessments and to provide tradecraft tips for putting standards into practice.

This tradecraft note addresses the aspect of counterintelligence (CI) on which the DI is most directly responsible for improved Agency performance: *Countering deception operations by foreign governments and organizations aimed at distorting the conclusions and judgments of analysts' assessments.*

A subsequent note will address related CI aspects on which DI substantive expertise and analytic skill can make important contributions, including (1) countering espionage by helping to identify the US secrets foreign intelligence services are most interested in obtaining and (2) analytic support of efforts to manipulate foreign intelligence operations to US advantage.

Deception is here defined as all efforts by a foreign intelligence service or adversarial group to distort and otherwise manipulate the perceptions of analysts in order to place analysts and their policy clients at a disadvantage in understanding and dealing with the perpetrating country or group. Deception operations can be divided into two closely related subsets:

- *Denial*—measures taken to protect secrets through concealment, camouflage, and other activities that degrade collection systems, including the information analysts receive from open sources, diplomatic channels, clandestine assets, and technical collection.

- *Disinformation*—operations to feed analysts false or partly false information through the use of double agents and manipulation of diplomatic and media as well as intelligence channels.

Countering Deception

For DI analysts, the first step in improving CI performance is to show increased respect for the deceiver's ability to manipulate perceptions and judgments by compromising collection systems and planting disinformation. Next, analysts must adjust the balance between *speed* and *care* in producing DI assessments. There is no "free lunch" here. The analysts' major

defense for countering deception—exercising increased care in evaluating information and in testing working assumptions—places pressures on the DI commitment to timeliness in servicing consumer demand for tailored products.

The key to holding down the opportunity costs of countering deception is to tie the effort as closely as possible to the normal processes analysts use to expand expertise and to ensure quality and policy utility in their memorandums and briefings:

- As analysts become more accomplished in countering deception they also become better qualified to provide value added to decisionmakers and action takers who need customized support based on *reliable* all-source information.

Warning Signs

Through an investment in understanding the warning signs that a deception operation may be under way, analysts become more expert about their subjects as well as about when and how to apply their main weapons for protecting the integrity of DI assessments:

- Skepticism about the reliability of *all information*, whether from human or technical collection, whether open source or classified, and no matter what the level of classification.

- Readiness to challenge and test even well-established assumptions about trends, patterns, and cause-and-effect relationships.

The first set of warning signs addresses the likelihood that a country or organization is engaged in an attempt to distort the analysts' perceptions:

1. ***Means***. The country or entity (for example, terrorist group) being assessed has the experience and means to undertake sophisticated deception operations. Nearly all countries and entities given priority attention under PDD 35 have well-practiced means to deceive, often in third countries as well as at home.

- Becoming more expert on foreign intelligence practices will also provide analysts with greater understanding of the political dynamics of the country or entity under study, especially when intelligence services are a vital part of the power equation.

2. ***Opportunity***. The foreign country or entity is known to have countered the collection systems or platforms on which the DI analyst is particularly dependent. For example, when a target country has knowledge of the periodicity and acuity of technical collection vehicles that pass over an area it wishes to protect, analysts have to be aware that the resultant information may be incomplete if not also deliberately distorted.

Enhanced knowledge of both the reach and the vulnerabilities of collection systems will also help analysts in dealing with the everyday challenges of evaluating incomplete and ambiguous information.

3. ***Motive***. A motive to deceive is believed to be present. Accomplished intelligence services—for example, in Russia, China, or Cuba—have the ability to mount elaborate denial and disinformation operations virtually across the board. Would they see a high payoff from distorting analyst and policymaker perceptions about the issue at hand?

- Knowledge of which secrets an adversary most seeks to protect adds a distinctive perspective to the analysts' understanding of the country's military, political, and economic priorities.

The second set of warning signs focuses on anomalies in the information available to the analyst. Investment in addressing these warning signs reinforces core skills regarding what the analysts know, how they know it, and what they do not know that could affect the outcomes in ways important to policy officials, warfighters, and law enforcement officials. See, for example, Tradecraft Note No. 5, *Facts and Sourcing* (July 1995).

These warning signs include:

4. ***Suspicious gaps in collection***. For example, when information central to the analysts' conclusions and judgments received through one collection channel is not supported to the extent expected from the take of other collection systems. In other words, the analysts are not receiving the range and volume of information they would expect if there was no deliberate tampering with sources and collection platforms.

5. ***Contradictions to carefully researched patterns.*** Does new information undercut the trends and relationships honed through past research? While analysts must be openminded about the possibility of unexpected change, they should examine critically information that signals an inexplicable change, for example, in an adversary's priorities and practices.

6. ***Suspicious confirmations***. For example, when a new stream of information from clandestine sources or technical collection seems to reinforce the rationale for or against a US policy initiative. In these circumstances, receiving the same "story" from more than one DO or diplomatic source does not in itself speak to the authenticity of the information.

Tradecraft Tips

The effort needed to meet the DI standard of ensuring appropriate protection against deception at the lowest net cost to timeliness will vary from case to case. For each assignment, analysts and managers will have to weigh the costs to credibility of being deceived against the opportunity costs of increased care. Below are general schemes for proceeding efficiently against two distinct levels of risk for DI assessments on complex issues.

Regular Issues. We recommend a two-step defense against deception for assessments on which there is no specific reason to suspect deception is at play and on which the primary value added to consumers is a general increase in understanding (as contrasted with tailored support for decision and action):

Step One. Organize the key information by setting it out, for example, on a yellow pad or blackboard, and examine it critically with warning signs of deception in mind. Are all the expected collection systems kicking in? Is the information appropriately consistent? Are the pieces of information on which conclusions and judgments are most heavily based from a *reliable* clandestine source or *uncompromised* collection platform?

- This investment of, say, one hour in questioning the authenticity of sources will occasionally turn up something suspicious. Even when it does not, analysts, as a result of the effort, will be better able to refine and defend their conclusions and judgments.

Step Two. Play Devil's Advocate and develop a hypothetical argument for the case that deception is taking place; that is, a foreign entity *is* attempting to manipulate perceptions through some combination of denial and disinformation. Then determine to what extent the information organized in Step One lends support to the case for the existence of a deception operation. Look for "hits and misses" between the information and the hypothetical case that substantially raise or diminish the likelihood of the presence of an elaborate deception effort.

- This investment of an additional hour or so will also at times raise suspicions that require more deliberate attention. The investment also enhances skill in structuring plausible low-probability, high-impact scenarios, a key to meeting the demands of policy officials for more help in contingency planning.

Suspect and Sensitive Issues. Where there is reason to suspect the presence of deception (based on general warning signs and the exercises outlined above), analysts should undertake a more elaborate defense of the integrity of their assessments. With or without cause for suspicion, an extended defense should also be employed on sensitive issues—those on which the policy officials may directly rely in making decisions on whether to take military, diplomatic, or economic actions to defend US interests.

On suspect and sensitive issues, we recommend that analysts prepare a textbox or annex that addresses the possibility that a deception operation is distorting the assessment's conclusions and estimative judgments. Managers should consider preparation and defense of the textbox

as an essential element of the analyst's effort, even in instances when they determine it is unnecessary to publish it.

The content of the recommended assessment of the integrity of information will vary with circumstances. But at a minimum it should convey that (1) the possibility of the presence of deception has been taken seriously, (2) analytic tests to determine the likelihood of deception have been executed, and (3) any reasonable doubts are forthrightly reported.

Specific questions that analysts can address with profit include:

1. What is known of the ability of the country or group under examination to engage in deception? About incentives to do so?

2. What is known about the reliability and integrity of the sources and collection platforms most heavily depended upon?

3. What can be said about the availability and consistency of information from all relevant sources and platforms?

4. What tradecraft tests were used to evaluate the authenticity of the information relied upon to reach key conclusions?

In sum, such a textbox provides the analysts with an answer to a question likely to be posed with greater frequency by Agency leaders and policy officials in the wake of the Ames case: *How do you know you are not being deceived?*

01-OSS 21 PRIMER Essential Elements of Information Joint Planning, Operations Other Than War and Open Source Intelligence - Link Page

Previous INTELLIGENCE ANALYSIS IN A NEW CENTURY: A CUMUDGEON'S VIEW

Return to Electronic Index Page

This Page Is Intentionally Left Blank

Psychology of Intelligence Analysis

by
Richards J. Heuer, Jr.

CENTER *for the* STUDY *of* INTELLIGENCE

Psychology of Intelligence Analysis

by
Richards J. Heuer, Jr.

CENTER *for the* STUDY *of* INTELLIGENCE
Central Intelligence Agency
1999

This book was prepared primarily for the use of US Government officials, and the format, coverage, and content were designed to meet their specific requirements.

Because this book is now out of print, this Portable Document File (PDF) is formatted for two-sided printing to facilitate desktop publishing. It may be used by US Government agencies to make copies for government purposes and by non-governmental organizations to make copies for educational purposes. Because this book may be subject to copyright restriction, copies may not be made for any commercial purpose.

This book will be available at www.odci.gov/csi.

All statements of fact, opinion, or analysis expressed in the main text of this book are those of the author. Similarly, all such statements in the Forward and the Introduction are those of the respective authors of those sections. Such statements of fact, opinion, or analysis do not necessarily reflect the official positions or views of the Central Intelligence Agency or any other component of the US Intelligence Community. Nothing in the contents of this book should be construed as asserting or implying US Government endorsement of factual statements or interpretations.

ISBN 1 929667-00-0

Originally published in 1999.

Psychology of Intelligence Analysis

by Richards J. Heuer, Jr.

Author's Preface vi

Foreword.....ix

Introduction xiii

PART I—OUR MENTAL MACHINERY.....1

Chapter 1: Thinking About Thinking 1

Chapter 2: Perception: Why Can't We See What Is There To Be Seen?.....7

Chapter 3: Memory: How Do We Remember What We Know?.....17

PART II—TOOLS FOR THINKING.....31

Chapter 4: Strategies for Analytical Judgment: Transcending the Limits of Incomplete Information ...31

Chapter 5: Do You Really Need More Information? ...51

Chapter 6: Keeping an Open Mind 65

Chapter 7: Structuring Analytical Problems 85

Chapter 8: Analysis of Competing Hypotheses 95

PART III—COGNITIVE BIASES.....111

Chapter 9: What Are Cognitive Biases?.....111

Chapter 10: Biases in Evaluation of Evidence.....115

Chapter 11: Biases in Perception of Cause and Effect 127

Chapter 12: Biases in Estimating Probabilities 147

Chapter 13: Hindsight Biases in Evaluation of Intelligence Reporting..... 161

PART IV—CONCLUSIONS 173

Chapter 14: Improving Intelligence Analysis..... 173

Author's Preface

This volume pulls together and republishes, with some editing, updating, and additions, articles written during 1978–86 for internal use within the CIA Directorate of Intelligence. Four of the articles also appeared in the Intelligence Community journal *Studies in Intelligence* during that time frame. The information is relatively timeless and still relevant to the never-ending quest for better analysis.

The articles are based on reviewing cognitive psychology literature concerning how people process information to make judgments on incomplete and ambiguous information. I selected the experiments and findings that seem most relevant to intelligence analysis and most in need of communication to intelligence analysts. I then translated the technical reports into language that intelligence analysts can understand and interpreted the relevance of these findings to the problems intelligence analysts face.

The result is a compromise that may not be wholly satisfactory to either research psychologists or intelligence analysts. Cognitive psychologists and decision analysts may complain of oversimplification, while the non-psychologist reader may have to absorb some new terminology. Unfortunately, mental processes are so complex that discussion of them does require some specialized vocabulary. Intelligence analysts who have read and thought seriously about the nature of their craft should have no difficulty with this book. Those who are plowing virgin ground may require serious effort.

I wish to thank all those who contributed comments and suggestions on the draft of this book: Jack Davis (who also wrote the Introduction); four former Directorate of Intelligence (DI) analysts whose names cannot be cited here; my current colleague, Prof. Theodore Sarbin; and my editor at the CIA's Center for the Study of Intelligence, Hank Appelbaum. All made many substantive and editorial suggestions that helped greatly to make this a better book.

—Richards J. Heuer, Jr.

Foreword

By Douglas MacEachin[1]

My first exposure to Dick Heuer's work was about 18 years ago, and I have never forgotten the strong impression it made on me then. That was at about the midpoint in my own career as an intelligence analyst. After another decade and a half of experience, and the opportunity during the last few years to study many historical cases with the benefit of archival materials from the former USSR and Warsaw Pact regimes, reading Heuer's latest presentation has had even more resonance.

I know from first-hand encounters that many CIA officers tend to react skeptically to treatises on analytic epistemology. This is understandable. Too often, such treatises end up prescribing models as answers to the problem. These models seem to have little practical value to intelligence analysis, which takes place not in a seminar but rather in a fast-breaking world of policy. But that is not the main problem Heuer is addressing.

What Heuer examines so clearly and effectively is how the human thought process builds its own models through which we process information. This is not a phenomenon unique to intelligence; as Heuer's research demonstrates, it is part of the natural functioning of the human cognitive process, and it has been demonstrated across a broad range of fields ranging from medicine to stock market analysis.

The process of analysis itself reinforces this natural function of the human brain. Analysis usually involves creating models, even though they may not be labeled as such. We set forth certain understandings and expectations about cause-and-effect relationships and then process and interpret information through these models or filters.

The discussion in Chapter 5 on the limits to the value of additional information deserves special attention, in my view—particularly for an

1. Douglas MacEachin is a former CIA Deputy Director of Intelligence. After 32 years with the Agency, he retired in 1997 and became a Senior Fellow at Harvard University's John F. Kennedy School of Government.

intelligence organization. What it illustrates is that too often, newly acquired information is evaluated and processed through the existing analytic model, rather than being used to reassess the premises of the model itself. The detrimental effects of this natural human tendency stem from the raison d'etre of an organization created to acquire special, critical information available only through covert means, and to produce analysis integrating this special information with the total knowledge base.

I doubt that any veteran intelligence officer will be able to read this book without recalling cases in which the mental processes described by Heuer have had an adverse impact on the quality of analysis. How many times have we encountered situations in which completely plausible premises, based on solid expertise, have been used to construct a logically valid forecast—with virtually unanimous agreement—that turned out to be dead wrong? In how many of these instances have we determined, with hindsight, that the problem was not in the logic but in the fact that one of the premises—however plausible it seemed at the time—was incorrect? In how many of these instances have we been forced to admit that the erroneous premise was not empirically based but rather a conclusion developed from its own model (sometimes called an assumption)? And in how many cases was it determined after the fact that information had been available which should have provided a basis for questioning one or more premises, and that a change of the relevant premise(s) would have changed the analytic model and pointed to a different outcome?

The commonly prescribed remedy for shortcomings in intelligence analysis and estimates—most vociferously after intelligence "failures"—is a major increase in expertise. Heuer's research and the studies he cites pose a serious challenge to that conventional wisdom. The data show that expertise itself is no protection from the common analytic pitfalls that are endemic to the human thought process. This point has been demonstrated in many fields beside intelligence analysis.

A review of notorious intelligence failures demonstrates that the analytic traps caught the experts as much as anybody. Indeed, the data show that when experts fall victim to these traps, the effects can be aggravated by the confidence that attaches to expertise—both in their own view and in the perception of others.

These observations should in no way be construed as a denigration of the value of expertise. On the contrary, my own 30-plus years in the business of intelligence analysis biased me in favor of the view that, end-

less warnings of information overload notwithstanding, there is no such thing as too much information or expertise. And my own observations of CIA analysts sitting at the same table with publicly renowned experts have given me great confidence that attacks on the expertise issue are grossly misplaced. The main difference is that one group gets to promote its reputations in journals, while the other works in a closed environment in which the main readers are members of the intelligence world's most challenging audience—the policymaking community.

The message that comes through in Heuer's presentation is that information and expertise are a necessary but not sufficient means of making intelligence analysis the special product that it needs to be. A comparable effort has to be devoted to the science of analysis. This effort has to start with a clear understanding of the inherent strengths and weaknesses of the primary analytic mechanism—the human mind—and the way it processes information.

I believe there is a significant cultural element in how intelligence analysts define themselves: Are we substantive experts employed by CIA, or are we professional analysts and intelligence officers whose expertise lies in our ability to adapt quickly to diverse issues and problems and analyze them effectively? In the world at large, substantive expertise is far more abundant than expertise on analytic science and the human mental processing of information. *Dick Heuer makes clear that the pitfalls the human mental process sets for analysts cannot be eliminated; they are part of us. What can be done is to train people how to look for and recognize these mental obstacles, and how to develop procedures designed to offset them.*

Given the centrality of analytic science for the intelligence mission, a key question that Heuer's book poses is: Compared with other areas of our business, have we committed a commensurate effort to the study of analytic science as a professional requirement? How do the effort and resource commitments in this area compare to, for example, the effort and commitment to the development of analysts' writing skills?

Heuer's book does not pretend to be the last word on this issue. Hopefully, it will be a stimulant for much more work.

Introduction

Improving Intelligence Analysis at CIA: Dick Heuer's Contribution to Intelligence Analysis

by Jack Davis[2]

I applaud CIA's Center for the Study of Intelligence for making the work of Richards J. Heuer, Jr. on the psychology of intelligence analysis available to a new generation of intelligence practitioners and scholars.

Dick Heuer's ideas on how to improve analysis focus on helping analysts compensate for the human mind's limitations in dealing with complex problems that typically involve ambiguous information, multiple players, and fluid circumstances. Such multi-faceted estimative challenges have proliferated in the turbulent post-Cold War world.

Heuer's message to analysts can be encapsulated by quoting two sentences from Chapter 4 of this book:

> Intelligence analysts should be self-conscious about their reasoning processes. They should think about *how* they make judgments and reach conclusions, not just about the judgments and conclusions themselves.

Heuer's ideas are applicable to any analytical endeavor. In this Introduction, I have concentrated on his impact—and that of other pioneer thinkers in the intelligence analysis field—at CIA, because that is the institution that Heuer and his predecessors, and I myself, know best, having spent the bulk of our intelligence careers there.

2. Jack Davis served with the Directorate of Intelligence (DI), the National Intelligence Council, and the Office of Training during his CIA career. He is now an independent contractor who specializes in developing and teaching analytic tradecraft. Among his publications is *Uncertainty, Surprise, and Warning* (1996).

Leading Contributors to Quality of Analysis

Intelligence analysts, in seeking to make sound judgments, are always under challenge from the complexities of the issues they address and from the demands made on them for timeliness and volume of production. Four Agency individuals over the decades stand out for having made major contributions on how to deal with these challenges to the quality of analysis.

My short list of the people who have had the greatest positive impact on CIA analysis consists of Sherman Kent, Robert Gates, Douglas MacEachin, and Richards Heuer. My selection methodology was simple. I asked myself: Whose insights have influenced me the most during my four decades of practicing, teaching, and writing about analysis?

Sherman Kent

Sherman Kent's pathbreaking contributions to analysis cannot be done justice in a couple of paragraphs, and I refer readers to fuller treatments elsewhere.[3] Here I address his general legacy to the analytical profession.

Kent, a professor of European history at Yale, worked in the Research and Analysis branch of the Office of Strategic Services during World War II. He wrote an influential book, *Strategic Intelligence for American World Power,* while at the National War College in the late 1940s. He served as Vice Chairman and then as Chairman of the DCI's Board of National Estimates from 1950 to 1967.

Kent's greatest contribution to the quality of analysis was to define an honorable place for the analyst—the thoughtful individual "applying the instruments of reason and the scientific method"—in an intelligence world then as now dominated by collectors and operators. In a second (1965) edition of *Strategic Intelligence,* Kent took account of the coming computer age as well as human and technical collectors in proclaiming the centrality of the analyst:

> Whatever the complexities of the puzzles we strive to solve and whatever the sophisticated techniques we may use to collect

3. See, in particular, the editor's unclassified introductory essay and "Tribute" by Harold P. Ford in Donald P. Steury, *Sherman Kent and the Board of National Estimates: Collected Essays* (CIA, Center for the Study of Intelligence, 1994). Hereinafter cited as Steury, *Kent*.

> the pieces and store them, there can never be a time when the thoughtful man can be supplanted as the intelligence device supreme.

More specifically, Kent advocated application of the techniques of "scientific" study of the past to analysis of complex ongoing situations and estimates of likely future events. Just as rigorous "impartial" analysis could cut through the gaps and ambiguities of information on events long past and point to the most probable explanation, he contended, the powers of the critical mind could turn to events that had not yet transpired to determine the most probable developments.[4]

To this end, Kent developed the concept of the analytic pyramid, featuring a wide base of factual information and sides comprised of sound assumptions, which pointed to the most likely future scenario at the apex.[5]

In his proselytizing and in practice, Kent battled against bureaucratic and ideological biases, which he recognized as impediments to sound analysis, and against imprecise estimative terms that he saw as obstacles to conveying clear messages to readers. Although he was aware of what is now called cognitive bias, his writings urge analysts to "make the call" without much discussion of how limitations of the human mind were to be overcome.

Not many Agency analysts read Kent nowadays. But he had a profound impact on earlier generations of analysts and managers, and his work continues to exert an indirect influence among practitioners of the analytic profession.

Robert Gates

Bob Gates served as Deputy Director of Central Intelligence (1986–1989) and as DCI (1991–1993). But his greatest impact on the quality of CIA analysis came during his 1982–1986 stint as Deputy Director for Intelligence (DDI).

4. Sherman Kent, *Writing History*, second edition (1967). The first edition was published in 1941, when Kent was an assistant professor of history at Yale. In the first chapter, "Why History," he presented ideas and recommendations that he later adapted for intelligence analysis.
5. Kent, "Estimates and Influence" (1968), in Steury, *Kent*.

Initially schooled as a political scientist, Gates earned a Ph.D. in Soviet studies at Georgetown while working as an analyst at CIA. As a member of the National Security Council staff during the 1970s, he gained invaluable insight into how policymakers use intelligence analysis. Highly intelligent, exceptionally hard-working, and skilled in the bureaucratic arts, Gates was appointed DDI by DCI William Casey in good part because he was one of the few insiders Casey found who shared the DCI's views on what Casey saw as glaring deficiencies of Agency analysts.[6] Few analysts and managers who heard it have forgotten Gates' blistering criticism of analytic performance in his 1982 "inaugural" speech as DDI.

Most of the public commentary on Gates and Agency analysis concerned charges of politicization levied against him, and his defense against such charges, during Senate hearings for his 1991 confirmation as DCI. The heat of this debate was slow to dissipate among CIA analysts, as reflected in the pages of *Studies in Intelligence,* the Agency journal founded by Sherman Kent in the 1950s.[7]

I know of no written retrospective on Gates' contribution to Agency analysis. My insights into his ideas about analysis came mostly through an arms-length collaboration in setting up and running an Agency training course entitled "Seminar on Intelligence Successes and Failures."[8] During his tenure as DDI, only rarely could you hold a conversation with analysts or managers without picking up additional viewpoints, thoughtful and otherwise, on what Gates was doing to change CIA analysis.

Gates's ideas for overcoming what he saw as insular, flabby, and incoherent argumentation featured the importance of distinguishing between what analysts know and what they believe—that is, to make clear what is "fact" (or reliably reported information) and what is the analyst's opinion (which had to be persuasively supported with evidence). Among his other tenets were the need to seek the views of non-CIA experts, in-

6. Casey, very early in his tenure as DCI (1981-1987), opined to me that the trouble with Agency analysts is that they went from sitting on their rear ends at universities to sitting on their rear ends at CIA, without seeing the real world.

7. "The Gates Hearings: Politicization and Soviet Analysis at CIA", *Studies in Intelligence* (Spring 1994). "Communication to the Editor: The Gates Hearings: A Biased Account," *Studies in Intelligence* (Fall 1994).

8. DCI Casey requested that the Agency's training office provide this seminar so that, at the least, analysts could learn from their own mistakes. DDI Gates carefully reviewed the statement of goals for the seminar, the outline of course units, and the required reading list.

cluding academic specialists and policy officials, and to present alternate future scenarios.

Gates's main impact, though, came from practice—from his direct involvement in implementing his ideas. Using his authority as DDI, he reviewed critically almost all in-depth assessments and current intelligence articles *prior to publication.* With help from his deputy and two rotating assistants from the ranks of rising junior managers, Gates raised the standards for DDI review dramatically—in essence, from "looks good to me" to "show me your evidence."

As the many drafts Gates rejected were sent back to managers who had approved them—accompanied by the DDI's comments about inconsistency, lack of clarity, substantive bias, and poorly supported judgments—the whole chain of review became much more rigorous. Analysts and their managers raised their standards to avoid the pain of DDI rejection. Both career advancement and ego were at stake.

The rapid and sharp increase in attention paid by analysts and managers to the underpinnings for their substantive judgments probably was without precedent in the Agency's history. The longer term benefits of the intensified review process were more limited, however, because insufficient attention was given to clarifying *tradecraft* practices that would promote analytic soundness. More than one participant in the process observed that a lack of guidelines for meeting Gates's standards led to a large amount of "wheel-spinning."

Gates's impact, like Kent's, has to be seen on two planes. On the one hand, little that Gates wrote on the craft of analysis is read these days. But even though his pre-publication review process was discontinued under his successors, an enduring awareness of his standards still gives pause at jumping to conclusions to many managers and analysts who experienced his criticism first-hand.

Douglas MacEachin

Doug MacEachin, DDI from 1993 to 1996, sought to provide an essential ingredient for ensuring implementation of sound analytic standards: *corporate tradecraft* standards for analysts. This new tradecraft was aimed in particular at ensuring that sufficient attention would be paid to cognitive challenges in assessing complex issues.

MacEachin set out his views on Agency analytical faults and correctives in *The Tradecraft of Analysis: Challenge and Change in the CIA.*[9] My commentary on his contributions to sound analysis is also informed by a series of exchanges with him in 1994 and 1995.

MacEachin's university major was economics, but he also showed great interest in philosophy. His Agency career—like Gates'—included an extended assignment to a policymaking office. He came away from this experience with new insights on what constitutes "value-added" intelligence usable by policymakers. Subsequently, as CIA's senior manager on arms control issues, he dealt regularly with a cadre of tough-minded policy officials who let him know in blunt terms what worked as effective policy support and what did not.

By the time MacEachin became DDI in 1993, Gates's policy of DDI front-office pre-publication review of nearly all DI analytical studies had been discontinued. MacEachin took a different approach; he read—mostly on weekends—and reflected on numerous already-published DI analytical papers. He did not like what he found. In his words, roughly a third of the papers meant to assist the policymaking process had no discernible argumentation to bolster the credibility of intelligence judgments, and another third suffered from flawed argumentation. This experience, along with pressures on CIA for better analytic performance in the wake of alleged "intelligence failures" concerning Iraq's invasion of Kuwait, prompted his decision to launch a major new effort to raise analytical standards.[10]

MacEachin advocated an approach to structured argumentation called "linchpin analysis," to which he contributed muscular terms designed to overcome many CIA professionals' distaste for academic nomenclature. The standard academic term "key variables" became *drivers.* "Hypotheses" concerning drivers became *linchpins*—assumptions underlying the argument—and these had to be explicitly spelled out. MacEachin also urged that greater attention be paid to analytical processes for alerting policymakers to changes in circumstances that would increase the likelihood of alternative scenarios.

9. Unclassified paper published in 1994 by the Working Group on Intelligence Reform, which had been created in 1992 by the Consortium for the Study of Intelligence, Washington, DC.
10. Discussion between MacEachin and the author of this Introduction, 1994.

MacEachin thus worked to put in place systematic and transparent standards for determining whether analysts had met their responsibilities for critical thinking. To spread understanding and application of the standards, he mandated creation of workshops on linchpin analysis for managers and production of a series of notes on analytical tradecraft. He also directed that the DI's performance on tradecraft standards be tracked and that recognition be given to exemplary assessments. Perhaps most ambitious, he saw to it that instruction on standards for analysis was incorporated into a new training course, "Tradecraft 2000." Nearly all DI managers and analysts attended this course during 1996–97.

As of this writing (early 1999), the long-term staying power of MacEachin's tradecraft initiatives is not yet clear. But much of what he advocated has endured so far. Many DI analysts use variations on his linchpin concept to produce soundly argued forecasts. In the training realm, "Tradecraft 2000" has been supplanted by a new course that teaches the same concepts to newer analysts. But examples of what MacEachin would label as poorly substantiated analysis are still seen. Clearly, ongoing vigilance is needed to keep such analysis from finding its way into DI products.

Richards Heuer

Dick Heuer was—and is—much less well known within the CIA than Kent, Gates, and MacEachin. He has not received the wide acclaim that Kent enjoyed as the father of professional analysis, and he has lacked the bureaucratic powers that Gates and MacEachin could wield as DDIs. But his impact on the quality of Agency analysis arguably has been at least as important as theirs.

Heuer received a degree in philosophy in 1950 from Williams College, where, he notes, he became fascinated with the fundamental epistemological question, "What is truth and how can we know it?" In 1951, while a graduate student at the University of California's Berkeley campus, he was recruited as part of the CIA's buildup during the Korean War. The recruiter was Richard Helms, OSS veteran and rising player in the Agency's clandestine service. Future DCI Helms, according to Heuer, was looking for candidates for CIA employment among recent graduates of Williams College, his own alma mater. Heuer had an added advantage

as a former editor of the college's newspaper, a position Helms had held some 15 years earlier.[11]

In 1975, after 24 years in the Directorate of Operations, Heuer moved to the DI. His earlier academic interest in how we know the truth was rekindled by two experiences. One was his involvement in the controversial case of Soviet KGB defector Yuriy Nosenko. The other was learning new approaches to social science methodology while earning a Master's degree in international relations at the University of Southern California's European campus.

At the time he retired in 1979, Heuer headed the methodology unit in the DI's political analysis office. He originally prepared most of the chapters in this book as individual articles between 1978 and 1986; many of them were written for the DI after his retirement. He has updated the articles and prepared some new material for inclusion in this book.

Heuer's Central Ideas

Dick Heuer's writings make three fundamental points about the cognitive challenges intelligence analysts face:

- The mind is poorly "wired" to deal effectively with both inherent uncertainty (the natural fog surrounding complex, indeterminate intelligence issues) and induced uncertainty (the man-made fog fabricated by denial and deception operations).

- Even increased awareness of cognitive and other "unmotivated" biases, such as the tendency to see information confirming an already-held judgment more vividly than one sees "disconfirming" information, does little by itself to help analysts deal effectively with uncertainty.

- Tools and techniques that gear the analyst's mind to apply higher levels of critical thinking can substantially improve analysis on complex issues on which information is incomplete, ambiguous, and often deliberately distorted. Key examples of such intellectu-

11. Letter to the author of this Introduction, 1998.

al devices include techniques for structuring information, challenging assumptions, and exploring alternative interpretations.

The following passage from Heuer's 1980 article entitled "Perception: Why Can't We See What Is There to be Seen?" shows that his ideas were similar to or compatible with MacEachin's concepts of linchpin analysis.

> Given the difficulties inherent in the human processing of complex information, a prudent management system should:
>
> - Encourage products that (a) clearly delineate their assumptions and chains of inference and (b) specify the degree and source of the uncertainty involved in the conclusions.
>
> - Emphasize procedures that expose and elaborate alternative points of view—analytic debates, devil's advocates, interdisciplinary brainstorming, competitive analysis, intra-office peer review of production, and elicitation of outside expertise.

Heuer emphasizes both the value and the dangers of *mental models,* or *mind-sets.* In the book's opening chapter, entitled "Thinking About Thinking," he notes that:

> [Analysts] construct their own version of "reality" on the basis of information provided by the senses, but this sensory input is mediated by complex mental processes that determine which information is attended to, how it is organized, and the meaning attributed to it. What people perceive, how readily they perceive it, and how they process this information after receiving it are all strongly influenced by past experience, education, cultural values, role requirements, and organizational norms, as well as by the specifics of the information received.
>
> This process may be visualized as perceiving the world through a lens or screen that channels and focuses and thereby may distort the images that are seen. To achieve the clearest possible image . . . analysts need more than information . . . They also

> need to understand the lenses through which this information passes. These lenses are known by many terms—mental models, mind-sets, biases, or analytic assumptions.

In essence, Heuer sees reliance on mental models to simplify and interpret reality as an unavoidable conceptual mechanism for intelligence analysts—often useful, but at times hazardous. What is required of analysts, in his view, is a commitment to *challenge, refine, and challenge again* their own working mental models, precisely because these steps are central to sound interpretation of complex and ambiguous issues.

Throughout the book, Heuer is critical of the orthodox prescription of "more and better information" to remedy unsatisfactory analytic performance. He urges that greater attention be paid instead to more intensive exploitation of information already on hand, and that in so doing, analysts continuously challenge and revise their mental models.

Heuer sees *mirror-imaging* as an example of an unavoidable cognitive trap. No matter how much expertise an analyst applies to interpreting the value systems of foreign entities, when the hard evidence runs out the tendency to project the analyst's own mind-set takes over. In Chapter 4, Heuer observes:

> To see the options faced by foreign leaders as these leaders see them, one must understand their values and assumptions and even their misperceptions and misunderstandings. Without such insight, interpreting foreign leaders' decisions or forecasting future decisions is often nothing more than partially informed speculation. Too frequently, foreign behavior appears "irrational" or "not in their own best interest." Such conclusions often indicate analysts have projected American values and conceptual frameworks onto the foreign leaders and societies, rather than understanding the logic of the situation as it appears to them.

Competing Hypotheses

To offset the risks accompanying analysts' inevitable recourse to mirror-imaging, Heuer suggests looking upon analysts' calculations about

foreign beliefs and behavior as hypotheses to be challenged. Alternative hypotheses need to be carefully considered—especially those that cannot be *disproved* on the basis of available information.

Heuer's concept of "Analysis of Competing Hypotheses" (ACH) is among his most important contributions to the development of an intelligence analysis methodology. At the core of ACH is the notion of competition among a series of plausible hypotheses to see which ones survive a gauntlet of testing for compatibility with available information. The surviving hypotheses—those that have not been disproved—are subjected to further testing. ACH, Heuer concedes, will not always yield the right answer. But it can help analysts overcome the cognitive limitations discussed in his book.

Some analysts who use ACH follow Heuer's full eight-step methodology. More often, they employ some elements of ACH—especially the use of available information to challenge the hypotheses that the analyst favors the most.

Denial and Deception

Heuer's path-breaking work on countering denial and deception (D&D) was not included as a separate chapter in this volume. But his brief references here are persuasive.

He notes, for example, that analysts often reject the possibility of deception because they see no evidence of it. He then argues that rejection is not justified under these circumstances. If deception is well planned and properly executed, one should not expect to see evidence of it readily at hand. Rejecting a plausible but unproven hypothesis too early tends to bias the subsequent analysis, because one does not then look for the evidence that might support it. The possibility of deception should not be rejected until it is disproved or, at least, until a systematic search for evidence has been made and none has been found.

Heuer's Impact

Heuer's influence on analytic tradecraft began with his first articles. CIA officials who set up training courses in the 1980s as part of then-DDI Gates's quest for improved analysis shaped their lesson plans partly on the basis of Heuer's findings. Among these courses were a seminar on intelligence successes and failures and another on intelligence analysis.

The courses influenced scores of DI analysts, many of whom are now in the managerial ranks. The designers and teachers of Tradecraft 2000 clearly were also influenced by Heuer, as reflected in reading selections, case studies, and class exercises.

Heuer's work has remained on reading lists and in lesson plans for DI training courses offered to all new analysts, as well as courses on warning analysis and on countering denial and deception. Senior analysts and managers who have been directly exposed to Heuer's thinking through his articles, or through training courses, continue to pass his insights on to newer analysts.

Recommendations

Heuer's advice to Agency leaders, managers, and analysts is pointed: To ensure sustained improvement in assessing complex issues, analysis must be treated as more than a substantive and organizational process. Attention also must be paid to techniques and tools for coping with the inherent limitations on analysts' mental machinery. He urges that Agency leaders take steps to:

- *Establish an organizational environment* that promotes and rewards the kind of critical thinking he advocates—or example, analysis on difficult issues that considers in depth a series of plausible hypotheses rather than allowing the first credible hypothesis to suffice.

- *Expand funding for research* on the role such mental processes play in shaping analytical judgments. An Agency that relies on sharp cognitive performance by its analysts must stay abreast of studies on how the mind works—i.e., on *how* analysts reach judgments.

- *Foster development of tools* to assist analysts in assessing information. On tough issues, they need help in improving their mental models and in deriving incisive findings from information they already have; they need such help at least as much as they need more information.

I offer some concluding observations and recommendations, rooted in Heuer's findings and taking into account the tough tradeoffs facing intelligence professionals:

- *Commit to a uniform set of tradecraft standards based on the insights in this book.* Leaders need to know if analysts have done their cognitive homework before taking corporate responsibility for their judgments. Although every analytical issue can be seen as one of a kind, I suspect that nearly all such topics fit into about a dozen recurring patterns of challenge based largely on variations in substantive uncertainty and policy sensitivity. Corporate standards need to be established for each such category. And the burden should be put on managers to explain why a given analytical assignment requires deviation from the standards. I am convinced that if tradecraft standards are made uniform and transparent, the time saved by curtailing personalistic review of quick-turnaround analysis (e.g., "It reads better to me this way") could be "re-invested" in doing battle more effectively against cognitive pitfalls. ("Regarding point 3, let's talk about your assumptions.")

- *Pay more honor to "doubt."* Intelligence leaders and policymakers should, in recognition of the cognitive impediments to sound analysis, establish ground rules that enable analysts, after doing their best to clarify an issue, to express doubts more openly. They should be encouraged to list gaps in information and other obstacles to confident judgment. Such conclusions as "We do not know" or "There are several potentially valid ways to assess this issue" should be regarded as badges of sound analysis, not as dereliction of analytic duty.

- *Find a couple of successors to Dick Heuer. Fund their research. Heed their findings.*

PART I—OUR MENTAL MACHINERY

Chapter 1

Thinking About Thinking

Of the diverse problems that impede accurate intelligence analysis, those inherent in human mental processes are surely among the most important and most difficult to deal with. Intelligence analysis is fundamentally a mental process, but understanding this process is hindered by the lack of conscious awareness of the workings of our own minds.

A basic finding of cognitive psychology is that people have no conscious experience of most of what happens in the human mind. Many functions associated with perception, memory, and information processing are conducted prior to and independently of any conscious direction. What appears spontaneously in consciousness is the result of thinking, not the process of thinking.

Weaknesses and biases inherent in human thinking processes can be demonstrated through carefully designed experiments. They can be alleviated by conscious application of tools and techniques that should be in the analytical tradecraft toolkit of all intelligence analysts.

* * * * * * * * * * * * * * * * * * * *

"When we speak of improving the mind we are usually referring to the acquisition of information or knowledge, or to the type of thoughts one should have, and not to the actual functioning of the mind. We spend little time monitoring our own thinking and comparing it with a more sophisticated ideal."[12]

When we speak of improving intelligence analysis, we are usually referring to the quality of writing, types of analytical products, relations between intelligence analysts and intelligence consumers, or organization

12. James L. Adams, *Conceptual Blockbusting: A Guide to Better Ideas* (New York: W.W. Norton, second edition, 1980), p. 3.

of the analytical process. Little attention is devoted to improving how analysts think.

Thinking analytically is a skill like carpentry or driving a car. It can be taught, it can be learned, and it can improve with practice. But like many other skills, such as riding a bike, it is not learned by sitting in a classroom and being told how to do it. Analysts learn by doing. Most people achieve at least a minimally acceptable level of analytical performance with little conscious effort beyond completing their education. With much effort and hard work, however, analysts can achieve a level of excellence beyond what comes naturally.

Regular running enhances endurance but does not improve technique without expert guidance. Similarly, expert guidance may be required to modify long-established analytical habits to achieve an optimal level of analytical excellence. An analytical coaching staff to help young analysts hone their analytical tradecraft would be a valuable supplement to classroom instruction.

One key to successful learning is motivation. Some of CIA's best analysts developed their skills as a consequence of experiencing analytical failure early in their careers. Failure motivated them to be more self-conscious about how they do analysis and to sharpen their thinking process.

This book aims to help intelligence analysts achieve a higher level of performance. It shows how people make judgments based on incomplete and ambiguous information, and it offers simple tools and concepts for improving analytical skills.

Part I identifies some limitations inherent in human mental processes. Part II discusses analytical tradecraft—simple tools and approaches for overcoming these limitations and thinking more systematically. Chapter 8, "Analysis of Competing Hypotheses," is arguably the most important single chapter. Part III presents information about cognitive biases—the technical term for predictable mental errors caused by simplified information processing strategies. A final chapter presents a checklist for analysts and recommendations for how managers of intelligence analysis can help create an environment in which analytical excellence flourishes.

Herbert Simon first advanced the concept of "bounded" or limited rationality.[13] Because of limits in human mental capacity, he argued, the

13. Herbert Simon, *Models of Man*, 1957.

mind cannot cope directly with the complexity of the world. Rather, we construct a simplified mental model of reality and then work with this model. We behave rationally within the confines of our mental model, but this model is not always well adapted to the requirements of the real world. The concept of bounded rationality has come to be recognized widely, though not universally, both as an accurate portrayal of human judgment and choice and as a sensible adjustment to the limitations inherent in how the human mind functions.[14]

Much psychological research on perception, memory, attention span, and reasoning capacity documents the limitations in our "mental machinery" identified by Simon. Many scholars have applied these psychological insights to the study of international political behavior.[15] A similar psychological perspective underlies some writings on intelligence failure and strategic surprise.[16]

This book differs from those works in two respects. It analyzes problems from the perspective of intelligence analysts rather than policymakers. And it documents the impact of mental processes largely through

14. James G. March., "Bounded Rationality, Ambiguity, and the Engineering of Choice," in David E. Bell, Howard Raiffa, and Amos Tversky, eds., *Decision Making: Descriptive, Normative, and Prescriptive Interactions* (Cambridge University Press, 1988).

15. Among the early scholars who wrote on this subject were Joseph De Rivera, *The Psychological Dimension of Foreign Policy* (Columbus, OH: Merrill, 1968), Alexander George and Richard Smoke, *Deterrence in American Foreign Policy* (New York: Columbia University Press, 1974), and Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976).

16. Christopher Brady, "Intelligence Failures: Plus Ca Change. . ." Intelligence and National Security, Vol. 8, No. 4 (October 1993). N. Cigar, "Iraq's Strategic Mindset and the Gulf War: Blueprint for Defeat," *The Journal of Strategic Studies*, Vol. 15, No. 1 (March 1992). J. J. Wirtz, *The Tet Offensive: Intelligence Failure in War* (New York, 1991). Ephraim Kam, *Surprise Attack* (Harvard University Press, 1988). Richard Betts, *Surprise Attack: Lessons for Defense Planning* (Brookings, 1982). Abraham Ben-Zvi, "The Study of Surprise Attacks," *British Journal of International Studies*, Vol. 5 (1979). *Iran: Evaluation of Intelligence Performance Prior to November 1978* (Staff Report, Subcommittee on Evaluation, Permanent Select Committee on Intelligence, US House of Representatives, January 1979). Richard Betts, "Analysis, War and Decision: Why Intelligence Failures Are Inevitable," *World Politics*, Vol. 31, No. 1 (October 1978). Richard W. Shryock, "The Intelligence Community Post-Mortem Program, 1973-1975," *Studies in Intelligence*, Vol. 21, No. 1 (Fall 1977). Avi Schlaim, "Failures in National Intelligence Estimates: The Case of the Yom Kippur War," *World Politics*, Vol. 28 (April 1976). Michael Handel, *Perception, Deception, and Surprise: The Case of the Yom Kippur War* (Jerusalem: Leonard Davis Institute of International Relations, Jerusalem Paper No. 19, 1976). Klaus Knorr, "Failures in National Intelligence Estimates: The Case of the Cuban Missiles," *World Politics*, Vol. 16 (1964).

experiments in cognitive psychology rather than through examples from diplomatic and military history.

A central focus of this book is to illuminate the role of the observer in determining what is observed and how it is interpreted. People construct their own version of "reality" on the basis of information provided by the senses, but this sensory input is mediated by complex mental processes that determine which information is attended to, how it is organized, and the meaning attributed to it. What people perceive, how readily they perceive it, and how they process this information after receiving it are all strongly influenced by past experience, education, cultural values, role requirements, and organizational norms, as well as by the specifics of the information received.

This process may be visualized as perceiving the world through a lens or screen that channels and focuses and thereby may distort the images that are seen. To achieve the clearest possible image of China, for example, analysts need more than information on China. They also need to understand their own lenses through which this information passes. These lenses are known by many terms—mental models, mind-sets, biases, or analytical assumptions.

In this book, the terms mental model and mind-set are used more or less interchangeably, although a mental model is likely to be better developed and articulated than a mind-set. An analytical assumption is one part of a mental model or mind-set. The biases discussed in this book result from how the mind works and are independent of any substantive mental model or mind-set.

Before obtaining a license to practice, psychoanalysts are required to undergo psychoanalysis themselves in order to become more aware of how their own personality interacts with and conditions their observations of others. The practice of psychoanalysis has not been so successful that its procedures should be emulated by the intelligence and foreign policy community. But the analogy highlights an interesting point: Intelligence analysts must understand themselves before they can understand others. Training is needed to (a) increase self-awareness concerning generic problems in how people perceive and make analytical judgments concerning foreign events, and (b) provide guidance and practice in overcoming these problems.

Not enough training is focused in this direction—that is, inward toward the analyst's own thought processes. Training of intelligence ana-

lysts generally means instruction in organizational procedures, methodological techniques, or substantive topics. More training time should be devoted to the mental act of thinking or analyzing. It is simply assumed, incorrectly, that analysts know how to analyze. This book is intended to support training that examines the thinking and reasoning processes involved in intelligence analysis.

As discussed in the next chapter, mind-sets and mental models are inescapable. They are, in essence, a distillation of all that we think we know about a subject. The problem is how to ensure that the mind remains open to alternative interpretations in a rapidly changing world.

The disadvantage of a mind-set is that it can color and control our perception to the extent that an experienced specialist may be among the last to see what is really happening when events take a new and unexpected turn. When faced with a major paradigm shift, analysts who know the most about a subject have the most to unlearn. This seems to have happened before the reunification of Germany, for example. Some German specialists had to be prodded by their more generalist supervisors to accept the significance of the dramatic changes in progress toward reunification of East and West Germany.

The advantage of mind-sets is that they help analysts get the production out on time and keep things going effectively between those watershed events that become chapter headings in the history books.[17]

A generation ago, few intelligence analysts were self-conscious and introspective about the process by which they did analysis. The accepted wisdom was the "common sense" theory of knowledge—that to perceive events accurately it was necessary only to open one's eyes, look at the facts, and purge oneself of all preconceptions and prejudices in order to make an objective judgment.

Today, there is greatly increased understanding that intelligence analysts do not approach their tasks with empty minds. They start with a set of assumptions about how events normally transpire in the area for which they are responsible. Although this changed view is becoming conventional wisdom, the Intelligence Community has only begun to scratch the surface of its implications.

If analysts' understanding of events is greatly influenced by the mind-set or mental model through which they perceive those events,

17. This wording is from a discussion with veteran CIA analyst, author, and teacher Jack Davis.

should there not be more research to explore and document the impact of different mental models?[18]

The reaction of the Intelligence Community to many problems is to collect more information, even though analysts in many cases already have more information than they can digest. What analysts need is more truly useful information—mostly reliable HUMINT from knowledgeable insiders—to help them make good decisions. Or they need a more accurate mental model and better analytical tools to help them sort through, make sense of, and get the most out of the available ambiguous and conflicting information.

Psychological research also offers to intelligence analysts additional insights that are beyond the scope of this book. Problems are not limited to how analysts perceive and process information. Intelligence analysts often work in small groups and always within the context of a large, bureaucratic organization. Problems are inherent in the processes that occur at all three levels—individual, small group, and organization. This book focuses on problems inherent in analysts' mental processes, inasmuch as these are probably the most insidious. Analysts can observe and get a feel for these problems in small-group and organizational processes, but it is very difficult, at best, to be self-conscious about the workings of one's own mind.

18. Graham Allison's work on the Cuban missile crisis (*Essence of Decision*, Little, Brown & Co., 1971) is an example of what I have in mind. Allison identified three alternative assumptions about how governments work--a rational actor model, an organizational process model, and a bureaucratic politics model. He then showed how an analyst's implicit assumptions about the most appropriate model for analyzing a foreign government's behavior can cause him or her to focus on different evidence and arrive at different conclusions. Another example is my own analysis of five alternative paths for making counterintelligence judgments in the controversial case of KGB defector Yuriy Nosenko: Richards J. Heuer, Jr., "Nosenko: Five Paths to Judgment," *Studies in Intelligence*, Vol. 31, No. 3 (Fall 1987), originally classified Secret but declassified and published in H. Bradford Westerfield, ed., *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal 1955-1992* (New Haven: Yale University Press, 1995).

Chapter 2

Perception: Why Can't We See What Is There To Be Seen?

The process of perception links people to their environment and is critical to accurate understanding of the world about us. Accurate intelligence analysis obviously requires accurate perception. Yet research into human perception demonstrates that the process is beset by many pitfalls. Moreover, the circumstances under which intelligence analysis is conducted are precisely the circumstances in which accurate perception tends to be most difficult. This chapter discusses perception in general, then applies this information to illuminate some of the difficulties of intelligence analysis.[19]

* * * * * * * * * * * * * * * * * * * *

People tend to think of perception as a passive process. We see, hear, smell, taste or feel stimuli that impinge upon our senses. We think that if we are at all objective, we record what is actually there. Yet perception is demonstrably an active rather than a passive process; it constructs rather than records "reality." Perception implies understanding as well as awareness. It is a process of inference in which people construct their own version of reality on the basis of information provided through the five senses.

As already noted, what people in general and analysts in particular perceive, and how readily they perceive it, are strongly influenced by their past experience, education, cultural values, and role requirements, as well as by the stimuli recorded by their receptor organs.

Many experiments have been conducted to show the extraordinary extent to which the information obtained by an observer depends upon the observer's own assumptions and preconceptions. For example, when

19. An earlier version of this article was published as part of "Cognitive Factors in Deception and Counterdeception," in Donald C. Daniel and Katherine L. Herbig, eds., *Strategic Military Deception* (Pergamon Press, 1982).

Figure 1

you looked at Figure 1 above, what did you see? Now refer to the footnote for a description of what is actually there.[20] Did you perceive Figure 1 correctly? If so, you have exceptional powers of observation, were lucky, or have seen the figure before. This simple experiment demonstrates one of the most fundamental principles concerning perception:

We tend to perceive what we expect to perceive.

A corollary of this principle is that it takes more information, and more unambiguous information, to recognize an unexpected phenomenon than an expected one.

One classic experiment to demonstrate the influence of expectations on perception used playing cards, some of which were gimmicked so the spades were red and the hearts black. Pictures of the cards were flashed briefly on a screen and, needless to say, the test subjects identified the normal cards more quickly and accurately than the anomalous ones. After test subjects became aware of the existence of red spades and black hearts, their performance with the gimmicked cards improved but still did not approach the speed or accuracy with which normal cards could be identified.[21]

20. The article is written twice in each of the three phrases. This is commonly overlooked because perception is influenced by our expectations about how these familiar phrases are normally written.

21. Jerome S. Bruner and Leo Postman, "On the Perception of Incongruity: A Paradigm," in Jerome S. Bruner and David Kraut, eds., *Perception and Personality: A Symposium* (New York: Greenwood Press, 1968).

This experiment shows that patterns of expectation become so deeply embedded that they continue to influence perceptions even when people are alerted to and try to take account of the existence of data that do not fit their preconceptions. Trying to be objective does not ensure accurate perception.

The position of the test subject identifying playing cards is analogous to that of the intelligence analyst or government leader trying to make sense of the paper flow that crosses his or her desk. What is actually perceived in that paper flow, as well as how it is interpreted, depends in part, at least, on the analyst's patterns of expectation. Analysts do not just have expectations about the color of hearts and spades. They have a set of assumptions and expectations about the motivations of people and the processes of government in foreign countries. Events consistent with these expectations are perceived and processed easily, while events that contradict prevailing expectations tend to be ignored or distorted in perception. Of course, this distortion is a subconscious or pre-conscious process, as illustrated by how you presumably ignored the extra words in the triangles in Figure 1.

This tendency of people to perceive what they *expect* to perceive is more important than any tendency to perceive what they *want* to perceive. In fact, there may be no real tendency toward wishful thinking. The commonly cited evidence supporting the claim that people tend to perceive what they want to perceive can generally be explained equally well by the expectancy thesis.[22]

Expectations have many diverse sources, including past experience, professional training, and cultural and organizational norms. All these influences predispose analysts to pay particular attention to certain kinds of information and to organize and interpret this information in certain ways. Perception is also influenced by the context in which it occurs. Different circumstances evoke different sets of expectations. People are more attuned to hearing footsteps behind them when walking in an alley at night than along a city street in daytime, and the meaning attributed to the sound of footsteps will vary under these differing circumstances. A military intelligence analyst may be similarly tuned to perceive indicators of potential conflict.

22. For discussion of the ambiguous evidence concerning the impact of desires and fears on judgment, see Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), Chapter 10.

Patterns of expectations tell analysts, subconsciously, what to look for, what is important, and how to interpret what is seen. These patterns form a mind-set that predisposes analysts to think in certain ways. A mind-set is akin to a screen or lens through which one perceives the world.

There is a tendency to think of a mind-set as something bad, to be avoided. According to this line of argument, one should have an open mind and be influenced only by the facts rather than by preconceived notions! That is an unreachable ideal. There is no such thing as "the facts of the case." There is only a very selective subset of the overall mass of data to which one has been subjected that one takes as facts and judges to be relevant to the question at issue.

Actually, mind-sets are neither good nor bad; they are unavoidable. People have no conceivable way of coping with the volume of stimuli that impinge upon their senses, or with the volume and complexity of the data they have to analyze, without some kind of simplifying preconceptions about what to expect, what is important, and what is related to what. "There is a grain of truth in the otherwise pernicious maxim that an open mind is an empty mind."[23] Analysts do not achieve objective analysis by avoiding preconceptions; that would be ignorance or self-delusion. Objectivity is achieved by making basic assumptions and reasoning as explicit as possible so that they can be challenged by others and analysts can, themselves, examine their validity.

One of the most important characteristics of mind-sets is:

Mind-sets tend to be quick to form but resistant to change.

Figure 2 illustrates this principle by showing part of a longer series of progressively modified drawings that change almost imperceptibly from a man into a woman.[24] The right-hand drawing in the top row, when viewed alone, has equal chances of being perceived as a man or a woman. When test subjects are shown the entire series of drawings one by one, their perception of this intermediate drawing is biased according to which end of the series they started from. Test subjects who start by viewing a picture that is clearly a man are biased in favor of continuing

23. Richard Betts, "Analysis, War and Decision: Why Intelligence Failures are Inevitable", *World Politics*, Vol. XXXI (October 1978), p. 84.
24. Drawings devised by Gerald Fisher in 1967.

Figure 2

Impressions resist change.

to see a man long after an "objective observer" (for example, an observer who has seen only a single picture) recognizes that the man is now a woman. Similarly, test subjects who start at the woman end of the series are biased in favor of continuing to see a woman. Once an observer has formed an image—that is, once he or she has developed a mind-set or expectation concerning the phenomenon being observed—this conditions future perceptions of that phenomenon.

This is the basis for another general principle of perception:

New information is assimilated to existing images.

This principle explains why gradual, evolutionary change often goes unnoticed. It also explains the phenomenon that an intelligence analyst assigned to work on a topic or country for the first time may generate accurate insights that have been overlooked by experienced analysts who have worked on the same problem for 10 years. A fresh perspective is sometimes useful; past experience can handicap as well as aid analysis. This tendency to assimilate new data into pre-existing images is greater "the more ambiguous the information, the more confident the actor is of

Figure 3

It is difficult to look at the same information from different perspectives.

the validity of his image, and the greater his commitment to the established view."[25]

The drawing in Figure 3 provides the reader an opportunity to test for him or herself the persistence of established images.[26] Look at Figure 3. What do you see—an old woman or a young woman? Now look again to see if you can visually and mentally reorganize the data to form a different image—that of a young woman if your original perception was of an old woman, or of the old woman if you first perceived the young one. If necessary, look at the footnote for clues to help you identify the other

25. Jervis, p. 195.
26. This picture was originally published in *Puck* magazine in 1915 as a cartoon entitled "My Wife and My Mother-in-Law."

image.[27] Again, this exercise illustrates the principle that mind-sets are quick to form but resistant to change.

When you have seen Figure 3 from *both* perspectives, try shifting back and forth from one perspective to the other. Do you notice some initial difficulty in making this switch? One of the more difficult mental feats is to take a familiar body of data and reorganize it visually or mentally to perceive it from a different perspective. Yet this is what intelligence analysts are constantly required to do. In order to understand international interactions, analysts must understand the situation as it appears to each of the opposing forces, and constantly shift back and forth from one perspective to the other as they try to fathom how each side interprets an ongoing series of interactions. Trying to perceive an adversary's interpretations of international events, as well as US interpretations of those same events, is comparable to seeing both the old and young woman in Figure 3. Once events have been perceived one way, there is a natural resistance to other perspectives.

A related point concerns the impact of substandard conditions of perception. The basic principle is:

> **Initial exposure to blurred or ambiguous stimuli interferes with accurate perception even after more and better information becomes available.**

This effect has been demonstrated experimentally by projecting onto a screen pictures of common, everyday subjects such as a dog standing on grass, a fire hydrant, and an aerial view of a highway cloverleaf intersection.[28] The initial projection was blurred in varying degrees, and the pictures were then brought into focus slowly to determine at what point test subjects could identify them correctly.

This experiment showed two things. First, those who started viewing the pictures when they were most out of focus had more difficulty identifying them when they became clearer than those who started view-

27. The old woman's nose, mouth, and eye are, respectively, the young woman's chin, necklace, and ear. The old woman is seen in profile looking left. The young woman is also looking left, but we see her mainly from behind so most facial features are not visible. Her eyelash, nose, and the curve of her cheek may be seen just above the old woman's nose.
28. Jerome S. Bruner and Mary C. Potter, "Interference in Visual Recognition," *Science*, Vol. 144 (1964), pp. 424-25.

ing at a less blurred stage. In other words, the greater the initial blur, the clearer the picture had to be before people could recognize it. Second, the longer people were exposed to a blurred picture, the clearer the picture had to be before they could recognize it.

What happened in this experiment is what presumably happens in real life; despite ambiguous stimuli, people form some sort of tentative hypothesis about what they see. The longer they are exposed to this blurred image, the greater confidence they develop in this initial and perhaps erroneous impression, so the greater the impact this initial impression has on subsequent perceptions. For a time, as the picture becomes clearer, there is no *obvious* contradiction; the new data are assimilated into the previous image, and the initial interpretation is maintained until the contradiction becomes so obvious that it forces itself upon our consciousness.

The early but incorrect impression tends to persist because the amount of information necessary to invalidate a hypothesis is considerably greater than the amount of information required to make an initial interpretation. The problem is not that there is any inherent difficulty in grasping new perceptions or new ideas, but that established perceptions are so difficult to change. People form impressions on the basis of very little information, but once formed, they do not reject or change them unless they obtain rather solid evidence. Analysts might seek to limit the adverse impact of this tendency by suspending judgment for as long as possible as new information is being received.

Implications for Intelligence Analysis

Comprehending the nature of perception has significant implications for understanding the nature and limitations of intelligence analysis. The circumstances under which accurate perception is most difficult are exactly the circumstances under which intelligence analysis is generally conducted—dealing with highly ambiguous situations on the basis of information that is processed incrementally under pressure for early judgment. This is a recipe for inaccurate perception.

Intelligence seeks to illuminate the unknown. Almost by definition, intelligence analysis deals with highly ambiguous situations. As previously noted, the greater the ambiguity of the stimuli, the greater the impact of expectations and pre-existing images on the perception of that

stimuli. Thus, despite maximum striving for objectivity, the intelligence analyst's own preconceptions are likely to exert a greater impact on the analytical product than in other fields where an analyst is working with less ambiguous and less discordant information.

Moreover, the intelligence analyst is among the first to look at new problems at an early stage when the evidence is very fuzzy indeed. The analyst then follows a problem as additional increments of evidence are received and the picture gradually clarifies—as happened with test subjects in the experiment demonstrating that initial exposure to blurred stimuli interferes with accurate perception even after more and better information becomes available. If the results of this experiment can be generalized to apply to intelligence analysts, the experiment suggests that an analyst who starts observing a potential problem situation at an early and unclear stage is at a disadvantage as compared with others, such as policymakers, whose first exposure may come at a later stage when more and better information is available.

The receipt of information in small increments over time also facilitates assimilation of this information into the analyst's existing views. No one item of information may be sufficient to prompt the analyst to change a previous view. The cumulative message inherent in many pieces of information may be significant but is attenuated when this information is not examined as a whole. The Intelligence Community's review of its performance before the 1973 Arab-Israeli War noted:

> The problem of incremental analysis—especially as it applies to the current intelligence process—was also at work in the period preceding hostilities. Analysts, according to their own accounts, were often proceeding on the basis of the day's take, hastily comparing it with material received the previous day. They then produced in 'assembly line fashion' items which may have reflected perceptive intuition but which [did not] accrue from a systematic consideration of an accumulated body of integrated evidence.[29]

And finally, the intelligence analyst operates in an environment that exerts strong pressures for what psychologists call premature closure.

29. *The Performance of the Intelligence Community Before the Arab-Israeli War of October 1973: A Preliminary Post-Mortem Report,* December 1973. The one-paragraph excerpt from this post-mortem, as quoted in the text above, has been approved for public release, as was the title of the post-mortem, although that document as a whole remains classified.

Customer demand for interpretive analysis is greatest within two or three days after an event occurs. The system requires the intelligence analyst to come up with an almost instant diagnosis before sufficient hard information, and the broader background information that may be needed to gain perspective, become available to make possible a well-grounded judgment. This diagnosis can only be based upon the analyst's preconceptions concerning how and why events normally transpire in a given society.

As time passes and more information is received, a fresh look at all the evidence might suggest a different explanation. Yet, the perception experiments indicate that an early judgment adversely affects the formation of future perceptions. Once an observer thinks he or she knows what is happening, this perception tends to resist change. New data received incrementally can be fit easily into an analyst's previous image. This perceptual bias is reinforced by organizational pressures favoring consistent interpretation; once the analyst is committed in writing, both the analyst and the organization have a vested interest in maintaining the original assessment.

That intelligence analysts perform as well as they do is testimony to their generally sound judgment, training, and dedication in performing a dauntingly difficult task.

The problems outlined here have implications for the management as well as the conduct of analysis. Given the difficulties inherent in the human processing of complex information, a prudent management system should:

- Encourage products that clearly delineate their assumptions and chains of inference and that specify the degree and source of uncertainty involved in the conclusions.
- Support analyses that periodically re-examine key problems from the ground up in order to avoid the pitfalls of the incremental approach.
- Emphasize procedures that expose and elaborate alternative points of view.
- Educate consumers about the limitations as well as the capabilities of intelligence analysis; define a set of realistic expectations as a standard against which to judge analytical performance.

Chapter 3

Memory: How Do We Remember What We Know?

Differences between stronger and weaker analytical performance are attributable in large measure to differences in the organization of data and experience in analysts' long-term memory. The contents of memory form a continuous input into the analytical process, and anything that influences what information is remembered or retrieved from memory also influences the outcome of analysis.

This chapter discusses the capabilities and limitations of several components of the memory system. Sensory information storage and short-term memory are beset by severe limitations of capacity, while long-term memory, for all practical purposes, has a virtually infinite capacity. With long-term memory, the problems concern getting information into it and retrieving information once it is there, not physical limits on the amount of information that may be stored. Understanding how memory works provides insight into several analytical strengths and weaknesses.

* * * * * * * * * * * * * * * * * * * *

Components of the Memory System

What is commonly called memory is not a single, simple function. It is an extraordinarily complex system of diverse components and processes. There are at least three, and very likely more, distinct memory processes. The most important from the standpoint of this discussion and best documented by scientific research are sensory information stor-

age (SIS), short-term memory (STM), and long-term memory (LTM).[30] Each differs with respect to function, the form of information held, the length of time information is retained, and the amount of information-handling capacity. Memory researchers also posit the existence of an interpretive mechanism and an overall memory monitor or control mechanism that guides interaction among various elements of the memory system.

Sensory Information Storage

Sensory information storage holds sensory images for several tenths of a second after they are received by the sensory organs. The functioning of SIS may be observed if you close your eyes, then open and close them again as rapidly as possible. As your eyes close, notice how the visual image is maintained for a fraction of a second before fading. Sensory information storage explains why a movie film shot at 16 separate frames per second appears as continuous movement rather than a series of still pictures. A visual trace is generally retained in SIS for about one-quarter of a second. It is not possible to consciously extend the time that sensory information is held in SIS. The function of SIS is to make it possible for the brain to work on processing a sensory event for longer than the duration of the event itself.

Short-Term Memory

Information passes from SIS into short-term memory, where again it is held for only a short period of time—a few seconds or minutes. Whereas SIS holds the complete image, STM stores only the interpretation of the image. If a sentence is spoken, SIS retains the sounds, while STM holds the words formed by these sounds.

Like SIS, short-term memory holds information temporarily, pending further processing. This processing includes judgments concerning meaning, relevance, and significance, as well as the mental actions necessary to integrate selected portions of the information into long-term

30. Memory researchers do not employ uniform terminology. Sensory information storage is also known as sensory register, sensory store, and eidetic and echoic memory. Short- and long-term memory are also referred to as primary and secondary memory. A variety of other terms are in use as well. I have adopted the terminology used by Peter H. Lindsay and Donald A. Norman in their text on *Human Information Processing* (New York: Academic Press, 1977). This entire chapter draws heavily from Chapters 8 through 11 of the Lindsay and Norman book.

memory. When a person forgets immediately the name of someone to whom he or she has just been introduced, it is because the name was not transferred from short-term to long-term memory.

A central characteristic of STM is the severe limitation on its capacity. A person who is asked to listen to and repeat a series of 10 or 20 names or numbers normally retains only five or six items. Commonly it is the last five or six. If one focuses instead on the first items, STM becomes saturated by this effort, and the person cannot concentrate on and recall the last items. People make a choice where to focus their attention. They can concentrate on remembering or interpreting or taking notes on information received moments ago, or pay attention to information currently being received. Limitations on the capacity of short-term memory often preclude doing both.

Retrieval of information from STM is direct and immediate because the information has never left the conscious mind. Information can be maintained in STM indefinitely by a process of "rehearsal"—repeating it over and over again. But while rehearsing some items to retain them in STM, people cannot simultaneously add new items. The severe limitation on the amount of information retainable in STM at any one time is physiological, and there is no way to overcome it. This is an important point that will be discussed below in connection with working memory and the utility of external memory aids.

Long-Term Memory

Some information retained in STM is processed into long-term memory. This information on past experiences is filed away in the recesses of the mind and must be retrieved before it can be used. In contrast to the immediate recall of current experience from STM, retrieval of information from LTM is indirect and sometimes laborious.

Loss of detail as sensory stimuli are interpreted and passed from SIS into STM and then into LTM is the basis for the phenomenon of selective perception discussed in the previous chapter. It imposes limits on subsequent stages of analysis, inasmuch as the lost data can never be retrieved. People can never take their mind back to what was *actually there* in sensory information storage or short-term memory. They can only retrieve their interpretation of what they *thought* was there as stored in LTM.

There are no practical limits to the amount of information that may be stored in LTM. The limitations of LTM are the difficulty of processing information into it and retrieving information from it. These subjects are discussed below.

The three memory processes comprise the storehouse of information or database that we call memory, but the total memory system must include other features as well. Some mental process must determine what information is passed from SIS into STM and from STM into LTM; decide how to search the LTM data base and judge whether further memory search is likely to be productive; assess the relevance of retrieved information; and evaluate potentially contradictory data.

To explain the operation of the total memory system, psychologists posit the existence of an interpretive mechanism that operates on the data base and a monitor or central control mechanism that guides and oversees the operation of the whole system. Little is known of these mechanisms and how they relate to other mental processes.

Despite much research on memory, little agreement exists on many critical points. What is presented here is probably the lowest common denominator on which most researchers would agree.

Organization of Information in Long-Term Memory. Physically, the brain consists of roughly 10 billion neurons, each analogous to a computer chip capable of storing information. Each neuron has octopus-like arms called axons and dendrites. Electrical impulses flow through these arms and are ferried by neurotransmitting chemicals across what is called the synaptic gap between neurons. Memories are stored as patterns of connections between neurons. When two neurons are activated, the connections or "synapses" between them are strengthened.

As you read this chapter, the experience actually causes physical changes in your brain. "In a matter of seconds, new circuits are formed that can change forever the way you think about the world."[31]

Memory records a lifetime of experience and thoughts. Such a massive data retrieval mechanism, like a library or computer system, must have an organizational structure; otherwise information that enters the system could never be retrieved. Imagine the Library of Congress if there were no indexing system.

31. George Johnson, *In the Palaces of Memory: How We Build the Worlds Inside Our Heads.* Vintage Books, 1992, p. xi.

There has been considerable research on how information is organized and represented in memory, but the findings remain speculative. Current research focuses on which sections of the brain process various types of information. This is determined by testing patients who have suffered brain damage from strokes and trauma or by using functional magnetic resonance imaging (fMRI) that "lights up" the active portion of the brain as a person speaks, reads, writes, or listens.

None of the current theories seems to encompass the full range or complexity of memory processes, which include memory for sights and sounds, for feelings, and for belief systems that integrate information on a large number of concepts. However useful the research has been for other purposes, analysts' needs are best served by a very simple image of the structure of memory.

Imagine memory as a massive, multidimensional spider web. This image captures what is, for the purposes of this book, perhaps the most important property of information stored in memory—its interconnectedness. One thought leads to another. It is possible to start at any one point in memory and follow a perhaps labyrinthine path to reach any other point. Information is retrieved by tracing through the network of interconnections to the place where it is stored.

Retrievability is influenced by the number of locations in which information is stored and the number and strength of pathways from this information to other concepts that might be activated by incoming information. The more frequently a path is followed, the stronger that path becomes and the more readily available the information located along that path. If one has not thought of a subject for some time, it may be difficult to recall details. After thinking our way back into the appropriate context and finding the general location in our memory, the interconnections become more readily available. We begin to remember names, places, and events that had seemed to be forgotten.

Once people have started thinking about a problem one way, the same mental circuits or pathways get activated and strengthened each time they think about it. This facilitates the retrieval of information. These same pathways, however, also become the mental ruts that make it difficult to reorganize the information mentally so as to see it from a different perspective. That explains why, in the previous chapter, once you saw the picture of the old woman it was difficult to see the young

woman, or vice versa. A subsequent chapter will consider ways of breaking out of mental ruts.

One useful concept of memory organization is what some cognitive psychologists call a "schema." A schema is *any pattern of relationships* among data stored in memory. It is any set of nodes and links between them in the spider web of memory that hang together so strongly that they can be retrieved and used more or less as a single unit.

For example, a person may have a schema for a bar that when activated immediately makes available in memory knowledge of the properties of a bar and what distinguishes a bar, say, from a tavern. It brings back memories of specific bars that may in turn stimulate memories of thirst, guilt, or other feelings or circumstances. People also have schemata (plural for schema) for abstract concepts such as a socialist economic system and what distinguishes it from a capitalist or communist system. Schemata for phenomena such as success or failure in making an accurate intelligence estimate will include links to those elements of memory that explain typical causes and implications of success or failure. There must also be schemata for processes that link memories of the various steps involved in long division, regression analysis, or simply making inferences from evidence and writing an intelligence report.

Any given point in memory may be connected to many different overlapping schemata. This system is highly complex and not well understood.

This conception of a schema is so general that it begs many important questions of interest to memory researchers, but it is the best that can be done given the current state of knowledge. It serves the purpose of emphasizing that memory does have structure. It also shows that how knowledge is connected in memory is critically important in determining what information is retrieved in response to any stimulus and how that information is used in reasoning.

Concepts and schemata stored in memory exercise a powerful influence on the formation of perceptions from sensory data. Recall the experiment discussed in the previous chapter in which test subjects were exposed very briefly to playing cards that had been doctored so that some hearts were black and spades red. When retained in SIS for a fraction of a second, the spades were indeed red. In the course of interpreting the sensory impression and transferring it to STM, however, the spades became black because the memory system has no readily available schema for a

red spade to be matched against the sensory impression. If information does not fit into what people know, or think they know, they have great difficulty processing it.

The content of schemata in memory is a principal factor distinguishing stronger from weaker analytical ability. This is aptly illustrated by an experiment with chess players. When chess grandmasters and masters and ordinary chess players were given five to 10 seconds to note the position of 20 to 25 chess pieces placed randomly on a chess board, the masters and ordinary players were alike in being able to remember the places of only about six pieces. If the positions of the pieces were taken from an actual game (unknown to the test subjects), however, the grandmasters and masters were usually able to reproduce almost all the positions without error, while the ordinary players were still able to place correctly only a half-dozen pieces.[32]

That the unique ability of the chess masters did not result from a pure feat of memory is indicated by the masters' inability to perform better than ordinary players in remembering randomly placed positions. Their exceptional performance in remembering positions from actual games stems from their ability to immediately perceive patterns that enable them to process many bits of information together as a single chunk or schema. The chess master has available in long-term memory many schemata that connect individual positions together in coherent patterns. When the position of chess pieces on the board corresponds to a recognized schema, it is very easy for the master to remember not only the positions of the pieces, but the outcomes of previous games in which the pieces were in these positions. Similarly, the unique abilities of the master analyst are attributable to the schemata in long-term memory that enable the analyst to perceive patterns in data that pass undetected by the average observer.

Getting Information Into and Out of Long-Term Memory. It used to be that how well a person learned something was thought to depend upon how long it was kept in short-term memory or the number of times they repeated it to themselves. Research evidence now suggests that neither of these factors plays the critical role. Continuous repetition does not necessarily guarantee that something will be remembered. The key

32. A. D. deGroot, *Thought and Choice in Chess* (The Hague: Mouton, 1965) cited by Herbert A. Simon, "How Big Is a Chunk?" *Science*, Vol. 183 (1974), p. 487.

factor in transferring information from short-term to long-term memory is the development of associations between the new information and schemata already available in memory. This, in turn, depends upon two variables: the extent to which the information to be learned relates to an already existing schema, and the level of processing given to the new information.

Take one minute to try to memorize the following items from a shopping list: bread, eggs, butter, salami, corn, lettuce, soap, jelly, chicken, and coffee. Chances are, you will try to burn the words into your mind by repeating them over and over. Such repetition, or maintenance rehearsal, is effective for maintaining the information in STM, but is an inefficient and often ineffective means of transferring it to LTM. The list is difficult to memorize because it does not correspond with any schema already in memory.

The words are familiar, but you do not have available in memory a schema that connects the words in this particular group to each other. If the list were changed to juice, cereal, milk, sugar, bacon, eggs, toast, butter, jelly, and coffee, the task would be much easier because the data would then correspond with an existing schema—items commonly eaten for breakfast. Such a list can be assimilated to your existing store of knowledge with little difficulty, just as the chess master rapidly assimilates the positions of many chessmen.

Depth of processing is the second important variable in determining how well information is retained. Depth of processing refers to the amount of effort and cognitive capacity employed to process information, and the number and strength of associations that are thereby forged between the data to be learned and knowledge already in memory. In experiments to test how well people remember a list of words, test subjects might be asked to perform different tasks that reflect different levels of processing. The following illustrative tasks are listed in order of the depth of mental processing required: say how many letters there are in each word on the list, give a word that rhymes with each word, make a mental image of each word, make up a story that incorporates each word.

It turns out that the greater the depth of processing, the greater the ability to recall words on a list. This result holds true regardless of whether the test subjects are informed in advance that the purpose of the experiment is to test them on their memory. Advising test subjects to expect a test makes almost no difference in their performance, presum-

ably because it only leads them to rehearse the information in short-term memory, which is ineffective as compared with other forms of processing.

There are three ways in which information may be learned or committed to memory: by rote, assimilation, or use of a mnemonic device. Each of these procedures is discussed below.[33]

By Rote. Material to be learned is repeated verbally with sufficient frequency that it can later be repeated from memory without use of any memory aids. When information is learned by rote, it forms a separate schema not closely interwoven with previously held knowledge. That is, the mental processing adds little by way of elaboration to the new information, and the new information adds little to the elaboration of existing schemata. Learning by rote is a brute force technique. It seems to be the least efficient way of remembering.

By Assimilation. Information is learned by assimilation when the structure or substance of the information fits into some memory schema already possessed by the learner. The new information is assimilated to or linked to the existing schema and can be retrieved readily by first accessing the existing schema and then reconstructing the new information. Assimilation involves learning by comprehension and is, therefore, a desirable method, but it can only be used to learn information that is somehow related to our previous experience.

By Using A Mnemonic Device. A mnemonic device is any means of organizing or encoding information for the purpose of making it easier to remember. A high school student cramming for a geography test might use the acronym "HOMES" as a device for remembering the first letter of each of the Great Lakes—Huron, Ontario, etc.

To learn the first grocery list of disconnected words, you would create some structure for linking the words to each other and/or to information already in LTM. You might imagine yourself shopping or putting the items away and mentally picture where they are located on the shelves at the market or in the kitchen. Or you might imagine a story concerning one or more meals that include all these items. Any form of processing information in this manner is a more effective aid to retention than rote repetition. Even more effective systems for quickly memorizing lists of

33. This discussion draws on Francis S. Bellezza, "Mnemonic Devices: Classification, Characteristics, and Criteria" (Athens, Ohio: Ohio University, pre-publication manuscript, January 1980).

names or words have been devised by various memory experts, but these require some study and practice in their use.

Mnemonic devices are useful for remembering information that does not fit any appropriate conceptual structure or schema already in memory. They work by providing a simple, artificial structure to which the information to be learned is then linked. The mnemonic device supplies the mental "file categories" that ensure retrievability of information. To remember, first recall the mnemonic device, then access the desired information.

Memory and Intelligence Analysis

An analyst's memory provides continuous input into the analytical process. This input is of two types—additional factual information on historical background and context, and schemata the analyst uses to determine the meaning of newly acquired information. Information from memory may force itself on the analyst's awareness without any deliberate effort by the analyst to remember; or, recall of the information may require considerable time and strain. In either case, anything that influences what information is remembered or retrieved from memory also influences intelligence analysis.

Judgment is the joint product of the available information and what the analyst brings to the analysis of this information. An experiment documenting differences between chess masters and ordinary chess players was noted earlier. Similar research with medical doctors diagnosing illness indicates that differences between stronger and weaker performers are to be found in the organization of information and experience in long-term memory.[34] The same presumably holds true for intelligence analysts. Substantive knowledge and analytical experience determine the store of memories and schemata the analyst draws upon to generate and evaluate hypotheses. The key is not a simple ability to recall facts, but the ability to recall patterns that relate facts to each other and to broader concepts—and to employ procedures that facilitate this process.

34. Arthur S. Elstein, Lee S. Shulman & Sarah A. Sprafka, *Medical Problem Solving: An Analysis of Clinical Reasoning* (Cambridge, MA: Harvard University Press, 1978), p. 276.

Stretching the Limits of Working Memory

Limited information is available on what is commonly thought of as "working memory"—the collection of information that an analyst holds in the forefront of the mind as he or she does analysis. The general concept of working memory seems clear from personal introspection. In writing this chapter, I am very conscious of the constraints on my ability to keep many pieces of information in mind while experimenting with ways to organize this information and seeking words to express my thoughts. To help offset these limits on my working memory, I have accumulated a large number of written notes containing ideas and half-written paragraphs. Only by using such external memory aids am I able to cope with the volume and complexity of the information I want to use.

A well-known article written over 40 years ago, titled "The Magic Number Seven—Plus or Minus Two," contends that seven—plus or minus two—is the number of things people can keep in their head all at once.[35] That limitation on working memory is the source of many problems. People have difficulty grasping a problem in all its complexity. This is why we sometimes have trouble making up our minds. For example, we think first about the arguments in favor, and then about the arguments against, and we can't keep all those pros and cons in our head at the same time to get an overview of how they balance off against each other.

The recommended technique for coping with this limitation of working memory is called externalizing the problem—getting it out of one's head and down on paper in some simplified form that shows the main elements of the problem and how they relate to each other. Chapter 7, "Structuring Analytical Problems," discusses ways of doing this. They all involve breaking down a problem into its component parts and then preparing a simple "model" that shows how the parts relate to the whole. When working on a small part of the problem, the model keeps one from losing sight of the whole.

A simple model of an analytical problem facilitates the assimilation of new information into long-term memory; it provides a structure to which bits and pieces of information can be related. The model defines the categories for filing information in memory and retrieving it on

35. George A. Miller, "The Magical Number Seven--Plus or Minus Two: Some Limits on our Capacity for Processing Information." *The Psychological Review*, Vol. 63, No. 2 (March 1956).

demand. In other words, it serves as a mnemonic device that provides the hooks on which to hang information so that it can be found when needed.

The model is initially an artificial construct, like the previously noted acronym "HOMES." With usage, however, it rapidly becomes an integral part of one's conceptual structure—the set of schemata used in processing information. At this point, remembering new information occurs by assimilation rather than by mnemonics. This enhances the ability to recall and make inferences from a larger volume of information in a greater variety of ways than would otherwise be possible.

"Hardening of the Categories". Memory processes tend to work with generalized categories. If people do not have an appropriate category for something, they are unlikely to perceive it, store it in memory, or be able to retrieve it from memory later. If categories are drawn incorrectly, people are likely to perceive and remember things inaccurately. When information about phenomena that are different in important respects nonetheless gets stored in memory under a single concept, errors of analysis may result. For example, many observers of international affairs had the impression that Communism was a monolithic movement, that it was the same everywhere and controlled from Moscow. All Communist countries were grouped together in a single, undifferentiated category called "international Communism" or "the Communist bloc." In 1948, this led many in the United States to downplay the importance of the Stalin-Tito split. According to one authority, it "may help explain why many Western minds, including scholars, remained relatively blind to the existence and significance of Sino-Soviet differences long after they had been made manifest in the realm of ideological formulae."[36]

"Hardening of the categories" is a common analytical weakness. Fine distinctions among categories and tolerance for ambiguity contribute to more effective analysis.

Things That Influence What Is Remembered. Factors that influence how information is stored in memory and that affect future retrievability include: being the first-stored information on a given topic, the amount of attention focused on the information, the credibility of the information, and the importance attributed to the information at the

36. Robert Tucker, "Communist Revolutions, National Cultures, and the Divided Nations," *Studies in Comparative Communism* (Autumn 1974), 235-245.

moment of storage. By influencing the content of memory, all of these factors also influence the outcome of intelligence analysis.

Chapter 12 on "Biases in Estimating Probabilities" describes how availability in memory influences judgments of probability. The more instances a person can recall of a phenomenon, the more probable that phenomenon seems to be. This is true even though ability to recall past examples is influenced by vividness of the information, how recently something occurred, its impact upon one's personal welfare, and many other factors unrelated to the actual probability of the phenomenon.

Memory Rarely Changes Retroactively. Analysts often receive new information that should, logically, cause them to reevaluate the credibility or significance of previous information. Ideally, the earlier information should then become either more salient and readily available in memory, or less so. But it does not work that way. Unfortunately, memories are seldom reassessed or reorganized retroactively in response to new information. For example, information that is dismissed as unimportant or irrelevant because it did not fit an analyst's expectations does not become more memorable even if the analyst changes his or her thinking to the point where the same information, received today, would be recognized as very significant.

Memory Can Handicap as Well as Help

Understanding how memory works provides some insight into the nature of creativity, openness to new information, and breaking mind-sets. All involve spinning new links in the spider web of memory—links among facts, concepts, and schemata that previously were not connected or only weakly connected.

Training courses for intelligence analysts sometimes focus on trying to open up an analyst's established mind-set, to get him or her to see problems from different perspectives in order to give a fairer shake to alternative explanations. More often than not, the reaction of experienced analysts is that they have devoted 20 years to developing their present mind-set, that it has served them well, and that they see no need to change it. Such analysts view themselves, often accurately, as comparable to the chess masters. They believe the information embedded in their long-term memory permits them to perceive patterns and make inferences that are beyond the reach of other observers. In one sense, they are quite correct in not wanting to change; it is, indeed, their existing

schemata or mind-set that enables them to achieve whatever success they enjoy in making analytical judgments.

There is, however, a crucial difference between the chess master and the master intelligence analyst. Although the chess master faces a different opponent in each match, the environment in which each contest takes place remains stable and unchanging: the permissible moves of the diverse pieces are rigidly determined, and the rules cannot be changed without the master's knowledge. Once the chess master develops an accurate schema, there is no need to change it. The intelligence analyst, however, must cope with a rapidly changing world. Many countries that previously were US adversaries are now our formal or de facto allies. The American and Russian governments and societies are not the same today as they were 20 or even 10 or five years ago. Schemata that were valid yesterday may no longer be functional tomorrow.

Learning new schemata often requires the unlearning of existing ones, and this is exceedingly difficult. It is always easier to learn a new habit than to unlearn an old one. Schemata in long-term memory that are so essential to effective analysis are also the principal source of inertia in recognizing and adapting to a changing environment. Chapter 6, "Keeping an Open Mind," identifies tools for dealing with this problem.

PART II—TOOLS FOR THINKING

Chapter 4

Strategies for Analytical Judgment: Transcending the Limits of Incomplete Information

When intelligence analysts make thoughtful analytical judgments, how do they do it? In seeking answers to this question, this chapter discusses the strengths and limitations of situational logic, theory, comparison, and simple immersion in the data as strategies for the generation and evaluation of hypotheses. The final section discusses alternative strategies for choosing among hypotheses. One strategy too often used by intelligence analysts is described as "satisficing"—choosing the first hypothesis that appears good enough rather than carefully identifying all possible hypotheses and determining which is most consistent with the evidence.[37]

* * * * * * * * * * * * * * * * * * * *

Intelligence analysts should be self-conscious about their reasoning process. They should think about *how* they make judgments and reach conclusions, not just about the judgments and conclusions themselves. Webster's dictionary defines judgment as arriving at a "decision or conclusion on the basis of indications and probabilities when the facts are not clearly ascertained." [38] Judgment is what analysts use to fill gaps in their knowledge. It entails going beyond the available information and is the principal means of coping with uncertainty. It always involves an analytical leap, from the known into the uncertain.

37. An earlier version of this chapter was published as an unclassified article in *Studies in Intelligence* in 1981, under the title "Strategies for Analytical Judgment."
38. Webster's *New International Dictionary*, unabridged, 1954.

Judgment is an integral part of all intelligence analysis. While the optimal goal of intelligence collection is complete knowledge, this goal is seldom reached in practice. Almost by definition of the intelligence mission, intelligence issues involve considerable uncertainty. Thus, the analyst is commonly working with incomplete, ambiguous, and often contradictory data. The intelligence analyst's function might be described as transcending the limits of incomplete information through the exercise of analytical judgment.

The ultimate nature of judgment remains a mystery. It is possible, however, to identify diverse strategies that analysts employ to process information as they prepare to pass judgment. Analytical strategies are important because they influence the data one attends to. They determine where the analyst shines his or her searchlight, and this inevitably affects the outcome of the analytical process.

Strategies for Generating and Evaluating Hypotheses

This book uses the term hypothesis in its broadest sense as a potential explanation or conclusion that is to be tested by collecting and presenting evidence. Examination of how analysts generate and evaluate hypotheses identifies three principal strategies—the application of theory, situational logic, and comparison—each of which is discussed at some length below. A "non-strategy," immersion in the data and letting the data speak for themselves, is also discussed. This list of analytical strategies is not exhaustive. Other strategies might include, for example, projecting one's own psychological needs onto the data at hand, but this discussion is not concerned with the pathology of erroneous judgment. Rather, the goal is to understand the several kinds of careful, conscientious analysis one would hope and expect to find among a cadre of intelligence analysts dealing with highly complex issues.

Situational Logic

This is the most common operating mode for intelligence analysts. Generation and analysis of hypotheses start with consideration of concrete elements of the current situation, rather than with broad generalizations that encompass many similar cases. The situation is regarded as one-of-a-kind, so that it must be understood in terms of its own unique logic, rather than as one example of a broad class of comparable events.

Starting with the known facts of the current situation and an understanding of the unique forces at work at that particular time and place, the analyst seeks to identify the logical antecedents or consequences of this situation. A scenario is developed that hangs together as a plausible narrative. The analyst may work backwards to explain the origins or causes of the current situation or forward to estimate the future outcome.

Situational logic commonly focuses on tracing cause-effect relationships or, when dealing with purposive behavior, means-ends relationships. The analyst identifies the goals being pursued and explains why the foreign actor(s) believe certain means will achieve those goals.

Particular strengths of situational logic are its wide applicability and ability to integrate a large volume of relevant detail. Any situation, however unique, may be analyzed in this manner.

Situational logic as an analytical strategy also has two principal weaknesses. One is that it is so difficult to understand the mental and bureaucratic processes of foreign leaders and governments. To see the options faced by foreign leaders as these leaders see them, one must understand their values and assumptions and even their misperceptions and misunderstandings. Without such insight, interpreting foreign leaders' decisions or forecasting future decisions is often little more than partially informed speculation. Too frequently, foreign behavior appears "irrational" or "not in their own best interest." Such conclusions often indicate analysts have projected American values and conceptual frameworks onto the foreign leaders and societies, rather than understanding the logic of the situation as it appears to them.

The second weakness is that situational logic fails to exploit the theoretical knowledge derived from study of similar phenomena in other countries and other time periods. The subject of national separatist movements illustrates the point. Nationalism is a centuries-old problem, but most Western industrial democracies have been considered well-integrated national communities. Even so, recent years have seen an increase in pressures from minority ethnic groups seeking independence or autonomy. Why has this phenomenon occurred recently in Scotland, southern France and Corsica, Quebec, parts of Belgium, and Spain—as well as in less stable Third World countries where it might be expected?

Dealing with this topic in a logic-of-the-situation mode, a country analyst would examine the diverse political, economic, and social groups whose interests are at stake in the country. Based on the relative power

positions of these groups, the dynamic interactions among them, and anticipated trends or developments that might affect the future positions of the interested parties, the analyst would seek to identify the driving forces that will determine the eventual outcome.

It is quite possible to write in this manner a detailed and seemingly well-informed study of a separatist movement in a single country while ignoring the fact that ethnic conflict as a generic phenomenon has been the subject of considerable theoretical study. By studying similar phenomena in many countries, one can generate and evaluate hypotheses concerning root causes that may not even be considered by an analyst who is dealing only with the logic of a single situation. For example, to what extent does the resurgence of long-dormant ethnic sentiments stem from a reaction against the cultural homogenization that accompanies modern mass communications systems?

Analyzing many examples of a similar phenomenon, as discussed below, enables one to probe more fundamental causes than those normally considered in logic-of-the-situation analysis. The proximate causes identified by situational logic appear, from the broader perspective of theoretical analysis, to be but symptoms indicating the presence of more fundamental causal factors. A better understanding of these fundamental causes is critical to effective forecasting, especially over the longer range. While situational logic may be the best approach to estimating short-term developments, a more theoretical approach is required as the analytical perspective moves further into the future.

Applying Theory

Theory is an academic term not much in vogue in the Intelligence Community, but it is unavoidable in any discussion of analytical judgment. In one popular meaning of the term, "theoretical" is associated with the terms "impractical" and "unrealistic". Needless to say, it is used here in a quite different sense.

A theory is a generalization based on the study of many examples of some phenomenon. It specifies that when a given set of conditions arises, certain other conditions will follow either with certainty or with some degree of probability. In other words, conclusions are judged to follow from a set of conditions and a finding that these conditions apply in the specific case being analyzed. For example, Turkey is a developing country in a precarious strategic position. This defines a set of conditions that

imply conclusions concerning the role of the military and the nature of political processes in that country, because analysts have an implicit if not explicit understanding of how these factors normally relate.

What academics refer to as theory is really only a more explicit version of what intelligence analysts think of as their basic understanding of how individuals, institutions, and political systems normally behave.

There are both advantages and drawbacks to applying theory in intelligence analysis. One advantage is that "theory economizes thought." By identifying the key elements of a problem, theory enables an analyst to sort through a mass of less significant detail. Theory enables the analyst to see beyond today's transient developments, to recognize which trends are superficial and which are significant, and to foresee future developments for which there is today little concrete evidence.

Consider, for example, the theoretical proposition that economic development and massive infusion of foreign ideas in a feudal society lead to political instability. This proposition seems well established. When applied to Saudi Arabia, it suggests that the days of the Saudi monarchy are numbered, although analysts of the Saudi scene using situational logic find little or no current evidence of a meaningful threat to the power and position of the royal family. Thus, the application of a generally accepted theoretical proposition enables the analyst to forecast an outcome for which the "hard evidence" has not yet begun to develop. This is an important strength of theoretical analysis when applied to real-world problems.

Yet this same example also illustrates a common weakness in applying theory to analysis of political phenomena. Theoretical propositions frequently fail to specify the time frame within which developments might be anticipated to occur. The analytical problem with respect to Saudi Arabia is not so much whether the monarchy will *eventually* be replaced, as when or under what conditions this might happen. Further elaboration of the theory relating economic development and foreign ideas to political instability in feudal societies would identify early warning indicators that analysts might look for. Such indicators would guide both intelligence collection and analysis of sociopolitical and socioeconomic data and lead to hypotheses concerning when or under what circumstances such an event might occur.

But if theory enables the analyst to transcend the limits of available data, it may also provide the basis for ignoring evidence that is truly

indicative of future events. Consider the following theoretical propositions in the light of popular agitation against the Shah of Iran in the late 1970s: (1) When the position of an authoritarian ruler is threatened, he will defend his position with force if necessary. (2) An authoritarian ruler enjoying complete support of effective military and security forces cannot be overthrown by popular opinion and agitation. Few would challenge these propositions, yet when applied to Iran in the late 1970s, they led Iran specialists to misjudge the Shah's chances for retaining the peacock throne. Many if not most such specialists seemed convinced that the Shah remained strong and that he would crack down on dissent when it threatened to get out of control. Many persisted in this assessment for several months after the accumulation of what in retrospect appears to have been strong evidence to the contrary.

Persistence of these assumptions is easily understood in psychological terms. When evidence is lacking or ambiguous, the analyst evaluates hypotheses by applying his or her general background knowledge concerning the nature of political systems and behavior. The evidence on the strength of the Shah and his intention to crack down on dissidents was ambiguous, but the Iranian monarch was an authoritarian ruler, and authoritarian regimes were assumed to have certain characteristics, as noted in the previously cited propositions. Thus beliefs about the Shah were embedded in broad and persuasive assumptions about the nature of authoritarian regimes *per se.* For an analyst who believed in the two aforementioned propositions, it would have taken far more evidence, including more unambiguous evidence, to infer that the Shah would be overthrown than to justify continued confidence in his future.[39]

Figure 4 below illustrates graphically the difference between theory and situational logic. Situational logic looks at the evidence within a single country on multiple interrelated issues, as shown by the column

39. Even in retrospect these two propositions still seem valid, which is why some aspects of the Shah's fall remain incredible. There are, in principle, three possible reasons why these seemingly valid theoretical assumptions failed to generate an accurate estimate on Iran: (1) One or more of the initial conditions posited by the theory did not in fact apply--for example, the Shah was not really an authoritarian ruler. (2) The theory is only partially valid, in that there are certain circumstances under which it does and does not apply. These limiting conditions need to be specified. (3) The theory is basically valid, but one cannot expect 100-percent accuracy from social science theories. Social science, as distinct from natural science, deals with a probabilistic environment. One cannot foresee all the circumstances that might cause an exception to the general rules, so the best that can be expected is that the given conditions will lead to the specified outcome most of the time.

Figure 4

	Country	Country	Country	Country
Issue	Evidence	Evidence	Evidence	Evidence
Issue	Evidence	Evidence	Evidence	Evidence
Issue	Evidence	Evidence	Evidence	Evidence
Issue	Evidence	Evidence	Evidence	Evidence

Situational Logic Vs. Theory

highlighted in gray. This is a typical area studies approach. Theoretical analysis looks at the evidence related to a single issue in multiple countries, as shown by the row highlighted in gray. This is a typical social science approach.

The distinction between theory and situational logic is not as clear as it may seem from this graphic, however. Logic-of-the-situation analysis also draws heavily on theoretical assumptions. How does the analyst select the most significant elements to describe the current situation, or identify the causes or consequences of these elements, without some implicit theory that relates the likelihood of certain outcomes to certain antecedent conditions?

For example, if the analyst estimating the outcome of an impending election does not have current polling data, it is necessary to look back at past elections, study the campaigns, and then judge how voters are likely to react to the current campaigns and to events that influence voter attitudes. In doing so, the analyst operates from a set of assumptions about human nature and what drives people and groups. These assumptions form part of a theory of political behavior, but it is a different sort of theory than was discussed under theoretical analysis. It does not illuminate the entire situation, but only a small increment of the situation, and it may not apply beyond the specific country of concern. Further, it is

much more likely to remain implicit, rather than be a focal point of the analysis.

Comparison with Historical Situations

A third approach for going beyond the available information is comparison. An analyst seeks understanding of current events by comparing them with historical precedents in the same country, or with similar events in other countries. Analogy is one form of comparison. When an historical situation is deemed comparable to current circumstances, analysts use their understanding of the historical precedent to fill gaps in their understanding of the current situation. Unknown elements of the present are assumed to be the same as known elements of the historical precedent. Thus, analysts reason that the same forces are at work, that the outcome of the present situation is likely to be similar to the outcome of the historical situation, or that a certain policy is required in order to avoid the same outcome as in the past.

Comparison differs from situational logic in that the present situation is interpreted in the light of a more or less explicit conceptual model that is created by looking at similar situations in other times or places. It differs from theoretical analysis in that this conceptual model is based on a single case or only a few cases, rather than on many similar cases. Comparison may also be used to generate theory, but this is a more narrow kind of theorizing that cannot be validated nearly as well as generalizations inferred from many comparable cases.

Reasoning by comparison is a convenient shortcut, one chosen when neither data nor theory are available for the other analytical strategies, or simply because it is easier and less time-consuming than a more detailed analysis. A careful comparative analysis starts by specifying key elements of the present situation. The analyst then seeks out one or more historical precedents that may shed light on the present. Frequently, however, a historical precedent may be so vivid and powerful that it imposes itself upon a person's thinking from the outset, conditioning them to perceive the present primarily in terms of its similarity to the past. This is reasoning by analogy. As Robert Jervis noted, "historical analogies often precede, rather than follow, a careful analysis of a situation."[40]

40. Robert Jervis, "Hypotheses on Misperception," *World Politics* 20 (April 1968), p. 471.

The tendency to relate contemporary events to earlier events as a guide to understanding is a powerful one. Comparison helps achieve understanding by reducing the unfamiliar to the familiar. In the absence of data required for a full understanding of the current situation, reasoning by comparison may be the only alternative. Anyone taking this approach, however, should be aware of the significant potential for error. This course is an implicit admission of the lack of sufficient information to understand the present situation in its own right, and lack of relevant theory to relate the present situation to many other comparable situations

The difficulty, of course, is in being certain that two situations are truly comparable. Because they are equivalent in some respects, there is a tendency to reason as though they were equivalent in all respects, and to assume that the current situation will have the same or similar outcome as the historical situation. This is a valid assumption only when based on in-depth analysis of both the current situation *and* the historical precedent to ensure that they are actually comparable in all relevant respects.

In a short book that ought to be familiar to all intelligence analysts, Ernest May traced the impact of historical analogy on US foreign policy.[41] He found that because of reasoning by analogy, US policymakers tend to be one generation behind, determined to avoid the mistakes of the previous generation. They pursue the policies that would have been most appropriate in the historical situation but are not necessarily well adapted to the current one.

Policymakers in the 1930s, for instance, viewed the international situation as analogous to that before World War I. Consequently, they followed a policy of isolation that would have been appropriate for preventing American involvement in the first World War but failed to prevent the second. Communist aggression after World War II was seen as analogous to Nazi aggression, leading to a policy of containment that could have prevented World War II.

More recently, the Vietnam analogy has been used repeatedly over many years to argue against an activist US foreign policy. For example, some used the Vietnam analogy to argue against US participation in the Gulf War—a flawed analogy because the operating terrain over which

41. Ernest May, *`Lessons' of the Past: The Use and Misuse of History in American Foreign Policy* (New York: Oxford University Press, 1973).

battles were fought was completely different in Kuwait/Iraq and much more in our favor there as compared with Vietnam.

May argues that policymakers often perceive problems in terms of analogies with the past, but that they ordinarily use history badly:

> When resorting to an analogy, they tend to seize upon the first that comes to mind. They do not research more widely. Nor do they pause to analyze the case, test its fitness, or even ask in what ways it might be misleading.[42]

As compared with policymakers, intelligence analysts have more time available to "analyze rather than analogize." Intelligence analysts tend to be good historians, with a large number of historical precedents available for recall. The greater the number of potential analogues an analyst has at his or her disposal, the greater the likelihood of selecting an appropriate one. The greater the depth of an analyst's knowledge, the greater the chances the analyst will perceive the differences as well as the similarities between two situations. Even under the best of circumstances, however, inferences based on comparison with a single analogous situation probably are more prone to error than most other forms of inference.

The most productive uses of comparative analysis are to suggest hypotheses and to highlight differences, not to draw conclusions. Comparison can suggest the presence or the influence of variables that are not readily apparent in the current situation, or stimulate the imagination to conceive explanations or possible outcomes that might not otherwise occur to the analyst. In short, comparison can generate hypotheses that then guide the search for additional information to confirm or refute these hypotheses. It should not, however, form the basis for conclusions unless thorough analysis of both situations has confirmed they are indeed comparable.

Data Immersion

Analysts sometimes describe their work procedure as immersing themselves in the data without fitting the data into any preconceived pattern. At some point an apparent pattern (or answer or explanation) emerges spontaneously, and the analyst then goes back to the data to check how well the data support this judgment. According to this view,

42. Ibid., p. xi.

objectivity requires the analyst to suppress any personal opinions or preconceptions, so as to be guided only by the "facts" of the case.

To think of analysis in this way overlooks the fact that information cannot speak for itself. The significance of information is always a joint function of the nature of the information and the context in which it is interpreted. The context is provided by the analyst in the form of a set of assumptions and expectations concerning human and organizational behavior. These preconceptions are critical determinants of which information is considered relevant and how it is interpreted.

Of course there are many circumstances in which the analyst has no option but to immerse himself or herself in the data. Obviously, an analyst must have a base of knowledge to work with before starting analysis. When dealing with a new and unfamiliar subject, the uncritical and relatively non-selective accumulation and review of information is an appropriate first step. But this is a process of absorbing information, not analyzing it.

Analysis begins when the analyst consciously inserts himself or herself into the process to select, sort, and organize information. This selection and organization can only be accomplished according to conscious or subconscious assumptions and preconceptions.

The question is not whether one's prior assumptions and expectations influence analysis, but only whether this influence is made explicit or remains implicit. The distinction appears to be important. In research to determine how physicians make medical diagnoses, the doctors who comprised the test subjects were asked to describe their analytical strategies. Those who stressed thorough collection of data as their principal analytical method were significantly less accurate in their diagnoses than those who described themselves as following other analytical strategies such as identifying and testing hypotheses.[43] Moreover, the collection of additional data through greater thoroughness in the medical history and physical examination did not lead to increased diagnostic accuracy.[44]

One might speculate that the analyst who seeks greater objectivity by suppressing recognition of his or her own subjective input actually has less valid input to make. Objectivity is gained by making assumptions

43. Arthur S. Elstein, Lee S. Shulman, and Sarah A. Sprafka, *Medical Problem Solving: An Analysis of Clinical Reasoning* (Cambridge, MA: Harvard University Press, 1978), p. 270.
44. Ibid., p. 281. For more extensive discussion of the value of additional information, see Chapter 5, "Do You Really Need More Information?"

explicit so that they may be examined and challenged, not by vain efforts to eliminate them from analysis.

Relationships Among Strategies

No one strategy is necessarily better than the others. In order to generate all relevant hypotheses and make maximum use of all potentially relevant information, it would be desirable to employ all three strategies at the early hypothesis generation phase of a research project. Unfortunately, analysts commonly lack the inclination or time to do so.

Different analysts have different analytical habits and preferences for analytical strategy. As a broad generalization that admits numerous exceptions, analysts trained in area studies or history tend to prefer situational logic, while those with a strong social science background are more likely to bring theoretical and comparative insights to bear on their work. The Intelligence Community as a whole is far stronger in situational logic than in theory. In my judgment, intelligence analysts do not generalize enough, as opposed to many academic scholars who generalize too much. This is especially true in political analysis, and it is not entirely due to unavailability of applicable political theory. Theoretical insights that are available are often unknown to or at least not used by political intelligence analysts.

Differences in analytical strategy may cause fundamental differences in perspective between intelligence analysts and some of the policymakers for whom they write. Higher level officials who are not experts on the subject at issue use far more theory and comparison and less situational logic than intelligence analysts. Any policymaker or other senior manager who lacks the knowledge base of the specialist and does not have time for detail must, of necessity, deal with broad generalizations. Many decisions must be made, with much less time to consider each of them than is available to the intelligence analyst. This requires the policymaker to take a more conceptual approach, to think in terms of theories, models, or analogies that summarize large amounts of detail. Whether this represents sophistication or oversimplification depends upon the individual case and, perhaps, whether one agrees or disagrees with the judgments made. In any event, intelligence analysts would do well to take this phenomenon into account when writing for their consumers.

Strategies for Choice Among Hypotheses

A systematic analytical process requires selection among alternative hypotheses, and it is here that analytical practice often diverges significantly from the ideal and from the canons of scientific method. The ideal is to generate a full set of hypotheses, systematically evaluate each hypothesis, and then identify the hypothesis that provides the best fit to the data. Scientific method, for its part, requires that one seek to disprove hypotheses rather than confirm them.

In practice, other strategies are commonly employed. Alexander George has identified a number of less-than-optimal strategies for making decisions in the face of incomplete information and multiple, competing values and goals. While George conceived of these strategies as applicable to how decisionmakers choose among alternative policies, most also apply to how intelligence analysts might decide among alternative analytical hypotheses.

The relevant strategies George identified are:

- "Satisficing"—selecting the first identified alternative that appears "good enough" rather than examining all alternatives to determine which is "best."

- Incrementalism—focusing on a narrow range of alternatives representing marginal change, without considering the need for dramatic change from an existing position.

- Consensus—opting for the alternative that will elicit the greatest agreement and support. Simply telling the boss what he or she wants to hear is one version of this.

- Reasoning by analogy—choosing the alternative that appears most likely to avoid some previous error or to duplicate a previous success.

- Relying on a set of principles or maxims that distinguish a "good" from a "bad" alternative.[45]

45. Alexander George, *Presidential Decisionmaking in Foreign Policy: The Effective Use of Information and Advice* (Boulder, CO: Westview Press, 1980), Chapter 2.

The intelligence analyst has another tempting option not available to the policymaker: to avoid judgment by simply describing the current situation, identifying alternatives, and letting the intelligence consumer make the judgment about which alternative is most likely. Most of these strategies are not discussed here. The following paragraphs focus only on the one that seems most prevalent in intelligence analysis.

"Satisficing"

I would suggest, based on personal experience and discussions with analysts, that most analysis is conducted in a manner very similar to the satisficing mode (selecting the first identified alternative that appears "good enough").[46] The analyst identifies what appears to be the most likely hypothesis—that is, the tentative estimate, explanation, or description of the situation that appears most accurate. Data are collected and organized according to whether they support this tentative judgment, and the hypothesis is accepted if it seems to provide a reasonable fit to the data. The careful analyst will then make a quick review of other possible hypotheses and of evidence not accounted for by the preferred judgment to ensure that he or she has not overlooked some important consideration.

This approach has three weaknesses: the selective perception that results from focus on a single hypothesis, failure to generate a complete set of competing hypotheses, and a focus on evidence that confirms rather than disconfirms hypotheses. Each of these is discussed below.

Selective Perception. Tentative hypotheses serve a useful function in helping analysts select, organize, and manage information. They narrow the scope of the problem so that the analyst can focus efficiently on data that are most relevant and important. The hypotheses serve as organizing frameworks in working memory and thus facilitate retrieval of information from memory. In short, they are essential elements of the analytical process. But their functional utility also entails some cost, because a hypothesis functions as a perceptual filter. Analysts, like people in general, tend to see what they are looking for and to overlook that which is not specifically included in their search strategy. They tend to limit the processed information to that which is relevant to the current hypothesis.

46. The concept of "satisficing," of seeking a satisfactory rather than an optimal solution, was developed by Herbert A. Simon and is widely used in the literature on decision analysis.

If the hypothesis is incorrect, information may be lost that would suggest a new or modified hypothesis.

This difficulty can be overcome by the simultaneous consideration of multiple hypotheses. This approach is discussed in detail in Chapter 8. It has the advantage of focusing attention on those few items of evidence that have the greatest diagnostic value in distinguishing among the validity of competing hypotheses. Most evidence is consistent with several different hypotheses, and this fact is easily overlooked when analysts focus on only one hypothesis at a time—especially if their focus is on seeking to confirm rather than disprove what appears to be the most likely answer.

Failure To Generate Appropriate Hypotheses. If tentative hypotheses determine the criteria for searching for information and judging its relevance, it follows that one may overlook the proper answer if it is not encompassed within the several hypotheses being considered. Research on hypothesis generation suggests that performance on this task is woefully inadequate.[47] When faced with an analytical problem, people are either unable or simply do not take the time to identify the full range of potential answers. Analytical performance might be significantly enhanced by more deliberate attention to this stage of the analytical process. Analysts need to take more time to develop a full set of competing hypotheses, using all three of the previously discussed strategies—theory, situational logic, and comparison.

Failure To Consider Diagnosticity of Evidence. In the absence of a complete set of alternative hypotheses, it is not possible to evaluate the "diagnosticity" of evidence. Unfortunately, many analysts are unfamiliar with the concept of diagnosticity of evidence. It refers to the extent to which any item of evidence helps the analyst determine the relative likelihood of alternative hypotheses.

To illustrate, a high temperature may have great value in telling a doctor that a patient is sick, but relatively little value in determining which illness the patient is suffering from. Because a high temperature is consistent with so many possible hypotheses about a patient's illness, it has limited diagnostic value in determining which illness (hypothesis) is the more likely one.

47. Charles Gettys et al., *Hypothesis Generation: A Final Report on Three Years of Research.* Technical Report 15-10-80. University of Oklahoma, Decision Processes Laboratory, 1980.

Evidence is diagnostic when it influences an analyst's judgment on the *relative* likelihood of the various hypotheses. If an item of evidence seems consistent with all the hypotheses, it may have no diagnostic value at all. It is a common experience to discover that most available evidence really is not very helpful, as it can be reconciled with all the hypotheses.

Failure To Reject Hypotheses

Scientific method is based on the principle of rejecting hypotheses, while tentatively accepting only those hypotheses that cannot be refuted. Intuitive analysis, by comparison, generally concentrates on confirming a hypothesis and commonly accords more weight to evidence supporting a hypothesis than to evidence that weakens it. Ideally, the reverse would be true. While analysts usually cannot apply the statistical procedures of scientific methodology to test their hypotheses, they can and should adopt the conceptual strategy of seeking to refute rather than confirm hypotheses.

There are two aspects to this problem: people do not naturally seek disconfirming evidence, and when such evidence is received it tends to be discounted. If there is any question about the former, consider how often people test their political and religious beliefs by reading newspapers and books representing an opposing viewpoint. Concerning the latter, we have noted in Chapter 2, "Perception: Why Can't We See What Is There to Be Seen?" the tendency to accommodate new information to existing images. This is easy to do if information supporting a hypothesis is accepted as valid, while information that weakens it is judged to be of questionable reliability or an unimportant anomaly. When information is processed in this manner, it is easy to "confirm" almost any hypothesis that one already believes to be true.

Apart from the psychological pitfalls involved in seeking confirmatory evidence, an important logical point also needs to be considered. The logical reasoning underlying the scientific method of rejecting hypotheses is that ". . . no confirming instance of a law is a verifying instance, but that any disconfirming instance is a falsifying instance."[48] In other words, a hypothesis can never be proved by the enumeration of even a large body of evidence consistent with that hypothesis, because

48. P. C. Wason, "On the Failure to Eliminate Hypotheses in a Conceptual Task," *The Quarterly Journal of Experimental Psychology*, Vol. XII, Part 3 (1960).

the same body of evidence may also be consistent with other hypotheses. A hypothesis may be disproved, however, by citing a single item of evidence that is incompatible with it.

P. C. Wason conducted a series of experiments to test the view that people generally seek confirming rather than disconfirming evidence.[49] The experimental design was based on the above point that the validity of a hypothesis can only be tested by seeking to disprove it rather than confirm it. Test subjects were given the three-number sequence, 2 - 4 - 6, and asked to discover the rule employed to generate this sequence. In order to do so, they were permitted to generate three-number sequences of their own and to ask the experimenter whether these conform to the rule. They were encouraged to generate and ask about as many sequences as they wished and were instructed to stop only when they believed they had discovered the rule.

There are, of course, many possible rules that might account for the sequence 2 - 4 - 6. The test subjects formulated tentative hypotheses such as any ascending sequence of even numbers, or any sequence separated by two digits. As expected, the test subjects generally took the incorrect approach of trying to confirm rather than eliminate such hypotheses. To test the hypothesis that the rule was any ascending sequence of even numbers, for example, they might ask if the sequence 8 - 10 - 14 conforms to the rule.

Readers who have followed the reasoning to this point will recognize that this hypothesis can never be proved by enumerating examples of ascending sequences of even numbers that are found to conform to the sought-for rule. One can only disprove the hypothesis by citing an ascending sequence of odd numbers and learning that this, too, conforms to the rule.

The correct rule was any three ascending numbers, either odd or even. Because of their strategy of seeking confirming evidence, only six of the 29 test subjects in Wason's experiment were correct the first time they thought they had discovered the rule. When this same experiment was repeated by a different researcher for a somewhat different purpose, none

49. Wason, ibid.

of the 51 test subjects had the right answer the first time they thought they had discovered the rule.[50]

In the Wason experiment, the strategy of seeking confirming rather than disconfirming evidence was particularly misleading because the 2 - 4 - 6 sequence is consistent with such a large number of hypotheses. It was easy for test subjects to obtain confirmatory evidence for almost any hypothesis they tried to confirm. It is important to recognize that comparable situations, when evidence is consistent with several different hypotheses, are extremely common in intelligence analysis.

Consider lists of early warning indicators, for example. They are designed to be indicative of an impending attack. Very many of them, however, are also consistent with the hypothesis that military movements are a bluff to exert diplomatic pressure and that no military action will be forthcoming. When analysts seize upon only one of these hypotheses and seek evidence to confirm it, they will often be led astray.

The evidence available to the intelligence analyst is in one important sense different from the evidence available to test subjects asked to infer the number sequence rule. The intelligence analyst commonly deals with problems in which the evidence has only a probabilistic relationship to the hypotheses being considered. Thus it is seldom possible to eliminate any hypothesis entirely, because the most one can say is that a given hypothesis is unlikely given the nature of the evidence, not that it is impossible.

This weakens the conclusions that can be drawn from a strategy aimed at eliminating hypotheses, but it does not in any way justify a strategy aimed at confirming them.

Circumstances and insufficient data often preclude the application of rigorous scientific procedures in intelligence analysis—including, in particular, statistical methods for testing hypotheses. There is, however, certainly no reason why the basic conceptual strategy of looking for contrary evidence cannot be employed. An optimal analytical strategy requires that analysts search for information to disconfirm their favorite theories, not employ a satisficing strategy that permits acceptance of the first hypothesis that seems consistent with the evidence.

50. Harold M. Weiss and Patrick A. Knight, "The Utility of Humility: Self-Esteem, Information Search, and Problem-Solving Efficiency," *Organizational Behavior and Human Performance*, Vol. 25, No. 2 (April 1980), 216-223.

Conclusion

There are many detailed assessments of intelligence failures, but few comparable descriptions of intelligence successes. In reviewing the literature on intelligence successes, Frank Stech found many examples of success but only three accounts that provide sufficient methodological details to shed light on the intellectual processes and methods that contributed to the successes. These dealt with successful American and British intelligence efforts during World War II to analyze German propaganda, predict German submarine movements, and estimate future capabilities and intentions of the German Air Force.[51]

Stech notes that in each of these highly successful efforts, the analysts employed procedures that ". . . facilitated the formulation and testing against each other of alternative hypothetical estimates of enemy intentions. Each of the three accounts stressed this pitting of competing hypotheses against the evidence."[52]

The simultaneous evaluation of multiple, competing hypotheses permits a more systematic and objective analysis than is possible when an analyst focuses on a single, most-likely explanation or estimate. The simultaneous evaluation of multiple, competing hypotheses entails far greater cognitive strain than examining a single, most-likely hypothesis. Retaining multiple hypotheses in working memory and noting how each item of evidence fits into each hypothesis add up to a formidable cognitive task. That is why this approach is seldom employed in intuitive analysis of complex issues. It can be accomplished, however, with the help of simple procedures described in Chapter 8, "Analysis of Competing Hypotheses."

51. Alexander George, *Propaganda Analysis: A Study of Inferences Made From Nazi Propaganda in World War II* (Evanston, IL: Row, Peterson, 1959); Patrick Beesly, *Very Special Intelligence: The Story of the Admiralty's Operational Intelligence Center 1939-1945* (London: Hamish Hamilton, 1977); and R. V. Jones, *Wizard War: British Scientific Intelligence 1939-1945* (New York: Coward, McCann & Geoghegan, 1978).

52. Frank J. Stech, Political and Military Intention Estimation: A Taxonometric Analysis, Final Report for Office of Naval Research (Bethesda, MD: MATHTECH, Inc., November 1979), p. 283.

Chapter 5

Do You Really Need More Information?

The difficulties associated with intelligence analysis are often attributed to the inadequacy of available information. Thus the US Intelligence Community invests heavily in improved intelligence collection systems while managers of analysis lament the comparatively small sums devoted to enhancing analytical resources, improving analytical methods, or gaining better understanding of the cognitive processes involved in making analytical judgments. This chapter questions the often-implicit assumption that lack of information is the principal obstacle to accurate intelligence judgments.[53]

* * * * * * * * * * * * * * * * * * * *

Using experts in a variety of fields as test subjects, experimental psychologists have examined the relationship between the amount of information available to the experts, the accuracy of judgments they make based on this information, and the experts' confidence in the accuracy of these judgments. The word "information," as used in this context, refers to the totality of material an analyst has available to work with in making a judgment.

Using experts in a variety of fields as test subjects, experimental psychologists have examined the relationship between the amount of information available to the experts, the accuracy of judgments they make based on this information, and the experts' confidence in the accuracy of these judgments. The word "information," as used in this context, refers

53. This is an edited version of an article that appeared in *Studies in Intelligence*, Vol. 23, No. 1 (Spring 1979). That *Studies in Intelligence* article was later reprinted in H. Bradford Westerfield, ed., *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal*, 1955-1992 (New Haven: Yale University Press, 1995). A slightly different version was published in *The Bureaucrat*, Vol. 8, 1979, under the title "Improving Intelligence Analysis: Some Insights on Data, Concepts, and Management in the Intelligence Community." For this book, portions of the original article dealing with improving intelligence analysis have been moved to Chapter 14 on "Improving Intelligence Analysis."

to the totality of material an analyst has available to work with in making a judgment.

Key findings from this research are:

- Once an experienced analyst has the minimum information necessary to make an informed judgment, obtaining additional information generally does not improve the accuracy of his or her estimates. Additional information does, however, lead the analyst to become more confident in the judgment, to the point of overconfidence.

- Experienced analysts have an imperfect understanding of what information they actually use in making judgments. They are unaware of the extent to which their judgments are determined by a few dominant factors, rather than by the systematic integration of all available information. Analysts actually use much less of the available information than they think they do.

As will be noted below, these experimental findings should not necessarily be accepted at face value. For example, circumstances exist in which additional information does contribute to more accurate analysis. However, there also are circumstances in which additional information—particularly contradictory information—decreases rather than increases an analyst's confidence.

To interpret the disturbing but not surprising findings from these experiments, it is necessary to consider four different types of information and discuss their relative value in contributing to the accuracy of analytical judgments. It is also helpful to distinguish analysis in which results are driven by the data from analysis that is driven by the conceptual framework employed to interpret the data.

Understanding the complex relationship between amount of information and accuracy of judgment has implications for both the management and conduct of intelligence analysis. Such an understanding suggests analytical procedures and management initiatives that may indeed contribute to more accurate analytical judgments. It also suggests that resources needed to attain a better understanding of the entire analytical process might profitably be diverted from some of the more costly intelligence collection programs.

These findings have broad relevance beyond the Intelligence Community. Analysis of information to gain a better understanding of current developments and to estimate future outcomes is an essential component of decisionmaking in any field. In fact, the psychological experiments that are most relevant have been conducted with experts in such diverse fields as medical and psychological diagnosis, stock market analysis, weather forecasting, and horserace handicapping. The experiments reflect basic human processes that affect analysis of any subject.

One may conduct experiments to demonstrate these phenomena in any field in which experts analyze a finite number of identifiable and classifiable kinds of information to make judgments or estimates that can subsequently be checked for accuracy. The stock market analyst, for example, commonly works with information concerning price-earnings ratios, profit margins, earnings per share, market volume, and resistance and support levels, and it is relatively easy to measure quantitatively the accuracy of the resulting predictions. By controlling the information made available to a group of experts and then checking the accuracy of judgments based on this information, it is possible to investigate how people use information to arrive at analytical judgments.

An Experiment: Betting on the Horses

A description of one such experiment serves to illustrate the procedure.[54] Eight experienced horserace handicappers were shown a list of 88 variables found on a typical past-performance chart—for example, the weight to be carried; the percentage of races in which horse finished first, second, or third during the previous year; the jockey's record; and the number of days since the horse's last race. Each handicapper was asked to identify, first, what he considered to be the five most important items of information—those he would wish to use to handicap a race if he were limited to only five items of information per horse. Each was then asked to select the 10, 20, and 40 most important variables he would use if limited to those levels of information.

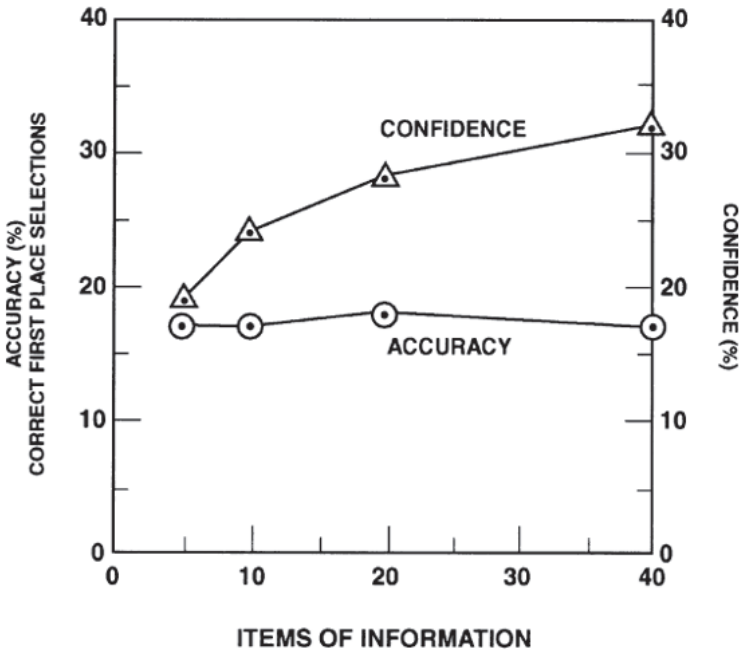
At this point, the handicappers were given true data (sterilized so that horses and actual races could not be identified) for 40 past races and

54. Paul Slovic, "Behavioral Problems of Adhering to a Decision Policy," unpublished manuscript, 1973.

were asked to rank the top five horses in each race in order of expected finish. Each handicapper was given the data in increments of the 5, 10, 20 and 40 variables he had judged to be most useful. Thus, he predicted each race four times—once with each of the four different levels of information. For each prediction, each handicapper assigned a value from 0 to 100 percent to indicate degree of confidence in the accuracy of his prediction.

When the handicappers' predictions were compared with the actual outcomes of these 40 races, it was clear that average accuracy of predictions remained the same regardless of how much information the handicappers had available. Three of the handicappers actually showed less accuracy as the amount of information increased, two improved their accuracy, and three were unchanged. All, however, expressed steadily increasing confidence in their judgments as more information was received. This relationship between amount of information, accuracy of the handi-

Figure 5



cappers' prediction of the first place winners, and the handicappers' confidence in their predictions is shown in Figure 5.

With only five items of information, the handicappers' confidence was well calibrated with their accuracy, but they became overconfident as additional information was received.

The same relationships among amount of information, accuracy, and analyst confidence have been confirmed by similar experiments in other fields.[55] In one experiment with clinical psychologists, a psychological case file was divided into four sections representing successive chronological periods in the life of a relatively normal individual. Thirty-two psychologists with varying levels of experience were asked to make judgments on the basis of this information. After reading each section of the case file, the psychologists answered 25 questions (for which there were known answers) about the personality of the subject of the file. As in other experiments, increasing information resulted in a strong rise in confidence but a negligible increase in accuracy.[56]

A series of experiments to examine the mental processes of medical doctors diagnosing illness found little relationship between thoroughness of data collection and accuracy of diagnosis. Medical students whose self-described research strategy stressed thorough collection of information (as opposed to formation and testing of hypotheses) were significantly below average in the accuracy of their diagnoses. It seems that the explicit formulation of hypotheses directs a more efficient and effective search for information.[57]

Modeling Expert Judgment

Another significant question concerns the extent to which analysts possess an accurate understanding of their own mental processes. How good is their insight into how they actually weight evidence in making judgments? For each situation to be analyzed, they have an implicit "mental model" consisting of beliefs and assumptions as to which vari-

55. For a list of references, see Lewis R. Goldberg, "Simple Models or Simple Processes? Some Research on Clinical Judgments," *American Psychologist*, 23 (1968), pp. 261-265.
56. Stuart Oskamp, "Overconfidence in Case-Study Judgments," *Journal of Consulting Psychology*, 29 (1965), pp. 261-265.
57. Arthur S. Elstein *et al., Medical Problem Solving: An Analysis of Clinical Reasoning* (Cambridge, MA and London: Harvard University Press, 1978), pp. 270 and 295.

ables are most important and how they are related to each other. If analysts have good insight into their own mental model, they should be able to identify and describe the variables they have considered most important in making judgments.

There is strong experimental evidence, however, that such self-insight is usually faulty. The expert perceives his or her own judgmental process, including the number of different kinds of information taken into account, as being considerably more complex than is in fact the case. Experts overestimate the importance of factors that have only a minor impact on their judgment and underestimate the extent to which their decisions are based on a few major variables. In short, people's mental models are simpler than they think, and the analyst is typically unaware not only of which variables *should* have the greatest influence, but also which variables *actually* are having the greatest influence.

All this has been demonstrated by experiments in which analysts were asked to make quantitative estimates concerning a relatively large number of cases in their area of expertise, with each case defined by a number of quantifiable factors. In one experiment, for example, stock market analysts were asked to predict long-term price appreciation for 50 securities, with each security being described in such terms as price/earnings ratio, corporate earnings growth trend, and dividend yield.[58] After completing this task, the analysts were asked to explain how they reached their conclusions, including how much weight they attached to each of the variables. They were instructed to be sufficiently explicit that another person going through the same information could apply the same judgmental rules and arrive at the same conclusions.

In order to compare this verbal rationalization with the judgmental policy reflected in the stock market analysts' actual decisions, multiple regression analysis or other similar statistical procedures can be used to develop a mathematical model of how each analyst actually weighed and combined information on the relevant variables.[59] There have been at least eight studies of this type in diverse fields,[60] including one involving

58. Paul Slovic, Dan Fleissner, and W. Scott Bauman, "Analyzing the Use of Information in Investment Decision Making: A Methodological Proposal," *The Journal of Business*, 45 (1972), pp. 283-301.

59. For a discussion of the methodology, see Slovic, Fleissner, and Bauman, op. cit.

60. For a list of references, see Paul Slovic and Sarah Lichtenstein, "Comparison of Bayesian and Regression Approaches to the Study of Information Processing in Judgment," *Organizational Behavior and Human Performance*, 6 (1971), p. 684.

prediction of future socioeconomic growth of underdeveloped nations.[61] The mathematical model based on the analyst's actual decisions is invariably a more accurate description of that analyst's decisionmaking than the analyst's own verbal description of how the judgments were made.

Although the existence of this phenomenon has been amply demonstrated, its causes are not well understood. The literature on these experiments contains only the following speculative explanation:

Possibly our feeling that we can take into account a host of different factors comes about because, although we remember that at some time or other we have attended to each of the different factors, we fail to notice that it is seldom more than one or two that we consider at any one time.[62]

When Does New Information Affect Our Judgment?

To evaluate the relevance and significance of these experimental findings in the context of intelligence analysts' experiences, it is necessary to distinguish four types of additional information that an analyst might receive:

- **Additional detail about variables already included in the analysis:** Much raw intelligence reporting falls into this category. One would not expect such supplementary information to affect the overall accuracy of the analyst's judgment, and it is readily understandable that further detail that is consistent with previous information increases the analyst's confidence. Analyses for which considerable depth of detail is available to support the conclusions tend to be more persuasive to their authors as well as to their readers.

- **Identification of additional variables:** Information on additional variables permits the analyst to take into account other factors that may affect the situation. This is the kind of additional information used in the horserace handicapper experi-

61. David A. Summers, J. Dale Taliaferro, and Donna J. Fletcher, "Subjective vs. Objective Description of Judgment Policy," *Psychonomic Science*, 18 (1970) pp. 249-250.
62. R. N. Shepard, "On Subjectively Optimum Selection Among Multiattribute Alternatives," in M. W. Shelly, II and G. L. Bryan, eds., *Human Judgments and Optimality* (New York: Wiley, 1964), p. 166.

ment. Other experiments have employed some combination of additional variables and additional detail on the same variables. The finding that judgments are based on a few critical variables rather than on the entire spectrum of evidence helps to explain why information on additional variables does not normally improve predictive accuracy. Occasionally, in situations when there are known gaps in an analyst's understanding, a single report concerning some new and previously unconsidered factor—for example, an authoritative report on a policy decision or planned coup d'etat—will have a major impact on the analyst's judgment. Such a report would fall into one of the next two categories of new information.

- **Information concerning the value attributed to variables already included in the analysis:** An example of such information would be the horserace handicapper learning that a horse he thought would carry 110 pounds will actually carry only 106. Current intelligence reporting tends to deal with this kind of information; for example, an analyst may learn that a dissident group is stronger than had been anticipated. New facts affect the accuracy of judgments when they deal with changes in variables that are critical to the estimates. Analysts' confidence in judgments based on such information is influenced by their confidence in the accuracy of the information as well as by the amount of information.

- **Information concerning which variables are most important and how they relate to each other:** Knowledge and assumptions as to which variables are most important and how they are interrelated comprise the mental model that tells the analyst how to analyze the data received. Explicit investigation of such relationships is one factor that distinguishes systematic research from current intelligence reporting and raw intelligence. In the context of the horserace handicapper experiment, for example, handicappers had to select which variables to include in their analysis. Is weight carried by a horse more, or less, important than several other variables that affect a horse's performance? Any information that affects this judgment influences how the handi-

capper analyzes the available data; that is, it affects his mental model.

The accuracy of an analyst's judgment depends upon both the accuracy of our mental model (the fourth type of information discussed above) and the accuracy of the values attributed to the key variables in the model (the third type of information discussed above). Additional detail on variables already in the analyst's mental model and information on other variables that do not in fact have a significant influence on our judgment (the first and second types of information) have a negligible impact on accuracy, but form the bulk of the raw material analysts work with. These kinds of information increase confidence because the conclusions seem to be supported by such a large body of data.

This discussion of types of new information is the basis for distinguishing two types of analysis- data-driven analysis and conceptually-driven analysis.

Data-Driven Analysis

In this type of analysis, accuracy depends primarily upon the accuracy and completeness of the available data. If one makes the reasonable assumption that the analytical model is correct and the further assumption that the analyst properly applies this model to the data, then the accuracy of the analytical judgment depends entirely upon the accuracy and completeness of the data.

Analyzing the combat readiness of a military division is an example of data-driven analysis. In analyzing combat readiness, the rules and procedures to be followed are relatively well established. The totality of these procedures comprises a mental model that influences perception of the intelligence collected on the unit and guides judgment concerning what information is important and how this information should be analyzed to arrive at judgments concerning readiness.

Most elements of the mental model can be made explicit so that other analysts may be taught to understand and follow the same analytical procedures and arrive at the same or similar results. There is broad, though not necessarily universal, agreement on what the appropriate model is. There are relatively objective standards for judging the quality

of analysis, inasmuch as the conclusions follow logically from the application of the agreed-upon model to the available data.

Conceptually Driven Analysis

Conceptually driven analysis is at the opposite end of the spectrum from data-driven analysis. The questions to be answered do not have neat boundaries, and there are many unknowns. The number of potentially relevant variables and the diverse and imperfectly understood relationships among these variables involve the analyst in enormous complexity and uncertainty. There is little tested theory to inform the analyst concerning which of the myriad pieces of information are most important and how they should be combined to arrive at probabilistic judgments.

In the absence of any agreed-upon analytical schema, analysts are left to their own devices. They interpret information with the aid of mental models that are largely implicit rather than explicit. Assumptions concerning political forces and processes in the subject country may not be apparent even to the analyst. Such models are not representative of an analytical consensus. Other analysts examining the same data may well reach different conclusions, or reach the same conclusions but for different reasons. This analysis is conceptually driven, because the outcome depends at least as much upon the conceptual framework employed to analyze the data as it does upon the data itself.

To illustrate further the distinction between data-driven and conceptually driven analysis, it is useful to consider the function of the analyst responsible for current intelligence, especially current political intelligence as distinct from longer term research. The daily routine is driven by the incoming wire service news, embassy cables, and clandestine-source reporting from overseas that must be interpreted for dissemination to consumers throughout the Intelligence Community. Although current intelligence reporting is driven by incoming information, this is not what is meant by data-driven analysis. On the contrary, the current intelligence analyst's task is often extremely concept-driven. The analyst must provide immediate interpretation of the latest, often unexpected events. Apart from his or her store of background information, the analyst may have no data other than the initial, usually incomplete report. Under these circumstances, interpretation is based upon an implicit mental model of how and why events normally transpire in the country for which the analyst is responsible. Accuracy of judgment depends almost exclusively

upon accuracy of the mental model, for there is little other basis for judgment.

It is necessary to consider how this mental model gets tested against reality, and how it can be changed to improve the accuracy of analytical judgment. Two things make it hard to change one's mental model. The first is the nature of human perception and information-processing. The second is the difficulty, in many fields, of learning what truly is an accurate model.

Partly because of the nature of human perception and information-processing, beliefs of all types tend to resist change. This is especially true of the implicit assumptions and supposedly self-evident truths that play an important role in forming mental models. Analysts are often surprised to learn that what are to them self-evident truths are by no means self-evident to others, or that self-evident truth at one point in time may be commonly regarded as uninformed assumption 10 years later.

Information that is consistent with an existing mind-set is perceived and processed easily and reinforces existing beliefs. Because the mind strives instinctively for consistency, information that is inconsistent with an existing mental image tends to be overlooked, perceived in a distorted manner, or rationalized to fit existing assumptions and beliefs.[63]

Learning to make better judgments through experience assumes systematic feedback on the accuracy of previous judgments and an ability to link the accuracy of a judgment with the particular configuration of variables that prompted an analyst to make that judgment. In practice, intelligence analysts get little systematic feedback, and even when they learn that an event they had foreseen has actually occurred or failed to occur, they typically do not know for certain whether this happened for the reasons they had foreseen. Thus, an analyst's personal experience may be a poor guide to revision of his or her mental mode.[64]

63. This refers, of course, to subconscious processes. No analyst will consciously distort information that does not fit his or her preconceived beliefs. Important aspects of the perception and processing of new information occur prior to and independently of any conscious direction, and the tendencies described here are largely the result of these subconscious or preconscious processes.

64. A similar point has been made in rebutting the belief in the accumulated wisdom of the classroom teacher. "It is actually very difficult for teachers to profit from experience. They almost never learn about their long-term successes or failures, and their short-term effects are not easily traced to the practices from which they presumably arose." B. F. Skinner, *The Technology of Teaching* (New York: Appleton-Century Crofts, 1968), pp. 112-113.

Mosaic Theory of Analysis

Understanding of the analytic process has been distorted by the mosaic metaphor commonly used to describe it. According to the mosaic theory of intelligence, small pieces of information are collected that, when put together like a mosaic or jigsaw puzzle, eventually enable analysts to perceive a clear picture of reality. The analogy suggests that accurate estimates depend primarily upon having all the pieces, that is, upon accurate and relatively complete information. It is important to collect and store the small pieces of information, as these are the raw material from which the picture is made; one never knows when it will be possible for an astute analyst to fit a piece into the puzzle. Part of the rationale for large technical intelligence collection systems is rooted in this mosaic theory.

Insights from cognitive psychology suggest that intelligence analysts do not work this way and that the most difficult analytical tasks cannot be approached in this manner. Analysts commonly find pieces that appear to fit many different pictures. Instead of a picture emerging from putting all the pieces together, analysts typically form a picture first and then select the pieces to fit. Accurate estimates depend at least as much upon the mental model used in forming the picture as upon the number of pieces of the puzzle that have been collected.

A more accurate analogy for describing how intelligence analysis should work is medical diagnosis. The doctor observes indicators (symptoms) of what is happening, uses his or her specialized knowledge of how the body works to develop hypotheses that might explain these observations, conducts tests to collect additional information to evaluate the hypotheses, then makes a diagnosis. This medical analogy focuses attention on the ability to identify and evaluate all plausible hypotheses. Collection is focused narrowly on information that will help to discriminate the relative probability of alternate hypothesis.

To the extent that this medical analogy is the more appropriate guide to understanding the analytical process, there are implications for the allocation of limited intelligence resources. While analysis and collection are both important, the medical analogy attributes more value to analysis and less to collection than the mosaic metaphor.

Conclusions

To the leaders and managers of intelligence who seek an improved intelligence product, these findings offer a reminder that this goal can be achieved by improving analysis as well as collection. There appear to be inherent practical limits on how much can be gained by efforts to improve collection. By contrast, an open and fertile field exists for imaginative efforts to improve analysis.

These efforts should focus on improving the mental models employed by analysts to interpret information and the analytical processes used to evaluate it. While this will be difficult to achieve, it is so critical to effective intelligence analysis that even small improvements could have large benefits. Specific recommendations are included the next three chapters and in Chapter 14, "Improving Intelligence Analysis."

Chapter 6

Keeping an Open Mind

Minds are like parachutes. They only function when they are open. After reviewing how and why thinking gets channeled into mental ruts, this chapter looks at mental tools to help analysts keep an open mind, question assumptions, see different perspectives, develop new ideas, and recognize when it is time to change their minds.

A new idea is the beginning, not the end, of the creative process. It must jump over many hurdles before being embraced as an organizational product or solution. The organizational climate plays a crucial role in determining whether new ideas bubble to the surface or are suppressed.

* * * * * * * * * * * * * * * * * * * *

Major intelligence failures are usually caused by failures of analysis, not failures of collection. Relevant information is discounted, misinterpreted, ignored, rejected, or overlooked because it fails to fit a prevailing mental model or mind-set.[65] The "signals" are lost in the "noise."[66] How can we ensure that analysts remain open to new experience and recognize

65. Christopher Brady, "Intelligence Failures: Plus Ca Change. . ." *Intelligence and National Security*, Vol. 8, No. 4 (October 1993). N. Cigar, "Iraq's Strategic Mindset and the Gulf War: Blueprint for Defeat," *The Journal of Strategic Studies*, Vol. 15, No. 1 (March 1992). J. J. Wirtz, *The Tet Offensive: Intelligence Failure in War* (New York, 1991). Ephraim Kam, *Surprise Attack* (Harvard University Press, 1988). Richard Betts, *Surprise Attack: Lessons for Defense Planning* (Brookings, 1982). Abraham Ben-Zvi, "The Study of Surprise Attacks," *British Journal of International Studies*, Vol. 5 (1979). *Iran: Evaluation of Intelligence Performance Prior to November 1978* (Staff Report, Subcommittee on Evaluation, Permanent Select Committee on Intelligence, US House of Representatives, January 1979). Richard Betts, "Analysis, War and Decision: Why Intelligence Failures Are Inevitable," *World Politics*, Vol. 31, No. 1 (October 1978). Richard W. Shryock, "The Intelligence Community Post-Mortem Program, 1973-1975," *Studies in Intelligence*, Vol. 21, No. 1 (Fall 1977). Avi Schlaim, "Failures in National Intelligence Estimates: The Case of the Yom Kippur War," *World Politics*, Vol. 28 (April 1976). Michael Handel, *Perception, Deception, and Surprise: The Case of the Yom Kippur War* (Jerusalem: Leonard Davis Institute of International Relations, Jerusalem Paper No. 19, 1976). Klaus Knorr, "Failures in National Intelligence Estimates: The Case of the Cuban Missiles," World Politics, Vol. 16 (1964).

66. Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford University Press, 1962). Roberta Wohlstetter, "Cuba and Pearl Harbor: Hindsight and Foresight," *Foreign Affairs*, Vol. 43, No. 4 (July 1965).

when long-held views or conventional wisdom need to be revised in response to a changing world?

Beliefs, assumptions, concepts, and information retrieved from memory form a mind-set or mental model that guides perception and processing of new information. The nature of the intelligence business forces us to deal with issues at an early stage when hard information is incomplete. If there were no gaps in the information on an issue or situation, and no ambiguity, it would not be an interesting intelligence problem. When information is lacking, analysts often have no choice but to lean heavily on prior beliefs and assumptions about how and why events normally transpire in a given country.

A mind-set is neither good nor bad. It is unavoidable. It is, in essence, a distillation of all that analysts think they know about a subject. It forms a lens through which they perceive the world, and once formed, it resists change.

Understanding Mental Ruts

Chapter 3 on memory suggested thinking of information in memory as somehow interconnected like a massive, multidimensional spider web. It is possible to connect any point within this web to any other point. When analysts connect the same points frequently, they form a path that makes it easier to take that route in the future. Once they start thinking along certain channels, they tend to continue thinking the same way and the path may become a rut. The path seems like the obvious and natural way to go. Information and concepts located near that path are readily available, so the same images keep coming up. Information not located near that path is less likely to come to mind.

Talking about breaking mind-sets, or creativity, or even just openness to new information is really talking about spinning new links and new paths through the web of memory. These are links among facts and concepts, or between schemata for organizing facts or concepts, that were not directly connected or only weakly connected before.

New ideas result from the association of old elements in new combinations. Previously remote elements of thought suddenly become as-

sociated in a new and useful combination.[67] When the linkage is made, the light dawns. This ability to bring previously unrelated information and ideas together in meaningful ways is what marks the open-minded, imaginative, creative analyst.

To illustrate how the mind works, consider my personal experience with a kind of mental block familiar to all analysts—writer's block. I often need to break a mental block when writing. Everything is going along fine until I come to one paragraph and get stuck. I write something down, know it is not quite right, but just cannot think of a better way to say it. However I try to change the paragraph, it still comes out basically the same way. My thinking has become channeled, and I cannot break out of that particular thought pattern to write it differently.

A common response to this problem is to take a break, work on something different for a while, and come back to the difficult portion later. With the passage of time, the path becomes less pronounced and it becomes easier to make other connections.

I have found another solution. I force myself to talk about it out loud. I close the door to my office—I am embarrassed to have anyone hear me talking to myself—and then stand up and walk around and talk. I say, okay, "What is the point of this paragraph? What are you trying to communicate?" I answer myself out loud as though talking to someone else. "The point I am trying to get across is that . . . ," and then it just comes. Saying it out loud breaks the block, and words start coming together in different ways.

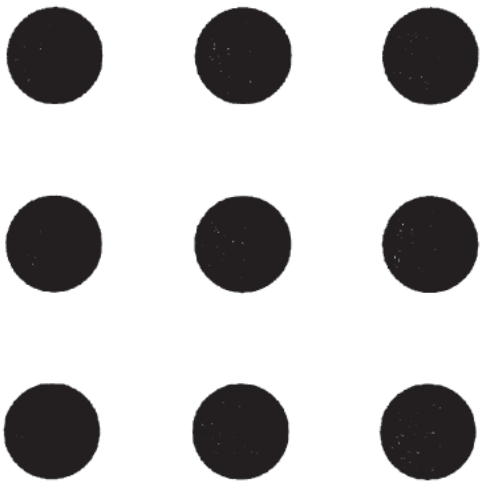
Recent research explains why this happens. Scientists have learned that written language and spoken language are processed in different parts of the brain.[68] They activate different neurons.

Problem-Solving Exercise

Before discussing how analysts can keep their minds open to new information, let us warm up to this topic with a brief exercise. Without lifting pencil from paper, draw no more than four straight lines that will cross through all nine dots in Figure 6.[69]

67. S. A. Mednick, "The Associative Basis of the Creative Process," *Psychological Review*, Vol. 69 (1962), p. 221.
68. Jerry E. Bishop, "Stroke Patients Yield Clues to Brain's Ability to Create Language," *Wall Street Journal*, Oct. 12, 1993, p.A1.
69. The puzzle is from James L. Adams, *Conceptual Blockbusting: A Guide to Better Ideas*. Second Edition (New York: W. W. Norton, 1980), p. 23.

Figure 6



After trying to solve the puzzle on your own, refer to the end of this chapter for answers and further discussion. Then consider that intelligence analysis is too often limited by similar, unconscious, self-imposed constraints or "cages of the mind."

You do not need to be constrained by conventional wisdom. It is often wrong. You do not *necessarily* need to be constrained by existing policies. They can sometimes be changed if you show a good reason for doing so. You do not *necessarily* need to be constrained by the specific analytical requirement you were given. The policymaker who originated the requirement may not have thought through his or her needs or the requirement may be somewhat garbled as it passes down through several echelons to you to do the work. You may have a better understanding than the policymaker of what he or she needs, or should have, or what is possible to do. You should not hesitate to go back up the chain of command with a suggestion for doing something a little different than what was asked for.

Mental Tools

People use various physical tools such as a hammer and saw to enhance their capacity to perform various physical tasks. People can also use simple mental tools to enhance their ability to perform mental tasks. These tools help overcome limitations in human mental machinery for perception, memory, and inference. The next few sections of this chapter discuss mental tools for opening analysts' minds to new ideas, while the next one (Chapter 7) deals with mental tools for structuring complex analytical problems.

Questioning Assumptions

It is a truism that analysts need to question their assumptions. Experience tells us that when analytical judgments turn out to be wrong, it usually was not because the information was wrong. It was because an analyst made one or more faulty assumptions that went unchallenged. The problem is that analysts cannot question everything, so where do they focus their attention?

Sensitivity Analysis. One approach is to do an informal sensitivity analysis. How sensitive is the ultimate judgment to changes in any of the major variables or driving forces in the analysis? Those linchpin assumptions that drive the analysis are the ones that need to be questioned. Analysts should ask themselves what could happen to make any of these assumptions out of date, and how they can know this has not already happened. They should try to disprove their assumptions rather than confirm them. If an analyst cannot think of anything that would cause a change of mind, his or her mind-set may be so deeply entrenched that the analyst cannot see the conflicting evidence. One advantage of the competing hypotheses approach discussed in Chapter 8 is that it helps identify the linchpin assumptions that swing a conclusion in one direction or another.

Identify Alternative Models. Analysts should try to identify alternative models, conceptual frameworks, or interpretations of the data by seeking out individuals who disagree with them rather than those who agree. Most people do not do that very often. It is much more comfortable to talk with people in one's own office who share the same basic mind-set. There are a few things that can be done as a matter of policy,

and that have been done in some offices in the past, to help overcome this tendency.

At least one Directorate of Intelligence component, for example, has had a peer review process in which none of the reviewers was from the branch that produced the report. The rationale for this was that an analyst's immediate colleagues and supervisor(s) are likely to share a common mind-set. Hence these are the individuals least likely to raise fundamental issues challenging the validity of the analysis. To avoid this mind-set problem, each research report was reviewed by a committee of three analysts from other branches handling other countries or issues. None of them had specialized knowledge of the subject. They were, however, highly accomplished analysts. Precisely because they had not been immersed in the issue in question, they were better able to identify hidden assumptions and other alternatives, and to judge whether the analysis adequately supported the conclusions.

Be Wary of Mirror Images. One kind of assumption an analyst should always recognize and question is mirror-imaging—filling gaps in the analyst's own knowledge by assuming that the other side is likely to act in a certain way because that is how the US would act under similar circumstances. To say, "if I were a Russian intelligence officer . . ." or "if I were running the Indian Government . . ." is mirror-imaging. Analysts may have to do that when they do not know how the Russian intelligence officer or the Indian Government is really thinking. But mirror-imaging leads to dangerous assumptions, because people in other cultures *do not* think the way we do. The frequent assumption that they do is what Adm. David Jeremiah, after reviewing the Intelligence Community failure to predict India's nuclear weapons testing, termed the "everybody-thinks-like-us mind-set."[70]

Failure to understand that others perceive their national interests differently from the way we perceive those interests is a constant source of problems in intelligence analysis. In 1977, for example, the Intelligence Community was faced with evidence of what appeared to be a South African nuclear weapons test site. Many in the Intelligence Community, especially those least knowledgeable about South Africa, tended to dismiss this evidence on the grounds that "Pretoria would not want a nucle-

70. Jim Wolf, "CIA Inquest Finds US Missed Indian `Mindset'," UPI wire service, June 3, 1998.

ar weapon, because there is no enemy they could effectively use it on."[71] The US perspective on what is in another country's national interest is usually irrelevant in intelligence analysis. Judgment must be based on how the other country perceives its national interest. If the analyst cannot gain insight into what the other country is thinking, mirror-imaging may be the only alternative, but analysts should never get caught putting much confidence in that kind of judgment.

Seeing Different Perspectives

Another problem area is looking at familiar data from a different perspective. If you play chess, you know you can see your own options pretty well. It is much more difficult to see all the pieces on the board as your opponent sees them, and to anticipate how your opponent will react to your move. That is the situation analysts are in when they try to see how the US Government's actions look from another country's perspective. Analysts constantly have to move back and forth, first seeing the situation from the US perspective and then from the other country's perspective. This is difficult to do, as you experienced with the picture of the old woman/young woman in Chapter 2 on perception.

Several techniques for seeing alternative perspectives exploit the general principle of coming at the problem from a different direction and asking different questions. These techniques break your existing mind-set by causing you to play a different and unaccustomed role.

Thinking Backwards. One technique for exploring new ground is thinking backwards. As an intellectual exercise, start with an assumption that some event you did not expect has actually occurred. Then, put yourself into the future, looking back to explain how this could have happened. Think what must have happened six months or a year earlier to set the stage for that outcome, what must have happened six months or a year before that to prepare the way, and so on back to the present.

Thinking backwards changes the focus from whether something might happen to how it might happen. Putting yourself into the future creates a different perspective that keeps you from getting anchored in the present. Analysts will often find, to their surprise, that they can construct a quite plausible scenario for an event they had previously thought unlikely. Thinking backwards is particularly helpful for events that have

71. Discussion with Robert Jaster, former National Intelligence Officer for Southern Africa.

a low probability but very serious consequences should they occur, such as a collapse or overthrow of the Saudi monarchy.

Crystal Ball. The crystal ball approach works in much the same way as thinking backwards.[72] Imagine that a "perfect" intelligence source (such as a crystal ball) has told you a certain assumption is wrong. You must then develop a scenario to explain how this could be true. If you can develop a plausible scenario, this suggests your assumption is open to some question.

Role playing. Role playing is commonly used to overcome constraints and inhibitions that limit the range of one's thinking. Playing a role changes "where you sit." It also gives one license to think and act differently. Simply trying to imagine how another leader or country will think and react, which analysts do frequently, is not role playing. One must actually act out the role and become, in a sense, the person whose role is assumed. It is only "living" the role that breaks an analyst's normal mental set and permits him or her to relate facts and ideas to each other in ways that differ from habitual patterns. An analyst cannot be expected to do this alone; some group interaction is required, with different analysts playing different roles, usually in the context of an organized simulation or game.

Most of the gaming done in the Defense Department and in the academic world is rather elaborate and requires substantial preparatory work. It does not have to be that way. The preparatory work can be avoided by starting the game with the current situation already known to analysts, rather than with a notional scenario that participants have to learn. Just one notional intelligence report is sufficient to start the action in the game. In my experience, it is possible to have a useful political game in just one day with almost no investment in preparatory work.

Gaming gives no "right" answer, but it usually causes the players to see some things in a new light. Players become very conscious that "where you stand depends on where you sit." By changing roles, the participants see the problem in a different context. This frees the mind to think differently.

Devil's Advocate. A devil's advocate is someone who defends a minority point of view. He or she may not necessarily agree with that view,

72. Jon Fallesen, Rex Michel, James Lussier, and Julia Pounds, "Practical Thinking: Innovation in Battle Command Instruction" *(Technical Report 1037, US Army Research Institute for the Behavioral and Social Sciences*, January 1996).

but may choose or be assigned to represent it as strenuously as possible. The goal is to expose conflicting interpretations and show how alternative assumptions and images make the world look different. It often requires time, energy, and commitment to see how the world looks from a different perspective.[73]

Imagine that you are the boss at a US facility overseas and are worried about the possibility of a terrorist attack. A standard staff response would be to review existing measures and judge their adequacy. There might well be pressure—subtle or otherwise—from those responsible for such arrangements to find them satisfactory. An alternative or supplementary approach would be to name an individual or small group as a devil's advocate assigned to develop actual plans for launching such an attack. The assignment to think like a terrorist liberates the designated person(s) to think unconventionally and be less inhibited about finding weaknesses in the system that might embarrass colleagues, because uncovering any such weaknesses is the assigned task.

Devil's advocacy has a controversial history in the Intelligence Community. Suffice it to say that some competition between conflicting views is healthy and must be encouraged; all-out political battle is counterproductive.

Recognizing When To Change Your Mind

As a general rule, people are too slow to change an established view, as opposed to being too willing to change. The human mind is conservative. It resists change. Assumptions that worked well in the past continue to be applied to new situations long after they have become outmoded.

Learning from Surprise. A study of senior managers in industry identified how some successful managers counteract this conservative bent. They do it, according to the study,

> By paying attention to their feelings of surprise when a particular fact does not fit their prior understanding, and then by highlighting rather than denying the novelty. Although surprise made them feel uncomfortable, it made them take the cause [of the surprise] seriously and inquire into it. . . . Rather than

73. For an interesting discussion of the strengths and potential weaknesses of the "devil's advocate" approach, see Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), pp. 415-418.

> deny, downplay, or ignore disconfirmation [of their prior view], successful senior managers often treat it as friendly and in a way cherish the discomfort surprise creates. As a result, these managers often perceive novel situations early on and in a frame of mind relatively undistorted by hidebound notions.[74]

Analysts should keep a record of unexpected events and think hard about what they might mean, not disregard them or explain them away. It is important to consider whether these surprises, however small, are consistent with some alternative hypothesis. One unexpected event may be easy to disregard, but a pattern of surprises may be the first clue that your understanding of what is happening requires some adjustment, is at best incomplete, and may be quite wrong.

Strategic Assumptions vs. Tactical Indicators. Abraham Ben-Zvi analyzed five cases of intelligence failure to foresee a surprise attack.[75] He made a useful distinction between estimates based on strategic assumptions and estimates based on tactical indications. Examples of strategic assumptions include the US belief in 1941 that Japan wished to avoid war at all costs because it recognized US military superiority, and the Israeli belief in 1973 that the Arabs would not attack Israel until they obtained sufficient air power to secure control of the skies. A more recent instance was the 1998 Indian nuclear test, which was widely viewed as a surprise and, at least in part, as a failure by the experts to warn of an impending test. The incorrect strategic assumption was that the new Indian Government would be dissuaded from testing nuclear weapons for fear of US economic sanctions.[76]

Tactical indicators are specific reports of preparations or intent to initiate hostile action or, in the recent Indian case, reports of preparations for a nuclear test. Ben-Zvi found that whenever strategic assumptions and tactical indicators of impending attack converged, an immediate threat was perceived and appropriate precautionary measures were taken.

74. Daniel J. Isenberg, "How Senior Managers Think," in David Bell, Howard Raiffa, and Amos Tversky, *Decision Making: Descriptive, Normative, and Prescriptive Interactions* (Cambridge University Press, 1988), p. 535.
75. Abraham Ben Zvi, "Hindsight and Foresight: A Conceptual Framework for the Analysis of Surprise Attacks," *World Politics*, April 1976.
76. Transcript of Admiral David Jeremiah's news conference on the Intelligence Community's performance concerning the Indian nuclear test, fourth and fifth paragraphs and first Q and A, 2 June 1998.

When discrepancies existed between tactical indicators and strategic assumptions in the five cases Ben-Zvi analyzed, the strategic assumptions always prevailed, and they were never reevaluated in the light of the increasing flow of contradictory information. Ben-Zvi concludes that tactical indicators should be given increased weight in the decisionmaking process. At a minimum, the emergence of tactical indicators that contradict our strategic assumption should trigger a higher level of intelligence alert. It may indicate that a bigger surprise is on the way.

Chapter 8, "Analysis of Competing Hypotheses," provides a framework for identifying surprises and weighing tactical indicators and other forms of current evidence against longstanding assumptions and beliefs.

Stimulating Creative Thinking

Imagination and creativity play important roles in intelligence analysis as in most other human endeavors. Intelligence judgments require the ability to imagine possible causes and outcomes of a current situation. All possible outcomes are not given. The analyst must think of them by imagining scenarios that explicate how they might come about. Similarly, imagination as well as knowledge is required to reconstruct how a problem appears from the viewpoint of a foreign government. Creativity is required to question things that have long been taken for granted. The fact that apples fall from trees was well known to everyone. Newton's creative genius was to ask "why?" Intelligence analysts, too, are expected to raise new questions that lead to the identification of previously unrecognized relationships or to possible outcomes that had not previously been foreseen.

A creative analytical product shows a flair for devising imaginative or innovative—but also accurate and effective—ways to fulfill any of the major requirements of analysis: gathering information, analyzing information, documenting evidence, and/or presenting conclusions. Tapping unusual sources of data, asking new questions, applying unusual analytic methods, and developing new types of products or new ways of fitting analysis to the needs of consumers are all examples of creative activity.

A person's intelligence, as measured by IQ tests, has little to do with creativity, but the organizational environment exercises a major influence. New but appropriate ideas are most likely to arise in an organizational climate that nurtures their development and communication.

The old view that creativity is something one is born with, and that it cannot be taught or developed, is largely untrue. While native talent, per se, is important and may be immutable, it is possible to learn to employ one's innate talents more productively. With understanding, practice, and conscious effort, analysts can learn to produce more imaginative, innovative, creative work.

There is a large body of literature on creativity and how to stimulate it. At least a half-dozen different methods have been developed for teaching, facilitating, or liberating creative thinking. All the methods for teaching or facilitating creativity are based on the assumption that the *process* of thinking can be separated from the *content* of thought. One learns mental strategies that can be applied to any subject.

It is not our purpose here to review commercially available programs for enhancing creativity. Such programmatic approaches can be applied more meaningfully to problems of new product development, advertising, or management than to intelligence analysis. It is relevant, however, to discuss several key principles and techniques that these programs have in common, and that individual intelligence analysts or groups of analysts can apply in their work.

Intelligence analysts must generate ideas concerning potential causes or explanations of events, policies that might be pursued or actions taken by a foreign government, possible outcomes of an existing situation, and variables that will influence which outcome actually comes to pass. Analysts also need help to jog them out of mental ruts, to stimulate their memories and imaginations, and to perceive familiar events from a new perspective.

Here are some of the principles and techniques of creative thinking that can be applied to intelligence analysis.

Deferred Judgment. The principle of deferred judgment is undoubtedly the most important. The idea-generation phase of analysis should be separated from the idea-evaluation phase, with evaluation deferred until all possible ideas have been brought out. This approach runs contrary to the normal procedure of thinking of ideas and evaluating them concurrently. Stimulating the imagination and critical thinking are both important, but they do not mix well. A judgmental attitude dampens the imagination, whether it manifests itself as self-censorship of one's own ideas or fear of critical evaluation by colleagues or supervisors. Idea generation should be a freewheeling, unconstrained, uncritical process.

New ideas are, by definition, unconventional, and therefore likely to be suppressed, either consciously or unconsciously, unless they are born in a secure and protected environment. Critical judgment should be suspended until after the idea-generation stage of analysis has been completed. A series of ideas should be written down and then evaluated later. This applies to idea searching by individuals as well as brainstorming in a group. Get all the ideas out on the table before evaluating any of them.

Quantity Leads to Quality. A second principle is that quantity of ideas eventually leads to quality. This is based on the assumption that the first ideas that come to mind will be those that are most common or usual. It is necessary to run through these conventional ideas before arriving at original or different ones. People have habitual ways of thinking, ways that they continue to use because they have seemed successful in the past. It may well be that these habitual responses, the ones that come first to mind, are the best responses and that further search is unnecessary. In looking for usable new ideas, however, one should seek to generate as many ideas as possible before evaluating any of them.

No Self-Imposed Constraints. A third principle is that thinking should be allowed—indeed encouraged—to range as freely as possible. It is necessary to free oneself from self-imposed constraints, whether they stem from analytical habit, limited perspective, social norms, emotional blocks, or whatever.

Cross-Fertilization of Ideas. A fourth principle of creative problem-solving is that cross-fertilization of ideas is important and necessary. Ideas should be combined with each other to form more and even better ideas. If creative thinking involves forging new links between previously unrelated or weakly related concepts, then creativity will be stimulated by any activity that brings more concepts into juxtaposition with each other in fresh ways. Interaction with other analysts is one basic mechanism for this. As a general rule, people generate more creative ideas when teamed up with others; they help to build and develop each other's ideas. Personal interaction stimulates new associations between ideas. It also induces greater effort and helps maintain concentration on the task.

These favorable comments on group processes are not meant to encompass standard committee meetings or coordination processes that force consensus based on the lowest common denominator of agreement. My positive words about group interaction apply primarily to

brainstorming sessions aimed at generating new ideas and in which, according to the first principle discussed above, all criticism and evaluation are deferred until after the idea generation stage is completed.

Thinking things out alone also has its advantages: individual thought tends to be more structured and systematic than interaction within a group. Optimal results come from alternating between individual thinking and team effort, using group interaction to generate ideas that supplement individual thought. A diverse group is clearly preferable to a homogeneous one. Some group participants should be analysts who are not close to the problem, inasmuch as their ideas are more likely to reflect different insights.

Idea Evaluation. All creativity techniques are concerned with stimulating the flow of ideas. There are no comparable techniques for determining which ideas are best. The procedures are, therefore, aimed at idea generation rather than idea evaluation. The same procedures do aid in evaluation, however, in the sense that ability to generate more alternatives helps one see more potential consequences, repercussions, and effects that any single idea or action might entail.

Organizational Environment

A new idea is not the end product of the creative process. Rather, it is the beginning of what is sometimes a long and tortuous process of translating an idea into an innovative product. The idea must be developed, evaluated, and communicated to others, and this process is influenced by the organizational setting in which it transpires. The potentially useful new idea must pass over a number of hurdles before it is embraced as an organizational product.

The following paragraphs describe in some detail research conducted by Frank Andrews to investigate the relationship among creative ability, organizational setting, and innovative research products.[77] The subjects of this research were 115 scientists, each of whom had directed a research project dealing with social-psychological aspects of disease. These scientists were given standardized tests that measure creative ability and intelligence. They were also asked to fill out an extensive questionnaire

77. Frank M. Andrews, "Social and Psychological Factors Which Influence the Creative Process," in Irving A. Taylor and Jacob W. Getzels, eds., *Perspectives in Creativity* (Chicago, Aldine Publishing, 1975).

concerning the environment in which their research was conducted. A panel of judges composed of the leading scientists in the field of medical sociology was asked to evaluate the principal published results from each of the 115 research projects.

Judges evaluated the research results on the basis of productivity and innovation. Productivity was defined as the "extent to which the research represents an addition to knowledge along established lines of research or as extensions of previous theory." Innovativeness was defined as "additions to knowledge through new lines of research or the development of new theoretical statements of findings that were not explicit in previous theory.[78] Innovation, in other words, involved raising new questions and developing new approaches to the acquisition of knowledge, as distinct from working productively within an already established framework. This same definition applies to innovation in intelligence analysis.

Andrews found virtually no relationship between the scientists' creative ability and the innovativeness of their research. (There was also no relationship between level of intelligence and innovativeness.) Those who scored high on tests of creative ability did not necessarily receive high ratings from the judges evaluating the innovativeness of their work. A possible explanation is that either creative ability or innovation, or both, were not measured accurately, but Andrews argues persuasively for another view. Various social and psychological factors have so great an effect on the steps needed to translate creative ability into an innovative research product that there is no measurable effect traceable to creative ability alone. In order to document this conclusion, Andrews analyzed data from the questionnaires in which the scientists described their work environment.

Andrews found that scientists possessing more creative ability produced more innovative work only under the following favorable conditions:

- When the scientist perceived himself or herself as responsible for initiating new activities. The opportunity for innovation, and the encouragement of it, are—not surprisingly—important variables.

78. Ibid., p. 122.

- When the scientist had considerable control over decisionmaking concerning his or her research program—in other words, the freedom to set goals, hire research assistants, and expend funds. Under these circumstances, a new idea is less likely to be snuffed out before it can be developed into a creative and useful product.

- When the scientist felt secure and comfortable in his or her professional role. New ideas are often disruptive, and pursuing them carries the risk of failure. People are more likely to advance new ideas if they feel secure in their positions.

- When the scientist's administrative superior "stayed out of the way." Research is likely to be more innovative when the superior limits himself or herself to support and facilitation rather than direct involvement.

- When the project was relatively small with respect to the number of people involved, budget, and duration. Small size promotes flexibility, and this in turn is more conducive to creativity.

- When the scientist engaged in other activities, such as teaching or administration, in addition to the research project. Other work may provide useful stimulation or help one identify opportunities for developing or implementing new ideas. Some time away from the task, or an incubation period, is generally recognized as part of the creative process."

The importance of any one of these factors was not very great, but their impact was cumulative. The presence of all or most of these conditions exerted a strongly favorable influence on the creative process. Conversely, the absence of these conditions made it quite unlikely that even highly creative scientists could develop their new ideas into innovative research results. Under unfavorable conditions, the most creatively inclined scientists produced even less innovative work than their less imaginative colleagues, presumably because they experienced greater frustration with their work environment.

In summary, some degree of innate creative talent may be a necessary precondition for innovative work, but it is unlikely to be of much value unless the organizational environment in which that work is done nurtures the development and communication of new ideas. Under unfavorable circumstances, an individual's creative impulses probably will find expression outside the organization.

There are, of course, exceptions to the rule. Some creativity occurs even in the face of intense opposition. A hostile environment can be stimulating, enlivening, and challenging. Some people gain satisfaction from viewing themselves as lonely fighters in the wilderness, but when it comes to conflict between a large organization and a creative individual within it, the organization generally wins.

Recognizing the role of organizational environment in stimulating or suppressing creativity points the way to one obvious set of measures to enhance creative organizational performance. Managers of analysis, from first-echelon supervisors to the Director of Central Intelligence, should take steps to strengthen and broaden the perception among analysts that new ideas are welcome. This is not easy; creativity implies criticism of that which already exists. It is, therefore, inherently disruptive of established ideas and organizational practices.

Particularly within his or her own office, an analyst needs to enjoy a sense of security, so that partially developed ideas may be expressed and bounced off others as sounding boards with minimal fear of criticism or ridicule for deviating from established orthodoxy. At its inception, a new idea is frail and vulnerable. It needs to be nurtured, developed, and tested in a protected environment before being exposed to the harsh reality of public criticism. It is the responsibility of an analyst's immediate supervisor and office colleagues to provide this sheltered environment.

Conclusions

Creativity, in the sense of new and useful ideas, is at least as important in intelligence analysis as in any other human endeavor. Procedures to enhance innovative thinking are not new. Creative thinkers have employed them successfully for centuries. The only new elements—and even they may not be new anymore—are the grounding of these procedures in psychological theory to explain how and why they work, and their formalization in systematic creativity programs.

Learning creative problem-solving techniques does not change an analyst's native-born talents but helps an analyst achieve his or her full potential. Most people have the ability to be more innovative than they themselves realize. The effectiveness of these procedures depends, in large measure, upon the analyst's motivation, drive, and perseverance in taking the time required for thoughtful analysis despite the pressures of day-to-day duties, mail, and current intelligence reporting.

A questioning attitude is a prerequisite to a successful search for new ideas. Any analyst who is confident that he or she already knows the answer, and that this answer has not changed recently, is unlikely to produce innovative or imaginative work. Another prerequisite to creativity is sufficient strength of character to suggest new ideas to others, possibly at the expense of being rejected or even ridiculed on occasion. "The ideas of creative people often lead them into direct conflict with the trends of their time, and they need the courage to be able to stand alone."[79]

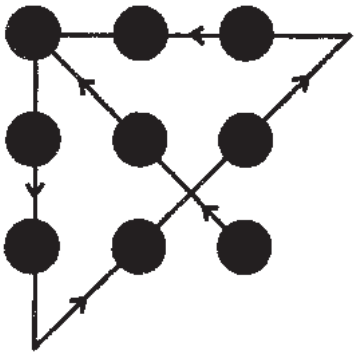
79. Robin Hogarth, *Judgment and Choice* (New York: Wiley, 1980), p. 117.

SOLUTIONS TO PUZZLE PRESENTED IN FIGURE 6

Figure 6

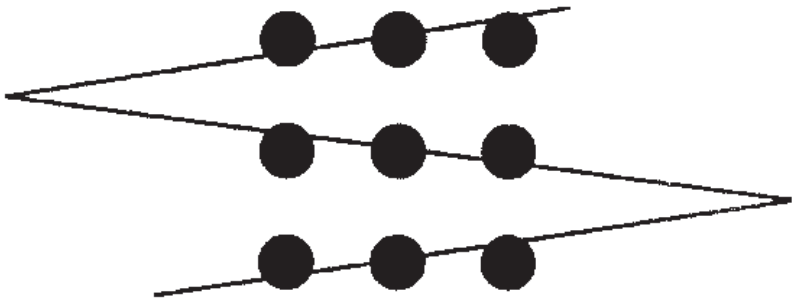
The nine-dots puzzle illustrated in Figure 6 above and earlier in this chapter is difficult to solve only if one defines the problem to narrowly. A surprising number of people assume they are not supposed to let the pencil go outside an imaginary square drawn around the nine dots.

Figure 7



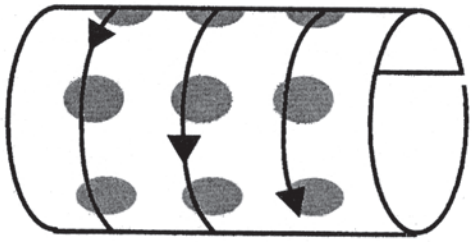
This unconscious constraint exists only in the mind of the problem-solver; it is not specified in the definition of the problem. With no limit on the length of lines, it should be relatively easy to come up with the answer shown in Figure 7.

Figure 8



Another common, unconscious constraint is the assumption that the lines must pass through the center of the dots. This constraint, too, exists only in the mind of the problem solver. Without it, the three-line solution in Figure 8 becomes rather obvious.

Figure 9



A more subtle and certainly more pervasive mental block is the assumption that such problems must be solved within a two-dimensional-plane. By rolling the paper to form a cylinder, it becomes possible to draw a single straight line that spirals through all nine dots, as in Figure 9.

Chapter 7

Structuring Analytical Problems

This chapter discusses various structures for decomposing and externalizing complex analytical problems when we cannot keep all the relevant factors in the forefront of our consciousness at the same time.

Decomposition means breaking a problem down into its component parts. Externalization means getting the problem out of our heads and into some visible form that we can work with.

* * * * * * * * * * * * * * * * * * * *

The discussion of working memory in Chapter 3 indicated that "The Magic Number Seven—Plus or Minus Two"[80] is the number of things most people can keep in working memory at one time. To experience firsthand this limitation on working memory while doing a mental task, try multiplying in your head any pair of two-digit numbers- for example, 46 times 78. On paper, this is a simple problem, but most people cannot keep track of that many numbers in their head.

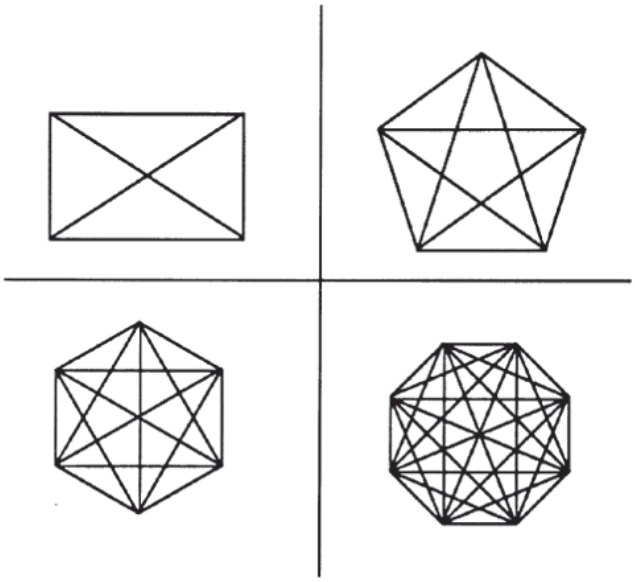
The limited capacity of working memory is the source of many problems in doing intelligence analysis. It is useful to consider just how complicated analysis can get, and how complexity might outstrip your working memory and impede your ability to make accurate judgments. Figure 10 illustrates how complexity increases geometrically as the number of variables in an analytical problem increases. The four-sided square shows that when a problem has just four variables, there are six possible interrelationships between those variables. With the pentagon, the five variables have 10 possible interrelationships. With six and eight variables, respectively, there are 15 and 28 possible interrelationships between variables.

The number of possible relationships between variables grows geometrically as the number of variables increases.

There are two basic tools for dealing with complexity in analysis—decomposition and externalization.

80. George A. Miller, "The Magical Number Seven, Plus or Minus Two: Some Limits on our Capacity for Processing Information." *The Psychological Review*, Vol. 63, No. 2 (March 1956).

Figure 10



The number of possible relationships between variables grows geometrically as the number of variables increases.

Decomposition means breaking a problem down into its component parts. That is, indeed, the essence of analysis. Webster's Dictionary defines analysis as division of a complex whole into its parts or elements.[81]

The spirit of decision analysis is to divide and conquer: Decompose a complex problem into simpler problems, get one's thinking straight in these simpler problems, paste these analyses together with a logical glue . . .[82]

Externalization means getting the decomposed problem out of one's head and down on paper or on a computer screen in some simplified form that shows the main variables, parameters, or elements of the problem and how they relate to each other. Writing down the multiplication problem, 46 times 78, is a very simple example of externalizing an ana-

81. *Webster's Ninth New Collegiate Dictionary*, 1988.
82. Howard Raiffa, *Decision Analysis* (Reading, MA: Addison-Wesley, 1968).

lytical problem. When it is down on paper, one can easily manipulate one part of the problem at a time and often be more accurate than when trying to multiply the numbers in one's head.

I call this drawing a picture of your problem. Others call it making a model of your problem. It can be as simple as just making lists pro and con.

This recommendation to compensate for limitations of working memory by decomposing and externalizing analytical problems is not new. The following quote is from a letter Benjamin Franklin wrote in 1772 to the great British scientist Joseph Priestley, the discoverer of oxygen:

> In the affair of so much importance to you, wherein you ask my advice, I cannot for want of sufficient premises, advise you what to determine, but if you please I will tell you how. When those difficult cases occur, they are difficult, chiefly because while we have them under consideration, all the reasons pro and con are not present to the mind at the same time, but sometimes one set present themselves, and at other times another, the first being out of sight. Hence the various purposes or inclinations that alternatively prevail, and the uncertainty that perplexes us.
>
> To get over this, my way is to divide half a sheet of paper by a line into two columns; writing over the one Pro, and over the other Con. Then, during three or four days of consideration, I put down under the different heads short hints of the different motives, that at different times occur to me, for or against the measure.
>
> When I have thus got them all together in one view, I endeavor to estimate their respective weights; and where I find two, one on each side, that seem equal, I strike them both out. If I find a reason pro equal to some two reasons con, I strike out the three . . . and thus proceeding I find at length where the balance lies; and if, after a day or two of further consideration, nothing new that is of importance occurs on either side, I come to a determination accordingly.

> And, though the weight of reasons cannot be taken with the precision of algebraic quantities, yet when each is thus considered, separately and comparatively, and the whole lies before me, I think I can judge better, and am less liable to make a rash step, and in fact I have found great advantage from this kind of equation. . . . [83]

It is noteworthy that Franklin over 200 years ago ident2ified the problem of limited working memory and how it affects one's ability to make judgments. As Franklin noted, decision problems are difficult because people cannot keep all the pros and cons in mind at the same time. We focus first on one set of arguments and then on another, ". . . hence the various purposes and inclinations that alternatively prevail, and the uncertainty that perplexes us."

Franklin also identified the solution—getting all the pros and cons out of his head and onto paper in some visible, shorthand form. The fact that this topic was part of the dialogue between such illustrious individuals reflects the type of people who use such analytical tools. These are not aids to be used by weak analysts but unneeded by the strong. Basic limitations of working memory affect everyone. It is the more astute and careful analysts who are most conscious of this and most likely to recognize the value gained by applying these very simple tools.

Putting ideas into visible form ensures that they will last. They will lie around for days goading you into having further thoughts. Lists are effective because they exploit people's tendency to be a bit compulsive—we want to keep adding to them. They let us get the obvious and habitual answers out of the way, so that we can add to the list by thinking of other ideas beyond those that came first to mind. One specialist in creativity has observed that "for the purpose of moving our minds, pencils can serve as crowbars"[84]—just by writing things down and making lists that stimulate new associations.

With the key elements of a problem written down in some abbreviated form, it is far easier to work with each of the parts while still keeping the problem as a whole in view. Analysts can generally take account of more factors than when making a global judgment. They can manipulate

83. J. Bigelow, ed., *The Complete Works of Benjamin Franklin* (New York: Putnam, 1887), p. 522.
84. Alex Osborn, *Applied Imagination*, Revised Edition (New York: Scribner's, 1979), p. 202.

individual elements of the problem to examine the many alternatives available through rearranging, combining, or modifying them. Variables may be given more weight or deleted, causal relationships reconceptualized, or conceptual categories redefined. Such thoughts may arise spontaneously, but they are more likely to occur when an analyst looks at each element, one by one, and asks questions designed to encourage and facilitate consideration of alternative interpretations.

Problem Structure

Anything that has parts also has a structure that relates these parts to each other. One of the first steps in doing analysis is to determine an appropriate structure for the analytical problem, so that one can then identify the various parts and begin assembling information on them. Because there are many different kinds of analytical problems, there are also many different ways to structure analysis.

Lists such as Franklin made are one of the simplest structures. An intelligence analyst might make lists of relevant variables, early warning indicators, alternative explanations, possible outcomes, factors a foreign leader will need to take into account when making a decision, or arguments for and against a given explanation or outcome.

Other tools for structuring a problem include outlines, tables, diagrams, trees, and matrices, with many sub-species of each. For example, trees include decision trees and fault trees. Diagrams includes causal diagrams, influence diagrams, flow charts, and cognitive maps.

Consideration of all those tools is beyond the scope of this book, but several such tools are discussed. Chapter 11, "Biases in Perception of Cause and Effect," has a section on Illusory Correlation that uses a (2x2) contingency table to structure analysis of the question: Is deception most likely when the stakes are very high? Chapter 8, "Analysis of Competing Hypotheses," is arguably the most useful chapter in this book. It recommends using a matrix to array evidence for and against competing hypotheses to explain what is happening now or estimate what may happen in the future.

The discussion below also uses a matrix to illustrate decomposition and externalization and is intended to prepare you for the next chapter on "Analysis of Competing Hypotheses." It demonstrates how to apply

these tools to a type of decision commonly encountered in our personal lives.

Car Purchase Matrix

In choosing among alternative purchases, such as when buying a car, a new computer, or a house, people often want to maximize their satisfaction on a number of sometimes-conflicting dimensions. They want a car at the lowest possible price, with the lowest maintenance cost, highest resale value, slickest styling, best handling, best gas mileage, largest trunk space, and so forth. They can't have it all, so they must decide what is most important and make tradeoffs. As Ben Franklin said, the choice is sometimes difficult. We vacillate between one choice and another, because we cannot keep in working memory at the same time all the characteristics of all the choices. We think first of one and then the other.

To handle this problem analytically, follow the divide-and-conquer principle and "draw a picture" of the problem as a whole that helps you identify and make the tradeoffs. The component parts of the car purchase problem are the cars you are considering buying and the attributes or dimensions you want to maximize. After identifying the desirable attributes that will influence your decision, weigh how each car stacks up on each attribute. A matrix is the appropriate tool for keeping track of your judgments about each car and each attribute, and then putting all the parts back together to make a decision.

Start by listing the important attributes you want to maximize, as shown for example in Figure 11.

Figure 11

Price

Maintenance Cost

Styling

Gas Mileage

Comfort

Handling

Next, quantify the relative importance of each attribute by dividing 100 percent among them. In other words, ask yourself what percentage of the decision should be based on price, on styling, etc. This forces you to ask relevant questions and make decisions you might have glossed over if you had not broken the problem down in this manner. How important is price versus styling, really? Do you really care what it looks like from the outside, or are you mainly looking for comfort on the inside and how

Figure 12

Price	**30%**
Operating Cost	**10%**
Styling	**20%**
Comfort	**20%**
Handling	**15%**
Safety	**5%**
Total	**100%**

it drives? Should safety be included in your list of important attributes? Because poor gas mileage can be offset by lower maintenance cost for repairs, perhaps both should be combined into a single attribute called operating cost.

This step might produce a result similar to Figure 12, depending on your personal preferences. If you do this together with your spouse, the exact basis of any difference of opinion will become immediately apparent and can be quantified.

Figure 13

	% Value	Car 1	Car 2	Car 3
Price	30%	3.5%	3.0%	3.5%
Operating Cost	10%	3.5%	2.0%	4.5%
Styling	20%	2.5%	4.5%	3.0%
Comfort	20%	4.0%	2.5%	3.5%
Handling	15%	3.0%	4.0%	3.0%
Safety	5%	3.5%	2.5%	4%

Next, identify the cars you are considering and judge how each one ranks on each of the six attributes shown in Figure 12. Set up a matrix as shown in Figure 13 and work across the rows of the matrix. For each attribute, take 10 points and divide it among the three cars based on how well they meet the requirements of that attribute. (This is the same as taking 100 percent and dividing it among the cars, but it keeps the numbers lower when you get to the next step.)

You now have a picture of your analytical problem—the comparative value you attribute to each of the principal attributes of a new car and a comparison of how various cars satisfy those desired attributes. If you have narrowed it down to three alternatives, your matrix will look something like Figure 13:

When all the cells of the matrix have been filled in, you can then calculate which car best suits your preferences. Multiply the percentage value you assigned to each attribute by the value you assigned to that attribute for each car, which produces the result in Figure 14. If the percentage values you assigned to each attribute accurately reflect your preferences, and if each car has been analyzed accurately, the analysis shows you will gain more satisfaction from the purchase of Car 3 than either of the alternatives.

Figure 14

	% Value	Car 1	Car 2	Car 3
Price	30%	105	90	105
Operating Cost	10%	35	20	45
Styling	20%	50	90	60
Comfort	20%	80	50	70
Handling	15%	45	60	45
Safety	5%	17.5	12.5	20
Totals		332.5	322.5	345

At this point, you do a sensitivity analysis to determine whether plausible changes in some values in the matrix would swing the decision to a different car. Assume, for example, that your spouse places different values than you on the relative importance of price versus styling. You can insert your spouse's percentage values for those two attributes and see if that makes a difference in the decision. (For example, one could reduce the importance of price to 20 percent and increase styling to 30 percent. That is still not quite enough to switch the choice to Car 2, which rates highest on styling.)

There is a technical name for this type of analysis. It is called Multiattribute Utility Analysis, and there are complex computer programs for doing it. In simplified form, however, it requires only pencil and paper and high school arithmetic. It is an appropriate structure for any purchase decision in which you must make tradeoffs between multiple competing preferences.

Conclusions

The car purchase example was a warmup for the following chapter. It illustrates the difference between just sitting down and thinking about a problem and really *analyzing* a problem. The essence of analysis is breaking down a problem into its component parts, assessing each part separately, then putting the parts back together to make a decision. The matrix in this example forms a "picture" of a complex problem by getting it out of our head and onto paper in a logical form that enables you to consider each of the parts individually.

You certainly would not want to do this type of analysis for all your everyday personal decisions or for every intelligence judgment. You may wish to do it, however, for an especially important, difficult, or controversial judgment, or when you need to leave an audit trail showing how you arrived at a judgment. The next chapter applies decomposition, externalization, and the matrix structure to a common type of intelligence problem.

Chapter 8

Analysis of Competing Hypotheses

Analysis of competing hypotheses, sometimes abbreviated ACH, is a tool to aid judgment on important issues requiring careful weighing of alternative explanations or conclusions. It helps an analyst overcome, or at least minimize, some of the cognitive limitations that make prescient intelligence analysis so difficult to achieve.

ACH is an eight-step procedure grounded in basic insights from cognitive psychology, decision analysis, and the scientific method. It is a surprisingly effective, proven process that helps analysts avoid common analytic pitfalls. Because of its thoroughness, it is particularly appropriate for controversial issues when analysts want to leave an audit trail to show what they considered and how they arrived at their judgment.[85]

* * * * * * * * * * * * * * * * * * * *

When working on difficult intelligence issues, analysts are, in effect, choosing among several alternative hypotheses. Which of several possible explanations is the correct one? Which of several possible outcomes is the most likely one? As previously noted, this book uses the term "hypothesis" in its broadest sense as a potential explanation or conclusion that is to be tested by collecting and presenting evidence.

Analysis of competing hypotheses (ACH) requires an analyst to explicitly identify all the reasonable alternatives and have them compete against each other for the analyst's favor, rather than evaluating their plausibility one at a time.

The way most analysts go about their business is to pick out what they suspect intuitively is the most likely answer, then look at the available information from the point of view of whether or not it supports this answer. If the evidence seems to support the favorite hypothesis,

85. The analysis of competing hypotheses procedure was developed by the author for use by intelligence analysts dealing with a set of particularly difficult problems.

analysts pat themselves on the back ("See, I knew it all along!") and look no further. If it does not, they either reject the evidence as misleading or develop another hypothesis and go through the same procedure again. Decision analysts call this a satisficing strategy. (See Chapter 4, Strategies for Analytical Judgment.) Satisficing means picking the first solution that seems satisfactory, rather than going through all the possibilities to identify the very best solution. There may be several seemingly satisfactory solutions, but there is only one best solution.

Chapter 4 discussed the weaknesses in this approach. The principal concern is that if analysts focus mainly on trying to confirm one hypothesis they think is probably true, they can easily be led astray by the fact that there is so much evidence to support their point of view. They fail to recognize that most of this evidence is also consistent with other explanations or conclusions, and that these other alternatives have not been refuted.

Simultaneous evaluation of multiple, competing hypotheses is very difficult to do. To retain three to five or even seven hypotheses in working memory and note how each item of information fits into each hypothesis is beyond the mental capabilities of most people. It takes far greater mental agility than listing evidence supporting a single hypothesis that was pre-judged as the most likely answer. It can be accomplished, though, with the help of the simple procedures discussed here. The box below contains a step-by-step outline of the ACH process.

Step 1

Identify the possible hypotheses to be considered. Use a group of analysts with different perspectives to brainstorm the possibilities.

Psychological research into how people go about generating hypotheses shows that people are actually rather poor at thinking of all the possibilities.[86] If a person does not even generate the correct hypothesis for consideration, obviously he or she will not get the correct answer.

86. Charles Gettys et al., *Hypothesis Generation: A Final Report on Three Years of Research*, Technical Report 15-10-80 (University of Oklahoma, Decision Processes Laboratory, 1980).

Step-by-Step Outline of Analysis of Competing Hypotheses

1. Identify the possible hypotheses to be considered. Use a group of analysts with different perspectives to brainstorm the possibilities.

2. Make a list of significant evidence and arguments for and against each hypothesis.

3. Prepare a matrix with hypotheses across the top and evidence down the side. Analyze the "diagnosticity" of the evidence and arguments—that is, identify which items are most helpful in judging the relative likelihood of the hypotheses.

4. Refine the matrix. Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value.

5. Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove the hypotheses rather than prove them.

6. Analyze how sensitive your conclusion is to a few critical items of evidence. Consider the consequences for your analysis if that evidence were wrong, misleading, or subject to a different interpretation.

7. Report conclusions. Discuss the relative likelihood of all the hypotheses, not just the most likely one.

8. Identify milestones for future observation that may indicate events are taking a different course than expected.

It is useful to make a clear distinction between the hypothesis generation and hypothesis evaluation stages of analysis. Step 1 of the recommended analytical process is to identify all hypotheses that merit detailed examination. At this early hypothesis generation stage, it is very useful to bring together a group of analysts with different backgrounds and perspectives. Brainstorming in a group stimulates the imagination and

may bring out possibilities that individual members of the group had not thought of. Initial discussion in the group should elicit every possibility, no matter how remote, before judging likelihood or feasibility. Only when all the possibilities are on the table should you then focus on judging them and selecting the hypotheses to be examined in greater detail in subsequent analysis.

When screening out the seemingly improbable hypotheses that you do not want to waste time on, it is necessary to distinguish hypotheses that appear to be *disproved* from those that are simply *unproven*. For an unproven hypothesis, there is no evidence that it is correct. For a disproved hypothesis, there is positive evidence that it is wrong. As discussed in Chapter 4, "Strategies for Analytical Judgment," and under Step 5 below, you should seek evidence that *disproves* hypotheses. Early rejection of unproven, but not disproved, hypotheses biases the subsequent analysis, because one does not then look for the evidence that might support them. Unproven hypotheses should be kept alive until they can be disproved.

One example of a hypothesis that often falls into this unproven but not disproved category is the hypothesis that an opponent is trying to deceive us. You may reject the possibility of denial and deception because you see no evidence of it, but rejection is not justified under these circumstances. If deception is planned well and properly implemented, one should not expect to find evidence of it readily at hand. The possibility should not be rejected until it is disproved, or, at least, until after a systematic search for evidence has been made and none has been found.

There is no "correct" number of hypotheses to be considered. The number depends upon the nature of the analytical problem and how advanced you are in the analysis of it. As a general rule, the greater your level of uncertainty, or the greater the policy impact of your conclusion, the more alternatives you may wish to consider. More than seven hypotheses may be unmanageable; if there are this many alternatives, it may be advisable to group several of them together for your initial cut at the analysis.

Step 2

Make a list of significant evidence and arguments for and against each hypothesis.

In assembling the list of relevant evidence and arguments, these terms should be interpreted very broadly. They refer to all the factors that have an impact on your judgments about the hypotheses. Do not limit yourself to concrete evidence in the current intelligence reporting. Also include your own assumptions or logical deductions about another person's or group's or country's intentions, goals, or standard procedures. These assumptions may generate strong preconceptions as to which hypothesis is most likely. Such assumptions often drive your final judgment, so it is important to include them in the list of "evidence."

First, list the general evidence that applies to all the hypotheses. Then consider each hypothesis individually, listing factors that tend to support or contradict each one. You will commonly find that each hypothesis leads you to ask different questions and, therefore, to seek out somewhat different evidence.

For each hypothesis, ask yourself this question: If this hypothesis is true, what should I expect to be seeing or not seeing? What are all the things that must have happened, or may still be happening, and that one should expect to see evidence of? If you are not seeing this evidence, why not? Is it because it has not happened, it is not normally observable, it is being concealed from you, or because you or the intelligence collectors have not looked for it?

Note the absence of evidence as well as its presence. For example, when weighing the possibility of military attack by an adversary, the steps the adversary has not taken to ready his forces for attack may be more significant than the observable steps that have been taken. This recalls the Sherlock Holmes story in which the vital clue was that the dog did *not* bark in the night. One's attention tends to focus on what is reported rather than what is not reported. It requires a conscious effort to think about what is missing but should be present if a given hypothesis were true.

Step 3

Prepare a matrix with hypotheses across the top and evidence down the side. Analyze the "diagnosticity" of the evidence and arguments- that is, identify which items are most helpful in judging the relative likelihood of alternative hypotheses.

Step 3 is perhaps the most important element of this analytical procedure. It is also the step that differs most from the natural, intuitive approach to analysis, and, therefore, the step you are most likely to overlook or misunderstand.

The procedure for Step 3 is to take the hypotheses from Step 1 and the evidence and arguments from Step 2 and put this information into a matrix format, with the hypotheses across the top and evidence and arguments down the side. This gives an overview of all the significant components of your analytical problem.

Then analyze how each piece of evidence relates to each hypothesis. This differs from the normal procedure, which is to look at one hypothesis at a time in order to consider how well the evidence supports that hypothesis. That will be done later, in Step 5. At this point, in Step 3, take one item of evidence at a time, then consider how consistent that evidence is with each of the hypotheses. Here is how to remember this distinction. In Step 3, you work *across* the rows of the matrix, examining one item of evidence at a time to see how consistent that item of evidence is with each of the hypotheses. In Step 5, you work *down* the columns of the matrix, examining one hypothesis at a time, to see how consistent that hypothesis is with all the evidence.

To fill in the matrix, take the first item of evidence and ask whether it is consistent with, inconsistent with, or irrelevant to each hypothesis. Then make a notation accordingly in the appropriate cell under each hypothesis in the matrix. The form of these notations in the matrix is a matter of personal preference. It may be pluses, minuses, and question marks. It may be C, I, and N/A standing for consistent, inconsistent, or not applicable. Or it may be some textual notation. In any event, it will be a simplification, a shorthand representation of the complex reasoning that went on as you thought about how the evidence relates to each hypothesis.

After doing this for the first item of evidence, then go on to the next item of evidence and repeat the process until all cells in the ma-

trix are filled. Figure 15 shows an example of how such a matrix might look. It uses as an example the intelligence question that arose after the US bombing of Iraqi intelligence headquarters in 1993: Will Iraq retaliate? The evidence in the matrix and how it is evaluated are hypothetical, fabricated for the purpose of providing a plausible example of the procedure. The matrix does not reflect actual evidence or judgments available at that time to the US Intelligence Community.

Figure 15

Question: Will Iraq Retaliate for US Bombing of Its Intelligence Headquarters?

Hypotheses:
H1 - Iraq will not retaliate.
H2 - It will sponsor some minor terrorist actions.
H3 - Iraq is planning a major terrorist attack, perhaps against one or more CIA installations.

	H1	H2	H3
E1. Saddam public statement of intent not to retaliate.	+	+	+
E2. Absence of terrorist offensive during the 1991 Gulf War.	+	+	−
E3. Assumption that Iraq would not want to provoke another US attack.	+	+	−
E4. Increase in frequency/length of monitored Iraqi agent radio broadcasts.	−	+	+
E5. Iraqi embassies instructed to take increased security precautions.	−	+	+
E6. Assumption that failure to retaliate would be unacceptable loss of face for Saddam.	−−	+	+

The matrix format helps you weigh the *diagnosticity* of each item of evidence, which is a key difference between analysis of competing hypotheses and traditional analysis. Diagnosticity of evidence is an important concept that is, unfortunately, unfamiliar to many analysts. It was introduced in Chapter 4, and that discussion is repeated here for your convenience.

Diagnosticity may be illustrated by a medical analogy. A high-temperature reading may have great value in telling a doctor that a patient is sick, but relatively little value in determining which illness a person is suffering from. Because a high temperature is consistent with so many possible hypotheses about a patient's illness, this evidence has limited diagnostic value in determining which illness (hypothesis) is the more likely one.

Evidence is diagnostic when it influences your judgment on the *relative* likelihood of the various hypotheses identified in Step 1. If an item of evidence seems consistent with all the hypotheses, it may have no diagnostic value. A common experience is to discover that most of the evidence supporting what you believe is the most likely hypothesis really is not very helpful, because that same evidence is also consistent with other hypotheses. When you do identify items that are highly diagnostic, these should drive your judgment. These are also the items for which you should re-check accuracy and consider alternative interpretations, as discussed in Step 6.

In the hypothetical matrix dealing with Iraqi intentions, note that evidence designated "E1" is assessed as consistent with all of the hypotheses. In other words, it has no diagnostic value. This is because we did not give any credence to Saddam's public statement on this question. He might say he will not retaliate but then do so, or state that he will retaliate and then not do it. On the other hand, E4 is diagnostic: increased frequency or length of Iraqi agent radio broadcasts is more likely to be observed if the Iraqis are planning retaliation than if they are not. The double minus for E6 indicates this is considered a very strong argument against H1. It is a linchpin assumption that drives the conclusion in favor of either H2 or H3. Several of the judgments reflected in this matrix will be questioned at a later stage in this analysis.

In some cases it may be useful to refine this procedure by using a numerical probability, rather than a general notation such as plus or minus, to describe how the evidence relates to each hypothesis. To do this, ask the following question for each cell in the matrix: If this hypothesis is true, what is the probability that I would be seeing this item of evidence? You may also make one or more additional notations in each cell of the matrix, such as:

- Adding a scale to show the intrinsic importance of each item of evidence.

- Adding a scale to show the ease with which items of evidence could be concealed, manipulated, or faked, or the extent to which one party might have an incentive to do so. This may be appropriate when the possibility of denial and deception is a serious issue.

Step 4

Refine the matrix. Reconsider the hypotheses and delete evidence and arguments that have no diagnostic value.

The exact wording of the hypotheses is obviously critical to the conclusions one can draw from the analysis. By this point, you will have seen how the evidence breaks out under each hypothesis, and it will often be appropriate to reconsider and reword the hypotheses. Are there hypotheses that need to be added, or finer distinctions that need to be made in order to consider all the significant alternatives? If there is little orno evidence that helps distinguish between two hypotheses, should they be combined into one?

Also reconsider the evidence. Is your thinking about which hypotheses are most likely and least likely influenced by factors that are not included in the listing of evidence? If so, put them in. Delete from the matrix items of evidence or assumptions that now seem unimportant or have no diagnostic value. Save these items in a separate list as a record of information that was considered.

Step 5

Draw tentative conclusions about the relative likelihood of each hypothesis. Proceed by trying to disprove hypotheses rather than prove them.

In Step 3, you worked across the matrix, focusing on a single item of evidence or argument and examining how it relates to each hypothesis. Now, work down the matrix, looking at each hypothesis as a whole. The matrix format gives an overview of all the evidence for and against all the hypotheses, so that you can examine all the hypotheses together and have them compete against each other for your favor.

In evaluating the relative likelihood of alternative hypotheses, start by looking for evidence or logical deductions that enable you to reject hypotheses, or at least to determine that they are unlikely. A fundamental precept of the scientific method is to proceed by rejecting or eliminating hypotheses, while tentatively accepting only those hypotheses that cannot be refuted. The scientific method obviously cannot be applied *in toto* to intuitive judgment, but the principle of seeking to disprove hypotheses, rather than confirm them, is useful.

No matter how much information is consistent with a given hypothesis, one cannot prove that hypothesis is true, because the same information may also be consistent with one or more other hypotheses. On the other hand, a single item of evidence that is inconsistent with a hypothesis may be sufficient grounds for rejecting that hypothesis. This was discussed in detail in Chapter 4, "Strategies for Analytical Judgment."

People have a natural tendency to concentrate on confirming hypotheses they already believe to be true, and they commonly give more weight to information that supports a hypothesis than to information that weakens it. This is wrong; we should do just the opposite. Step 5 again requires doing the *opposite* of what comes naturally.

In examining the matrix, look at the minuses, or whatever other notation you used to indicate evidence that may be inconsistent with a hypothesis. The hypotheses with the fewest minuses is probably the most likely one. The hypothesis with the most minuses is probably the least likely one. The fact that a hypothesis is inconsistent with the evidence is certainly a sound basis for rejecting it. The pluses, indicating evidence that is consistent with a hypothesis, are far less significant. It does not follow that the hypothesis with the most pluses is the most likely one, because a long list of evidence that is consistent with almost any reasonable hypothesis can be easily made. What is difficult to find, and is most significant when found, is hard evidence that is clearly inconsistent with a reasonable hypothesis.

This initial ranking by number of minuses is only a rough ranking, however, as some evidence obviously is more important than other evidence, and degrees of inconsistency cannot be captured by a single notation such as a plus or minus. By reconsidering the exact nature of the relationship between the evidence and the hypotheses, you will be able to judge how much weight to give it.

Analysts who follow this procedure often realize that their judgments are actually based on very few factors rather than on the large mass of information they thought was influencing their views. Chapter 5, "Do You Really Need More Information?," makes this same point based on experimental evidence.

The matrix should *not* dictate the conclusion to you. Rather, it should accurately reflect your judgment of what is important and how these important factors relate to the probability of each hypothesis. You, not the matrix, must make the decision. The matrix serves only as an aid to thinking and analysis, to ensure consideration of all the possible interrelationships between evidence and hypotheses and identification of those few items that really swing your judgment on the issue.

When the matrix shows that a given hypothesis is probable or unlikely, you may disagree. If so, it is because you omitted from the matrix one or more factors that have an important influence on your thinking. Go back and put them in, so that the analysis reflects your best judgment. If following this procedure has caused you to consider things you might otherwise have overlooked, or has caused you to revise your earlier estimate of the relative probabilities of the hypotheses, then the procedure has served a useful purpose. When you are done, the matrix serves as a shorthand record of your thinking and as an audit trail showing how you arrived at your conclusion.

This procedure forces you to spend more analytical time than you otherwise would on what you had thought were the less likely hypotheses. This is desirable. The seemingly less likely hypotheses usually involve plowing new ground and, therefore, require more work. What you started out thinking was the most likely hypothesis tends to be based on a continuation of your own past thinking. A principal advantage of the analysis of competing hypotheses is that it forces you to give a fairer shake to all the alternatives.

Step 6

Analyze how sensitive your conclusion is to a few critical items of evidence. Consider the consequences for your analysis if that evidence were wrong, misleading, or subject to a different interpretation.

In Step 3 you identified the evidence and arguments that were most diagnostic, and in Step 5 you used these findings to make tentative judgments about the hypotheses. Now, go back and question the few linchpin assumptions or items of evidence that really drive the outcome of your analysis in one direction or the other. Are there questionable assumptions that underlie your understanding and interpretation? Are there alternative explanations or interpretations? Could the evidence be incomplete and, therefore, misleading?

If there is any concern at all about denial and deception, this is an appropriate place to consider that possibility. Look at the sources of your key evidence. Are any of the sources known to the authorities in the foreign country? Could the information have been manipulated? Put yourself in the shoes of a foreign deception planner to evaluate motive, opportunity, means, costs, and benefits of deception as they might appear to the foreign country.

When analysis turns out to be wrong, it is often because of key assumptions that went unchallenged and proved invalid. It is a truism that analysts should identify and question assumptions, but this is much easier said than done. The problem is to determine which assumptions merit questioning. One advantage of the ACH procedure is that it tells you what needs to be rechecked.

In Step 6 you may decide that additional research is needed to check key judgments. For example, it may be appropriate to go back to check original source materials rather than relying on someone else's interpretation. In writing your report, it is desirable to identify critical assumptions that went into your interpretation and to note that your conclusion is dependent upon the validity of these assumptions.

Step 7

Report conclusions. Discuss the relative likelihood of all the hypotheses, not just the most likely one.

If your report is to be used as the basis for decisionmaking, it will be helpful for the decisionmaker to know the relative likelihood of all the alternative possibilities. Analytical judgments are never certain. There is always a good possibility of their being wrong. Decisionmakers need to make decisions on the basis of a full set of alternative possibilities, not

just the single most likely alternative. Contingency or fallback plans may be needed in case one of the less likely alternatives turns out to be true.

If you say that a certain hypothesis is probably true, that could mean anywhere from a 55-percent to an 85-percent chance that future events will prove it correct. That leaves anywhere from a 15-percent to 45 percent possibility that a decision based on your judgment will be based on faulty assumptions and will turn out wrong. Can you be more specific about how confident you are in your judgment? Chapter 12, "Biases in Estimating Probabilities," discusses the difference between such "subjective probability" judgments and statistical probabilities based on data on relative frequencies.

When one recognizes the importance of proceeding by eliminating rather than confirming hypotheses, it becomes apparent that any written argument for a certain judgment is incomplete unless it also discusses alternative judgments that were considered and why they were rejected. In the past, at least, this was seldom done.

The narrative essay, which is the dominant art form for the presentation of intelligence judgments, does not lend itself to comparative evaluation of competing hypotheses. Consideration of alternatives adds to the length of reports and is perceived by many analysts as detracting from the persuasiveness of argument for the judgment chosen. Analysts may fear that the reader could fasten on one of the rejected alternatives as a good idea. Discussion of alternative hypotheses is nonetheless an important part of any intelligence appraisal, and ways can and should be found to include it.

Step 8

Identify milestones for future observation that may indicate events are taking a different course than expected.

Analytical conclusions should always be regarded as tentative. The situation may change, or it may remain unchanged while you receive new information that alters your appraisal. It is always helpful to specify in advance things one should look for or be alert to that, if observed, would suggest a significant change in the probabilities. This is useful for

intelligence consumers who are following the situation on a continuing basis. Specifying in advance what would cause you to change your mind will also make it more difficult for you to rationalize such developments, if they occur, as not really requiring any modification of your judgment.

Summary and Conclusion

Three key elements distinguish analysis of competing hypotheses from conventional intuitive analysis.

- Analysis starts with a full set of alternative possibilities, rather than with a most likely alternative for which the analyst seeks confirmation. This ensures that alternative hypotheses receive equal treatment and a fair shake.

- Analysis identifies and emphasizes the few items of evidence or assumptions that have the greatest diagnostic value in judging the relative likelihood of the alternative hypotheses. In conventional intuitive analysis, the fact that key evidence may also be consistent with alternative hypotheses is rarely considered explicitly and often ignored.

- Analysis of competing hypotheses involves seeking evidence to refute hypotheses. The most probable hypothesis is usually the one with the least evidence against it, not the one with the most evidence for it. Conventional analysis generally entails looking for evidence to confirm a favored hypothesis.

The analytical effectiveness of this procedure becomes apparent when considering the Indian nuclear weapons testing in 1998. According to Admiral Jeremiah, the Intelligence Community had reported that " there was no indication the Indians would test in the near term."[87] Such a conclusion by the Community would fail to distinguish an unproven hypothesis from a disproved hypothesis. An absence of evidence does not necessarily disprove the hypothesis that India will indeed test nuclear weapons.

87. Transcript of Adm. Jeremiah's news conference, last sentence of third paragraph, 2 June 1998.

If the ACH procedure had been used, one of the hypotheses would certainly have been that India is planning to test in the near term but will conceal preparations for the testing to forestall international pressure to halt such preparations.

Careful consideration of this alternative hypothesis would have required evaluating India's motive, opportunity, and means for concealing its intention until it was too late for the US and others to intervene. It would also have required assessing the ability of US intelligence to see through Indian denial and deception if it were being employed. It is hard to imagine that this would not have elevated awareness of the possibility of successful Indian deception.

A principal lesson is this. Whenever an intelligence analyst is tempted to write the phrase "there is no evidence that . . . ," the analyst should ask this question: If this hypothesis is true, can I realistically expect to see evidence of it? In other words, if India were planning nuclear tests while deliberately concealing its intentions, could the analyst realistically expect to see evidence of test planning? The ACH procedure leads the analyst to identify and face these kinds of questions.

Once you have gained practice in applying analysis of competing hypotheses, it is quite possible to integrate the basic concepts of this procedure into your normal analytical thought process. In that case, the entire eight-step procedure may be unnecessary, except on highly controversial issues.

There is no guarantee that ACH or any other procedure will produce a correct answer. The result, after all, still depends on fallible intuitive judgment applied to incomplete and ambiguous information. **Analysis of competing hypotheses does, however, guarantee an appropriate *process of analysis. This procedure leads you through a rational, systematic process that avoids some common analytical pitfalls. It increases the odds of getting the right answer, and it leaves an audit trail showing the evidence used in your analysis and how this evidence was interpreted. If others disagree with your judgment, the matrix can be used to highlight the precise area of disagreement. Subsequent discussion can then focus productively on the ultimate source of the differences.***

A common experience is that analysis of competing hypotheses attributes greater likelihood to alternative hypotheses than would conventional analysis. One becomes less confident of what one thought one

knew. In focusing more attention on alternative explanations, the procedure brings out the full uncertainty inherent in any situation that is poor in data but rich in possibilities. Although such uncertainty is frustrating, it may be an accurate reflection of the true situation. As Voltaire said, "Doubt is not a pleasant state, but certainty is a ridiculous one."[88]

The ACH procedure has the offsetting advantage of focusing attention on the few items of critical evidence that cause the uncertainty or which, if they were available, would alleviate it. This can guide future collection, research, and analysis to resolve the uncertainty and produce a more accurate judgment.

88. M. Rogers, ed., *Contradictory Quotations* (England: Longman Group, Ltd., 1983).

PART III—COGNITIVE BIASES

Chapter 9

What Are Cognitive Biases?

This mini-chapter discusses the nature of cognitive biases in general. The four chapters that follow it describe specific cognitive biases in the evaluation of evidence, perception of cause and effect, estimation of probabilities, and evaluation of intelligence reporting.

* * * * * * * * * * * * * * * * * * * *

Fundamental limitations in human mental processes were identified in Chapters 2 and 3. A substantial body of research in cognitive psychology and decisionmaking is based on the premise that these cognitive limitations cause people to employ various simplifying strategies and rules of thumb to ease the burden of mentally processing information to make judgments and decisions.[89] These simple rules of thumb are often useful in helping us deal with complexity and ambiguity. Under many circumstances, however, they lead to predictably faulty judgments known as cognitive biases.

Cognitive biases are mental errors caused by our simplified information processing strategies. It is important to distinguish cognitive biases from other forms of bias, such as cultural bias, organizational bias, or bias that results from one's own self-interest. In other words, a cognitive bias does not result from any emotional or intellectual predisposition toward a certain judgment, but rather from subconscious mental procedures for processing information. A cognitive bias is a mental error that is consistent and predictable. For example:

89. Much of this research was stimulated by the seminal work of Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science*, 27 September 1974, Vol. 185, pp. 1124-1131. It has been summarized by Robin Hogarth, *Judgement and Choice* (New York: John Wiley & Sons, 1980), Richard Nisbett and Lee Ross, *Human Inference: Strategies and Shortcomings of Human Judgment* (Englewood Cliffs, NJ: Prentice-Hall, 1980), and Robyn Dawes, *Rational Choice in an Uncertain World* (New York: Harcourt Brace Jovanovich College Publishers, 1988). The Hogarth book contains an excellent bibliography of research in this field, organized by subject.

> The apparent distance of an object is determined in part by its clarity. The more sharply the object is seen, the closer it appears to be. This rule has some validity, because in any given scene the more distant objects are seen less sharply than nearer objects. However, the reliance on this rule leads to systematic errors in estimation of distance. Specifically, distances are often overestimated when visibility is poor because the contours of objects are blurred. On the other hand, distances are often underestimated when visibility is good because the objects are seen sharply. Thus the reliance on clarity as an indication of distance leads to common biases.[90]

This rule of thumb about judging distance is very useful. It usually works and helps us deal with the ambiguity and complexity of life around us. Under certain predictable circumstances, however, it will lead to biased judgment.

Cognitive biases are similar to optical illusions in that the error remains compelling even when one is fully aware of its nature. Awareness of the bias, by itself, does not produce a more accurate perception. Cognitive biases, therefore, are, exceedingly difficult to overcome.

Psychologists have conducted many experiments to identify the simplifying rules of thumb that people use to make judgments on incomplete or ambiguous information, and to show—at least in laboratory situations—how these rules of thumb prejudice judgments and decisions. The following four chapters discuss cognitive biases that are particularly pertinent to intelligence analysis because they affect the evaluation of evidence, perception of cause and effect, estimation of probabilities, and retrospective evaluation of intelligence reports.

Before discussing the specific biases, it is appropriate to consider the nature of such experimental evidence and the extent to which one can generalize from these experiments to conclude that the same biases are prevalent in the Intelligence Community.

When psychological experiments reveal the existence of a bias, this does not mean that every judgment by every individual person will be biased. It means that in any group of people, the bias will exist to a greater or lesser degree in most judgments made by most of the group. On the basis of this kind of experimental evidence, one can only generalize about

90. Tversky and Kahneman, ibid.

the tendencies of groups of people, not make statements about how any specific individual will think.

I believe that conclusions based on these laboratory experiments can be generalized to apply to intelligence analysts. In most, although not all cases, the test subjects were experts in their field. They were physicians, stock market analysts, horserace handicappers, chess masters, research directors, and professional psychologists, not undergraduate students as in so many psychological experiments. In most cases, the mental tasks performed in these experiments were realistic; that is, they were comparable to the judgments that specialists in these fields are normally required to make.

Some margin for error always exists when extrapolating from experimental laboratory to real-world experience, but classes of CIA analysts to whom these ideas were presented found them relevant and enlightening. I replicated a number of the simpler experiments with military officers in the National Security Affairs Department of the Naval Postgraduate School.

Chapter 10

Biases in Evaluation of Evidence

Evaluation of evidence is a crucial step in analysis, but what evidence people rely on and how they interpret it are influenced by a variety of extraneous factors. Information presented in vivid and concrete detail often has unwarranted impact, and people tend to disregard abstract or statistical information that may have greater evidential value. We seldom take the absence of evidence into account. The human mind is also oversensitive to the consistency of the evidence, and insufficiently sensitive to the reliability of the evidence. Finally, impressions often remain even after the evidence on which they are based has been totally discredited.[91]

* * * * * * * * * * * * * * * * * * * *

The intelligence analyst works in a somewhat unique informational environment. Evidence comes from an unusually diverse set of sources: newspapers and wire services, observations by American Embassy officers, reports from controlled agents and casual informants, information exchanges with foreign governments, photo reconnaissance, and communications intelligence. Each source has its own unique strengths, weaknesses, potential or actual biases, and vulnerability to manipulation and deception. The most salient characteristic of the information environment is its diversity—multiple sources, each with varying degrees of reliability, and each commonly reporting information which by itself is incomplete and sometimes inconsistent or even incompatible with reporting from other sources. Conflicting information of uncertain reliability is endemic to intelligence analysis, as is the need to make rapid judgments on current events even before all the evidence is in.

The analyst has only limited control over the stream of information. Tasking of sources to report on specific subjects is often a cumbersome and time-consuming process. Evidence on some important topics is sporadic or nonexistent. Most human-source information is second hand at best.

91. An earlier version of this chapter was published as an unclassified article in *Studies in Intelligence* in summer 1981, under the same title.

Recognizing and avoiding biases under such circumstances is particularly difficult. Most of the biases discussed in this chapter are unrelated to each other and are grouped together here only because they all concern some aspect of the evaluation of evidence.

The Vividness Criterion

The impact of information on the human mind is only imperfectly related to its true value as evidence.[92] Specifically, information that is vivid, concrete, and personal has a greater impact on our thinking than pallid, abstract information that may actually have substantially greater value as evidence. For example:

- Information that people perceive directly, that they hear with their own ears or see with their own eyes, is likely to have greater impact than information received secondhand that may have greater evidential value.

- Case histories and anecdotes will have greater impact than more informative but abstract aggregate or statistical data.

Events that people experience personally are more memorable than those they only read about. Concrete words are easier to remember than abstract words,[93] and words of all types are easier to recall than numbers. In short, information having the qualities cited in the preceding paragraph is more likely to attract and hold our attention. It is more likely to be stored and remembered than abstract reasoning or statistical summaries, and therefore can be expected to have a greater immediate effect as well as a continuing impact on our thinking in the future.

Intelligence analysts generally work with secondhand information. The information that analysts receive is mediated by the written words of others rather than perceived directly with their own eyes and ears. Partly because of limitations imposed by their open CIA employment, many intelligence analysts have spent less time in the country they are

92. Most of the ideas and examples in this section are from Richard Nisbett and Lee Ross, *Human Inference: Strategies and Shortcomings of Social Judgment* (Englewood Cliffs, NJ: Prentice-Hall, 1980), Chapter 3.
93. A. Paivio, *Imagery and Verbal Processes* (New York: Holt, Rinehart & Winston, 1971).

analyzing and had fewer contacts with nationals of that country than their academic and other government colleagues. Occasions when an analyst does visit the country whose affairs he or she is analyzing, or speaks directly with a national from that country, are memorable experiences. Such experiences are often a source of new insights, but they can also be deceptive.

That concrete, sensory data do and should enjoy a certain priority when weighing evidence is well established. When an abstract theory or secondhand report is contradicted by personal observation, the latter properly prevails under most circumstances. There are a number of popular adages that advise mistrust of secondhand data: "Don't believe everything you read," "You can prove anything with statistics," "Seeing is believing," "I'm from Missouri. . ."

It is curious that there are no comparable maxims to warn against being misled by our own observations. Seeing should not always be believing.

Personal observations by intelligence analysts and agents can be as deceptive as secondhand accounts. Most individuals visiting foreign countries become familiar with only a small sample of people representing a narrow segment of the total society. Incomplete and distorted perceptions are a common result.

A familiar form of this error is the single, vivid case that outweighs a much larger body of statistical evidence or conclusions reached by abstract reasoning. When a potential car buyer overhears a stranger complaining about how his Volvo turned out to be a lemon, this may have as much impact on the potential buyer's thinking as statistics in *Consumer Reports* on the average annual repair costs for foreign-made cars. If the personal testimony comes from the potential buyer's brother or close friend, it will probably be given even more weight. Yet the logical status of this new information is to increase by one the sample on which the *Consumer Reports* statistics were based; the personal experience of a single Volvo owner has little evidential value.

Nisbett and Ross label this the "man-who" syndrome and provide the following illustrations:[94]

- "But I know a *man who* smoked three packs of cigarettes a day and lived to be ninety-nine."

- "I've never been to Turkey but just last month I met a *man who* had, and he found it . . ."

Needless to say, a "man-who" example seldom merits the evidential weight intended by the person citing the example, or the weight often accorded to it by the recipient.

The most serious implication of vividness as a criterion that determines the impact of evidence is that certain kinds of very valuable evidence will have little influence simply because they are abstract. Statistical data, in particular, lack the rich and concrete detail to evoke vivid images, and they are often overlooked, ignored, or minimized.

For example, the Surgeon General's report linking cigarette smoking to cancer should have, logically, caused a decline in per-capita cigarette consumption. No such decline occurred for more than 20 years. The reaction of physicians was particularly informative. All doctors were aware of the statistical evidence and were more exposed than the general population to the health problems caused by smoking. How they reacted to this evidence depended upon their medical specialty. Twenty years after the Surgeon General's report, radiologists who examine lung x-rays every day had the lowest rate of smoking. Physicians who diagnosed and treated lung cancer victims were also quite unlikely to smoke. Many other types of physicians continued to smoke. The probability that a physician continued to smoke was directly related to the distance of the physician's specialty from the lungs. In other words, even physicians, who were well qualified to understand and appreciate the statistical data, were more influenced by their vivid personal experiences than by valid statistical data.[95]

Personal anecdotes, actual accounts of people's responsiveness or indifference to information sources, and controlled experiments can all be cited *ad infinitum* "to illustrate the proposition that data summaries, de-

94. Nisbett and Ross, p. 56.
95. Ibid.

spite their logically compelling implications, have less impact than does inferior but more vivid evidence."[96] It seems likely that intelligence analysts, too, assign insufficient weight to statistical information.

Analysts should give little weight to anecdotes and personal case histories unless they are known to be typical, and perhaps no weight at all if aggregate data based on a more valid sample can be obtained.

Absence of Evidence

A principal characteristic of intelligence analysis is that key information is often lacking. Analytical problems are selected on the basis of their importance and the perceived needs of the consumers, without much regard for availability of information. Analysts have to do the best they can with what they have, somehow taking into account the fact that much relevant information is known to be missing.

Ideally, intelligence analysts should be able to recognize what relevant evidence is lacking and factor this into their calculations. They should also be able to estimate the potential impact of the missing data and to adjust confidence in their judgment accordingly. Unfortunately, this ideal does not appear to be the norm. Experiments suggest that "out of sight, out of mind" is a better description of the impact of gaps in the evidence.

This problem has been demonstrated using fault trees, which are schematic drawings showing all the things that might go wrong with any endeavor. Fault trees are often used to study the fallibility of complex systems such as a nuclear reactor or space capsule.

A fault tree showing all the reasons why a car might not start was shown to several groups of experienced mechanics.[97] The tree had seven major branches—insufficient battery charge, defective starting system, defective ignition system, defective fuel system, other engine problems, mischievous acts or vandalism, and all other problems—and a number of subcategories under each branch. One group was shown the full tree and asked to imagine 100 cases in which a car won't start. Members of this group were then asked to estimate how many of the 100 cases were

96. Nisbett and Ross, p. 57.
97. Baruch Fischhoff, Paul Slovic, and Sarah Lichtenstein, *Fault Trees: Sensitivity of Estimated Failure Probabilities to Problem Representation*, Technical Report PTR- 1 042-77-8 (Eugene, OR: Decision Research, 1977).

attributable to each of the seven major branches of the tree. A second group of mechanics was shown only an incomplete version of the tree: three major branches were omitted in order to test how sensitive the test subjects were to what was left out.

If the mechanics' judgment had been fully sensitive to the missing information, then the number of cases of failure that would normally be attributed to the omitted branches should have been added to the "Other Problems" category. In practice, however, the "Other Problems" category was increased only half as much as it should have been. This indicated that the mechanics shown the incomplete tree were unable to fully recognize and incorporate into their judgments the fact that some of the causes for a car not starting were missing. When the same experiment was run with non-mechanics, the effect of the missing branches was much greater.

As compared with most questions of intelligence analysis, the "car won't start" experiment involved rather simple analytical judgments based on information that was presented in a well-organized manner. That the presentation of relevant variables in the abbreviated fault tree was incomplete could and should have been recognized by the experienced mechanics selected as test subjects. Intelligence analysts often have similar problems. Missing data is normal in intelligence problems, but it is probably more difficult to recognize that important information is absent and to incorporate this fact into judgments on intelligence questions than in the more concrete "car won't start" experiment.

As an antidote for this problem, analysts should identify explicitly those relevant variables on which information is lacking, consider alternative hypotheses concerning the status of these variables, and then modify their judgment and especially confidence in their judgment accordingly. They should also consider whether the absence of information is normal or is itself an indicator of unusual activity or inactivity.

Oversensitivity to Consistency

The internal consistency in a pattern of evidence helps determine our confidence in judgments based on that evidence.[98] In one sense, consistency is clearly an appropriate guideline for evaluating evidence.

98. Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science*, Vol. 185 (27 September 1974), 1126.

People formulate alternative explanations or estimates and select the one that encompasses the greatest amount of evidence within a logically consistent scenario. Under some circumstances, however, consistency can be deceptive. Information may be consistent only because it is highly correlated or redundant, in which case many related reports may be no more informative than a single report. Or it may be consistent only because information is drawn from a very small sample or a biased sample.

Such problems are most likely to arise in intelligence analysis when analysts have little information, say on political attitudes of Russian military officers or among certain African ethnic groups. If the available evidence is consistent, analysts will often overlook the fact that it represents a very small and hence unreliable sample taken from a large and heterogeneous group. This is not simply a matter of necessity—of having to work with the information on hand, however imperfect it may be. Rather, there is an illusion of validity caused by the consistency of the information.

The tendency to place too much reliance on small samples has been dubbed the "law of small numbers."[99] This is a parody on the law of large numbers, the basic statistical principle that says very large samples will be highly representative of the population from which they are drawn. This is the principle that underlies opinion polling, but most people are not good intuitive statisticians. People do not have much intuitive feel for how large a sample has to be before they can draw valid conclusions from it. The so-called law of small numbers means that, intuitively, we make the mistake of treating small samples as though they were large ones.

This has been shown to be true even for mathematical psychologists with extensive training in statistics. Psychologists designing experiments have seriously incorrect notions about the amount of error and unreliability inherent in small samples of data, unwarranted confidence in the early trends from the first few data points, and unreasonably high expectations of being able to repeat the same experiment and get the same results with a different set of test subjects.

Are intelligence analysts also overly confident of conclusions drawn from very little data—especially if the data seem to be consistent? When working with a small but consistent body of evidence, analysts need to consider how representative that evidence is of the total body of poten-

99. Tversky and Kahneman (1974), p. 1125-1126.

tially available information. If more reporting were available, how likely is it that this information, too, would be consistent with the already available evidence? If an analyst is stuck with only a small amount of evidence and cannot determine how representative this evidence is, confidence in judgments based on this evidence should be low regardless of the consistency of the information.

Coping with Evidence of Uncertain Accuracy

There are many reasons why information often is less than perfectly accurate: misunderstanding, misperception, or having only part of the story; bias on the part of the ultimate source; distortion in the reporting chain from subsource through source, case officer, reports officer, to analyst; or misunderstanding and misperception by the analyst. Further, much of the evidence analysts bring to bear in conducting analysis is retrieved from memory, but analysts often cannot remember even the source of information they have in memory let alone the degree of certainty they attributed to the accuracy of that information when it was first received.

The human mind has difficulty coping with complicated probabilistic relationships, so people tend to employ simple rules of thumb that reduce the burden of processing such information. In processing information of uncertain accuracy or reliability, analysts tend to make a simple yes or no decision. If they reject the evidence, they tend to reject it fully, so it plays no further role in their mental calculations. If they accept the evidence, they tend to accept it wholly, ignoring the probabilistic nature of the accuracy or reliability judgment. This is called a "best guess" strategy.[100] Such a strategy simplifies the integration of probabilistic information, but at the expense of ignoring some of the uncertainty. If analysts have information about which they are 70- or 80-percent certain but treat this information as though it were 100-percent certain, judgments based on that information will be overconfident.

A more sophisticated strategy is to make a judgment based on an assumption that the available evidence is perfectly accurate and reliable,

100. See Charles F. Gettys, Clinton W. Kelly III, and Cameron Peterson, "The Best Guess Hypothesis in Multistage Inference," *Organizational Behavior and Human Performance, 10*, 3 (1973), 365-373; and David A. Schum and Wesley M. DuCharme, "Comments on the Relationship Between the Impact and the Reliability of Evidence," *Organizational Behavior and Human Performance, 6* (1971), 111-131.

then reduce the confidence in this judgment by a factor determined by the assessed validity of the information. For example, available evidence may indicate that an event probably (75 percent) will occur, but the analyst cannot be certain that the evidence on which this judgment is based is wholly accurate or reliable. Therefore, the analyst reduces the assessed probability of the event (say, down to 60 percent) to take into account the uncertainty concerning the evidence. This is an improvement over the best-guess strategy but generally still results in judgments that are overconfident when compared with the mathematical formula for calculating probabilities.[101]

In mathematical terms, the joint probability of two events is equal to the product of their individual probabilities. Imagine a situation in which you receive a report on event X that is probably (75 percent) true. *If the report on event X is true,* you judge that event Y will probably (75 percent) happen. The actual probability of Y is only 56 percent, which is derived by multiplying 75 percent times 75 percent.

In practice, life is not nearly so simple. Analysts must consider many items of evidence with different degrees of accuracy and reliability that are related in complex ways with varying degrees of probability to several potential outcomes. Clearly, one cannot make neat mathematical calculations that take all of these probabilistic relationships into account. In making intuitive judgments, we unconsciously seek shortcuts for sorting through this maze, and these shortcuts involve some degree of ignoring the uncertainty inherent in less-than-perfectly-reliable information. There seems to be little an analyst can do about this, short of breaking the analytical problem down in a way that permits assigning probabilities to individual items of information, and then using a mathematical formula to integrate these separate probability judgments.

The same processes may also affect our reaction to information that is plausible but known from the beginning to be of questionable authenticity. Ostensibly private statements by foreign officials are often reported though intelligence channels. In many instances it is not clear whether such a private statement by a foreign ambassador, cabinet member, or other official is an actual statement of private views, an indiscretion, part of a deliberate attempt to deceive the US Government, or part of an ap-

101. Edgar M. Johnson, "The Effect of Data Source Reliability on Intuitive Inference," Technical Paper 251 (Arlington, VA: US Army Research Institute for the Behavioral and Social Sciences, 1974).

proved plan to convey a truthful message that the foreign government believes is best transmitted through informal channels.

The analyst who receives such a report often has little basis for judging the source's motivation, so the information must be judged on its own merits. In making such an assessment, the analyst is influenced by plausible causal linkages. If these are linkages of which the analyst was already aware, the report has little impact inasmuch as it simply supports existing views. If there are plausible new linkages, however, thinking is restructured to take these into account. It seems likely that the impact on the analyst's thinking is determined solely by the substance of the information, and that the caveat concerning the source does not attenuate the impact of the information at all. Knowing that the information comes from an uncontrolled source who may be trying to manipulate us does not necessarily reduce the impact of the information.

Persistence of Impressions Based on Discredited Evidence

Impressions tend to persist even after the evidence that created those impressions has been fully discredited. Psychologists have become interested in this phenomenon because many of their experiments require that the test subjects be deceived. For example, test subjects may be made to believe they were successful or unsuccessful in performing some task, or that they possess certain abilities or personality traits, when this is not in fact the case. Professional ethics require that test subjects be disabused of these false impressions at the end of the experiment, but this has proved surprisingly difficult to achieve.

Test subjects' erroneous impressions concerning their logical problem-solving abilities persevered even after they were informed that manipulation of good or poor teaching performance had virtually guaranteed their success or failure.[102] Similarly, test subjects asked to distinguish true from fictitious suicide notes were given feedback that had no relationship to actual performance. The test subjects had been randomly divided into two groups, with members of one group being given the impression of above-average success and the other of relative failure at this task. The subjects' erroneous impressions of the difficulty of the task

102. R. R. Lau, M. R. Lepper, and L. Ross, "Persistence of Inaccurate and Discredited Personal Impressions: A Field Demonstration of Attributional Perseverance," paper presented at 56th Annual Meeting of the Western Psychological Association (Los Angeles, April 1976).

and of their own performance persisted even after they were informed of the deception—that is, informed that their alleged performance had been preordained by their assignment to one or the other test group. Moreover, the same phenomenon was found among observers of the experiment as well as the immediate participants.[103]

There are several cognitive processes that might account for this phenomenon. The tendency to interpret new information in the context of pre-existing impressions is relevant but probably not sufficient to explain why the pre-existing impression cannot be eradicated even when new information authoritatively discredits the evidence on which it is based.

An interesting but speculative explanation is based on the strong tendency to seek causal explanations, as discussed in the next chapter. When evidence is first received, people postulate a set of causal connections that explains this evidence. In the experiment with suicide notes, for example, one test subject attributed her apparent success in distinguishing real from fictitious notes to her empathetic personality and the insights she gained from the writings of a novelist who committed suicide. Another ascribed her apparent failure to lack of familiarity with people who might contemplate suicide. The stronger the perceived causal linkage, the stronger the impression created by the evidence.

Even after learning that the feedback concerning their performance was invalid, these subjects retained this plausible basis for inferring that they were either well or poorly qualified for the task. The previously perceived causal explanation of their ability or lack of ability still came easily to mind, independently of the now-discredited evidence that first brought it to mind.[104] Colloquially, one might say that once information rings a bell, the bell cannot be unrung.

The ambiguity of most real-world situations contributes to the operation of this perseverance phenomenon. Rarely in the real world is evidence so thoroughly discredited as is possible in the experimental laboratory. Imagine, for example, that you are told that a clandestine source who has been providing information for some time is actually under hostile control. Imagine further that you have formed a number

103. Lee Ross, Mark R. Lepper, and Michael Hubbard, "Perseverance in Self-Perception and Social Perception: Biased Attributional Processes in the Debriefing Paradigm," *Journal of Personality and Social Psychology, 32*, 5, (1975), 880-892.
104. Lee Ross, Mark R. Lepper, Fritz Strack, and Julia Steinmetz, "Social Explanation and Social Expectation: Effects of Real and Hypothetical Explanations on Subjective Likelihood," *Journal of Personality and Social Psychology, 33*, 11 (1977), 818.

of impressions on the basis of reporting from this source. It is easy to rationalize maintaining these impressions by arguing that the information was true despite the source being under control, or by doubting the validity of the report claiming the source to be under control. In the latter case, the perseverance of the impression may itself affect evaluation of the evidence that supposedly discredits the impression.

Chapter 11

Biases in Perception of Cause and Effect

Judgments about cause and effect are necessary to explain the past, understand the present, and estimate the future. These judgments are often biased by factors over which people exercise little conscious control, and this can influence many types of judgments made by intelligence analysts. Because of a need to impose order on our environment, we seek and often believe we find causes for what are actually accidental or random phenomena. People overestimate the extent to which other countries are pursuing a coherent, coordinated, rational plan, and thus also overestimate their own ability to predict future events in those nations. People also tend to assume that causes are similar to their effects, in the sense that important or large effects must have large causes.

When inferring the causes of behavior, too much weight is accorded to personal qualities and dispositions of the actor and not enough to situational determinants of the actor's behavior. People also overestimate their own importance as both a cause and a target of the behavior of others. Finally, people often perceive relationships that do not in fact exist, because they do not have an intuitive understanding of the kinds and amount of information needed to prove a relationship.

* * * * * * * * * * * * * * * * * * * *

We cannot see cause and effect in the same sense that we see a desk or a tree. Even when we observe one billiard ball striking another and then watch the previously stationary ball begin to move, we are not perceiving cause and effect. The conclusion that one ball *caused* the other to move results only from a complex process of inference, not from direct sensory perception. That inference is based on the juxtaposition of events in time and space plus some theory or logical explanation as to why this happens.

There are several modes of analysis by which one might infer cause and effect. In more formal analysis, inferences are made through procedures that collectively comprise the scientific method. The scientist advances a hypothesis, then tests this hypothesis by the collection and statistical analysis of data on many instances of the phenomenon in question. Even then, causality cannot be proved beyond all possible doubt.

The scientist seeks to disprove a hypothesis, not to confirm it. A hypothesis is accepted only when it cannot be rejected.

Collection of data on many comparable cases to test hypotheses about cause and effect is not feasible for most questions of interest to the Intelligence Community, especially questions of broad political or strategic import relating to another country's intentions. To be sure, it is feasible more often than it is done, and increased use of scientific procedures in political, economic, and strategic research is much to be encouraged. But the fact remains that the dominant approach to intelligence analysis is necessarily quite different. It is the approach of the historian rather than the scientist, and this approach presents obstacles to accurate inferences about causality.

The procedures and criteria most historians use to attribute causality are less well defined than the scientist's.

> The historian's aim [is] to make a coherent whole out of the events he studies. His way of doing that, I suggest, is to look for certain dominant concepts or leading ideas by which to illuminate his facts, to trace the connections between those ideas themselves, and then to show how the detailed facts became intelligible in the light of them by constructing a "significant" narrative of the events of the period in question.[105]

The key ideas here are coherence and narrative. These are the principles that guide the organization of observations into meaningful structures and patterns. The historian commonly observes only a single case, not a pattern of covariation (when two things are related so that change in one is associated with change in the other) in many comparable cases. Moreover, the historian observes simultaneous changes in so many variables that the principle of covariation generally is not helpful in sorting out the complex relationships among them. The narrative story, on the other hand, offers a means of organizing the rich complexity of the historian's observations. The historian uses imagination to construct a coherent story out of fragments of data.

The intelligence analyst employing the historical mode of analysis is essentially a storyteller. He or she constructs a plot from the previous

105. W. H. Walsh, *Philosophy of History: An Introduction* (Revised Edition: New York: Harper and Row, 1967), p. 61.

events, and this plot then dictates the possible endings of the incomplete story. The plot is formed of the "dominant concepts or leading ideas" that the analyst uses to postulate patterns of relationships among the available data. The analyst is not, of course, preparing a work of fiction. There are constraints on the analyst's imagination, but imagination is nonetheless involved because there is an almost unlimited variety of ways in which the available data might be organized to tell a meaningful story. The constraints are the available evidence and the principle of coherence. The story must form a logical and coherent whole and be internally consistent as well as consistent with the available evidence.

Recognizing that the historical or narrative mode of analysis involves telling a coherent story helps explain the many disagreements among analysts, inasmuch as coherence is a subjective concept. It assumes some prior beliefs or mental model about what goes with what. More relevant to this discussion, the use of coherence rather than scientific observation as the criterion for judging truth leads to biases that presumably influence all analysts to some degree. Judgments of coherence may be influenced by many extraneous factors, and if analysts tend to favor certain types of explanations as more coherent than others, they will be biased in favor of those explanations.

Bias in Favor of Causal Explanations

One bias attributable to the search for coherence is a tendency to favor causal explanations. Coherence implies order, so people naturally arrange observations into regular patterns and relationships. If no pattern is apparent, our first thought is that we lack understanding, not that we are dealing with random phenomena that have no purpose or reason. As a last resort, many people attribute happenings that they cannot understand to God's will or to fate, which is somehow preordained; they resist the thought that outcomes may be determined by forces that interact in random, unpredictable ways. People generally do not accept the notion of chance or randomness. Even dice players behave as though they exert some control over the outcome of a throw of dice.[106] The prevalence of the word "because" in everyday language reflects the human tendency to seek to identify causes.

106. Ellen J. Langer, "The Psychology of Chance," *Journal for the Theory of Social Behavior,* 7 (1977), 185-208.

People expect patterned events to look patterned, and random events to look random, but this is not the case. Random events often look patterned. The random process of flipping a coin six times may result in six consecutive heads. Of the 32 possible sequences resulting from six coin flips, few actually look "random."[107] This is because randomness is a property of the process that generates the data that are produced. Randomness may in some cases be demonstrated by scientific (statistical) analysis. However, events will almost never be perceived intuitively as being random; one can find an apparent pattern in almost any set of data or create a coherent narrative from any set of events.

Because of a need to impose order on their environment, people seek and often believe they find causes for what are actually random phenomena. During World War II, Londoners advanced a variety of causal explanations for the pattern of German bombing. Such explanations frequently guided their decisions about where to live and when to take refuge in air raid shelters. Postwar examination, however, determined that the clustering of bomb hits was close to a random distribution.[108]

The Germans presumably intended a purposeful pattern, but purposes changed over time and they were not always achieved, so the net result was an almost random pattern of bomb hits. Londoners focused their attention on the few clusters of hits that supported their hypotheses concerning German intentions—not on the many cases that did not.

Some research in paleobiology seems to illustrate the same tendency. A group of paleobiologists has developed a computer program to simulate evolutionary changes in animal species over time. But the transitions from one time period to the next are not determined by natural selection or any other regular process: they are determined by computer-generated random numbers. The patterns produced by this program are similar to the patterns in nature that paleobiologists have been trying to understand. Hypothetical evolutionary events that seem, intuitively, to have a strong pattern were, in fact, generated by random processes.[109]

Yet another example of imposing causal explanations on random events is taken from a study dealing with the research practices of psy-

107. Daniel Kahneman and Amos Tversky, "Subjective Probability: A Judgment of Representativeness," *Cognitive Psychology*, 3 (1972), 430-54.
108. W. Feller, *An Introduction to Probability Theory and Its Applications* (3rd Edition; New York: Wiley, 1968), p. 160.
109. Gina Bari Kolata, "Paleobiology: Random Events over Geological Time," *Science*, 189 (1975), 625-626.

chologists. When experimental results deviated from expectations, these scientists rarely attributed the deviation to variance in the sample. They were always able to come up with a more persuasive causal explanation for the discrepancy.[110]

B. F. Skinner even noted a similar phenomenon in the course of experiments with the behavioral conditioning of pigeons. The normal pattern of these experiments was that the pigeons were given positive reinforcement, in the form of food, whenever they pecked on the proper lever at the proper time. To obtain the food regularly, they had to learn to peck in a certain sequence. Skinner demonstrated that the pigeons "learned" and followed a pattern (which Skinner termed a superstition) even when the food was actually dispensed randomly.[111]

These examples suggest that in military and foreign affairs, where the patterns are at best difficult to fathom, there may be many events for which there are no valid causal explanations. This certainly affects the predictability of events and suggests limitations on what might logically be expected of intelligence analysts.

Bias Favoring Perception of Centralized Direction

Very similar to the bias toward causal explanations is a tendency to see the actions of other governments (or groups of any type) as the intentional result of centralized direction and planning. ". . .most people are slow to perceive accidents, unintended consequences, coincidences, and small causes leading to large effects. Instead, coordinated actions, plans and conspiracies are seen."[112] Analysts overestimate the extent to which other countries are pursuing coherent, rational, goal-maximizing policies, because this makes for more coherent, logical, rational explanations. This bias also leads analysts and policymakers alike to overestimate the predictability of future events in other countries.

Analysts know that outcomes are often caused by accident, blunder, coincidence, the unintended consequence of well-intentioned policy, improperly executed orders, bargaining among semi-independent bu-

110. Amos Tversky and Daniel Kahneman, "Belief in the Law of Small Numbers," *Psychological Bulletin*, 72, 2 (1971), 105-110.
111. B. F. Skinner, "Superstition in the Pigeon," *Journal of Experimental Psychology*, 38 (1948), 168-172.
112. Robert Jervis, *Perception and Misperception in International Politics* (Princeton, NJ: Princeton University Press, 1976), p. 320.

reaucratic entities, or following standard operating procedures under inappropriate circumstances.[113] But a focus on such causes implies a disorderly world in which outcomes are determined more by chance than purpose. It is especially difficult to incorporate these random and usually unpredictable elements into a coherent narrative, because evidence is seldom available to document them on a timely basis. It is only in historical perspective, after memoirs are written and government documents released, that the full story becomes available.

This bias has important consequences. Assuming that a foreign government's actions result from a logical and centrally directed plan leads an analyst to:

- Have expectations regarding that governmentÍs actions that may not be fulfilled if the behavior is actually the product of shifting or inconsistent values, bureaucratic bargaining, or sheer confusion and blunder.

- Draw far-reaching but possibly unwarranted inferences from isolated statements or actions by government officials who may be acting on their own rather than on central direction.

- Overestimate the United States' ability to influence the other government's actions.

- Perceive inconsistent policies as the result of duplicity and Machiavellian maneuvers, rather than as the product of weak leadership, vacillation, or bargaining among diverse bureaucratic or political interests.

Similarity of Cause and Effect

When systematic analysis of covariation is not feasible and several alternative causal explanations seem possible, one rule of thumb people use to make judgments of cause and effect is to consider the similarity between attributes of the cause and attributes of the effect. Properties of the cause are ". . .inferred on the basis of being correspondent with or

113. For many historical examples, see Jervis, ibid., p. 321-23.

similar to properties of the effect."[114] Heavy things make heavy noises; dainty things move daintily; large animals leave large tracks. When dealing with physical properties, such inferences are generally correct.

People tend, however, to reason in the same way under circumstances when this inference is not valid. Thus, analysts tend to assume that economic events have primarily economic causes, that big events have important consequences, and that little events cannot affect the course of history. Such correspondence between cause and effect makes a more logical and persuasive—a more coherent—narrative, but there is little basis for expecting such inferences to correspond to historical fact.

Fischer labels the assumption that a cause must somehow resemble its effect the "fallacy of identity,"[115] and he cites as an example the historiography of the Spanish Armada. Over a period of several centuries, historians have written of the important consequences of the English defeat of the Spanish Armada in 1588. After refuting each of these arguments, Fischer notes:

> In short, it appears that the defeat of the Armada, mighty and melodramatic as it was, may have been remarkably barren of result. Its defeat may have caused very little, except the disruption of the Spanish strategy that sent it on its way. That judgment is sure to violate the patriotic instincts of every Englishman and the aesthetic sensibilities of us all. A big event *must* have big results, we think.[116]

The tendency to reason according to similarity of cause and effect is frequently found in conjunction with the previously noted bias toward inferring centralized direction. Together, they explain the persuasiveness of conspiracy theories. Such theories are invoked to explain large effects for which there do not otherwise appear to be correspondingly large causes. For example, it seems ". . .outrageous that a single, pathetic, weak figure like Lee Harvey Oswald should alter world history."[117] Because the purported motive for the assassination of John Kennedy is so dissimilar

114. Harold H. Kelley, "The Processes of Causal Attribution," *American Psychologist* (February 1973), p. 121.
115. David Hackett Fischer, *Historian's Fallacies* (New York: Harper Torchbooks, 1970), p. 177.
116. Ibid, p. 167.
117. Richard E. Nisbett and Timothy DeC. Wilson, "Telling More Than We Can Know: Verbal Reports on Mental Processes," *Psychological Review* (May 1977), p. 252.

from the effect it is alleged to explain, in the minds of many it fails to meet the criterion of a coherent narrative explanation. If such "little" causes as mistakes, accidents, or the aberrant behavior of a single individual have big effects, then the implication follows that major events happen for reasons that are senseless and random rather than by purposeful direction.

Intelligence analysts are more exposed than most people to hard evidence of real plots, coups, and conspiracies in the international arena. Despite this—or perhaps because of it—most intelligence analysts are not especially prone to what are generally regarded as conspiracy theories. Although analysts may not exhibit this bias in such extreme form, the bias presumably does influence analytical judgments in myriad little ways. In examining causal relationships, analysts generally construct causal explanations that are somehow commensurate with the magnitude of their effects and that attribute events to human purposes or predictable forces rather than to human weakness, confusion, or unintended consequences.

Internal vs. External Causes of Behavior

Much research into how people assess the causes of behavior employs a basic dichotomy between internal determinants and external determinants of human actions. Internal causes of behavior include a person's attitudes, beliefs, and personality. External causes include incentives and constraints, role requirements, social pressures, or other forces over which the individual has little control. The research examines the circumstances under which people attribute behavior either to stable dispositions of the actor or to characteristics of the situation to which the actor responds.

Differences in judgments about what causes another person's or government's behavior affect how people respond to that behavior. How people respond to friendly or unfriendly actions by others may be quite different if they attribute the behavior to the nature of the person or government than if they see the behavior as resulting from situational constraints over which the person or government has little control.

A fundamental error made in judging the causes of behavior is to overestimate the role of internal factors and underestimate the role of external factors. When observing another's behavior, people are too in-

clined to infer that the behavior was caused by broad personal qualities or dispositions of the other person and to expect that these same inherent qualities will determine the actor's behavior under other circumstances. Not enough weight is assigned to external circumstances that may have influenced the other person's choice of behavior. This pervasive tendency has been demonstrated in many experiments under quite diverse circumstances[118] and has often been observed in diplomatic and military interactions.[119]

Susceptibility to this biased attribution of causality depends upon whether people are examining their own behavior or observing that of others. It is the behavior of others that people tend to attribute to the nature of the actor, whereas they see their own behavior as conditioned almost entirely by the situation in which they find themselves. This difference is explained largely by differences in information available to actors and observers. People know a lot more about themselves.

The actor has a detailed awareness of the history of his or her own actions under similar circumstances. In assessing the causes of our own behavior, we are likely to consider our previous behavior and focus on how it has been influenced by different situations. Thus situational variables become the basis for explaining our own behavior. This contrasts with the observer, who typically lacks this detailed knowledge of the other person's past behavior. The observer is inclined to focus on how the other person's behavior compares with the behavior of others under similar circumstances.[120] This difference in the type and amount of information available to actors and observers applies to governments as well as people.

An actor's personal involvement with the actions being observed enhances the likelihood of bias. "Where the observer is also an actor, he is likely to exaggerate the uniqueness and emphasize the dispositional origins of the responses of others to his own actions."[121] This is because the observer assumes his or her own actions are unprovocative, clearly

118. Lee Ross, "The Intuitive Psychologist and his Shortcomings: Distortions in the Attribution Process," in Leonard Berkowitz, ed., *Advances in Experimental Social Psychology*, Volume 10 (New York: Academic Press, 1977), p. 184.
119. Jervis, ibid., Chapter 2.
120. Edward E. Jones, "How Do People Perceive the Causes of Behavior?" *American Scientist*, 64 (1976), p. 301.
121. Daniel Heradstveit, *The Arab-Israeli Conflict: Psychological Obstacles to Peace* (Oslo: Universitetsforlaget, 1979), p. 25.

understood by other actors, and well designed to elicit a desired response. Indeed, an observer interacting with another actor sees himself as determining the situation to which the other actor responds. When the actor does not respond as expected, the logical inference is that the response was caused by the nature of the actor rather than by the nature of the situation.

Intelligence analysts are familiar with the problem of weighing internal versus external causes of behavior in a number of contexts. When a new leader assumes control of a foreign government, analysts assess the likely impact of changed leadership on government policy. For example, will the former Defense Minister who becomes Prime Minister continue to push for increases in the defense budget? Analysts weigh the known predispositions of the new Prime Minister, based on performance in previous positions, against the requirements of the situation that constrain the available options. If relatively complete information is available on the situational constraints, analysts may make an accurate judgment on such questions. Lacking such information, they tend to err on the side of assuming that the individual's personal predispositions will prompt continuation of past behavior.

Consider the Soviet invasion of Afghanistan. The Soviets' perception of their own behavior was undoubtedly very different from the American perception. Causal attribution theory suggests that Soviet leaders would see the invasion as a reaction to the imperatives of the situation in South Asia at that time, such as the threat of Islamic nationalism spreading from Iran and Afghanistan into the Soviet Union. Further, they would perceive US failure to understand their "legitimate" national interests as caused by fundamental US hostility.[122]

122. See Richards J. Heuer, Jr., "Analyzing the Soviet Invasion of Afghanistan: Hypotheses from Causal Attribution Theory," *Studies in Comparative Communism*, Winter 1980. These comments concerning the Soviet invasion of Afghanistan are based solely on the results of psychological research, not on information concerning Soviet actions in Afghanistan or the US reaction thereto. The nature of generalizations concerning how people normally process information is that they apply "more or less" to many cases but may not offer a perfect fit to any single instance. There were obviously many other factors that influenced analysis of Soviet actions, including preconceptions concerning the driving forces behind Soviet policy. The intent is to illustrate the relevance of psychological research on the analytical process, not to debate the merits of alternative interpretations of Soviet policy. Thus I leave to the reader to judge how much his or her own interpretation of the Soviet invasion of Afghanistan may be influenced by these attributional tendencies.

Conversely, observers of the Soviet invasion would be inclined to attribute it to the aggressive and expansionist nature of the Soviet regime. Dislike of the Soviet Union and lack of information on the situational constraints as perceived by the Soviets themselves would be likely to exacerbate the attributional bias.[123] Further, to the extent that this bias stemmed from insufficient knowledge of situational pressures and constraints, one might expect policymakers who were not Soviet experts to have had a stronger bias than analysts specializing in the Soviet Union. With their greater base of information on the situational variables, the specialists may be better able to take these variables into account.

Specialists on occasion become so deeply immersed in the affairs of the country they are analyzing that they begin to assume the perspective—and the biases—of that country's leaders. During the Cold War, there was a persistent difference between CIA specialists in Soviet affairs and specialists in Chinese affairs when dealing with Sino-Soviet relations. During border clashes in 1969, for example, specialists on the USSR argued that the Chinese were being "provocative." These specialists tended to accept the Soviet regime's versions as to the history and alignment of the border. Specialists in Chinese affairs tended to take the opposite view—that is, that the arrogant Russians were behaving like Russians often do, while the Chinese were simply reacting to the Soviet high-handedness.[124] In other words, the analysts assumed the same biased perspective as the leaders of the country about which they were most knowledgeable. An objective account of causal relationships might have been somewhere between these two positions.

The Egypt-Israel peace negotiations in 1978–1979 offered another example of apparent bias in causal attribution. In the words of one observer at the time:

> Egyptians attribute their willingness to sign a treaty with Israel as due to their inherent disposition for peace; Israelis explain Egyptian willingness to make peace as resulting from a deteriorating economy and a growing awareness of Israel's military superiority. On the other hand, Israelis attribute their own orientation for accommodation as being due to their ever-present

123. Edward Jones and Richard Nisbett, "The Actor and the Observer: Divergent Perceptions of Their Behavior," in Edward Jones *et al., Attribution: Perceiving the Causes of Behavior* (New Jersey: General Learning Press, 1971), p. 93.
124. Based on personal discussion with CIA analysts.

> preference for peace. Egypt, however, explains Israel's compromises regarding, for example, Sinai, as resulting from external pressures such as positive inducements and threats of negative sanctions by the United States. In addition, some Egyptians attribute Israel's undesirable behavior, such as establishment of Jewish settlements on the West Bank of the Jordan River, as stemming from Zionist expansionism. If Israel should not place settlements in that territory, Egyptians might account for such desirable behavior as being due to external constraints, such as Western condemnation of settlements. Israelis, on the other hand explain undesirable behavior, such as Egypt's past tendency to issue threats to drive them into the sea, as resulting from Egypt's inherent opposition to a Jewish state in the Middle East. When Egyptians ceased to make such threats, Israelis attributed this desirable behavior as emanating from external circumstances, such as Israel's relative military superiority.[125]

The persistent tendency to attribute cause and effect in this manner is not simply the consequence of self-interest or propaganda by the opposing sides. Rather, it is the readily understandable and predictable result of how people normally attribute causality under many different circumstances.

As a general rule, biased attribution of causality helps sow the seeds of mistrust and misunderstanding between people and between governments. We tend to have quite different perceptions of the causes of each other's behavior.

Overestimating Our Own Importance

Individuals and governments tend to overestimate the extent to which they successfully influence the behavior of others.[126] This is an exception to the previously noted generalization that observers attribute the behavior of others to the nature of the actor. It occurs largely because a person is so familiar with his or her own efforts to influence another, but much less well informed about other factors that may have influenced the other's decision.

125. Raymond Tanter, "Bounded Rationality and Decision Aids," essay prepared for the Strategies of Conflict seminar, Mont Pelerin, Switzerland, 11-16 May 1980.
126. This section draws heavily upon Jervis, Chapter 9.

In estimating the influence of US policy on the actions of another government, analysts more often than not will be knowledgeable of US actions and what they are intended to achieve, but in many instances they will be less well informed concerning the internal processes, political pressures, policy conflicts, and other influences on the decision of the target government.

This bias may have played a role in the recent US failure to anticipate Indian nuclear weapons testing even though the new Indian Government was elected partly on promises it would add nuclear weapons to India's military arsenal. Most US intelligence analysts apparently discounted the promises as campaign rhetoric, believing that India would be dissuaded from joining the nuclear club by economic sanctions and diplomatic pressure. Analysts overestimated the ability of US policy to influence Indian decisions.

When another country's actions are consistent with US desires, the most obvious explanation, in the absence of strong evidence to the contrary, is that US policy effectively influenced the decision.[127] Conversely, when another country behaves in an undesired manner, this is normally attributed to factors beyond US control. People and governments seldom consider the possibility that their own actions have had unintended consequences. They assume that their intentions have been correctly perceived and that actions will have the desired effect unless frustrated by external causes.

Many surveys and laboratory experiments have shown that people generally perceive their own actions as the cause of their successes but not of their failures. When children or students or workers perform well, their parents, teachers, or supervisors take at least part of the credit; when they do poorly, their mentors seldom assume any blame. Successful candidates for Congress generally believe their own behavior contributed strongly to their victory, while unsuccessful candidates blame defeat on factors beyond their control.

Another example is the chest thumping that some Americans engaged in after the fall of the Soviet Union. According to some, the demise of the USSR was caused by strong US policies, such as increased defense expenditures and the Strategic Defense Initiative, which caused Soviet leaders to realize they could no longer compete with the United

127. It follows from the same reasoning that we may underestimate the consequences of our actions on nations that are not the *intended* target of our influence.

States. The US news media played this story for several weeks, interviewing many people—some experts, some not—on why the Soviet Union collapsed. Most serious students understood that there were many reasons for the Soviet collapse, the most important of which were internal problems caused by the nature of the Soviet system.

People and governments also tend to overestimate their own importance as the target of others' actions. They are sensitive to the impact that others' actions have on them, and they generally assume that people and governments intend to do what they do and intend it to have the effect that it has. They are much less aware of, and consequently tend to downgrade the importance of, other causes or results of the action.

In analyzing the reasons why others act the way they do, it is common to ask, "What goals are the person or government pursuing?" But goals are generally inferred from the effects of behavior, and the effects that are best known and often seem most important are the effects upon ourselves. Thus actions that hurt us are commonly interpreted as intentional expressions of hostility directed at ourselves. Of course, this will often be an accurate interpretation, but people sometimes fail to recognize that actions that seem directed at them are actually the unintended consequence of decisions made for other reasons.

Illusory Correlation

At the start of this chapter, covariation was cited as one basis for inferring causality. It was noted that covariation may either be observed intuitively or measured statistically. This section examines the extent to which the intuitive perception of covariation deviates from the statistical measurement of covariation.

Statistical measurement of covariation is known as correlation. Two events are correlated when the existence of one event implies the existence of the other. Variables are correlated when a change in one variable implies a similar degree of change in another. Correlation alone does not necessarily imply causation. For example, two events might co-occur because they have a common cause, rather than because one causes the other. But when two events or changes do co-occur, and the time sequence is such that one always follows the other, people often infer that the first caused the second. Thus, inaccurate perception of correlation leads to inaccurate perception of cause and effect.

Judgments about correlation are fundamental to all intelligence analysis. For example, assumptions that worsening economic conditions lead to increased political support for an opposition party, that domestic problems may lead to foreign adventurism, that military government leads to unraveling of democratic institutions, or that negotiations are more successful when conducted from a position of strength are all based on intuitive judgments of correlation between these variables. In many cases these assumptions are correct, but they are seldom tested by systematic observation and statistical analysis.

Much intelligence analysis is based on common-sense assumptions about how people and governments normally behave. The problem is that people possess a great facility for invoking contradictory "laws" of behavior to explain, predict, or justify different actions occurring under similar circumstances. "Haste makes waste" and "He who hesitates is lost" are examples of inconsistent explanations and admonitions. They make great sense when used alone and leave us looking foolish when presented together. "Appeasement invites aggression" and "agreement is based upon compromise" are similarly contradictory expressions.

When confronted with such apparent contradictions, the natural defense is that "it all depends on. . . ." Recognizing the need for such qualifying statements is one of the differences between subconscious information processing and systematic, self-conscious analysis. Knowledgeable analysis might be identified by the ability to fill in the qualification; careful analysis by the frequency with which one remembers to do so.[128]

Illusory correlation occurs when people perceive a relationship that does not in fact exist. In looking at a series of cases, it seems that people often focus on instances that support the existence of a relationship but ignore those cases that fail to support it. Several experiments have demonstrated that people do not have an intuitive understanding of what information is really needed to assess the relationship between two events or two variables. There appears to be nothing in people's intuitive understanding that corresponds with the statistical concept of correlation.

Nurses were tested on their ability to learn through experience to judge the relationship, or correlation, between a symptom and the di-

128. This paragraph draws heavily from the ideas and phraseology of Baruch Fischhoff, "For Those Condemned to Study the Past: Reflections on Historical Judgment," in R. A. Shweder and D. W. Fiske, eds., *New Directions for Methodology of Behavioral Science: Fallible Judgment in Behavioral Research* (San Francisco: Jossey-Bass, 1980).

agnosis of illness.[129] The nurses were each shown 100 cards; every card ostensibly represented one patient. The cards had a row of four letters at the top representing various symptoms and another row of four letters at the bottom representing diagnoses. The nurses were instructed to focus on just one letter (A) representing one symptom and one letter (F) representing one diagnosis, and then to judge whether the symptom A was related to the diagnosis F. In other words, on the basis of experience with these 100 "patients," does the presence of symptom A help to diagnose the presence of illness F? The experiment was run a number of times using different degrees of relationship between A and F.

Put yourself briefly in the position of a test subject. You have gone through the cards and noticed that on about 25 of them, or a quarter of the cases, the symptom and the disease, A and F, are both present. Would you say there is a relationship? Why? Is it appropriate to make a judgment solely on the basis of the frequency of cases which support the hypothesis of a relationship between A and F? What else do you need to know? Would it be helpful to have the number of cases in which the symptom (A) was present without the disease (F)? Let us say this was also true on 25 cards, so that out of the 100 cards, 50 had A and 25 of those cards with A also had F. In other words, the disease was present in half the cases in which the symptom was observed. Is this sufficient to establish a relationship, or is it also necessary to know the number of times the disease was present without the symptom?

Actually, to determine the existence of such a relationship, one needs information to fill all four cells of a 2 x 2 contingency table. Figure 16 shows such a table for one test run of this experiment. The table shows the number of cases of patients having each of four possible combinations of symptom and disease.

Eighteen of 19 test subjects given the 100 cards representing this particular combination of A and F thought there was at least a weak relationship, and several thought there was a strong relationship, when in fact, there is no correlation at all. More than half the test subjects based their judgment solely on the frequency of cases in which both A and F were present. This is the upper left cell of the table. These subjects were trying to determine if there was a relationship between A and F. When looking through the cards, 25 percent of the cases they looked at were

129. Jan Smedslund, "The Concept of Correlation in Adults," *Scandinavian Journal of Psychology*, Vol. 4 (1963), 165-73.

Figure 16

	A	Not A
F	25	25
Not F	25	25

consistent with the belief that symptom and diagnosis were perfectly correlated; this appears to be a lot of evidence to support the hypothesized relationship. Another smaller group of test subjects used somewhat more sophisticated reasoning. They looked at the total number of A cases and then asked in how many of these cases F was also present. This is the left side of the table in Figure 16. A third group resisted the basic concept of making a statistical generalization. When asked to describe their reasoning, they said that sometimes a relationship was present while in other cases it was not.

Of the 86 test subjects involved in several runnings of this experiment, not a single one showed any intuitive understanding of the concept of correlation. That is, no one understood that to make a proper judgment about the existence of a relationship, one must have information on all four cells of the table. Statistical correlation in its most elementary form is based on the ratio of the sums of the frequencies in the diagonal cells of a 2 x 2 table. In other words, a predominance of entries along either diagonal represents a strong statistical relationship between the two variables.

Let us now consider a similar question of correlation on a topic of interest to intelligence analysts. What are the characteristics of strategic deception and how can analysts detect it? In studying deception, one of the important questions is: what are the correlates of deception? Historically, when analysts study instances of deception, what else do they see that goes along with it, that is somehow related to deception, and that might be interpret as an indicator of deception? Are there certain practices relating to deception, or circumstances under which deception is most likely to occur, that permit one to say, that, because we have seen x or y or z, this most likely means a deception plan is under way? This would be comparable to a doctor observing certain symptoms and

concluding that a given disease may be present. This is essentially a problem of correlation. If one could identify several correlates of deception, this would significantly aid efforts to detect it.

The hypothesis has been advanced that deception is most likely when the stakes are exceptionally high.[130] If this hypothesis is correct, analysts should be especially alert for deception in such instances. One can cite prominent examples to support the hypothesis, such as Pearl Harbor, the Normandy landings, and the German invasion of the Soviet Union. It seems as though the hypothesis has considerable support, given that it is so easy to recall examples of high stakes situations in which deception was employed. But consider what it would take to prove, empirically, that such a relationship actually exists. Figure 17 sets up the problem as a 2 x 2 contingency table.

Figure 17

	High Stakes	Not High Stakes
Deception	68	?
No Deception	35	?

Barton Whaley researched 68 cases in which surprise or deception was present in strategic military operations between 1914 and 1968.[131] Let us assume that some form of deception, as well as surprise, was present in all 68 cases and put this number in the upper left cell of the table. How many cases are there with high stakes when deception was not used? That is a lot harder to think about and to find out about; researchers seldom devote much effort to documenting negative cases, when something did not occur. Fortunately, Whaley did make a rough estimate that both deception and surprise were absent in one-third to one-half of the cases of "grand strategy" during this period, which is the basis for putting the number 35 in the lower left cell of Figure 17.

130. Robert Axelrod, "The Rational Timing of Surprise," *World Politics*, XXXI (January 1979), pp. 228-246.
131. Barton Whaley, *Stratagem: Deception and Surprise in War*, (Cambridge, MA: Massachusetts Institute of Technology, unpublished manuscript, 1969), p. 247.

How common is deception when the stakes are not high? This is the upper right cell of Figure 17. Entries for this cell and the lower right cell are difficult to estimate; they require defining a universe of cases that includes low-stakes situations. What is a low-stakes situation in this context? High-stakes situations are definable, but there is an almost infinite number and variety of low-stakes situations. Because of this difficulty, it may not be feasible to use the full 2 x 2 table to analyze the relationship between deception and high stakes.

Perhaps it is necessary to be content with only the left side of the Figure 17 table. But then we cannot demonstrate empirically that one should be more alert to deception in high-stakes situations, because there is no basis for comparing high-stakes and low-stakes cases. If deception is even more common in tactical situations than it is in high stakes strategic situations, then analysts should not be more inclined to suspect deception when the stakes are high.

It is not really clear whether there is a relationship between deception and high-stakes situations, because there are not enough data. Intuitively, your gut feeling may tell you there is, and this feeling may well be correct. But you may have this feeling mainly because you are inclined to focus only on those cases in the upper left cell that do suggest such a relationship. People tend to overlook cases where the relationship does not exist, inasmuch as these are much less salient.

The lesson to be learned is not that analysts should do a statistical analysis of every relationship. They usually will not have the data, time, or interest for that. But analysts should have a general understanding of what it takes to know whether a relationship exists. This understanding is definitely not a part of people's intuitive knowledge. It does not come naturally. It has to be learned. When dealing with such issues, analysts have to force themselves to think about all four cells of the table and the data that would be required to fill each cell.

Even if analysts follow these admonitions, there are several factors that distort judgment when one does not follow rigorous scientific procedures in making and recording observations. These are factors that influence a person's ability to recall examples that fit into the four cells. For example, people remember occurrences more readily than non-occurrences. "History is, by and large, a record of what people did, not what they failed to do."[132]

132. E. H. Carr, *What is History?* (London: Macmillan, 1961), p. 126, cited by Fischhoff, *op. cit*.

Thus, instances in which deception occurred are easier to recall than instances in which it did not. Analysts remember occurrences that support the relationship they are examining better than those that do not. To the extent that perception is influenced by expectations, analysts may have missed or discounted the contrary instances. People also have a better memory for recent events, events in which they were personally involved, events that had important consequences, and so forth. These factors have a significant influence on perceptions of correlation when analysts make a gut judgment without consciously trying to think of all four cells of the table.

Many erroneous theories are perpetuated because they seem plausible and because people record their experience in a way that supports rather than refutes them. Ross describes this process as follows:

> . . .the intuitive observer selectively codes those data potentially relevant to the relationship between X and Y. Data points that fit his hypotheses and predictions are accepted as reliable, valid, representative, and free of error or "third-variable influences." Such data points are seen as reflective of the "real". . .relationship between X and Y. By contrast, data points that deviate markedly from the intuitive . . . expectations or theory are unlikely to be given great weight and tend to be dismissed as unreliable, erroneous, unrepresentative, or the product of contaminating third-variable influences. Thus the intuitive scientist who believes that fat men are jolly, or more specifically that fatness causes jolliness, will see particular fat and jolly men as strong evidence for this theory; he will not entertain the hypothesis that an individual's jollity is mere pretense or the product of a particularly happy home life rather than obesity. By contrast, fat and morose individuals will be examined very carefully before gaining admission to that scientist's store of relevant data. He might, for instance, seek to determine whether the individual's moroseness on the day in question is atypical, or the result of a nagging cold or a disappointing day, rather than the reflection of some stable attribute. It need hardly be emphasized that even a randomly generated [set of data] can yield a relatively high correlation if coded in the manner just outlined.[133]

133. Ross, *op. cit.*, pp. 208-209.

Chapter 12

Biases in Estimating Probabilities

In making rough probability judgments, people commonly depend upon one of several simplified rules of thumb that greatly ease the burden of decision. Using the "availability" rule, people judge the probability of an event by the ease with which they can imagine relevant instances of similar events or the number of such events that they can easily remember. With the "anchoring" strategy, people pick some natural starting point for a first approximation and then adjust this figure based on the results of additional information or analysis. Typically, they do not adjust the initial judgment enough.

Expressions of probability, such as possible and probable, are a common source of ambiguity that make it easier for a reader to interpret a report as consistent with the reader's own preconceptions. The probability of a scenario is often miscalculated. Data on "prior probabilities" are commonly ignored unless they illuminate causal relationships.

* * * * * * * * * * * * * * * * * * * *

Availability Rule

One simplified rule of thumb commonly used in making probability estimates is known as the availability rule. In this context, "availability" refers to imaginability or retrievability from memory. Psychologists have shown that two cues people use unconsciously in judging the probability of an event are the ease with which they can imagine relevant instances of the event and the number or frequency of such events that they can easily remember.[134] People are using the availability rule of thumb whenever they estimate frequency or probability on the basis of how easily they can recall or imagine instances of whatever it is they are trying to estimate.

134. Amos Tversky and Daniel Kahneman, "Availability: A Heuristic for Judging Frequency and Probability," *Cognitive Psychology*, 5 (1973), pp. 207-232.

Normally this works quite well. If one thing actually occurs more frequently than another and is therefore more probable, we probably can recall more instances of it. Events that are likely to occur usually are easier to imagine than unlikely events. People are constantly making inferences based on these assumptions. For example, we estimate our chances for promotion by recalling instances of promotion among our colleagues in similar positions and with similar experience. We estimate the probability that a politician will lose an election by imagining ways in which he may lose popular support.

Although this often works well, people are frequently led astray when the ease with which things come to mind is influenced by factors unrelated to their probability. The ability to recall instances of an event is influenced by how recently the event occurred, whether we were personally involved, whether there were vivid and memorable details associated with the event, and how important it seemed at the time. These and other factors that influence judgment are unrelated to the true probability of an event.

Consider two people who are smokers. One had a father who died of lung cancer, whereas the other does not know anyone who ever had lung cancer. The one whose father died of lung cancer will normally perceive a greater probability of adverse health consequences associated with smoking, even though one more case of lung cancer is statistically insignificant when weighing such risk. How about two CIA officers, one of whom knew Aldrich Ames and the other who did not personally know anyone who had ever turned out to be a traitor? Which one is likely to perceive the greatest risk of insider betrayal?

It was difficult to imagine the breakup of the Soviet Union because such an event was so foreign to our experience of the previous 50 years. How difficult is it now to imagine a return to a Communist regime in Russia? Not so difficult, in part because we still have vivid memories of the old Soviet Union. But is that a sound basis for estimating the likelihood of its happening? When analysts make quick, gut judgments without really analyzing the situation, they are likely to be influenced by the availability bias. The more a prospective scenario accords with one's experience, the easier it is to imagine and the more likely it seems.

Intelligence analysts may be less influenced than others by the availability bias. Analysts are evaluating all available information, not making quick and easy inferences. On the other hand, policymakers and journal-

ists who lack the time or access to evidence to go into details must necessarily take shortcuts. The obvious shortcut is to use the availability rule of thumb for making inferences about probability.

Many events of concern to intelligence analysts

> . . .are perceived as so unique that past history does not seem relevant to the evaluation of their likelihood. In thinking of such events we often construct scenarios, i.e., stories that lead from the present situation to the target event. The plausibility of the scenarios that come to mind, or the difficulty of producing them, serve as clues to the likelihood of the event. If no reasonable scenario comes to mind, the event is deemed impossible or highly unlikely. If several scenarios come easily to mind, or if one scenario is particularly compelling, the event in question appears probable.[135]

US policymakers in the early years of our involvement in Vietnam had to imagine scenarios for what might happen if they did or did not commit US troops to the defense of South Vietnam. In judging the probability of alternative outcomes, our senior leaders were strongly influenced by the ready availability of two seemingly comparable scenarios—the failure of appeasement prior to World War II and the successful intervention in Korea.

Many extraneous factors influence the imaginability of scenarios for future events, just as they influence the retrievability of events from memory. Curiously, one of these is the act of analysis itself. The act of constructing a detailed scenario for a possible future event makes that event more readily imaginable and, therefore, increases its perceived probability. This is the experience of CIA analysts who have used various tradecraft tools that require, or are especially suited to, the analysis of unlikely but nonetheless possible and important hypotheses. (Such techniques were discussed in Chapter 6, "Keeping an Open Mind" and Chapter 8, "Analysis of Competing Hypotheses.") The analysis usually results in the "unlikely" scenario being taken a little more seriously. This phenomenon has also been demonstrated in psychological experiments.[136]

135. Ibid., p. 229.
136. John S. Carroll, "The Effect of Imagining an Event on Expectations for the Event: An Interpretation in Terms of the Availability Heuristic", *Journal of Experimental Social Psychology*, 14 (1978), pp. 88-96.

In sum, the availability rule of thumb is often used to make judgments about likelihood or frequency. People would be hard put to do otherwise, inasmuch as it is such a timesaver in the many instances when more detailed analysis is not warranted or not feasible. Intelligence analysts, however, need to be aware when they are taking shortcuts. They must know the strengths and weaknesses of these procedures, and be able to identify when they are most likely to be led astray. For intelligence analysts, recognition that they are employing the availability rule should raise a caution flag. Serious analysis of probability requires identification and assessment of the strength and interaction of the many variables that will determine the outcome of a situation.

Anchoring

Another strategy people seem to use intuitively and unconsciously to simplify the task of making judgments is called anchoring. Some natural starting point, perhaps from a previous analysis of the same subject or from some partial calculation, is used as a first approximation to the desired judgment. This starting point is then adjusted, based on the results of additional information or analysis. Typically, however, the starting point serves as an anchor or drag that reduces the amount of adjustment, so the final estimate remains closer to the starting point than it ought to be.

Anchoring can be demonstrated very simply in a classroom exercise by asking a group of students to estimate one or more known quantities, such as the percentage of member countries in the United Nations that are located in Africa. Give half the students a low-percentage number and half a high-percentage number. Ask them to start with this number as an estimated answer, then, as they think about the problem, to adjust this number until they get as close as possible to what they believe is the correct answer. When this was done in one experiment that used this question, those starting with an anchor of 10 percent produced adjusted estimates that averaged 25 percent. Those who started with an anchor of 65 percent produced adjusted estimates that averaged 45 percent.[137]

Because of insufficient adjustment, those who started out with an estimate that was too high ended with significantly higher estimates than

137. Amos Tversky and Daniel Kahneman, "Judgment under Uncertainty: Heuristics and Biases," *Science*, Vol. 185, Sept. 27, 1974, pp. 1124-1131.

those who began with an estimate that was too low. Even the totally arbitrary starting points acted as anchors, causing drag or inertia that inhibited fulladjustment of estimates.

Whenever analysts move into a new analytical area and take over responsibility for updating a series of judgments or estimates made by their predecessors, the previous judgments may have such an anchoring effect. Even when analysts make their own initial judgment, and then attempt to revise this judgment on the basis of new information or further analysis, there is much evidence to suggest that they usually do not change the judgment enough.

Anchoring provides a partial explanation of experiments showing that analysts tend to be overly sure of themselves in setting confidence ranges. A military analyst who estimates future missile or tank production is often unable to give a specific figure as a point estimate. The analyst may, therefore, set a range from high to low, and estimate that there is, say, a 75-percent chance that the actual production figure will fall within this range. If a number of such estimates are made that reflect an appropriate degree of confidence, the true figure should fall within the estimated range 75 percent of the time and outside this range 25 percent of the time. In experimental situations, however, most participants are overconfident. The true figure falls outside the estimated range a much larger percentage of the time.[138]

If the estimated range is based on relatively hard information concerning the upper and lower limits, the estimate is likely to be accurate. If, however, the range is determined by starting with a single best estimate that is simply adjusted up and down to arrive at estimated maximum and minimum values, then anchoring comes into play, and the adjustment is likely to be insufficient.

Reasons for the anchoring phenomenon are not well understood. The initial estimate serves as a hook on which people hang their first impressions or the results of earlier calculations. In recalculating, they take this as a starting point rather than starting over from scratch, but why this should limit the range of subsequent reasoning is not clear.

138. Experiments using a 98-percent confidence range found that the true value fell outside the estimated range 40 to 50 percent of the time. Amos Tversky and Daniel Kahneman, "Anchoring and Calibration in the Assessment of Uncertain Quantities," (Oregon Research Institute Research Bulletin, 1972, Nov. 12, No. 5), and M. Alpert and H. Raiffa, "A Progress Report on The Training of Probability Assessors," Unpublished manuscript, Harvard University, 1968.

There is some evidence that awareness of the anchoring problem is not an adequate antidote.[139] This is a common finding in experiments dealing with cognitive biases. The biases persist even after test subjects are informed of them and instructed to try to avoid them or compensate for them.

One technique for avoiding the anchoring bias, to weigh anchor so to speak, may be to ignore one's own or others' earlier judgments and rethink a problem from scratch. In other words, consciously avoid any prior judgment as a starting point. There is no experimental evidence to show that this is possible or that it will work, but it seems worth trying. Alternatively, it is sometimes possible to avoid human error by employing formal statistical procedures. Bayesian statistical analysis, for example, can be used to revise prior judgments on the basis of new information in a way that avoids anchoring bias.[140]

Expression of Uncertainty

Probabilities may be expressed in two ways. Statistical probabilities are based on empirical evidence concerning relative frequencies. Most intelligence judgments deal with one-of-a-kind situations for which it is impossible to assign a statistical probability. Another approach commonly used in intelligence analysis is to make a "subjective probability" or "personal probability" judgment. Such a judgment is an expression of the analyst's personal belief that a certain explanation or estimate is correct. It is comparable to a judgment that a horse has a three-to-one chance of winning a race.

Verbal expressions of uncertainty—such as "possible," "probable," "unlikely," "may," and "could"—are a form of subjective probability judgment, but they have long been recognized as sources of ambiguity and misunderstanding. To say that something could happen or is possible

139. Alpert and Raiffa, ibid.

140. Nicholas Schweitzer, "Bayesian Analysis: Estimating the Probability of Middle East Conflict," in Richards J. Heuer, Jr., ed., *Quantitative Approaches to Political Intelligence: The CIA Experience* (Boulder, CO: Westview Press, 1979). Jack Zlotnick, "Bayes' Theorem for Intelligence Analysis," *Studies in Intelligence*, Vol. 16, No. 2 (Spring 1972). Charles E. Fisk, "The Sino-Soviet Border Dispute: A Comparison of the Conventional and Bayesian Methods for Intelligence Warning", *Studies in Intelligence*, vol. 16, no. 2 (Spring 1972), originally classified Secret, now declassified. Both the Zlotnick and Fisk articles were republished in H. Bradford Westerfield, *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992*, (New Haven: Yale University Press, 1995).

may refer to anything from a 1-percent to a 99-percent probability. To express themselves clearly, analysts must learn to routinely communicate uncertainty using the language of numerical probability or odds ratios.

As explained in Chapter 2 on "Perception," people tend to see what they expect to see, and new information is typically assimilated to existing beliefs. This is especially true when dealing with verbal expressions of uncertainty. By themselves, these expressions have no clear meaning. They are empty shells. The reader or listener fills them with meaning through the context in which they are used and what is already in the reader's or listener's mind about that context.

When intelligence conclusions are couched in ambiguous terms, a reader's interpretation of the conclusions will be biased in favor of consistency with what the reader already believes. This may be one reason why many intelligence consumers say they do not learn much from intelligence reports.[141]

It is easy to demonstrate this phenomenon in training courses for analysts. Give students a short intelligence report, have them underline all expressions of uncertainty, then have them express their understanding of the report by writing above each expression of uncertainty the numerical probability they believe was intended by the writer of the report. This is an excellent learning experience, as the differences among students in how they understand the report are typically so great as to be quite memorable.

In one experiment, an intelligence analyst was asked to substitute numerical probability estimates for the verbal qualifiers in one of his own earlier articles. The first statement was: "The cease-fire is holding but could be broken within a week." The analyst said he meant there was about a 30-percent chance the cease-fire would be broken within a week. Another analyst who had helped this analyst prepare the article said she thought there was about an 80-percent chance that the cease-fire would be broken. Yet, when working together on the report, both analysts had believed they were in agreement about what could happen.[142] Obviously, the analysts had not even communicated effectively with each other, let alone with the readers of their report.

141. For another interpretation of this phenomenon, see Chapter 13, "Hindsight Biases in Evaluation of Intelligence Reporting."
142. Scott Barclay et al, *Handbook for Decision Analysis*. (McLean, VA: Decisions and Designs, Inc. 1977), p. 66.

Sherman Kent, the first director of CIA's Office of National Estimates, was one of the first to recognize problems of communication caused by imprecise statements of uncertainty. Unfortunately, several decades after Kent was first jolted by how policymakers interpreted the term "serious possibility" in a national estimate, this miscommunication between analysts and policymakers, and between analysts, is still a common occurrence.[143]

I personally recall an ongoing debate with a colleague over the bona fides of a very important source. I argued he was probably bona fide. My colleague contended that the source was probably under hostile control. After several months of periodic disagreement, I finally asked my colleague to put a number on it. He said there was at least a 51-percent chance of the source being under hostile control. I said there was at least a 51-percent chance of his being bona fide. Obviously, we agreed that there was a great deal of uncertainty. That stopped our disagreement. The problem was not a major difference of opinion, but the ambiguity of the term probable.

The table in Figure 18 shows the results of an experiment with 23 NATO military officers accustomed to reading intelligence reports. They were given a number of sentences such as: "It is highly unlikely that. . . ." All the sentences were the same except that the verbal expressions of probability changed. The officers were asked what percentage probability they would attribute to each statement if they read it in an intelligence report. Each dot in the table represents one officer's probability assignment.[144] While there was broad consensus about the meaning of "better than even," there was a wide disparity in interpretation of other probability expressions. The shaded areas in the table show the ranges proposed by Kent.[145]

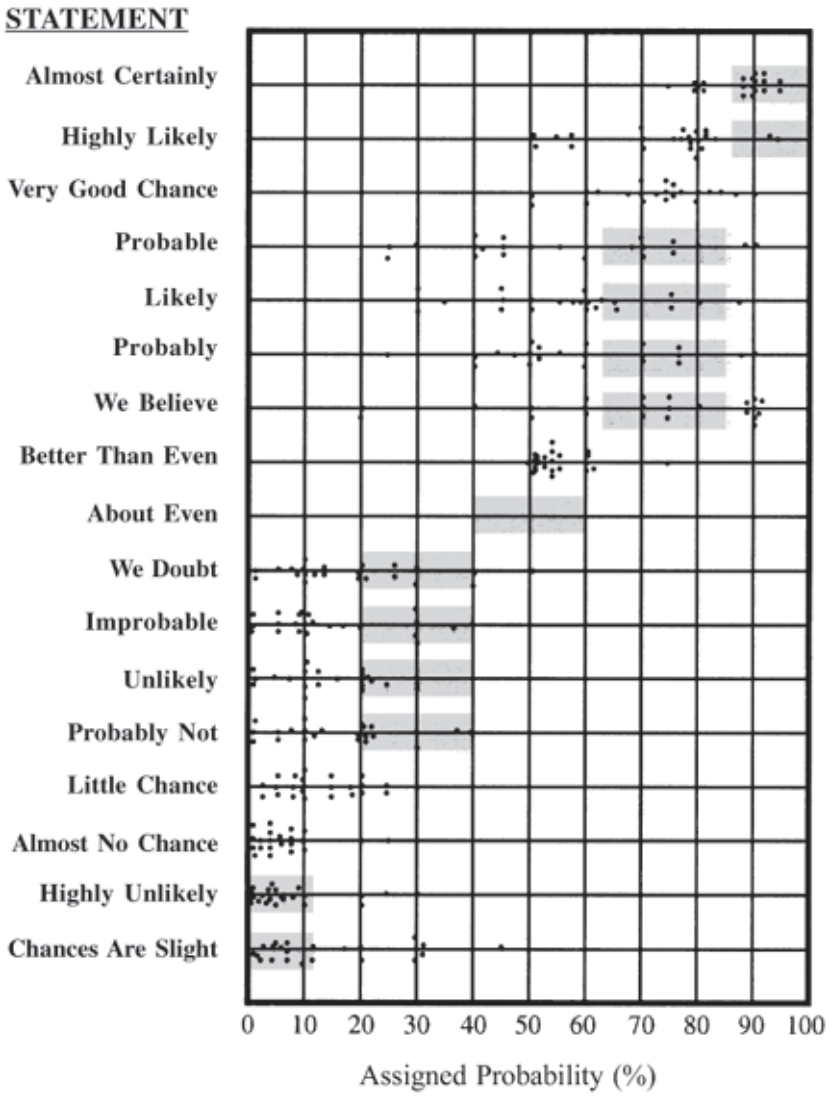
The main point is that an intelligence report may have no impact on the reader if it is couched in such ambiguous language that the reader can easily interpret it as consistent with his or her own preconceptions. This

143. Sherman Kent, "Words of Estimated Probability," in Donald P. Steury, ed., *Sherman Kent and the Board of National Estimates: Collected Essays* (CIA, Center for the Study of Intelligence, 1994).

144. Scott Barclay et al, p. 76-68.

145. Probability ranges attributed to Kent in this table are slightly different from those in Sherman Kent, "Words of Estimated Probability," in Donald P. Steury, ed., *Sherman Kent and the Board of National Estimates: Collected Essays* (CIA, Center for the Study of Intelligence, 1994).

Figure 18: Measuring Perceptions of Uncertainty



ambiguity can be especially troubling when dealing with low-probability, high-impact dangers against which policymakers may wish to make contingency plans.

Consider, for example, a report that there is little chance of a terrorist attack against the American Embassy in Cairo at this time. If the Ambassador's preconception is that there is no more than a one-in-a-hundred chance, he may elect to not do very much. If the Ambassador's preconception is that there may be as much as a one-in-four chance of an attack, he may decide to do quite a bit. The term "little chance" is consistent with either of those interpretations, and there is no way to know what the report writer meant.

Another potential ambiguity is the phrase "at this time." Shortening the time frame for prediction lowers the probability, but may not decrease the need for preventive measures or contingency planning. An event for which the timing is unpredictable may "at this time" have only a 5-percent probability of occurring during the coming month, but a 60-percent probability if the time frame is extended to one year (5 percent per month for 12 months).

How can analysts express uncertainty without being unclear about how certain they are? Putting a numerical qualifier in parentheses after the phrase expressing degree of uncertainty is an appropriate means of avoiding misinterpretation. This may be an odds ratio (less than a one-in-four chance) or a percentage range (5 to 20 percent) or (less than 20 percent). Odds ratios are often preferable, as most people have a better intuitive understanding of odds than of percentages.

Assessing Probability of a Scenario

Intelligence analysts sometimes present judgments in the form of a scenario—a series of events leading to an anticipated outcome. There is evidence that judgments concerning the probability of a scenario are influenced by amount and nature of detail in the scenario in a way that is unrelated to actual likelihood of the scenario.

A scenario consists of several events linked together in a narrative description. To calculate mathematically the probability of a scenario, the proper procedure is to multiply the probabilities of each individual event. Thus, for a scenario with three events, each of which will probably (70 percent certainty) occur, the probability of the scenario is .70 x .70

x .70 or slightly over 34 percent. Adding a fourth probable (70 percent) event to the scenario would reduce its probability to 24 percent.

Most people do not have a good intuitive grasp of probabilistic reasoning. One approach to simplifying such problems is to assume (or think as though) one or more probable events have already occurred. This eliminates some of the uncertainty from the judgment. Another way to simplify the problem is to base judgment on a rough average of the probabilities of each event. In the above example, the averaging procedure gives an estimated probability of 70 percent for the entire scenario. Thus, the scenario appears far more likely than is in fact the case.

When the averaging strategy is employed, highly probable events in the scenario tend to offset less probable events. This violates the principle that a chain cannot be stronger than its weakest link. Mathematically, the least probable event in a scenario sets the upper limit on the probability of the scenario as a whole. If the averaging strategy is employed, additional details may be added to the scenario that are so plausible they increase the perceived probability of the scenario, while, mathematically, additional events must necessarily reduce its probability.[146]

Base-Rate Fallacy

In assessing a situation, an analyst sometimes has two kinds of evidence available—specific evidence about the individual case at hand, and numerical data that summarize information about many similar cases. This type of numerical information is called a base rate or prior probability. The base-rate fallacy is that the numerical data are commonly ignored unless they illuminate a causal relationship. This is illustrated by the following experiment.[147]

During the Vietnam War, a fighter plane made a non-fatal strafing attack on a US aerial reconnaissance mission at twilight. Both Cambodian and Vietnamese jets operate in the area. You know the following facts:

(a) Specific case information: The US pilot identified the fighter as Cambodian. The pilot's aircraft recognition capabilities were tested under appropriate visibility and flight conditions. When presented

146. Paul Slovic, Baruch Fischhoff, and Sarah Lichtenstein, "Cognitive Processes and Societal Risk Taking," in J. S. Carroll and J.W. Payne, eds., *Cognition and Social Behavior* (Potomac, MD: Lawrence Erlbaum Associates, 1976), pp. 177-78.

147. This is a modified version, developed by Frank J. Stech, of the blue and green taxicab question used by Kahneman and Tversky, "On Prediction and Judgment," Oregon Research Institute Research Bulletin, 12, 14, 1972.

with a sample of fighters (half with Vietnamese markings and half with Cambodian) the pilot made correct identifications 80 percent of the time and erred 20 percent of the time.

(b) Base rate data: 85 percent of the jet fighters in that area are Vietnamese; 15 percent are Cambodian.

Question: What is the probability that the fighter was Cambodian rather than Vietnamese?

A common procedure in answering this question is to reason as follows: We know the pilot identified the aircraft as Cambodian. We also know the pilot's identifications are correct 80 percent of the time; therefore, there is an 80 percent probability the fighter was Cambodian. This reasoning appears plausible but is incorrect. It ignores the base rate—that 85 percent of the fighters in that area are Vietnamese. The base rate, or prior probability, is what you can say about any hostile fighter in that area before you learn anything about the specific sighting.

It is actually more likely that the plane was Vietnamese than Cambodian despite the pilot's "probably correct" identification. Readers who are unfamiliar with probabilistic reasoning and do not grasp this point should imagine 100 cases in which the pilot has a similar encounter. Based on paragraph (a), we know that 80 percent or 68 of the 85 Vietnamese aircraft will be correctly identified as Vietnamese, while 20 percent or 17 will be incorrectly identified as Cambodian. Based on paragraph (b), we know that 85 of these encounters will be with Vietnamese aircraft, 15 with Cambodian.

Similarly, 80 percent or 12 of the 15 Cambodian aircraft will be correctly identified as Cambodian, while 20 percent or three will be incorrectly identified as Vietnamese. This makes a total of 71 Vietnamese and 29 Cambodian sightings, of which only 12 of the 29 Cambodian sightings are correct; the other 17 are incorrect sightings of Vietnamese aircraft. Therefore, when the pilot claims the attack was by a Cambodian fighter, the probability that the craft was actually Cambodian is only 12/29ths or 41 percent, despite the fact that the pilot's identifications are correct 80 percent of the time.

This may seem like a mathematical trick, but it is not. The difference stems from the strong prior probability of the pilot observing a Vietnamese aircraft. The difficulty in understanding this arises because untrained intuitive judgment does not incorporate some of the basic statistical principles of probabilistic reasoning. Most people do not incor-

porate the prior probability into their reasoning because it does not seem relevant. It does not seem relevant because there is no causal relationship between the background information on the percentages of jet fighters in the area and the pilot's observation.[148] The fact that 85 percent of the fighters in the area were Vietnamese and 15 percent Cambodian did not *cause* the attack to be made by a Cambodian rather than a Vietnamese.

To appreciate the different impact made by causally relevant background information, consider this alternative formulation of the same problem. In paragraph (b) of the problem, substitute the following:

(b) Although the fighter forces of the two countries are roughly equal in number in this area, 85 percent of all harassment incidents involve Vietnamese fighters, while 15 percent involve Cambodian fighters.

The problem remains mathematically and structurally the same. Experiments with many test subjects, however, show it is quite different psychologically because it readily elicits a causal explanation relating the prior probabilities to the pilot's observation. If the Vietnamese have a propensity to harass and the Cambodians do not, the prior probability that Vietnamese harassment is more likely than Cambodian is no longer ignored. Linking the prior probability to a cause and effect relationship immediately raises the possibility that the pilot's observation was in error.

With this revised formulation of the problem, most people are likely to reason as follows: We know from past experience in cases such as this that the harassment is usually done by Vietnamese aircraft. Yet, we have a fairly reliable report from our pilot that it was a Cambodian fighter. These two conflicting pieces of evidence cancel each other out. Therefore, we do not know—it is roughly 50-50 whether it was Cambodian or Vietnamese. In employing this reasoning, we use the prior probability information, integrate it with the case-specific information, and arrive at a conclusion that is about as close to the optimal answer (still 41 percent) as one is going to get without doing a mathematical calculation.

There are, of course, few problems in which base rates are given as explicitly as in the Vietnamese/Cambodian aircraft example. When base

148. Maya Bar-Hillel, "The Base-Rate Fallacy in Probability Judgments," *Acta Psychologica*, 1980.

rates are not well known but must be inferred or researched, they are even less likely to be used.[149]

The so-called planning fallacy, to which I personally plead guilty, is an example of a problem in which base rates are not given in numerical terms but must be abstracted from experience. In planning a research project, I may estimate being able to complete it in four weeks. This estimate is based on relevant case-specific evidence: desired length of report, availability of source materials, difficulty of the subject matter, allowance for both predictable and unforeseeable interruptions, and so on. I also possess a body of experience with similar estimates I have made in the past. Like many others, I almost never complete a research project within the initially estimated time frame! But I am seduced by the immediacy and persuasiveness of the case-specific evidence. All the causally relevant evidence about the project indicates I should be able to complete the work in the time allotted for it. Even though I know from experience that this never happens, I do not learn from this experience. I continue to ignore the non-causal, probabilistic evidence based on many similar projects in the past, and to estimate completion dates that I hardly ever meet. (Preparation of this book took twice as long as I had anticipated. These biases are, indeed, difficult to avoid!)

149. Many examples from everyday life are cited in Robyn M. Dawes, *Rational Choice in an Uncertain World* (Harcourt Brace Jovanovich College Publishers, 1988), Chapter 5.

Chapter 13

Hindsight Biases in Evaluation of Intelligence Reporting

Evaluations of intelligence analysis—analysts' own evaluations of their judgments as well as others' evaluations of intelligence products—are distorted by systematic biases. As a result, analysts overestimate the quality of their analytical performance, and others underestimate the value and quality of their efforts. These biases are not simply the product of self-interest and lack of objectivity. They stem from the nature of human mental processes and are difficult and perhaps impossible to overcome.[150]

* * * * * * * * * * * * * * * * * * * *

Hindsight biases influence the evaluation of intelligence reporting in three ways:

- Analysts normally overestimate the accuracy of their past judgments.
- Intelligence consumers normally underestimate how much they learned from intelligence reports.
- Overseers of intelligence production who conduct postmortem analyses of an intelligence failure normally judge that events were more readily foreseeable than was in fact the case.

None of the biases is surprising. Analysts have observed these tendencies in others, although probably not in themselves. What may be

150. This chapter was first published as an unclassified article in *Studies in Intelligence*, Vol. 22, No. 2 (Summer 1978), under the title "Cognitive Biases: Problems in Hindsight Analysis." It was later published in H. Bradford Westerfield, editor, *Inside CIA's Private World: Declassified Articles from the Agency's Internal Journal, 1955-1992* (New Haven: Yale University Press, 1995.)

unexpected is that these biases are not only the product of self-interest and lack of objectivity. They are examples of a broader phenomenon that is built into human mental processes and that cannot be overcome by the simple admonition to be more objective.

Psychologists who conducted the experiments described below tried to teach test subjects to overcome these biases. Experimental subjects with no vested interest in the results were briefed on the biases and encouraged to avoid them or compensate for them, but could not do so. Like optical illusions, cognitive biases remain compelling even after we become aware of them.

The analyst, consumer, and overseer evaluating analytical performance all have one thing in common. They are exercising hindsight. They take their current state of knowledge and compare it with what they or others did or could or should have known before the current knowledge was received. This is in sharp contrast with intelligence estimation, which is an exercise in foresight, and it is the difference between these two modes of thought—hindsight and foresight—that seems to be a source of bias.

The amount of good information that is available obviously is greater in hindsight than in foresight. There are several possible explanations of how this affects mental processes. One is that the additional information available for hindsight changes perceptions of a situation so naturally and so immediately that people are largely unaware of the change. When new information is received, it is immediately and unconsciously assimilated into our pre-existing knowledge. If this new information adds significantly to our knowledge—that is, if it tells the outcome of a situation or the answer to a question about which we were previously uncertain—our mental images are restructured to take the new information into account. With the benefit of hindsight, for example, factors previously considered relevant may become irrelevant, and factors previously thought to have little relevance may be seen as determinative.

After a view has been restructured to assimilate the new information, there is virtually no way to accurately reconstruct the pre-existing mental set. Once the bell has rung, it cannot be unrung. A person may *remember* his or her previous judgments if not much time has elapsed and the judgments were precisely articulated, but apparently people cannot accurately *reconstruct* their previous thinking. The effort to reconstruct what we previously thought about a given situation, or what we would

have thought about it, is inevitably influenced by our current thought patterns. Knowing the outcome of a situation makes it harder to imagine other outcomes that might have been considered. Unfortunately, simply understanding that the mind works in this fashion does little to help overcome the limitation.

The overall message to be learned from an understanding of these biases, as shown in the experiments described below, is that an analyst's intelligence judgments are not as good as analysts think they are, or as bad as others seem to believe. Because the biases generally cannot be overcome, they would appear to be facts of life that analysts need to take into account in evaluating their own performance and in determining what evaluations to expect from others. This suggests the need for a more systematic effort to:

- Define what should be expected from intelligence analysts.
- Develop an institutionalized procedure for comparing intelligence judgments and estimates with actual outcomes.
- Measure how well analysts live up to the defined expectations.

The discussion now turns to the experimental evidence demonstrating these biases from the perspective of the analyst, consumer, and overseer of intelligence.

The Analyst's Perspective

Analysts interested in improving their own performance need to evaluate their past estimates in the light of subsequent developments. To do this, analysts must either remember (or be able to refer to) their past estimates or must reconstruct their past estimates on the basis of what they remember having known about the situation at the time the estimates were made. The effectiveness of the evaluation process, and of the learning process to which it gives impetus, depends in part upon the accuracy of these remembered or reconstructed estimates.

Experimental evidence suggests a systematic tendency toward faulty memory of past estimates.[151] That is, when events occur, people tend to overestimate the extent to which they had previously expected them to occur. And conversely, when events do not occur, people tend to underestimate the probability they had previously assigned to their occurrence. In short, events generally seem less surprising than they should on the basis of past estimates. This experimental evidence accords with analysts' intuitive experience. Analysts rarely appear—or allow themselves to appear—very surprised by the course of events they are following.

In experiments to test the bias in memory of past estimates, 119 subjects were asked to estimate the probability that a number of events would or would not occur during President Nixon's trips to Peking and Moscow in 1972. Fifteen possible outcomes were identified for each trip, and each subject assigned a probability to each of these outcomes. The outcomes were selected to cover the range of possible developments and to elicit a wide range of probability values.

At varying time periods after the trips, the same subjects were asked to remember or reconstruct their own predictions as accurately as possible. (No mention was made of the memory task at the time of the original prediction.) Then the subjects were asked to indicate whether they thought each event had or had not occurred during these trips.

When three to six months were allowed to elapse between the subjects' estimates and their recollection of these estimates, 84 percent of the subjects exhibited the bias when dealing with events they believed actually did happen. That is, the probabilities they remembered having estimated were higher than their actual estimates of events they believed actually did occur. Similarly, for events they believed did not occur, the probabilities they remembered having estimated were lower than their actual estimates, although here the bias was not as great. For both kinds of events, the bias was more pronounced after three to six months had elapsed than when subjects were asked to recall estimates they had given only two weeks earlier.

In summary, knowledge of the outcomes somehow affected most test subjects' memory of their previous estimates of these outcomes, and the more time that was allowed for memories to fade, the greater the

151. This section is based on research reported by Baruch Fischoff and Ruth Beyth in "I Knew It Would Happen: Remembered Probabilities of Once-Future Things," *Organizational Behavior and Human Performance*, 13 (1975), pp. 1-16.

effect of the bias. The developments during the President's trips were perceived as less surprising than they would have been if actual estimates were compared with actual outcomes. For the 84 percent of subjects who showed the anticipated bias, their retrospective evaluation of their estimative performance was clearly more favorable than warranted by the facts.

The Consumer's Perspective

When consumers of intelligence reports evaluate the quality of the intelligence product, they ask themselves the question: "How much did I learn from these reports that I did not already know?" In answering this question, there is a consistent tendency for most people to underestimate the contribution made by new information. This "I knew it all along" bias causes consumers to undervalue the intelligence product.[152]

That people do in fact commonly react to new information in this manner was tested in a series of experiments involving some 320 people, each of whom answered the same set of 75 factual questions taken from almanacs and encyclopedias. As a measure of their confidence in their answers, the subjects assigned to each question a number ranging from 50 percent to 100 percent, indicating their estimate of the probability that they had chosen the correct answer.

As a second step in the experiment, subjects were divided into three groups. The first group was given 25 of the previously asked questions and instructed to respond to them exactly as they had previously. This simply tested the subjects' ability to remember their previous answers. The second group was given the same set of 25 questions but with the correct answers circled "for your [the subjects'] general information." They, too, were asked to respond by reproducing their previous answers. This tested the extent to which learning the correct answers distorted the subjects' memories of their own previous answers, thus measuring the same bias in recollection of previous estimates that was discussed above from the analyst's perspective.

The third group was given a different set of 25 questions they had not previously seen, but which were of similar difficulty so that results

152. Experiments described in this section are reported in Baruch Fischhoff, *The Perceived Informativeness of Factual Information*, Technical Report DDI- I (Eugene, OR: Oregon Research Institute, 1976).

would be comparable with the other two groups. The correct answers were marked on the questionnaire, and the subjects were asked to respond to the questions as they would have responded had they not been told the answer. This tested their ability to recall accurately how much they had known before they learned the correct answer. The situation is comparable to that of intelligence consumers who are asked to evaluate how much they learned from a report, and who can do this only by trying to recollect the extent of their knowledge before they read the report.

The most significant results came from this third group of subjects. The group clearly overestimated what they had known originally and underestimated how much they learned from having been told the answer. For 19 of 25 items in one running of the experiment and 20 of 25 items in another running, this group assigned higher probabilities to the correct alternatives than it is reasonable to expect they would have assigned had they not already known the correct answers.

In summary, the experiment confirmed the results of the previous experiment showing that people exposed to an answer tend to remember having known more than they actually did. It also demonstrates that people have an even greater tendency to exaggerate the likelihood that they would have known the correct answer if they had not been informed of it. In other words, people tend to underestimate both how much they learn from new information and the extent to which new information permits them to make correct judgments with greater confidence. To the extent that intelligence consumers manifest these same biases, they will tend to underrate the value to them of intelligence reporting.

The Overseer's Perspective

An overseer, as the term is used here, is one who investigates intelligence performance by conducting apostmortemexamination of a high-profile intelligence failure. Such investigations are carried out by Congress, the Intelligence Community staff, and CIA or DI management. For those outside the executive branch who do not regularly read the intelligence product, this sort of retrospective evaluation of known intelligence failures is a principal basis for judgments about the quality of intelligence analysis.

A fundamental question posed in anypostmorteminvestigation of intelligence failure is this: Given the information that was available at the

time, should analysts have been able to foresee what was going to happen? Unbiased evaluation of intelligence performance depends upon the ability to provide an unbiased answer to this question.[153]

Unfortunately, once an event has occurred, it is impossible to erase from our mind the knowledge of that event and reconstruct what our thought processes would have been at an earlier point in time. In reconstructing the past, there is a tendency toward determinism, toward thinking that what occurred was inevitable under the circumstances and therefore predictable. In short, there is a tendency to believe analysts should have foreseen events that were, in fact, unforeseeable on the basis of the information available at the time.

The experiments reported in the following paragraphs tested the hypotheses that knowledge of an outcome increases the perceived inevitability of that outcome, and that people who are informed of the outcome are largely unaware that this information has changed their perceptions in this manner.

A series of sub-experiments used brief (150-word) summaries of several events for which four possible outcomes were identified. One of these events was the struggle between the British and the Gurkhas in India in 1814. The four possible outcomes for this event were 1) British victory, 2) Gurkha victory, 3) military stalemate with no peace settlement, and 4) military stalemate with a peace settlement. Five groups of 20 subjects each participated in each sub-experiment. One group received the 150-word description of the struggle between the British and the Gurkhas with no indication of the outcome. The other four groups received the identical description but with one sentence added to indicate the outcome of the struggle—a different outcome for each group.

The subjects in all five groups were asked to estimate the likelihood of each of the four possible outcomes and to evaluate the relevance to their judgment of each datum in the event description. Those subjects who were informed of an outcome were placed in the same position as an overseer of intelligence analysis preparing a postmortem analysis of an intelligence failure. This person tries to assess the probability of an outcome

153. Experiments described in this section are reported in Baruch Fischhoff, "Hindsight does not equal Foresight: The Effect of Outcome Knowledge on Judgment Under Uncertainty," *Journal of Experimental Psychology: Human Perception and Performance*, 1, 3 (1975), pp. 288-299.

Figure 19

Experimental Groups	Average Probabilities Assigned to Outcomes			
	1	2	3	4
Not Told Outcome	33.8	21.3	32.3	12.3
Told Outcome 1	57.2	14.3	15.3	13.4
Told Outcome 2	30.3	38.4	20.4	10.5
Told Outcome 3	25.7	17.0	48.4	9.9
Told Outcome 4	33.0	15.8	24.3	27.0

based only on the information available before the outcome was known. The results are shown in Figure 18.

The group not informed of any outcome judged the probability of Outcome 1 as 33.8 percent, while the group told that Outcome 1 was the actual outcome perceived the probability of this outcome as 57.2 percent. The estimated probability was clearly influenced by knowledge of the outcome. Similarly, the control group with no outcome knowledge estimated the probability of Outcome 2 as 21.3 percent, while those informed that Outcome 2 was the actual outcome perceived it as having a 38.4 percent probability.

An average of all estimated outcomes in six sub-experiments (a total of 2,188 estimates by 547 subjects) indicates that the knowledge or belief that one of four possible outcomes has occurred approximately doubles the perceived probability of that outcome as judged with hindsight as compared with foresight.

The relevance that subjects attributed to any datum was also strongly influenced by which outcome, if any, they had been told was true. As Roberta Wohlstetter has written, "It is much easier after the fact to sort the relevant from the irrelevant signals. After the event, of course, a signal is always crystal clear. We can now see what disaster it was signaling since

the disaster has occurred, but before the event it is obscure and pregnant with conflicting meanings."[154] The fact that outcome knowledge automatically restructures a person's judgments about the relevance of available data is probably one reason it is so difficult to reconstruct how our thought processes were or would have been without this outcome knowledge.

In several variations of this experiment, subjects were asked to respond as though they did not know the outcome, or as others would respond if they did not know the outcome. The results were little different, indicating that subjects were largely unaware of how knowledge of the outcome affected their own perceptions. The experiment showed that subjects were unable to empathize with how others would judge these situations. Estimates of how others would interpret the data without knowing the outcome were virtually the same as the test subjects' own retrospective interpretations.

These results indicate that overseers conducting postmortemevaluations of what analysts should have been able to foresee, given the available information, will tend to perceive the outcome of that situation as having been more predictable than was, in fact, the case. Because they are unable to reconstruct a state of mind that views the situation only with foresight, not hindsight, overseers will tend to be more critical of intelligence performance than is warranted.

Discussion of Experiments

Experiments that demonstrated these biases and their resistance to corrective action were conducted as part of a research program in decision analysis funded by the Defense Advanced Research Projects Agency. Unfortunately, the experimental subjects were students, not members of the Intelligence Community. There is, nonetheless, reason to believe the results can be generalized to apply to the Intelligence Community. The experiments deal with basic human mental processes, and the results do seem consistent with personal experience in the Intelligence Community. In similar kinds of psychological tests, in which experts, including intelligence analysts, were used as test subjects, the experts showed the same pattern of responses as students.

154. Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962), p. 387. Cited by Fischhoff.

My own imperfect effort to replicate one of these experiments using intelligence analysts also supports the validity of the previous findings. To test the assertion that intelligence analysts normally overestimate the accuracy of their past judgments, there are two necessary preconditions. First, analysts must make a series of estimates in quantitative terms—that is, they must say not just that a given occurrence is probable, but that there is, for example, a 75-percent chance of its occurrence. Second, it must be possible to make an unambiguous determination whether the estimated event did or did not occur. When these two preconditions are present, one can go back and check the analysts' recollections of their earlier estimates. Because CIA estimates are rarely stated in terms of quantitative probabilities, and because the occurrence of an estimated event within a specified time period often cannot be determined unambiguously, these preconditions are seldom met.

I did, however, identify several analysts who, on two widely differing subjects, had made quantitative estimates of the likelihood of events for which the subsequent outcome was clearly known. I went to these analysts and asked them to recall their earlier estimates. The conditions for this mini-experiment were far from ideal and the results were not clear-cut, but they did tend to support the conclusions drawn from the more extensive and systematic experiments described above.

All this leads to the conclusion that the three biases are found in Intelligence Community personnel as well as in the specific test subjects. In fact, one would expect the biases to be even greater in foreign affairs professionals whose careers and self-esteem depend upon the presumed accuracy of their judgments.

Can We Overcome These Biases?

Analysts tend to blame biased evaluations of intelligence performance at best on ignorance and at worst on self-interest and lack of objectivity. Both these factors may also be at work, but the experiments suggest the nature of human mental processes is also a principal culprit. This is a more intractable cause than either ignorance or lack of objectivity.

The self-interest of the experimental subjects was not at stake, yet they showed the same kinds of bias with which analysts are familiar. Moreover, in these experimental situations the biases were highly resis-

tant to efforts to overcome them. Subjects were instructed to make estimates as if they did not already know the answer, but they were unable to do so. One set of test subjects was briefed specifically on the bias, citing the results of previous experiments. This group was instructed to try to compensate for the bias, but it was unable to do so. Despite maximum information and the best of intentions, the bias persisted.

This intractability suggests the bias does indeed have its roots in the nature of our mental processes. Analysts who try to recall a previous estimate after learning the actual outcome of events, consumers who think about how much a report has added to their knowledge, and overseers who judge whether analysts should have been able to avoid an intelligence failure, all have one thing in common. They are engaged in a mental process involving hindsight. They are trying to erase the impact of knowledge, so as to remember, reconstruct, or imagine the uncertainties they had or would have had about a subject prior to receipt of more or less definitive information.

It appears, however, that the receipt of what is accepted as definitive or authoritative information causes an immediate but unconscious restructuring of a person's mental images to make them consistent with the new information. Once past perceptions have been restructured, it seems very difficult, if not impossible, to reconstruct accurately what one's thought processes were or would have been before this restructuring.

There is one procedure that may help to overcome these biases. It is to pose such questions as the following: Analysts should ask themselves, "If the opposite outcome had occurred, would I have been surprised?" Consumers should ask, "If this report had told me the opposite, would I have believed it?" And overseers should ask, "If the opposite outcome had occurred, would it have been predictable given the information that was available?" These questions may help one recall or reconstruct the uncertainty that existed prior to learning the content of a report or the outcome of a situation.

This method of overcoming the bias can be tested by readers of this chapter, especially those who believe it failed to tell them much they had not already known. If this chapter had reported that psychological experiments show no consistent pattern of analysts overestimating the accuracy of their estimates, or of consumers underestimating the value of our product, would you have believed it? (Answer: Probably not.) If it had reported that psychological experiments show these biases to be

caused only by self-interest and lack of objectivity, would you have believed this? (Answer: Probably yes.) And would you have believed it if this chapter had reported these biases can be overcome by a conscientious effort at objective evaluation? (Answer: Probably yes.)

These questions may lead you, the reader, to recall the state of your knowledge or beliefs before reading this chapter. If so, the questions will highlight what you learned here—namely, that significant biases in the evaluation of intelligence estimates are attributable to the nature of human mental processes, not just to self-interest and lack of objectivity, and that they are, therefore, exceedingly difficult to overcome.

PART IV—CONCLUSIONS

Chapter 14

Improving Intelligence Analysis

This chapter offers a checklist for analysts—a summary of tips on how to navigate the minefield of problems identified in previous chapters. It also identifies steps that managers of intelligence analysis can take to help create an environment in which analytical excellence can flourish.

* * * * * * * * * * * * * * * * * * * *

How can intelligence analysis be improved? That is the challenge. A variety of traditional approaches are used in pursuing this goal: collecting more and better information for analysts to work with, changing the management of the analytical process, increasing the number of analysts, providing language and area studies to improve analysts' substantive expertise, revising employee selection and retention criteria, improving report-writing skills, fine-tuning the relationship between intelligence analysts and intelligence consumers, and modifying the types of analytical products.

Any of these measures may play an important role, but analysis is, above all, a mental process. Traditionally, analysts at all levels devote little attention to improving how they think. To penetrate the heart and soul of the problem of improving analysis, it is necessary to better understand, influence, and guide the mental processes of analysts themselves.

Checklist for Analysts

This checklist for analysts summarizes guidelines for maneuvering through the minefields encountered while proceeding through the analytical process. Following the guidelines will help analysts protect themselves from avoidable error and improve their chances of making the right calls. The discussion is organized around six key steps in the analytical process: defining the problem, generating hypotheses, collecting information, evaluating hypotheses, selecting the most likely hypothesis, and the ongoing monitoring of new information.

Defining the Problem

Start out by making certain you are asking—or being asked—the right questions. Do not hesitate to go back up the chain of command with a suggestion for doing something a little different from what was asked for. The policymaker who originated the requirement may not have thought through his or her needs, or the requirement may be somewhat garbled as it passes down through several echelons of management. You may have a better understanding than the policymaker of what he or she needs, or should have, or what is possible to do. At the outset, also be sure your supervisor is aware of any tradeoff between quality of analysis and what you can accomplish within a specified time deadline.

Generating Hypotheses

Identify all the plausible hypotheses that need to be considered. Make a list of as many ideas as possible by consulting colleagues and outside experts. Do this in a brainstorming mode, suspending judgment for as long as possible until all the ideas are out on the table.

Then whittle the list down to a workable number of hypotheses for more detailed analysis. Frequently, one of these will be a deception hypothesis—that another country or group is engaging in denial and deception to influence US perceptions or actions.

At this stage, do not screen out reasonable hypotheses only because there is no evidence to support them. This applies in particular to the deception hypothesis. If another country is concealing its intent through denial and deception, you should probably not expect to see evidence of it without completing a very careful analysis of this possibility. The deception hypothesis and other plausible hypotheses for which there may be no immediate evidence should be carried forward to the next stage of analysis until they can be carefully considered and, if appropriate, rejected with good cause.

Collecting Information

Relying only on information that is automatically delivered to you will probably not solve all your analytical problems. To do the job right, it will probably be necessary to look elsewhere and dig for more information. Contact with the collectors, other Directorate of Operations personnel, or first-cut analysts often yields additional information. Also check academic specialists, foreign newspapers, and specialized journals.

Collect information to evaluate all the reasonable hypotheses, not just the one that seems most likely. Exploring alternative hypotheses that have not been seriously considered before often leads an analyst into unexpected and unfamiliar territory. For example, evaluating the possibility of deception requires evaluating another country's or group's motives, opportunities, and means for denial and deception. This, in turn, may require understanding the strengths and weaknesses of US human and technical collection capabilities.

It is important to suspend judgment while information is being assembled on each of the hypotheses. It is easy to form impressions about a hypothesis on the basis of very little information, but hard to change an impression once it has taken root. If you find yourself thinking you already know the answer, ask yourself what would cause you to change your mind; then look for that information.

Try to develop alternative hypotheses in order to determine if some alternative—when given a fair chance—might not be as compelling as your own preconceived view. Systematic development of an alternative hypothesis usually increases the perceived likelihood of that hypothesis. "A willingness to play with material from different angles and in the context of unpopular as well as popular hypotheses is an essential ingredient of a good detective, whether the end is the solution of a crime or an intelligence estimate."[155]

Evaluating Hypotheses

Do not be misled by the fact that so much evidence supports your preconceived idea of which is the most likely hypothesis. That same evidence may be consistent with several different hypotheses. Focus on developing arguments *against* each hypothesis rather than trying to confirm hypotheses. In other words, pay particular attention to evidence or assumptions that suggest one or more hypotheses are *less* likely than the others.

Recognize that your conclusions may be driven by assumptions that determine how you interpret the evidence rather than by the evidence itself. Especially critical are assumptions about what is in another country's national interest and how things are usually done in that country. Assumptions are fine as long as they are made explicit in your analysis

155. Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford: Stanford University Press, 1962), p. 302.

and you analyze the sensitivity of your conclusions to those assumptions. Ask yourself, would different assumptions lead to a different interpretation of the evidence and different conclusions?

Consider using the matrix format discussed in Chapter 8, "Analysis of Competing Hypotheses," to keep track of the evidence and how it relates to the various hypotheses.

Guard against the various cognitive biases. Especially dangerous are those biases that occur when you lack sufficient understanding of how a situation appears from another country's point of view. Do not fill gaps in your knowledge by assuming that the other side is likely to act in a certain way because that is how the US Government would act, or other Americans would act, under similar circumstances.

Recognize that the US perception of another country's national interest and decisionmaking processes often differs from how that country perceives its own interests and how decisions are actually made in that country. In 1989–90, for example, many analysts of Middle Eastern affairs clearly assumed that Iraq would demobilize part of its armed forces after the lengthy Iran-Iraq war so as to help rehabilitate the Iraqi economy. They also believed Baghdad would see that attacking a neighboring Arab country would not be in Iraq's best interest. We now know they were wrong.

When making a judgment about what another country is likely to do, invest whatever time and effort are needed to consult with whichever experts have the best understanding of what that country's government is actually thinking and how the decision is likely to be made.

Do not assume that every foreign government action is based on a rational decision in pursuit of identified goals. Recognize that government actions are sometimes best explained as a product of bargaining among semi-independent bureaucratic entities, following standard operating procedures under inappropriate circumstances, unintended consequences, failure to follow orders, confusion, accident, or coincidence.

Selecting the Most Likely Hypothesis

Proceed by trying to reject hypotheses rather than confirm them. The most likely hypothesis is usually the one with the least evidence against it, not the one with the most evidence for it.

In presenting your conclusions, note all the reasonable hypotheses that were considered. Cite the arguments and evidence supporting your

judgment, but also justify briefly why other alternatives were rejected or considered less likely. To avoid ambiguity, insert an odds ratio or probability range in parentheses after expressions of uncertainty in key judgments.

Ongoing Monitoring

In a rapidly changing, probabilistic world, analytical conclusions are always tentative. The situation may change, or it may remain unchanged while you receive new information that alters your understanding of it. Specify things to look for that, if observed, would suggest a significant change in the probabilities.

Pay particular attention to any feeling of surprise when new information does not fit your prior understanding. Consider whether this surprising information is consistent with an alternative hypothesis. A surprise or two, however small, may be the first clue that your understanding of what is happening requires some adjustment, is at best incomplete, or may be quite wrong.

Management of Analysis

The cognitive problems described in this book have implications for the management as well as the conduct of intelligence analysis. This concluding section looks at what managers of intelligence analysis can do to help create an organizational environment in which analytical excellence flourishes. These measures fall into four general categories: research, training, exposure to alternative mind-sets, and guiding analytical products.

Support for Research

Management should support research to gain a better understanding of the cognitive processes involved in making intelligence judgments. There is a need for better understanding of the thinking skills involved in intelligence analysis, how to test job applicants for these skills, and how to train analysts to improve these skills. Analysts also need a fuller understanding of how cognitive limitations affect intelligence analysis and how to minimize their impact. They need simple tools and techniques to help protect themselves from avoidable error. There is so much research to be done that it is difficult to know where to start.

Scholars selected for tours of duty in the Intelligence Community should include cognitive psychologists or other scholars of various backgrounds who are interested in studying the thinking processes of intelligence analysts. There should also be post-doctoral fellowships for promising scholars who could be encouraged to make a career of research in this field. Over time, this would contribute to building a better base of knowledge about how analysts do and/or should make analytical judgments and what tools or techniques can help them.

Management should also support research on the mind-sets and implicit mental models of intelligence analysts. Because these mind-sets or models serve as a "screen" or "lens" through which analysts perceive foreign developments, research to determine the nature of this "lens" may contribute as much to accurate judgments as does research focused more directly on the foreign areas themselves.[156]

Training

Most training of intelligence analysts is focused on organizational procedures, writing style, and methodological techniques. Analysts who write clearly are assumed to be thinking clearly. Yet it is quite possible to follow a faulty analytical process and write a clear and persuasive argument in support of an erroneous judgment.

More training time should be devoted to the thinking and reasoning processes involved in making intelligence judgments, and to the tools of the trade that are available to alleviate or compensate for the known cognitive problems encountered in analysis. This book is intended to support such training.

Training will be more effective if supplemented with ongoing advice and assistance. An experienced coach who can monitor and guide ongoing performance is a valuable supplement to classroom instruction

156. Graham Allison's work on the Cuban missile crisis (Essence of Decision, Little, Brown & Co., 1971) is an example of what I have in mind. Allison identified three alternative assumptions about how governments work--the rational actor model, organizational process model, and bureaucratic politics model. He then showed how an analystÍs implicit assumptions about the most appropriate model for analyzing a foreign government's behavior cause him or her to focus on different evidence and arrive at different conclusions. Another example is my own analysis of five alternative paths for making counterintelligence judgments in the controversial case of KGB defector Yuriy Nosenko. Richards J. Heuer, Jr., "Nosenko: Five Paths to Judgment," *Studies in Intelligence*, Vol. 31, No. 3 (Fall 1987), originally classified Secret but declassified and published in H. Bradford Westerfield, ed., *Inside CIA's Private World: Declassified Articles from the Agency Internal Journal 1955-1992* (New Haven: Yale University Press, 1995).

in many fields, probably including intelligence analysis. This is supposed to be the job of the branch chief or senior analyst, but these officers are often too busy responding to other pressing demands on their time.

It would be worthwhile to consider how an analytical coaching staff might be formed to mentor new analysts or consult with analysts working particularly difficult issues. One possible model is the SCORE organization that exists in many communities. SCORE stands for Senior Corps of Retired Executives. It is a national organization of retired executives who volunteer their time to counsel young entrepreneurs starting their own businesses. It should be possible to form a small group of retired analysts who possess the skills and values that should be imparted to new analysts, and who would be willing to volunteer (or be hired) to come in several days a week to counsel junior analysts.

New analysts could be required to read a specified set of books or articles relating to analysis, and to attend a half-day meeting once a month to discuss the reading and other experiences related to their development as analysts. A comparable voluntary program could be conducted for experienced analysts. This would help make analysts more conscious of the procedures they use in doing analysis. In addition to their educational value, the required readings and discussion would give analysts a common experience and vocabulary for communicating with each other, and with management, about the problems of doing analysis.

My suggestions for writings that would qualify for a mandatory reading program include: Robert Jervis' *Perception and Misperception in International Politics* (Princeton University Press, 1977); Graham Allison's *Essence of Decision: Explaining the Cuban Missile Crisis* (Little, Brown, 1971); Ernest May's "*Lessons" of the Past: The Use and Misuse of History in American Foreign Policy* (Oxford University Press, 1973); Ephraim Kam's, *Surprise Attack* (Harvard University Press, 1988); Richard Betts' "Analysis, War and Decision: Why Intelligence Failures Are Inevitable," *World Politics,* Vol. 31, No. 1 (October 1978); Thomas Kuhn's *The Structure of Scientific Revolutions* (University of Chicago Press, 1970); and Robin Hogarth's *Judgement and Choice* (John Wiley, 1980). Although these were all written many years ago, they are classics of permanent value. Current analysts will doubtless have other works to recommend. CIA and Intelligence Community postmortem analyses of intelligence failure should also be part of the reading program.

To facilitate institutional memory and learning, thorough postmortem analyses should be conducted on all significant intelligence failures. Analytical (as distinct from collection) successes should also be studied. These analyses should be collated and maintained in a central location, available for review to identify the common characteristics of analytical failure and success. A meta-analysis of the causes and consequences of analytical success and failure should be widely distributed and used in training programs to heighten awareness of analytical problems.

To encourage learning from experience, even in the absence of a high-profile failure, management should require more frequent and systematic retrospective evaluation of analytical performance. One ought not generalize from any single instance of a correct or incorrect judgment, but a series of related judgments that are, or are not, borne out by subsequent events can reveal the accuracy or inaccuracy of the analyst's mental model. Obtaining systematic feedback on the accuracy of past judgments is frequently difficult or impossible, especially in the political intelligence field. Political judgments are normally couched in imprecise terms and are generally conditional upon other developments. Even in retrospect, there are no objective criteria for evaluating the accuracy of most political intelligence judgments as they are presently written.

In the economic and military fields, however, where estimates are frequently concerned with numerical quantities, systematic feedback on analytical performance is feasible. Retrospective evaluation should be standard procedure in those fields in which estimates are routinely updated at periodic intervals. The goal of learning from retrospective evaluation is achieved, however, only if it is accomplished as part of an objective search for improved understanding, not to identify scapegoats or assess blame. This requirement suggests that retrospective evaluation should be done routinely within the organizational unit that prepared the report, even at the cost of some loss of objectivity.

Exposure to Alternative Mind-Sets

The realities of bureaucratic life produce strong pressures for conformity. Management needs to make conscious efforts to ensure that well-reasoned competing views have the opportunity to surface within the Intelligence Community. Analysts need to enjoy a sense of security, so that partially developed new ideas may be expressed and bounced off

others as sounding boards with minimal fear of criticism for deviating from established orthodoxy.

Much of this book has dealt with ways of helping analysts remain more open to alternative views. Management can help by promoting the kinds of activities that confront analysts with alternative perspectives—consultation with outside experts, analytical debates, competitive analysis, devil's advocates, gaming, and interdisciplinary brainstorming.

Consultation with outside experts is especially important as a means of avoiding what Adm. David Jeremiah called the "everybody-thinks-like-us mindset" when making significant judgments that depend upon knowledge of a foreign culture. Intelligence analysts have often spent less time living in and absorbing the culture of the countries they are working on than outside experts on those countries. If analysts fail to understand the foreign culture, they will not see issues as the foreign government sees them. Instead, they may be inclined to mirror-image—that is, to assume that the other country's leaders think like we do. The analyst assumes that the other country will do what we would do if we were in their shoes.

Mirror-imaging is a common source of analytical error, and one that reportedly played a role in the Intelligence Community failure to warn of imminent Indian nuclear weapons testing in 1998. After leading a US Government team that analyzed this episode, Adm. Jeremiah recommended more systematic use of outside expertise whenever there is a major transition that may lead to policy changes, such as the Hindu nationalists' 1998 election victory and ascension to power in India.[157]

Pre-publication review of analytical reports offers another opportunity to bring alternative perspectives to bear on an issue. Review procedures should explicitly question the mental model employed by the analyst in searching for and examining evidence. What assumptions has the analyst made that are not discussed in the draft itself, but that underlie the principal judgments? What alternative hypotheses have been considered but rejected, and for what reason? What could cause the analyst to change his or her mind?

Ideally, the review process should include analysts from other areas who are not specialists in the subject matter of the report. Analysts within the same branch or division often share a similar mind-set. Past experience with review by analysts from other divisions or offices indi-

157. Transcript of Adm. David Jeremiah's news conference at CIA, 2 June 1998.

cates that critical thinkers whose expertise is in other areas make a significant contribution. They often see things or ask questions that the author has not seen or asked. Because they are not so absorbed in the substance, they are better able to identify the assumptions and assess the argumentation, internal consistency, logic, and relationship of the evidence to the conclusion. The reviewers also profit from the experience by learning standards for good analysis that are independent of the subject matter of the analysis.

Guiding Analytical Products

On key issues, management should reject most single-outcome analysis—that is, the single-minded focus on what the analyst believes is probably happening or most likely will happen. When we cannot afford to get it wrong, or when deception is a serious possibility, management should consider mandating a systematic analytical process such as the one described in Chapter 8, "Analysis of Competing Hypotheses." Analysts should be required to identify alternatives that were considered, justify why the alternatives are deemed less likely, and clearly express the degree of likelihood that events may not turn out as expected.

Even if the analyst firmly believes the odds are, say, three-to-one against something happening, that leaves a 25-percent chance that it will occur. Making this explicit helps to better define the problem for the policymaker. Does that 25-percent chance merit some form of contingency planning?

If the less likely hypothesis happens to be, for example, that a new Indian Government will actually follow through on its election campaign promise to conduct nuclear weapons testing, as recently occurred, even a 25-percent chance might be sufficient to put technical collection systems on increased alert.

Verbal expressions of uncertainty—such as possible, probable, unlikely, may, and could—have long been recognized as sources of ambiguity and misunderstanding. By themselves, most verbal expressions of uncertainty are empty shells. The reader or listener fills them with meaning through the context in which they are used and what is already in the reader's or listener's mind about that subject. An intelligence consumer's interpretation of imprecise probability judgments will always be biased in favor of consistency with what the reader already believes. That means the intelligence reports will be undervalued and have little impact on the

consumer's judgment. This ambiguity can be especially troubling when dealing with low-probability, high-impact dangers against which policymakers may wish to make contingency plans.

Managers of intelligence analysis need to convey to analysts that it is okay to be uncertain, as long as they clearly inform readers of the degree of uncertainty, sources of uncertainty, and what milestones to watch for that might clarify the situation. Inserting odds ratios or numerical probability ranges in parentheses to clarify key points of an analysis should be standard practice.

The likelihood of future surprises can be reduced if management assigns more resources to monitoring and analyzing seemingly low-probability events that will have a significant impact on US policy if they do occur. Analysts are often reluctant, on their own initiative, to devote time to studying things they do not believe will happen. This usually does not further an analyst's career, although it can ruin a career when the unexpected does happen. Given the day-to-day pressures of current events, it is necessary for managers and analysts to clearly identify which unlikely but high-impact events need to be analyzed and to allocate the resources to cover them.

One guideline for identifying unlikely events that merit the specific allocation of resources is to ask the following question: Are the chances of this happening, however small, sufficient that if policymakers fully understood the risks, they might want to make contingency plans or take some form of preventive or preemptive action? If the answer is yes, resources should be committed to analyze even what appears to be an unlikely outcome.

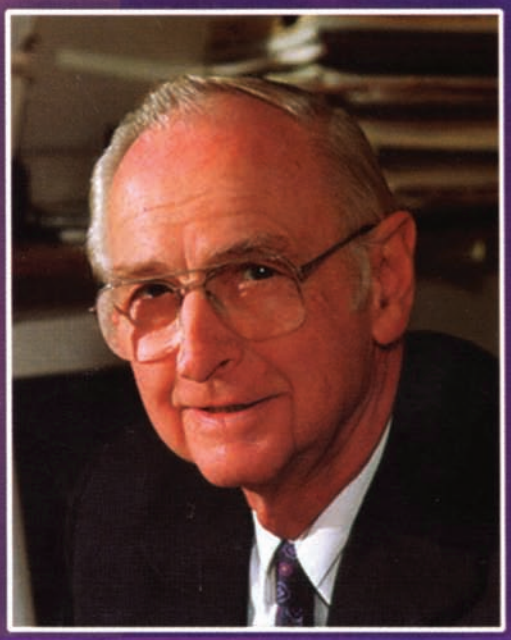
Managers of intelligence should support analyses that periodically re-examine key problems from the ground up in order to avoid the pitfalls of the incremental approach. Receipt of information in small increments over time facilitates assimilation of this information to the analyst's existing views. No one item of information may be sufficient to prompt the analyst to change a previous view. The cumulative message inherent in many pieces of information may be significant but is attenuated when this information is not examined as a whole.

Finally, management should educate consumers concerning the limitations as well as the capabilities of intelligence analysis and should define a set of realistic expectations as a standard against which to judge analytical performance.

The Bottom Line

Analysis can be improved! None of the measures discussed in this book will guarantee that accurate conclusions will be drawn from the incomplete and ambiguous information that intelligence analysts typically work with. Occasional intelligence failures must be expected. Collectively, however, the measures discussed here can certainly improve the odds in the analysts' favor.

The Author



Richards J. Heuer, Jr. worked for the CIA for nearly 45 years—first as a staff officer from 1951 until his retirement in 1979 and then as a contractor on a variety of projects until 1995. He began his career in the Directorate of Operations and later transferred to the Directorate of Intelligence, where he headed the unit working on analytic methods in the Office of Political Analysis. He is now a consultant for the Defense Security Service's Security Research Center in Monterey, California.

Mr. Heuer was awarded the Agency Seal Medallion in 1987 for developing and teaching an innovative methodology for addressing complex and challenging problems facing the Intelligence Community. He was recognized in 1988 for his "outstanding contribution to the literature of intelligence," and again in 1996 for "superior accomplishment." In addition to his work on the psychology of intelligence analysis, Mr. Heuer is a published author on counterintelligence, deception, analytical methodology, and personnel security issues.

Many of the chapters in this book were originally written for the Directorate of Intelligence in the 1980s. They were recently edited and assembled, along with additional material that Mr. Heuer prepared specifically for this book, under the auspices of the CIA's Center for the Study of Intelligence.

I have been a fan of Richards Heuer ever since I met him and read some of his material 20 years ago. This book combines Dick's many years of experience with his extensive knowledge of psychological research. He examines impediments to good intelligence analysis and points the way to how to overcome them. The volume should be of real assistance to people faced with the need to draw sound estimates from changing and ambiguous information.

Robert Jervis
Professor, Institute of
War and Peace Studies
Columbia University

This Page Is Intentionally Left Blank

AU/ACSC/2016

AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

MASTERS OF ANALYTICAL TRADECRAFT: CERTIFYING THE STANDARDS AND ANALYTIC RIGOR OF INTELLIGENCE PRODUCTS

by

J. Tucker Rojas, Lt Col, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements

Advisor: Dr. Fred Stone

Maxwell Air Force Base, Alabama

April 2016

Disclaimer

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the US government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

TABLE OF CONTENTS

Page

DISCLAIMER.....ii

TABLE OF CONTENTS.....iii

LIST OF FIGURES.....iv

LIST OF TABLES.....v

ABSTRACT.....vi

Section 1: INTRODUCTION.....1

Section 2: BACKGROUND.....3

Section 3: SUFFICIENCY OF ANALYTICAL RIGOR.....11

Section 4: PROPOSAL.....15

Section 5: RESEARCH METHODOLOGY.....16

Section 6: ANALYSIS / EVALUATION.....17

Section 7: RECOMMENDATIONS.....23

BIBLIOGRAPHY.....30

LIST OF FIGURES

Page

Figure 1: Visualization of Zelik, et al. Rigor Metric.....10

Figure 2: Proposed MAT Rating Badges.....16

LIST OF TABLES

Page

Table 1: ICD 203 Standards compared to AFI 140-133 Standards.....13

ABSTRACT

This paper explores analysis in intelligence and evaluates a proposal to certify and convey analytical rigor as it relates to intelligence products. To accomplish this, an examination of intelligence failures is conducted to assess the application of analytical rigor across historic case studies. The historic failures demonstrate gaps in standardization and insufficiencies in analytical rigor. This paper proposes establishing unit level certified Masters of Analytic Tradecraft (MAT) analysts to be trained and entrusted to evaluate and rate the standards and analytical rigor of intelligence products prior to publication. This certification model is based on research of the structure of professional civilian corporations. Implementing the MAT analyst certification will allow decision-makers the ability to judge when analysis is robust or shallow so that they can meter their trust accordingly. This certification will hold the IC accountable in their adherence to the established analytical standards, ensure compliance is properly conveyed, and promote a quality of analysis.

Section 1: INTRODUCTION

Research has shown the difficulty in recognizing inadequacies of analytical rigor when consuming intelligence analysis within information domains.[1] For the purposes of this paper, analytical rigor is defined as "an emergent multi-attribute measure of sufficiency."[2] The term analytic rigor is used to convey the level of analytic tradecraft application: sometimes robust and other times weak. Decision makers should be provided "with actionable data backed by analytical rigor."[3] When evaluating a problem-set, an intelligence consumer's perceived analytical rigor (based on perceived cues) ideally should meet or exceed effective rigor (based on analytical process).[4] To accomplish this, decision makers should not be left to their own perceptions in judging the analytic rigor of given intelligence product, they need to be provided fidelity on the level of analytical rigor; they need to know when analysis is robust or shallow so that they can meter their trust accordingly.

Unfortunately, examples of high-consequence, high profile intelligence fails have been common, revealing a consistent lack of analytical sufficiency and raising concerns about the condition of United States (U.S.) intelligence.[5] The 2003 assessment of Iraq's weapons of mass destruction (WMD) is one example of a catastrophic failure on the part of the IC.[6] The WMD Commission Report summarized the assessment failures that informed the 2003 invasion of Iraq in this way: "This failure was in large part the result of analytical shortcomings; intelligence analysts were too wedded to their assumptions about Saddam's intentions... We conclude that the Intelligence Community was dead wrong in almost all of its pre-war judgments about Iraq's weapons of mass destruction…[there existed] serious errors in analyzing… [and a] failure to make clear just how much of its analysis was based on assumptions, rather than good evidence…"[7]

Where it is typical for analysts to use tradecraft language to convey likeliness and confidence, no such effort is afforded to articulating analytical rigor. If an assurance of standards and a conveyed level of rigor accompanied assessment, it would empower decision makers as they evaluate and measure the level of confidence they should apply to the assessment. U.S. law has mandated that that the Office of the Director of National Intelligence (ODNI) conduct post-production, after-action quality assurance spot checks, however there is not a universal method or qualifying standard of analytical rigor prior to the publication of intelligence reports. Perceived levels of rigor can be misled by the appearance product quality, with the perception of "sufficient rigor" evolving once insight to the analytical process is provided. [8]

The application of a certification model will challenge analysts and organizations to meet higher levels of analytical rigor while providing process insight to decision makers. In the civilian world certifications are used to help regulate professional fields such as medicine, law, and engineering by: 1) establishing minimally acceptable standards, 2) providing accountability and reassuring consumers that the professionals are deserving of trust, 3) improving quality by providing guidance and by capturing and disseminating best practices.[9] The U.S. Green Building Council (USGBC), an organization that promotes sustainability-focused construction practices, has a unique approach in their Leadership in Energy and Environmental Design (LEED) program.[10] USGBC not only credentials its associates (builders, architects, designers), but has a four tiered rating system to certify standards of construction for a given project. The LEED tiered rating system quantifies and clearly conveys that standard to consumers.

This paper will evaluate the achievability of certifying intelligence products by first

providing context and initial historical and current analysis of intelligence practices. It will define sufficiency of analytical rigor by evaluating its independent attributes and analyzing how ODNI, and the Air Force guidance define analytical standards. A proposal for both an analyst and pre-publication product certification process will be presented and evaluated to assess if a certification process should be incorporated across the IC and whether or not that process would or would not affect how analytical rigor is conveyed to decision makers.

Section 2: BACKGROUND

Today, seventeen agencies and organizations comprise the IC, with over 1,200 sub-organizations and over 1,900 private companies, comprising a 50+ billion dollar budget and employ over 800,000 people with TOP SECRET clearances.[11] Its collective analytical might culminates in intelligence reports like the *President's Daily Brief* (PDB), *Worldwide Intelligence Review* (WIRe), *National Intelligence Estimate* (NIE), *Secretary of Defense/Chairman of the Joint Chiefs of Staff Daily Intelligence Update* (SECDEF/CJCS J2 Daily Intelligence Update), and the *Secretary's Morning Summary* (SMS).[12] The IC's effectiveness has been the topic of much investigation. How analysis is accomplished and communicated varies greatly across the IC's 17 agencies and organizations, which continually battle tendencies to stovepipe information behind shrouds of secrecy and "need-to-know" compartmentalized barriers. Many experts have pointed to an IC that is obsessed with the churn of data and overly focused on the tactical and current intelligence needed to impact the tactical battlefield in real-time; going as far to reference this phenomena as "tyranny": the tyranny of current intelligence, tyranny of taskings, tyranny of daily operations, and the tyranny of the immediate to name a few.[13] Although valued by its consumers, a focus on the immediate

has detracted from the strategic intelligence priorities that inform national level decision makers and requires deep understanding required for strategic, long-term analysis.[14] The propagation of information and the availability of real-time interconnected data has "exacerbated the risk of shallow information analysis."[15] Where a tactical real-time focus can save lives and assists in capturing adversaries on the battlefield, strategic intelligence has the power to both justify and deter wars. Under production pressures, this collection-driven, real-time focus is much desired by war-fighters, albeit at the detriment of deep understanding; lacking the sustained expert scrutiny required to do the long-term analysis necessary to evaluate and inform strategic problem-sets. Tactical and strategic assessments are not mutually exclusive, for they inform one another. A strategic, deep understanding of a target-system or a target-country is informed through the aggregation of hundreds, if not thousands of tactical and operational assessments.

The 2008 RAND repot, *Assessing the Tradecraft of Intelligence Analysis*, phrases this tension as "intelligence reporting" verses "intelligence analysis;" intelligence reporting requiring little if any critical thinking, application of tradecraft, or utilization of structured analytical techniques.[16] This same report suggested: "The need for a focal point in analysis, and analytic tradecraft is striking, and this need will only grow as the Community strives to be more 'joint' in the wake of the December 2004 intelligence reform law and the creation of a director of national intelligence."[17] Community-wide standards are essential for analysts to be effective in how they communicate assessments to their customers.

The "intelligence process" pulls collection from the operational environment, takes that data and processes it into information. [18] Once put through the rigors of analysis, information then becomes intelligence. Actionable, timely, and relevant intelligence informs national decision makers and the warfighter consumers. This requirement driven intelligence process is enabled through analysis, which is the "thinking" part of intelligence.[19] Analysis is the pursuit of

situational understanding and thus facilitates the goal of bold, predictive, and informative assessments. The tradecraft of analysis is the underpinning of the intelligence cycle and is key to the development of deliverable intelligence.[20]

A review of intelligence failures has shown deficiencies in analysis to be a consistent cause of IC shortcomings.[21] Poor application of analytical tradecraft standards, not employing structured analytic techniques, and applying levels of mediocre analytical rigor have caused strategic assumptions, dating back over a half century, which were not appropriately challenged. Some examples include: the 1962 Cuban Missile Crisis, the 1973 Yom Kippur War, the 1989 German Unification, and the 1998 Indian Nuclear Test.[22]

Effective analysis is the key to preventing shortfalls such as those highlighted in the surprise attacks of September 11th. The 9-11 Commission relied on Staff Statement No. 11, The *Performance of the Intelligence Community* to inform their understanding of the IC's performance leading up to the September 11 attacks on the United States. This document described how the IC's emphasis on analysis waned in the 1990's as budgets cuts prevailed and competition with operations and collection further detracted from the importance of analysis.[23] Analysis competed with the introduction of the 24-hour news cycle and analytical production was driven away from strategic, long-range, deep analysis and instead shifted towards current, tactical intelligence. The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) acted on these shortfalls and mandated that the Director of National Intelligence convey analytical tradecraft standards and implement processes to ensure that the Intelligence Community production meets a standard of high analytical rigor.[24]

An analysis of the 2002 National Intelligence Estimate (NIE) on Iraq's weapons of mass destruction (WMD) and the prewar intelligence leading up to the invasion of Iraq was accomplished by the Senate Select Committee on Intelligence (SSCI), which exposed significant

analytical shortcomings. [25] This extensive review highlighted that groupthink dynamics, failure to challenge key assumptions, and instances of low rigor analysis that built on previous reports without critically challenging their findings were all contributing factors that led to a misleading, low-rigor analytical assessment.[26] An additional review, the *2005 Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (The Robb-Silberman Report), confirmed the need to more thoroughly train analysts on analytical tradecraft requirements and emphasized the need for analysts to challenge assumptions through heightened analytical rigor.[27]

Recent intelligence case studies further highlight the need for increased analytical rigor. These cases include how the IC failed to predict the 2012 attacks on the U.S. Embassy in Benghazi, underestimated the 2014 rise of the Islamic State in Iraq, and failed to predict the 2014 Russian invasion of Crimea. The retrospective review of these recent examples is still ongoing and has yet to be fully evaluated. The exception is the 2014 Senate Intelligence Committee report, *S. Rpt. 113-134 Review of the Terrorist Attacks on U.S. Facilities in Benghazi, Libya, September 11-12, 2012*, which is one of seven investigations on the topic containing varying degrees of focus on the State Department and specifically Secretary Hillary Clinton's role. This particular report focuses on the analysis and actions of the IC and poor application of rigor and lack of emphasis in conducting open-source analysis.[28]

The lessons from these failures require evaluation and application to the ever-changing and challenging intelligence environment of today. Analysts should not only understand their target systems and target countries through their available collection sources; they must also be able to identify nuanced inferences and cultural undertones in their analysis. Operating in an environment of fragmented ambiguity, with undefined adversaries, they are presented with challenging and evolving problem-sets. Analysts are expected to provide thorough analysis with limited time,

scarce resources, evolving technologies, complex geostrategic conditions and extremely agile adversaries. The IC is asked to be predictive, assessing intent and understanding the probability of events that have yet to occur. The IC is operating under the pressures of ongoing, time critical wars, and is continually fighting to identify and prevent the next catastrophic event. The IC strives to be right 100% of the time, where the adversary only needs to be right once. It is a daunting challenge, which requires adaptability and agility. It is a challenge that must be approached methodically with a sustained and communicated application of analytical rigor.

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA) provided a foundational change in its mandate to establish a Director of National Intelligence (DNI) "to be responsible for ensuring that finished intelligence products produced by any element or elements of the intelligence community are timely, objective, independent of political considerations, based upon all sources of available intelligence, and employ the standards of proper analytic tradecraft".[29] IRTPA additionally mandated for the DNI to assign an individual responsible to establish processes to ensure "alternative analysis" (commonly referred to as structured analytic techniques (SATs)), and perform regular reviews of finished intelligence products in order to "draft lessons learned, identify best practices, or make recommendations for improvement to the analytic tradecraft." The Office of the Director on National Intelligence established a Deputy Director of National Intelligence for Intelligence Integration (DDNI/II) who then established the Mission Integration Division's Analytic Integrity and Standards group (AIS). The AIS was established to stimulate analytic integrity, promote rigor, encourage learning, and institutionalize tradecraft across the analytic community.[30] The ODNI's Analytic Integrity and Standards group has a unique requirement to evaluate samples of the IC's analytical products for adherence to the nine analytic tradecraft standards identified in ICD 203. To do this, AIS staff evaluators are thoroughly trained

(but not certified) to use a published rating scale to ensure that they evaluate sampled intelligence products and analysis in a fair, consistent, measured, and largely unbiased manner.

On 21 June 2007, the AIS presented a milestone effort in the publication of *Intelligence Community Directive 203, Analytic Standards* (ICD 203). ICD 203 was intended to serve as a foundational document, seeding IC training and education initiatives while promoting a culture of analytic rigor and excellence. Additionally, ICD 203 serves as the pre-production baseline, and the post-intelligence standard by which the ODNI evaluates IC analytic products. While the ICD 203 presents 14 different analytic and analytic tradecraft standards, it is a mere five and a half pages long, including introductory materials and a section outlining the DDNI//II responsibilities. ICD 203 provides the expectations of analytic standards, but does little to describe how these standards should be applied. As a compliment to ICD 203, the ODNI has published a *Rating Scale for Evaluating Analytic Tradecraft Standards*, which is primarily intended to guide ODNI evaluators in their analysis of post-production intelligence products, but also encouraged as a guide for analysts to enhance their tradecraft. As an impromptu survey to judge penetration of these ODNI initiatives, thirty professional Air Force intelligence analysts, officers and enlisted, across three unique and independent squadrons (two geospatial targeting squadrons, two cyber intelligence, reconnaissance, and surveillance squadrons, and one remotely piloted aircraft squadron) were asked if they knew of the existence of these foundational, standard setting documents; none had any awareness of ICD 203 or the rating scale, evaluation document.

With the 29 March 2016 publication of Air Force Instruction 14-133, *Intelligence Analysis* (AFI 14-133), the Air Force is set to improve organization-wide visibility of analytical standards. AFI 14-133 is the Air Force's attempt to recognize the foundational importance of analysis and to codify standards, roles, and responsibilities. It focuses primarily on Air Force level, Major Command (MAJCOM) and National Air and Space Intelligence Center roles and responsibilities.

How this regulation will translate to unit level analysis, adaption rates, and cultural change are all unknowns as it relates to the Air Force's effort to translate ICD 203's tradecraft standards across the entirety AF ISR Enterprise.

While Congressional reports have identified issues at a surface level, an abundance of additional research conducted in the timeframe since 9-11has provided both retrospective and forward thinking assessments on the state of analysis across the IC. *The 9-11 Commission Report* states that there is a, "Lack of common standards and practices across the foreign-domestic divide…holding the work—wherever it is done—to a common standard of quality in how it is collected, processed (e.g., translated), reported, shared, and analyzed…"[31] The 2008 RAND report identified "quality of intelligence" as the number one most frequently mentioned analytic concern, with 54% of respondents identifying the issue in interviews.[32] Mr. Jeffrey Cooper, a senior Central Intelligence Agency (CIA) analyst has identified the analytical pathologies that permeate all levels of analysis across the entirety of the IC.[33] He and many others have emphasized and praised the standards found in the professional practices of law, medicine, and science and offer tools, both practical and cognitive, which can be leveraged to improve the tradecraft of analysis. David Moore, career senior analysts at the National Security Agency (NSA), authored both 2007 *Critical Thinking and Intelligence Analysis* and 2011 *Sensemaking: A Structure For An Intelligence Revolution,* arguing that critical thinking needs to be woven into the process of analysis in order to maximize an analyst's ability to produce effective intelligence assessments while minimizing the potential for intelligence failures. Another prolific author in the field is Richard Heuer. Heuer, a CIA veteran whose research on structure analytical techniques (SAT) is the foundation for the Air Force's 14N Intelligence Officer analysis teachings, emphasizes separate analytical techniques that range across eight different categories of analysis, thus informing much of the research to follow.

Doctors Daniel Zelik, Emily Patterson, and David Woods from Ohio State University published two Department of Defense sponsored papers, *Understanding Rigor in Information Systems* and *Judging Sufficiency: How Professional Intelligence Analysts Assess Analytical Rigor*, which highlight the importance of analytical rigor and evaluate how sufficiency of rigor is perceived and communicated.[34] These papers explore the attributes of analytical rigor, and describe rigor as building on a process-driven approach of standardized adherence and achieved sufficiency. The researchers built an attribute-based metric to assess analytical rigor against eight unique attributes as shown in Figure 1 below.

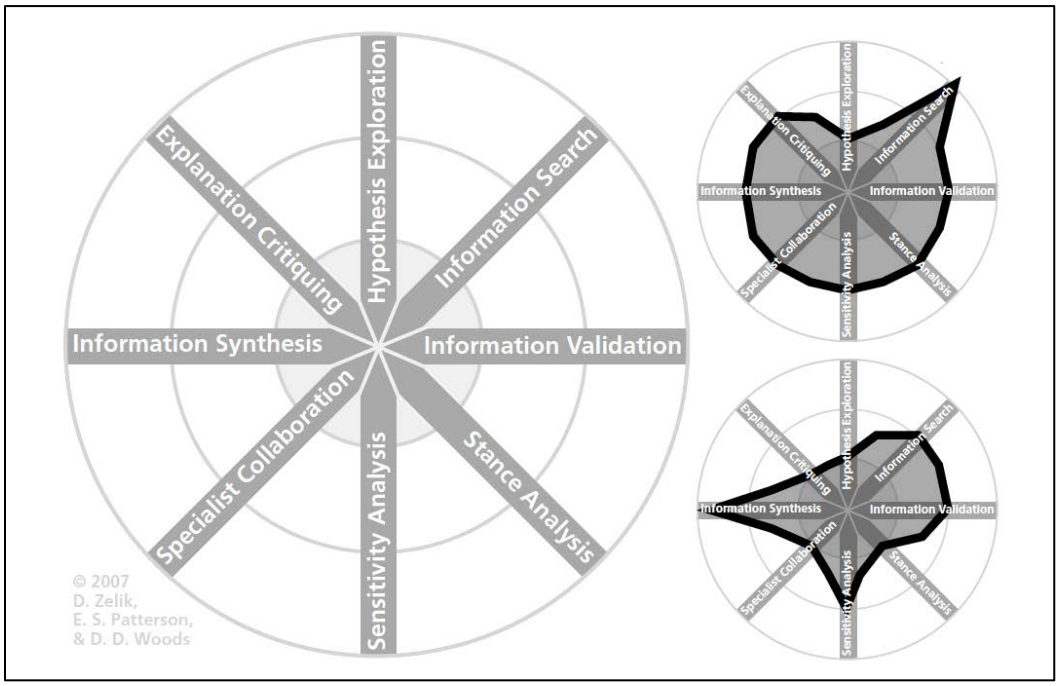


Figure 1. Visualization of Zelik, et al. Rigor Metric (Adapted from Understanding Rigor in Information Analysis, 2007)

Zelik et al. underscore the pressures driving analysts to low rigor analysis, including data rich overload and production pressure. In turn, it is extremely difficult for decision makers to recognize insufficient rigor balanced against a given decision and the consequences of failure. The above rigor metric helps frame an understanding of analytical rigor, which can be leveraged to

reduce shallow analysis by bolstering and conveying analytical rigor visually. Zelik et al. recommend a "participatory exchange model" in which the analysts and decision makers have a dialogue on analytical rigor as opposed to a one-way transfer of information. Zelik et al. apply this model to a briefing type exchange, but a logical inference would suggest that conveying analytical rigor along with written intelligence reports would also have similar value.

Advanced analysis brings a high level of analytical rigor and applied tradecraft in order to fulfill sufficiency to the above stated measurables. To achieve rigor, both critical thinking and structured analytic techniques (SATs) should be applied. Structured analytic techniques are used to challenge assessments, identify cognitive bias, stimulate creativity, and measure uncertainty.[35] SATs include mental network analysis, structured brainstorming, analysis of competing hypothesis, red hat analysis, pre-mortem analysis, devil's advocacy, and structured debate to name a few.[36] These techniques fall into broad categories like visualization, decomposition, challenge analysis, idea generation, hypothesis generation/testing, and others. SATs are a process driven approach that when combined with intuition, critical thinking, and subject matter expertise reduce analytical error and promote quality, effective, and rigorous analysis.

Section 3: SUFFICIENCY OF ANALYTICAL RIGOR

ICD 203 and Joint Publication 2-0, Joint *Intelligence* both articulate an expectation of analytical rigor required to facilitate the intelligence process, but in close review of these documents, the expected level of rigor is not specifically defined, quantified, or communicated.[37] They have not provided any process or training required to achieve this standard, nor have they provided the mechanism for analysts to communicate a measure of applied rigor. This is not to say that standards do not exist; in ICD 203 tradecraft standards are classified into five "Analytic Standards" which include nine "Analytic Tradecraft Standards."[38] ICD 203 introduces these broad

categories of expectations in just a two-page overview and goes no further.[39] A literary review quickly provides a depth of academic thought on how things like structured analytical techniques, estimative language, sourcing, assumption checks, critical thinking, alternative hypotheses exploration, should be applied, but the academic explanation does not translate well to regulatory guidance. Derived from and similar to ICD 203, AFI 14-133 again labels and categorizes analytic standards, but does little else to elaborate on the processes required to facilitate and achieve success. Additionally, AFI 14-133 uses slightly different terminology than ICD 203, showing that the Air Force's attempt to convey and uphold standards breaks down quickly as the two documents are unable to agree on which standards to uphold and how they should be labeled. For example, the Air Force has injected confusion by introducing "Tenants" in the place of ICD 203's "Analytic Standards", and using "Integrity" in place of "Independent of political consideration." To highlight the differences between ICD 203 and AFI 14-133, Table 1 below lists the standards as conveyed in the respective documents. This example shows how quickly ICD 203's standards migrated with the publication of the Air Force Instruction. How the remaining 15 members of the IC implement ICD 203's standards were not analyzed.

ICD 203 Analytic Standards	AFI 14-133 Intelligence Analysis
Analytic Standards	AF Intelligence Analysis Tenets
a. Objective	3.1.1. Objectivity
b. Independent of political consideration	3.1.2. Integrity
c. Timely	3.1.3. Synthesis
d. Based on all available sources of intelligence information	3.1.4. Collaboration
e. Implements and exhibits Analytic Tradecraft Standards, specifically:	3.1.5. Anticipation
(1) Properly describes quality and credibility of underlying sources, data, and methodologies	3.1.6. Requirements
(2) Properly express and explains uncertainties associated with major analytic judgments	AF Intelligence Analysis Standards
(3) Properly distinguishes between underlying intelligence information and analysts' assumptions and judgments	3.2.1. Timeliness
(4) Incorporates analysis of alternatives	3.2.2. Appropriate Sourcing
(5) Demonstrates consumer relevance and address implications	3.2.3. Accuracy
(6) Uses clear and logical argumentation	3.2.4. Level of Confidence
(7) Explains change to or consistency of analytic judgments	3.2.5. Assumptions vs. Judgements
(8) Makes accurate judgments and assessments	3.2.6. Analysis of Alternatives
(9) Incorporates effective visual information	3.2.7. Relevance
	3.2.8. Logical Argumentation
	3.2.9. Utility
	3.2.10. Customer Engagement

Table 1. ICD 203 Standards compared to AFI 140-133 Standards

Additionally, the AFI 14-202 *Intelligence* series provides regulatory guidance to the Air Force intelligence enterprise across three independent volumes; *Training, Standards and Evaluation*, and *General Intelligence Rules,* but does not expand upon or reference the overarching intelligence standards that have been directed by the Office of the Director of National Intelligence; ICD 203. The ODNI attempts to provide the IC with the principles of analysis through a top down application of analytical standards, but these standards do not penetrate to line unit analysts. With AFI 14-133 introducing the service to analytic standards, the regulation falls well short of defining and delineating analytical rigor. This regulation suggests to its readers that one must meet all of the standards, but fails to provide measures of success. The ODNI's *Rating Scale for Evaluating Analytic Tradecraft Standards* provides what the Air Force has failed to adapt, it acknowledges that analysis is not binary; that there are variations in quality and sufficiency. The ODNI rating scale is

intended primarily for ODNI evaluators to conduct post-production evaluations. This document provides amplified guidance for evaluators and assists them in judging ICD 203 compliance on a scale of: Poor (0), Fair (1), Good (2), and Excellent (4). ODNI evaluators provide post-production quality control for review purposes. This information is currently not shared with intelligence consumers or decision makers, thus having a tool to provide consumers a rating of effective rigor and analytic compliance, but not sharing the information. The historical failures previously discussed in this paper have shown that when decision makers perceive a sufficient amount rigor, yet the rigor is weak, it can result in catastrophic consequences.

Expected dialog between analysts and consumers is implied in the evaluation and feedback section of the intelligence process, but this feedback process has limited structure. At best, an intelligence product goes out and feedback comes back. There are many mechanisms to facilitate this type of feedback, but this does not meet the expectation of dialogue. Dialogue, as opposed to monologue, requires two-way communication. There is an expectation by the intelligence consumer that the analysis being presented is sufficiently rigorous yet there is currently no systematic mechanism or standard for an analyst to quantify, convey, and certify analytical rigor prior to publication of intelligence products. The IC's current evaluation capabilities are in compliance with the *Intelligence Reform and Terrorism Prevention Act of 2004* requirements to conduct postproduction, after action reviews. Rigor and accuracy are mutually exclusive; one does not guarantee the other. This is understood in the tradecraft, and indeed the ICD 203 analytic tradecraft standard requiring analysts to "properly express and explain uncertainties associated with major analytic judgments" was established to standardize how confidence levels and expressions of likelihood are conveyed to consumers, which is different than conveying rigor. It is safe to say that national policymakers consuming a National Intelligence Estimate would expect high rigor, where a combatant commander digesting current intelligence might accept the risk of low analytical rigor

given time constraints or limited corroboration. High rigor analysis can appropriately result in a low confidence assessment.

Section 4: PROPOSAL

This paper will analyze the impacts and costs of establishing an ODNI center of excellence, a schoolhouse designed to train and certify Masters of Analytic Tradecraft (MAT) analysts. The primary purpose of MAT analysts is to evaluate and rate intelligence products for adherence to ICD 203 *Analytic Standards* and to assess and convey analytical rigor to production analysts and intelligence consumers. The ODNI's Analytic Integrity and Standards group (AIS) currently has evaluation and rating processes that are employed to assess post publication intelligence as spot-check, quality control, and review mechanisms in accordance with section 1019 of the *Intelligence Reform and Terrorism Prevention Act of 2004*, "shall perform, on a regular basis, detailed reviews of finished intelligence product(s)."[40] MAT analysts and their evaluation capability would differ from and potentially complement existing AIS processes in that MAT analysts would 1) be embedded at the unit and organizational levels, 2) evaluate intelligence reporting prior to publication, 3) exponentially robust current efforts in manpower and capability, and 4) culturally build a cadre across the Intelligence Community that is focused of ICD 203 compliance and the adherence to analytical rigor expectations. Certified MAT analysts will be effectively trained to certify the level of analytical rigor prior to publication of intelligence publications. This certification will accompany the intelligence report in the form of a unique and branded label, thus providing a simple, standardized, and easily recognizable conveyance of analytical rigor that is stamped with the license number of the MAT analysts thus communicating an authoritative assessment of analytical rigor and adherence to ICD 203 *Analytic Standards*.

Figure 2. Proposed MAT Rating Badges (as conceptualized by the author)

Evaluations and MAT certifications of analytical rigor will be a unique capability of certified MAT analysts. Only certified MAT analysts will be empowered to evaluate and certify intelligence products. The following analysis will determine if an AIS sponsored schoolhouse, certified MAT analysts, certified intelligence products would or would not increase adherence to ICD 203 standards and improve the culture of analytical rigor across IC.

Section 5: RESEARCH METHODOLOGY

The following analysis evaluates the above proposal utilizing the following criteria:

Evaluation Criterion 1: Effectiveness

Criterion one will analyze how effective given proposals might be towards achieving the goals of promoting and conveying analytical rigor across the IC, ensuring that the rigor is standardized, and assessing how effective a given proposal might be in facilitating communication. It is recognized that given the classified nature of the materials and the limited amount of unclassified data, effectiveness will be difficult to measure.

Evaluation Criterion 2: Implementation

The proposal will be evaluated against identified barriers to implementation. Along this line, the evaluation will strive to understand and identify barriers such as training, manpower, and support requirements. From a resourcing perspective, proposals will be evaluated for cost

effectiveness and will explore resourcing implications.

Evaluation Criterion 3: Adaptation

The adaption is the final criterion by which proposed processes will be evaluated. Factors effecting adaption include consensus, leadership buy-in, cooperative elements, feasibility, target population, performance measures, and goals. Given the size of the IC, the paper will evaluate how long it will take to implement the given proposals and subsequently evaluate how long it will take to effectively penetrate the proposals to the unit level.

Section 6: ANALYSIS / EVALUATION

Evaluation Criterion 1: Effectiveness

Evaluating the certification proposal against existing processes suggests this would be an effective approach on multiple levels. By establishing a center of excellence facility to train MAT analysts under the authority of the ODNI would be another step in consolidating a fragmented analytic community that was so aptly described in the 9-11 Commission Report: "It is hard to "break down stovepipes" when there are so many stoves that are legally and politically entitled to have cast-iron pipes of their own."[41] The ODNI currently sponsors two training initiatives that can be used as a model for MAT analysts training. The ODNI's Analysis 101/201 courses are intended for relatively new analysts and focus on the fundamentals of analysis and analytical collaboration respectively. By building intelligence product evaluators who are trained and certified to evaluate on ICD 203 standards, MAT training would further promote a Joint Intelligence Community culture verses a culture of independent CIA, NSA, DIA, Air Force analysts. Cultural affiliation with independent intelligence agencies is not a bad thing as long as there is a touchstone to a larger, interconnected culture consolidated under the ODNI and its ICD 203 standards. This is inline with the 9-11 and WMD commission recommendations and meets the underlying intent of the IRTPA

when it established a Director of National Intelligence and the ODNI's responsibilities.

Having ODNI certified MAT analysts to evaluate and certify intelligence products prior to production would be an unprecedented approach at the scale that is being suggested. Current quality assurance efforts are fragmented and scatted across the entirety of the IC. As AFI 14-133 has demonstrated, ICD 203 interpretation evolves as the organizational process gets further away from the originating source. To certify MAT analysts as evaluators would consolidate the tribe and extend the ODNI's ICD 203 penetration into the disparate organizations and agencies of the IC. Given that many organizations already have standards and evaluation (StanEval) or quality control (QC) functions established, a certification process would take the same billets and efforts and align them across the IC. If an IC component wanted to exceed a given standard, there would be no resistance, but a foundational, tiered evaluation and analytical rating scale would be the baseline. Unifying the IC efforts under one recognized certification process would be healthy as it relates to establishing a feedback mechanism and evaluating and promoting analytical rigor, thus benefiting intelligence consumers and analysts alike. Having MAT evaluators certify intelligence products and share their findings would be revolutionary; for the first time giving decision makers an understanding of the quality of analytical rigor that informed the consumed intelligence products that they base their decision making processes on. This would effectively empower intelligence consumers to judge sufficiency for themselves.

Given the known analysis issues leading up the invasion of Iraq and the level of dependence of the nation's decision makers on the 2002 NIE, it is assessed that had the NIE been accompanied by a pre-production evaluation of analytical rigor and adherence utilizing today's tradecraft standards, then decision makers would have been informed on the insufficiency of process and thus demanded addition rigor. Instead, decision makers perceived rigor and falsely trusted the analysis, resulting an over two trillion dollar expense and almost 190,000 lives lost over the course of the

Iraq conflict.[42] This is not to suggest that a MAT Analysts certification alone would have prevented the war in Iraq. There were many issues identified, many of which were addressed in the 2004 IRTPA, but a MAT certification of the 2002 NIE would have been a valuable tool in communicating sufficiency of analytical rigor.

MAT evaluators would be vulnerable to error, thus requiring continued training. To carry authority, MAT analysts would need to come to this training seasoned by years of analytical experience. MAT evaluators would require currency training, and a mechanism to communicate and collaborate with senior evaluators. Evaluations would need to be reviewed for quality control and adherence to yet to be established or vetted processes.

The credentials of MAT evaluators would continually be tested. Mistakes could damage the MAT "brand" and in turn devalue the initiative. Trust in the MAT brand would require time, a consistent product, and diligent individuals all of which could be variable and undermined by missteps as the process is created.

Evaluation Criterion 2: Implementation

Implementation of a MAT analyst training and certification process will have challenges. For this analysis I assumed: 1) The course will be one month long, tripling the current Analysis 101 timeframe due to the expanded syllabus and certification requirements. 2) The class size will be twenty-five which is a typical classroom size for this type of instructor lead engagement and is also modeled after the approximate ODNI Analysis 101 class size.[43]

The barriers to implementation are training, manpower, and support requirements. For a schoolhouse to be established, facilities, instructor cadre, administrative overhead, syllabus development would all need to be established. To stand up a schoolhouse would require a significant amount of funding. Fortunately, much of this work has already been accomplished.

The ODNI's AIS already has a means for training evaluators and amplified guidance foe evaluators already exists in the form of the ODNI's *Rating Scale for Evaluation Analytic Tradecraft Standards*. Instructor cadre and infrastructure are already established at the Chantilly, VA training facility. The current efforts would need to be scaled at a cost that would require further evaluation beyond to scope of this paper. If the return on investment of the Analysis 101 course is deemed cost effective, a MAT certification would be a double down on this same investment. Most organization across the IC offer some form of analytical training, the Air Force offers such a class at Goodfellow Air Force Base. If the Air Force were to dissolve its service specific analysis training in trade for Joint, ODNI sponsored training then the cost of implementation would be negligible from the Air Force's perspective.

A 2008 RAND report on *Assessing the Tradecraft of Intelligence Analysis* recommended instituting IC-wide tradecraft training, and was quick to acknowledge both the need for and the difficulty of implementing such Community-wide training. As compared to the RAND recommendations, this proposal is surgical in its execution. One given benchmark of success is the ODNI Analysis 101 course, which has graduated over 7,000 students from over thirty different intelligence and law enforcement organizations since its conception in February of 2007.[44] A similar scale of effort would be appropriate for a MAT certification program, with the goal of providing MAT trained analysts embedded at various organizational levels.

Manpower being a valued commodity, it is not expected that additional billets funded on unit manning documents for MAT analysts. Therefore this capability and function would have to be absorbed by an already stressed of manpower. Most organizations have a section dedicated to StanEval or QC, but currently these functions are not aligned to the ODNI and ICD 203 analytic standards. For implementation to be successful, IC elements would have to shift current StanEval and QC functions to align with ODNI direction. In many ways this would require disparate

elements across the IC to defer some control to the ODNI, which would be politically challenging. For example, AFI 14-133 defines the Air Force's established analytic standards, which differ from established ODNI standards. For this proposal to be successful, Air Forces standards would have to defer to ODNI standards. The Air Force could implement higher standards if it chooses, but could not relax those standards without the consent of the ODNI.

Instead of forcing MAT certified analysts upon the entirety of the IC, one implementation approach would be to offer MAT certification as an enhancement to current unit level processes. IC organizations that elect to invest in and train MAT certified analysts would then be allowed to self-evaluate and certify their intelligence products with the branded MAT certification badges offered above. Those organizations electing to opt out would not be able to certify their products.

Evaluation Criterion 3: Adaptation

Given the exclusive and unique qualities of the MAT analyst's ability to evaluate and label intelligence with branded rating labels, it is possible that once intelligence consumers become aware of MAT certification, they would be a driving force in encouraging implementation, but this is a currently an unknown demand. It is foreseeable that reporting intelligence agencies would want this capability as a way to laud their own due diligence and adherence to ODNI established processes. It is also foreseeable that intelligence consumers, once educated on the MAT certification program, will push for the intelligence products that they consume to be pre-evaluated and MAT rated for rigor and standard adherence. Given that MAT certification is additive in nature, resistance from intelligence consumers is not likely, but since the burden of certifying products falls to the intelligence producers it is foreseeable that analysts and organizations would push back if they are unable to see the value. If MAT certification were to become coveted by senior analysts and organizational leaders, then buy-in from both analysts and decision makers

would be likely.

A phase-in approach would provide minimal risk on investment, with scale and IC penetration growing as MAT analysts obtain certification and initiate the evaluation of their organization's intelligence assessments. It is foreseeable that once products are accompanied by analytical rigor ratings, intelligence consumers will request the highest ratings possible of the products they are digesting. When MAT ratings fall below the intelligence consumer's sufficient requirements for analytic rigor this could facilitate further and potentially healthy dialogue between IC components and consumers concerning such topics as resources, capabilities, time requirements, collection, analysis and depth of expertise.

Adapting MAT certified analysts would not require day one, mass, IC-wide adaptation. A measured and steady implementation of the proposal would be a feasible. No changes to the current intelligence process would be required with MAT certification being an additive supplement to established baseline intelligence production. Minimal penetration could still present positive results. Success would beget success. If MAT analysts conducting per-publication evaluations proves to be a failure, then the investment lost would be measured and relative to the number of graduates. The first year of implementation could be considered a beta, proof of concept, thus further managing expectations as some of the trial and error implementation is worked out.

Where establishment of MAT analysts would robust existing processes, the cultural change and adaptation across 17 unique IC organizations and agencies would be difficult. ODNI directives would need to be written and enforced to ensue IC-wide adaptation. It has taken multiple congressional investigations and the passing of the 2004 IRTPA to get to the two and a half pages of analytic standards outlined in ICD 203, to see MAT certification fully adapted would require more that IC-wide buy-in, it would require mandated adherence.

Section 7: RECOMMENDATIONS

Modeling after the civilian sector's U.S. Green Building Council's (USGBC) Leadership in Energy and Environmental Design (LEED) program and borrowing from the medical and legal professions, it is recommended that the ODNI establish a certification board process to credential analysts as Masters of Analytic Tradecraft (MAT). MAT analysts would be certified to employ the ODNI's analytic rating scale, evaluate analytic products, and certify the rigor of those products prior to publication. To become MAT certified, analysts would need to attend a centralized training schoolhouse. This center of excellence would be sponsored by the ODNI, thus being joint in nature and linked across the IC. Having this level of consolidated analytical tradecraft training at the top of the IC, with a joint cadre of senior analysts teaching curriculum would be a top down approach currently lacking in the IC. Graduation would require the passing of a board style examination. Although ICD 203 has provided unifying direction, it is this author of this paper's opinion that resultant training opportunities continue to be disjointed, stove-piped, and fragmented across agency lines, resulting in poorly disseminated standards and divergent lines of effort. An IC, enterprise-wide analytical center of excellence is needed to raise the focus on analysis and analytical tradecraft. This schoolhouse would be the driving force behind standards, collaboration, continued learning, the sharing of best practices, quantifying and communicating analytical rigor, and certifying MAT analysts.

The curriculum of MAT certifying course would be focused on both the application and the evaluation of analytic tradecraft standards. This would be different from existing agency and service specific analysis training courses in that MAT analysts would graduate uniquely certified as Office of the Director of National Intelligence analytic tradecraft evaluators and thus able to evaluate assessments and rate associated analytical rigor. This would take what is currently a post report quality control spot check that is conducted by a small portion of ODNI staff and turn it into

an IC, enterprise-wide self-evaluation of analytical rigor that happens prior to an intelligence report ever being published.

By establishing a certification process, a MAT analyst would be trained and empowered (by virtue of their unique ODNI certification) to uphold established standards. Quantifying and evaluating the level of analytical rigor that informed an organization's assessment and publishing the resultant rating in the intelligence report will inform decision makers the amount and quality of analytical rigor that informed the analysis upon which they are trusting. It is then intelligence consumer's responsibility to determine if the rated level of rigor is sufficient for their needs. Due to the overt evaluation of intelligence products, this rating system would award analysts to strive for high levels of rigor.

It is recommended that the IC mimic the LEED model, certifying MAT analysts to evaluate their assessments for analytical rigor and standardization by applying their training and utilizing the ODNI's *Rating Scale for Evaluating Analytic Tradecraft Standards*. The resultant evaluation findings would accompany the assessment. This rating could only be given by certified MAT analysts and would be branded in a standardized way as to convey the amount of analytical rigor that went into the published intelligence report. Similar to how USGBC uses LEED certifications to convey a level of environmental performance and adherence to standards and established practices, so would MAT certification convey a level of analytical rigor to the intelligence consumer. In the case of analysis, MAT analysts would measure and certify rigor using the ODNI rating scale, and convey the findings utilizing a conformed branding scale. Departing from the current ODNI scale of poor, fair, good, and excellent, the badges displayed above (Figure 1) envision a level one through four criteria with level one equating to low rigor and building up to a level four which would equate to excellent rigor. Similar to how a licensed engineer might stamp their work with a seal containing their license number, so it is recommended that MAT analysts

certify their evaluations by including their assigned MAT number.

Currently ODNI encourages analysts across the IC to become familiar with the ODNI rating scale as a way to enhance analytic tradecraft. The MAT certification proposal goes much further, intensively training MAT analysts to be evaluators of ICD 203 analytic tradecraft standards, having intelligence reports assessed for analytical rigor before publication, communicating that rigor to intelligence consumers, and providing an immediate feedback loop to the analysts who are presenting their analysis. By embedding MAT analysts at the unit level and connecting them to the intelligence production process, the ICD 203 standards would be effectively pushed down and permeated across the IC.

An additional requirement to maintain MAT certification would be to complete and track continuing education (CE). Keeping with the LEED model, MAT analyst would be required to earn 30 CE hours every two years.[45] Qualifying CE opportunities would be defined and tracked by ODNI's Analytic Integrity and Standards group and thus ensure currency and proficiency of MAT analysts.

Additional benefits of establishing MAT certified analysts would be the duel hatted nature of these analysts as both evaluators of analytic products and as embedded subject matter experts expected to act as analysis tradecraft instructors and leaders. MAT analysts would provide advanced unit level instruction on ICD 203's nine analytic tradecraft standards. Beyond their individual instructor roles, a community of close-knit MAT analysts would be developed, thus facilitating effective cross talk and communication. ODNI would use MAT analysts to maintain dialogue, convey best practices, provide feedback avenues, disseminate time sensitive bulletins, build and maintain unit level libraries, capture and convey tactics, techniques, and procedures as they pertain to analysis, and provide analytical experts who conduct post-product after action reviews and assess where analysis went right and where it came up short. MAT analysis will be

unit and organizational level focal points, ensuring ICD 203 integration and coordination. MAT analysts could also fill an advisory role to intelligence production commanders and leaders, ensuring that the need for analytical rigor has a voice amongst the myriad of competing force: manning, resources, and production rates, to name a few. Additionally, MAT analysts could liaise between intelligence consumers and production analysts to ensure feedback is provided and absorbed.

In addition to the civil sector professions that require certification (doctors, lawyers, engineers, LEED associates, etc.), the Air Force's Weapons Instructor Courses (WIC) provides another model, which could be adapted by the ODNI and applied to MAT certification. The Air Force's WIC prides itself on its ability to develop an institutional pool of tactical and operational experts.[46] Embodying a creed of "humble, approachable and credible" the aggregate of WIC graduates form a fraternity of trusted experts and valued problem-solvers.[47] Upon completing an intensive, graduate-level curriculum, Air Force WIC graduates integrate at the unit level and provide a wide spectrum of academic and advisory support. They facilitate the collection of tactical level knowledge and use it to inform and author tactical doctrine. This collective of the Air Force's best weapon's officers forms a self-aware, continually improving, and always communicating trust of knowledge that both informs and enables best practices across the multi-domain tactical environments in which the Air Force fights.[48]

In this same vein, but transcending any one service or agency, MAT analysts would be ODNI trained and credentialed, providing unit and organizational level experts in analytical tradecraft and informing and upholding ICD 203's standards of analysis. Empowered as evaluators of analytical rigor, MAT analysts would rate assessments utilizing the afore-mentioned branded rating system, to ensure and convey rigor while concurrently fulfilling the roles of trainer and trusted advisor.

Notes

(All notes appear in shortened form. For full details, see the appropriate entry in the bibliography)

[1] Zelik et al., "Understanding Rigor in Information Analysis," 1.
[2] Ibid.
[3] JP 2-0, *Joint Intelligence*, I-22.
[4] Zelik et al., "Understanding Rigor in Information Analysis," 3.
[5] Johnson, *Analytic culture in the US Intelligence Community: An ethnographic study*, 7.
Cooper, *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis.* 4.
[6] CIA, *A Tradecraft Primer*, 3.
[7] U.S., *WMD Commission Report*, opening letter.
[8] Zelik, et al., "Judging Sufficiency: How Professional Analysts Assess Analytical Rigor."
[9] Sutherland, "Does certification improve medical standards?"
[10] USGBC, http://www.usgbc.org/about
[11] Keck, "US Intelligence Community: The World's 4th Largest Military?"
Priest, "A Hidden World, Growing Beyond Control."
[12] Rosenbach, *Confrontation or Collaboration?* 11.
[13] Cooper, *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*, xx.
Bartholomees, *The U.S. Army War College Guide to National Security Issues: Volume II: National Security Policy and Strategy, 5th Edition*, 133.
RAND, *Assessing The Tradecraft Intelligence Analysis*, xi.
[14] RAND, *Assessing The Tradecraft Intelligence Analysis*, xi.
JP 2-0, *Joint Intelligence*, xx.
[15] Zelik, "Understanding Rigor in Information Analysis," xx.
[16] RAND, *Assessing The Tradecraft Intelligence Analysis*, 1.
[17] Ibid.
[18] JP 2-0, *Joint Intelligence*, I5.
[19] Pigg, "Common Analytic Standards: Intelligence Community Directive # 203 and U.S. Marine Corps Intelligence." http://smallwarsjournal.com/jrnl/art/ic-directive-203-and-usmc-intelligence
[20] Ibid.
[21] Cooper, *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*, 3.
[22] CIA, *A Tradecraft Primer*, 3.
[23] *The Performance of the Intelligence Community, Staff Statement No. 11*, 3.
[24] IRTPA, sec. 1001 – sec. 1020.
[25] SSCI, U.*S. Intelligence Community's Prewar Intelligence Assessments on Iraq*.
U.S., *WMD Commission Report*.
[26] SSCI, *U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*.
Rosenbach, *Confrontation or Collaboration?*, 38.
[27] U.S., *WMD Commission Report*, 12.
[28] U.S. Senate Report, *Review of the Terrorist Attacks on U.S. Facilities in Benghazi, Libya*.
[29] IRTPA, c. 1001 – sec. 1020.
[30] *Intellipedia*, "Office of the Assistant Deputy Director of National Intelligence for Analytic Integrity and Standards."
[31] *The 9/11 Commission Report*, 409.

[32] RAND, *Assessing The Tradecraft Intelligence Analysis*, 11.
[33] Cooper, *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*.
[34] Zelik, "Understanding Rigor in Information Analysis."
Zelik, "Judging Sufficiency: How Professional Analysts Assess Analytical Rigor."
[35] CIA, *A Tradecraft Primer*, 2.
[36] Heuer, *Structured Analytic Techniques for Intelligence Analysis*.
[37] ODNI, ICD 203.
JP 2-0, *Joint Intelligence*.
[38] ODNI, ICD 203.
[39] Ibid.
[40] IRTPA, sec. 1019.
[41] *The 9/11 Commission Report*, 403.
[42] Trotta, "Iraq war costs U.S. more than $2 trillion: study."
[43] *Intellipedia*, "Analysis 101."
[44] *Ibid*.
[45] USBCG, "Credential maintenance."
[46] Nellis AFB, "United States Air Force Weapons School."
[47] Ibid.
[48] Ibid.

BIBLIOGRAPHY

A Tradecraft Primer: Structured Analytic Techniques for Improving Intelligence Analysis. Washington, D.C.: U.S. Central Intelligence Agency, Center for the Study of Intelligence, 2009.

Bartholomees, J. Boone., Jr. *The U.S. Army War College Guide to National Security Issues: Volume II: National Security Policy and Strategy, 5th Edition*, Carlisle, PA : Strategic Studies Institute, U.S. Army War College, June 2012.

Cooper, Jeffrey R., *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis.* Washington, DC: Center *for the* Study *of* Intelligence, 2005.

Dahl, Maj Arden B., *Command Dysfunction: Minding the Cognitive War*. Maxwell Air Force Base, AL: Air University Press, 1998.

Folker, MSgt Robert D., Jr. "Intelligence Analysis In Theater Joint Intelligence Centers: An Experiment In Applying Structured Methods." Occasional Paper no 7. Bolling AFB, Washington, DC: Joint Military Intelligence College, 2000.

Hall, Wayne H., and Gary Citrenbaum, *Intelligence Analysis: How to Think in Complex Environments*. Santa Barbara, CA: Praeger Security International, 2010.

Heuer, Richards J., Jr., and Randolph H. Pherson. *Structured Analytic Techniques for Intelligence Analysis.* Thousand Oaks, CA: CQ Press, 2014.

Intelligence Community Directive (ICD) 203. *Analytic Standards*, Office of the Director of National Intelligence (ODNI), 2 January 2015.

Intellipedia contributors, (Unclassified) "Office of the Assistant Deputy Director of National Intelligence for Analytic Integrity and Standards," *Intellipedia*. (accessed April 2016)

Intellipedia contributors, (Unclassified) "Analysis 101," *Intellipedia*. (accessed April 2016)

Johnston, Rob, *Analytic Culture in the US Intelligence Community: An Ethnographic Study.* Washington, DC: Center *for the* Study *of* Intelligence, 2005.

Joint Publication (JP) 2-0. *Joint Intelligence*. 22 October 2013.

Keck, Zachry. "US Intelligence Community: The World's 4th Largest Military?" The Diplomat, 30 August 2013. http://thediplomat.com/2013/08/us-intelligence-community-the-worlds-4th-largest-military/

Moore, David T., "Critical Thinking and Intelligence Analysis." Occasional Paper no 14. Bolling AFB, Washington, DC: National Defense Intelligence College, 2007.

Moore, David T., *Sensemaking: A Structure For An Intelligence Revolution*. National Defense Intelligence College, Washington, DC: NDIC Press, 2011.

Nellis Air Force Base, "Fact Sheets: United States Air Force Weapons School." http://www.nellis.af.mil/AboutUs/FactSheets/Display/tabid/6485/Article/284156/united-states-air-force-weapons-school.aspx

Pigg, LTC Von H. "Common Analytic Standards: Intelligence Community Directive # 203 and U.S. Marine Corps Intelligence," *Small Wars Journal*, June 16, 2009. http://smallwarsjournal.com/jrnl/art/ic-directive-203-and-usmc-intelligence

Priest, Dana, and William M. Arkin. "A Hidden World, Growing Beyond Control," Top Secret America: A Washington Post Investigation, 2010. http://projects.washingtonpost.com/top-secret-america/articles/

Rosenbach, Eric, and Aki J. Peritz. *Confrontation or Collaboration? Congress and the Intelligence Community*. Cambridge, Mass: The Belfer Center, Harvard University, June 2009.

Senate Select Committee on Intelligence (SSCI), *Review of the Terrorist Attacks on U.S. Facilities in Benghazi, Libya, S. Rpt. 113-134*, Washington, D.C.: 123th Congress, July 2004.

Senate Select Committee on Intelligence (SSCI), *U.S. Senate Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*, Washington, D.C.: 108th Congress, 7 July 2004.

Sutherland, Kim, and Sheila Leatherman. "Does certification improve medical standards?" *British Medical Journal*, BMJ 2006;333:439, 24 August 2006. http://www.ncbi.nlm.nih.gov/pmc/articles/PMC1553526/

The 9/11 Commission Report: Final Report of the National Commission on Terrorist Attacks upon the United States. Official Government Edition: U.S. Government Printing Office Washington D.C., 22 July 2004.

The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (The Robb- Silberman Report), *Report to the President of the United States*, Washington, DC: WMD Commission, 31 March 2005.

The House Permanent Select Committee On Intelligence, and The Senate Select Committee On Intelligence, *Joint Inquiry into Intelligence Community Activities Before and After the Terrorist Attacks of September 11, 2001*, S. REPT. NO. 107- 351 and H. REPT. NO. 107-792, Washington, D.C.: 107th Cong., 2d sess., December 2002. http://fas.org/irp/congress/2002_rpt/911rept.pdf

The Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Public Law 108-458, 108th Cong., 2d sess., 17 December 2004.

The Performance of the Intelligence Community Staff Statement No. 11. Washington, D.C.: National Commission on Terrorist Attacks upon the United States, 2004.

Treverton, Gregory F., and C. Bryan Gabbard. *Assessing the Tradecraft of Intelligence Analysis,* RAND Technical Report. Santa Monica, CA: RAND, 2008.

Trotta, Daniel. "Iraq War Costs U.S. More Than $2 Trillion: Study," *Reuters*, 14 March 2013. http://www.reuters.com/article/us-iraq-war-anniversary-idUSBRE92D0PG20130314

U.S. Green Building Council (USBCG). "Credential maintenance." http://www.usgbc.org/help-topic/credential-maintenance

United States. Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction: Report to the President of the United States.* Washington, D.C.: Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction, 2005.

Zelik, Daniel, Emily S. Patterson, and David D. Wood. "Judging Sufficiency: How Professional Intelligence Analysts Assess Analytical Rigor," Department of Defense Research no. BAA-001-04. Paper presented at the Human Factors and Ergonomics Society 51st Annual Meeting. Baltimore, MD. October 2007.

Zelik, Daniel, Emily S. Patterson, and David D. Wood. "Understanding Rigor in Information Analysis." Proceedings of the Eighth International NDM Conference (Eds. K. Mosier & U. Fischer). Pacific Grove, CA, June 2007.

This Page Is Intentionally Left Blank

NATIONAL INTELLIGENCE UNIVERSITY

USING INDUSTRY ANALYSIS FOR STRATEGIC INTELLIGENCE

Capabilities and Strategic Intent

Chuck Howe

DISCUSSION PAPER NUMBER 17

USING INDUSTRY ANALYSIS FOR STRATEGIC INTELLIGENCE

Capabilities and Strategic Intent

by Chuck Howe

National Intelligence University
Washington, DC

January 2015

Using Industry Analysis for Strategic Intelligence: Capabilities and Strategic Intent

In Chuck Howe's *Using Industry Analysis for Strategic Intelligence: Capabilities and Strategic Intent*, the author argues that the Intelligence Community should evaluate globalization as a strategic factor affecting interdependencies between nations. He outlines a variety of industry analysis techniques—including the Five Forces Model, the External Environment Model, and the Value Chain Model—that could be valuable to analysts. Using the semiconductor industry as a case study, Howe illustrates methods that analysts should use in deriving strategic insights from industrial capability.

Using Industry Analysis for Strategic Intelligence is part of the National Intelligence (NI) Press Occasional Paper Series. Occasional Papers examine topics of unique value to the Intelligence Community.

The goal of the NI Press is to publish high-quality, valuable, and timely books on topics of concern to the Intelligence Community and the U.S. government. Books published by the NI Press undergo peer review by senior officials in the U.S. government and by outside experts.

This publication has been cleared for unrestricted distribution. The views expressed in this publication are those of the author and do not necessarily reflect the official policy or position of the Department of Defense, the Intelligence Community, or the U.S. government. Authors of NI Press publications enjoy full academic freedom, provided that they do not disclose classified information, jeopardize operations security, or misrepresent official U.S. policy. Such academic freedom empowers authors to offer new and sometimes controversial perspectives in the interest of furthering debate on key issues. This publication is subject to Title 17, U.S. Code, Sections 101 and 105. It is in the public domain and may not be copyrighted.

How to order this book: Everyone may download a free electronic copy from our website at *http://www.NI-U.edu.* U.S. government employees may request a complimentary copy by contacting us at *Press@ni-u.edu*. The general public may purchase a copy from the Government Printing Office (GPO) at *http://bookstore.gpo.gov.*

Editor, NI Press
Office of Research
National Intelligence University
Defense Intelligence Agency
Joint Base Anacostia-Bolling
Washington, DC 20340-5100

ACKNOWLEDGMENTS

First and foremost, I thank Jeff Stillman, in the Office of Analytic Integrity and Standards, for leaving my fellowship research proposal on the "stack" for consideration by the ODNI Exceptional Analyst Fellowship selection committee. Even though I am not an intelligence analyst, he recognized the value of a different perspective, and throughout encouraged my project.

Also critical to the existence of this project was the support of my leadership in AT&F, especially Wally Coggins, to gap my position for the year and allow me the time to research, write, and produce this introduction to industry analysis for the analytic community.

Many thanks to current and former faculty members at the Industrial College of the Armed Forces (now Dwight D. Eisenhower School for National Security and Resource Strategy). There are several war colleges in the Department of Defense, but only one Industrial College. Drs. Linda Brandt and Rich Shipe reviewed my research proposal and spent even more of their time to provide an outside review of the manuscript. When I was a student at ICAF many years ago, Dr. Gerald Abbott introduced me to the primary sources on industry structure economics and analysis; I appreciate his continuing mentorship in this subject area. Last, but not least, CAPT Susan Maybaumwisniewski, USN (ret.), a former colleague at ICAF, now at BENS, provided early brainstorming and outline direction to this project—a wonderful person to kick an idea around with.

I would be remiss if I did not mention the semiconductor industry that I have followed for the last six years. There are no better representatives than the outstanding people at SEMI and EDAC. They are exemplars of an industry that is always willing to educate others on the challenges they face at the leading edge of this global industry.

I started my understanding of the analytic community by taking Analysis 101 and Open Source Academy courses. It was great meeting the "up-and-coming" crop of intelligence analysts, and they showed me they had the wherewithal to try new analytic methods. Outside of the classroom, the development of the industry analysis methodology was aided immeasurably by the meetings with analysts across the Intelligence Community. At each of meetings I would repeat

the mantra "industry analysis models are a tool, not a solution," to assure the analyst I was looking to complement their analytical skill set. Intelligence analysts remain the target audience for this book, and it is hoped that they will add it to their toolkit.

In my travels across the analytic community, I came upon a small but very productive team at the Institute for Analysis. They listened to and critiqued several iterations of my project, and their director, Donn Treese, even provided an outside review of the manuscript.

Dr. Cathryn Thurston, the acting vice president of OOR, provided unflagging support to this book, even when that support had to compete with construction projects, the relocation of the office, staff departures to early retirements, and the never-ending lineup of master's thesis aspirants at NDIC (now NIU). Her editorial direction on draft submissions kept my initial intent intact, while greatly improving its delivery.

Finally, I want to recognize my wife, Cindy, an extraordinary teacher, for her unfailing support throughout this endeavor. Thank you, Cindy.

Contents

Chapter One: Introduction 1
Organization of Discussion 3
Background 3
Globalization and National Competitiveness 3
Role of Intelligence Community: 1950s to 1980s 4
Moving Intelligence Community Out of Its Comfort Zone 6
Competing Analysis: Short-Term Crises and Long-Term Problems 7
Chapter Two: Industry Analysis 9
Overview of Financial Activity of Firm 10
Porter Five Forces Model 11
External Environment Model 14
Value Chain Model 16
Chapter Three: Putting It All Together—The Five Steps 21
Step 1: Select the Industry 21
Step 2: Define the Industry 23
Step 3: Identify Sources of Information 27
Step 4: Collect Information 29
Industry Observations from Data Collection 32
Step 5: Analyze Results 52
East Asia: Semiconductor Industry 52
Strategic Intelligence Insight 58
Chapter Four: Conclusion 69
Conclusion 69

Contents continued

Applying Industry Analysis 69
Follow the Steps 69
Utility of Industry Analysis 70
Increased Attention by the Intelligence Community to Globalization 71

APPENDIXES

Appendix A: External Environment Model Segments and Elements 73
Appendix B: Semiconductor Industry Tutorial 75
Appendix C: Information Sources Specific to Semiconductor Industry 89

BIBLIOGRAPHY 95

ABOUT THE AUTHOR 123

Chapter One

Introduction

The U.S. Intelligence Community needs to augment its primary focus on political and military dimensions to address the potential for strategic surprise due to the changing nature of business, industry, and national competitiveness in a global economy. The Council on Competitiveness, a nonpartisan, nongovernmental organization of American chief executive officers, university presidents, and labor leaders, highlights the complex nature of these changes (see box).[1]

Lens of Competitiveness

A rising standard of living for all Americans is not guaranteed. The United States now operates in a truly global economy:

- Companies are outsourcing and spreading their value chains globally
- Hundreds of nations are trading tens of trillions of dollars daily in the financial markets
- Strong markets and talent pools have emerged in the developing world
- Businesses and governments operate across highly integrated regional economies
- Vast communications networks allow for immediate global connectivity and information transfer and also create unprecedented vulnerabilities
- New risks, such as competition for natural resources, climate change and terrorism, now affect the competitiveness of countries, companies, and communities

Whether our citizens and businesses will thrive in the new global economy depends largely on our ability to understand and act upon these prevailing forces of change and attract high-value economic activity to regions across America.

Source: Council on Competitiveness, *www.compete.org*.

The opening observations from the Council on Competitiveness highlight the major strategic shifts in a *global* economy and their importance to our country. The developing economies of the world are driving these shifts, and their industrial capability is a major component of their success. Analyzing an industry in another country or region of the world can yield strategic insights about a nation's capabilities and strategic intent.

While the U.S. Intelligence Community is aware of the discussion, as evidenced in the 2009 *National Intelligence Strategy*, it still needs to pay closer attention to the strategic implications of these changes. In particular, intelligence analysts must be able to gauge the global competitiveness of other nations in order to ensure that this dimension is a consideration in strategic assessments.

A key indicator of competitiveness is industrial capability. A nation's industrial capability is an economic engine, producing jobs, growth, and ultimately prosperity. Developed and developing nations realize this and want to build an industrial engine to reap the benefits. Relatively recent advances in information technology that produce unprecedented amounts of open-source information help these nations.[2] Business strategists and competitive intelligence professionals use many analysis tools to mine the plethora of open sources—to understand the plans and intentions of other firms and the global market—so that they can achieve a competitive advantage.

Although the Intelligence Community is not collecting information on individual businesses, it is interested in national- or regional-level plans and aspirations. To shed light on sometimes-opaque economic plans and strategic intentions, the all-source intelligence analyst can use open-source data, industry analysis tools, and a nation's interest in growing its economy.

In short, a nation's policy and investment decisions to grow and sustain its industrial capability are visible through their interactions with industry. The thesis of this book is that an all-source intelligence analyst can employ the analysis tools of business strategists and competitive intelligence professionals to develop strategic intelligence insights regarding a nation's plans and intentions.

Organization of Discussion

To support the thesis and intelligence focus of this book, the remaining chapters of this book are all oriented toward the all-source analyst. The book consists of four chapters. This first chapter provides general background information, to help orient the reader. Chapter 2 introduces industry analysis and proposes a methodology for application in the Intelligence Community. Chapter 3 describes the five steps an all-source analyst would go through to provide inputs for an intelligence assessment. Chapter 4 presents concluding discussions on the value of industry analysis to the U.S. Intelligence Community. There are also three appendixes. Appendix A provides a template for one of the industry analysis models presented in Chapter 2. Appendixes B and C, respectively, provide a semiconductor tutorial, as well as information related to the semiconductor industry—of use in understanding the discussion in the main chapters.

Background

Before starting our discussion of industry analysis and its application, there are two personal observations operating in the background.[3] The first is that globalization and its potential for strategic impact on national competitiveness has not yet grabbed the full attention of the Intelligence Community. The second observation concerns the Intelligence Community's grasp of other nations' industrial capabilities; outside of leading-edge science and technology, defense issues, dual-use technologies, and nonproliferation, the Intelligence Community is largely silent. The following two subsections briefly provide the background for these observations.

Globalization and National Competitiveness

The term *globalization* has many definitions. Suzanne Berger, in her book *How We Compete: What Companies around the World Are Doing to Make It in Today's Global Economy*, describes globalization as "the acceleration of the processes in the international economy and in domestic economies that operate toward unifying world markets."[4] These changes and the domestic concerns they cause are not unprecedented. There was an earlier period bracketing the

turn of the nineteenth century that also saw the same levels of capital mobility, trade, and immigration among countries. This early period of globalization was broken by World War I, and it was not until the 1980s that the world economy returned to the same high levels of capital mobility, foreign direct investment, and trade. An important point regarding the end of this earlier period of globalization is that nations were largely able to shut off their ties to the outside world (from the 1920s through the 1980s) and continue economic growth.

Role of the Intelligence Community: 1950s to 1980s

A look at the history of the Intelligence Community, specifically foreign economic intelligence during the Cold War, reveals that one of the stated purposes, "To assist in divining the intentions of potential enemies in the conviction that how they act in the economic sphere is likely to reveal intentions," generated a lot of support for industry-sector analysis.[5]

This initial interest in industry-sector analysis in the early years of the Cold War was also due to a sense among policymakers that the Soviet Union could possibly outperform the United States economically and militarily.[6] To address this concern, the Central Intelligence Agency devoted considerable analytical resources to industry studies. These studies of selected sectors are characterized as assessing

> the strengths, weaknesses, and prospects of these sectors in detail and on a continuing basis. These studies generally had a special focus on the technological level of the given industry. They supported not only intelligence objectives but, as contributions to publications of the Joint Economic Committee of Congress, contributed to the general pool of knowledge on the Soviet economy.[7]

These analyses focused on vulnerabilities in the Soviet economy and, especially, areas where progress could hamper their economic development. As the Cold War progressed, increasing emphasis on international and military topics resulted in the transfer of analyst resources away from Soviet economic performance and specific industry-sector analysis of the Soviet Union.[8]

While it is clear that globalization and the practice of industry analysis by the Intelligence Community are not unprecedented, what has been the role of the Intelligence Community in more recent experience? Michael L. Dertouzos, Richard K. Lester, and Robert M. Solow, a group of MIT researchers, made this prediction in their 1989 book, *Made in America*:

> To live well, a nation must produce well. In recent years many observers have charged that American industry is not producing as well as it ought to produce, or as well as it used to produce, or as well as the industries of some other nations have learned to produce. If the charges are true and if the trend cannot be reversed, then sooner or later, the American standard of living must pay the penalty.[9]

Mark Lowenthal describes the corresponding debate in the Intelligence Community at that time:

> During the late 1980s some people maintained that several of these issues (overseas competitiveness, trading relations, foreign economic espionage, **industrial espionage** undertaken by businesses, and possible countermeasures) could be addressed, in part, through a closer connection between intelligence and U.S. businesses [emphasis in original]. Few advocates of closer intelligence–business collaboration, however, had substantial answers for some of the more compelling questions that it raised (which is one reason that this approach was quickly rejected).[10]

This description is the most up-to-date open-source assessment of the Intelligence Community's consideration of industry analysis. In 2006, Suzanne Berger, who was a major contributor to the work of Dertouzos et al., the MIT group that provided important observations and prescriptions in *Made in America*, released the book *How We Compete*. In it, Berger observed that all of the industry prescriptions they had made in 1989 had become the basic operating code of American companies. But Berger also said, "[A]mong our greatest concerns today is one that was not on the list in the 1980s—how to make good companies and good jobs stick in the United States."[11] She further observed:

> Then, our challenge seemed to be import penetration. Today, the fragmentation of the system of production has changed the problem. Now it's the prospect that the resources available to companies abroad—and well-educated and lower cost workers are one of the main attractions—will induce businesses to shift their activities abroad.

Globalization is upon us, and, unlike the early twentieth century, nations cannot "turn it off" and build or sustain industrial capability.

Moving the Intelligence Community Out of Its Comfort Zone

The Intelligence Community's internal discussions in the 1980s about sharing intelligence with business to foster our national competitiveness should not be confused with what is being advocated here—the development of strategic intelligence insights from understanding the development of industrial capability *in other nations* and the consideration of these strategic insights in producing intelligence products for our national policymakers. Although globalization is all around us, the *National Intelligence Strategy* fails to push the Intelligence Community out of the traditional political-military sphere.[12] As Fareed Zakaria observes of America's traditional perspective, "At the political-military level, we remain in a single-superpower world. But in every other dimension—industrial, financial, educational, social, cultural—the distribution of power is shifting, moving away from American dominance."[13]

To be fair, the Intelligence Community is not ignoring globalization; it is just not actively pursuing it. But a closer look at the first of its four strategic goals in the 2009 *National Intelligence Strategy*, "Enable wise national security policies," could provide an avenue for collection and analysis of trends in globalization.[14] In support of that goal, the Intelligence Community further explains it "will provide policymakers with strategic intelligence that helps them understand countries, regions, issues, and the potential outcomes of their decisions. We will also provide feedback to policymakers on the impact of their decisions."[15] So, if the Intelligence Community is aware of globalization and one of its strategic goals could support analysis of global trends, what is the argument for operating outside its spheres of comfort by taking a closer look at other nations' industrial capability?

Competing Analysis: Short-Term Crises and Long-Term Problems

We cannot ignore that the Intelligence Community is heavily engaged in our nation's current overseas military commitments. Plus, the Intelligence Community is also charged with addressing transnational issues, such as criminal organizations, failed states, ungoverned spaces, the global economic crisis, climate change, energy competition, rapid technological change, and dissemination of information.[16] But the main question of this book is: who in the Intelligence Community is monitoring the industrial capabilities of other nations and regions, which may have a major impact on American interests and security?

While the National Intelligence Council provides a forecast of economic changes occurring over the next 15 years, these observations are based on general trends forecasting major economic shifts, strategic materials, and energy.[17] Outside of the Intelligence Community, there is already recognition of the need for new tools to understand and communicate the nature of global economic integration. Timothy Sturgeon highlights that "studies that rely solely on macro-level statistics such as trade and investment cannot help but render invisible the detailed contours of the world economy."[18] The main point here is that while statistics and analysis on global economic information are readily available for purchase over the Internet, there is also strategic intelligence of interest to the Intelligence Community and policymakers in the "contours." The tools and methods used by industry analysts highlighted in the following chapters will enable the all-source analyst to see some of the contours in the world economy and gain strategic intelligence insights of use to national policymakers.

The opening observations from the Council on Competitiveness highlight the major strategic shifts in a *global* economy and their importance to our country. The developing economies of the world are driving these shifts, and their industrial capability is a major component of their success. Analyzing an industry in another country or region of the world can yield strategic insights about a nation's capabilities and strategic intent. Chapter 2 introduces industry analysis and proposes a methodology for applying it in the Intelligence Community.

Chapter Two

Industry Analysis

There are innumerable analytical tools employed in business. Our purpose is to identify and employ the analytical tools that can provide strategic insights into a nation's industrial capability. The industry analysis involves a detailed review of the external and competitive forces that influence the way an industry develops.[19] This is what sets industry analysis apart from an all-source analyst simply performing a keyword search for information sources about an industry. The three analytical tools discussed here are widely used in business. They are the Porter Five Forces Model, the External Environment Model, and the Value Chain Model.

Long-term background preparation for this book—and in particular selection of these three analytical models—stems from various sources: experience as an acquisition officer in the Department of Defense; early exposure to the disciplines of business and industry analysis as part of preparing for a master's of business administration degree; continuing professional education at the Industrial College of the Armed Forces (ICAF), analyzing industry sectors and their importance to national security, as well as learning to look beyond the numbers to appreciate the strategic interplay between government and industry; and teaching industry analysis to graduate-level students at ICAF, where use of the Five Forces Model and the Value Chain Model proved the most valuable for students to appreciate the structure of an industry, and where use of the External Environment Model broadened their understanding of the interaction between industry and government. The open-source methodology and data-collection approaches for this book resulted from that experience at ICAF.

That said, the industry analysis approach introduced in this chapter and elaborated on in the following chapters is easily understood and does not require the intelligence analyst to have a business or technical background. In fact, the intelligence analyst may have a head start in comprehending its application due to his or her training in other analysis techniques, such as the analysis of competing hypotheses. To begin our discussion of the industry analysis models, we will start with a brief look at the nature of a firm or corporation.

Overview of the Financial Activity of a Firm

A firm's performance has two components—survival and profitability.[20] The measure of survival is obvious, but the profitability component is measured by profit maximization, whereby a firm determines the price and quantity of output that delivers the greatest profit. Figure 2.1 provides a top-level view of a firm's financial activity.

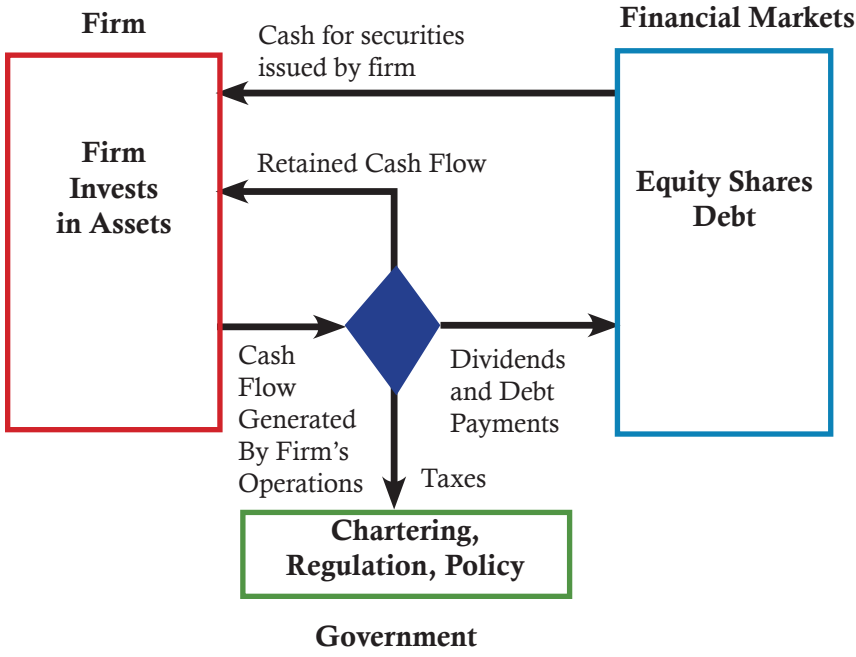


Figure 2.1: Financial Activity of a Firm[21]

Figure 2.1 shows that the firm (red block) generates cash by issuing stocks to or borrowing from financial markets (blue block). The firm uses this cash in developing goods or services and the resulting cash flow generated is then used within the firm (retained earnings), paid out to the financial community (stock dividends, debt repayments), and paid to the government (taxes).

This simple model allows the reader to visualize the effects of a country's public policy, financial, or market announcements that are reported regarding a firm or even an entire industry. For example, when a government announces

a 10-year exemption for the collection of any taxes from a firm that relocates to their country, the firm can now use more of its cash flow, via retained earnings, to fund research and development, buy additional assets, or use it to enhance its standing with the financial community by retiring debt or increasing dividends. The reality is much more complex, but this basic model and the economic maxim of profit maximization are useful for understanding interactions between governments and industry.

Academics studying business and industry economics develop models by observing how firms organize and perform against their competitors and in the marketplace. As the business world changes, these academic communities find some insights to be timeless, while others are modified or even discarded. Businesses also use many of these models to analyze their competitors. The Strategic and Competitive Intelligence Professionals (SCIP) organization bridges the academic and business world and provides good sources for exploring and discussing the methods of competitive intelligence.[22] According to Robert Grant's *Contemporary Strategy Analysis*, one of the most comprehensive industry texts, competitive intelligence has three main purposes:

- Forecast competitors' future strategies and decisions.
- Predict competitors' likely reactions to a firm's strategic initiatives.
- Determine how competitors' behavior can be influenced to make it more favorable.[23]

In academia and the competitive world of business, as long as the models and associated analytical methods are of use, they will survive—although not without some tailoring. The following discussion will describe the key elements of each model. This will help the all-source analyst to understand the industry structure to the extent that it yields, in combination with the other models, strategic intelligence insights regarding a nation's plans and intentions.

Porter Five Forces Model

The first model carries the name of its developer, Michael Porter of Harvard University. Porter arguably produced the seminal text on industry analysis, *Competitive Strategy*, which describes his Five Forces Model.[24] The model is meant to convey the forces acting on an industry. Our usage of the model is

very different from that of the business analyst who is working to understand competitors. For our collection purposes, the Five Forces Model provides a mental construct to use in reviewing and determining which data to keep for further analysis. For example, when reading an article, is it possible to determine who is the buyer and who is the supplier? What is the threat of product substitution if prices rise too high? What are the barriers to entry to the industry? Can a government overcome this barrier to entry through policy decisions? How intense is competition within the industry? Is the intensity of competition inviting government involvement? Today, thirty years later, the business community still uses this model to describe their industry and gain insights into how it is changing.

In economic terms, an industry can be defined as "a group of firms producing products that are close substitutes."[25] The Five Forces Model, shown in Figure 2.2, is meant to convey the primary forces that affect the structure and conduct of the industry. In business, the end result of conducting industry analysis via the Five Forces Model is a description of the industry that the company will use to determine a strategy it will pursue in the future. The main point is that a firm does not want to pursue a strategy that is not going to lead to a competitive advantage. For the intelligence analyst, however, the end result of conducting industry analysis via the Five Forces Model is a conceptual understanding of the industry that will then aid in the collection and analysis of information on the industry in all of its global locations.

Figure 2.2 shows the five forces affecting the structure and conduct of an industry: threat of new entrants, bargaining power of buyers, bargaining power of suppliers, threat of substitute products or services, and rivalry among existing competitors.

The *threat of new entrants* concerns how easily a new competitor emerges from outside the industry. Intense price competition is one sign that it is easy for other firms to enter into the industry. And if it is easy for new entrants to appear, firms already in the industry may choose to pursue future investment opportunities outside of the industry. Examples of barriers to entry are large capital costs for plants and equipment, unique process or product technologies, and government regulation.

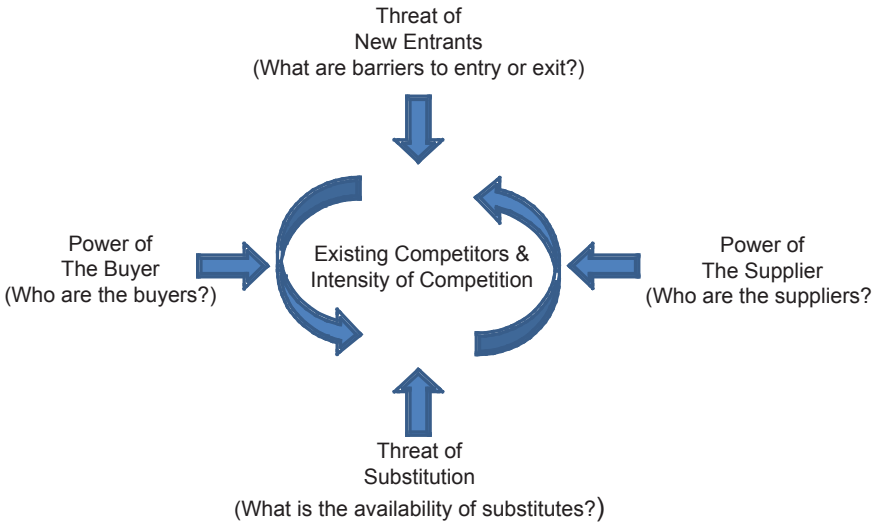


Figure 2.2: Porter Five Forces Model[26]

The *bargaining power of the buyer or supplier* is meant to capture the extent to which the industry determines the prices in their industry. If suppliers to the industry hold a unique material required for an industry to continue, then they may temporarily hold an advantage in setting prices for the industry. Similarly, if the buyers of the industry product or service have a lot of power, they can dictate prices or demand features in the products they buy. The word "temporary" applies in all of these cases, as industry and business operate in dynamic environments.

The *threat of substitution* concerns the potential for buyers to buy substitute products or services if the industry demands high prices or does not respond to buyer requirements.

The *rivalry among competitors* is central to the Five Forces Model. This is the intensity of competition among firms and the characteristics of that competition. One obvious factor in the intensity of the rivalry is market growth (slowing, increasing); a not-so-obvious factor is exit costs. A company in an industry with intense rivalries may find few options for pursuing other ventures (including

exiting) due to large investments in plants and equipment (e.g., automotive industry, oil refining industry). Contrast this last point with the earlier discussion on the threat of new entrants.

In summary, the Five Forces Model captures the key factors that determine the profits earned by firms in an industry, the value of the product to the buyer, the power of the supplier to set prices, and the intensity of competition.

External Environment Model

For the business analyst, the External Environment Model complements the Five Forces Model in support of business planning. But for our purposes, we will use the External Environment Model as our collection framework to gain strategic insights into a nation's capabilities and strategic intent.

The External Environment Model moves our inward-looking frame of reference for the industry outward to the strategic level.[27] The premise behind considering the external environment is simply that firms and industries operate in an environment that can have a large impact on their competitiveness. While the external environment has an effect on the structure and conduct of an industry and the firms within, the specific segments of the external environment for examination will vary according to the user. These different segments are often denoted by the acronyms applied to the External Environment Model in use. For example, "PEST" stands for political/legal, economic, social, and technological segments, while "STEEP" refers to social, technological, economic, ecological, and political/legal segments.[28] Reflecting the increasing emphasis on "green" issues, there is also "STEER," which stands for socio-cultural, technological, economic, ecological, and regulatory segments.[29] The definition of the segments selected is all oriented toward identifying external forces or impacts on the industry. For example, referring to PEST, one aspect of the political/legal segment is looking for the degree to which government regulation directs or influences the conduct of industry. One element of the economic segment is the impact of the global economy on the domestic economy and markets. Another element of the social segment is workforce education and skill levels, and an element of the technological segment is the level and focus of government expenditures for research and development.

While the selection and definition of segments vary, the important point for our purposes is the value of having a framework to guide the collection of information for further analysis. And these models can be combined to make new models, too. For example, Fleisher developed the Nine Forces Model by applying STEEP/PEST factors in conjunction with the Five Forces Model (four PEST segments plus five forces equals nine forces).[30] Similarly, we will also integrate the knowledge we gain from the Porter Five Forces Model with relevant external segments to form a generic overview of an industry from both inside and out. Figure 2.3 shows a framework displaying the segments and elements we will use to collect information (a step discussed later).

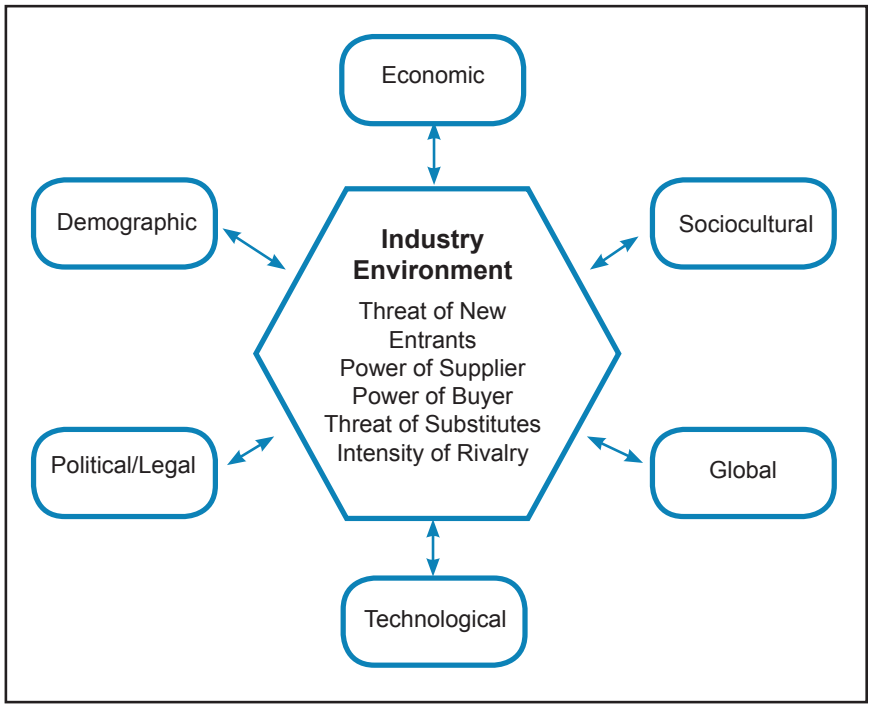


Figure 2.3: Framework for Information Collection[31]

The hexagon in the middle of the figure represents the industry environment and lists the forces described by the Five Forces Model. The segments arrayed around the hexagon represent the external environment that surrounds

an industry. The segments of this framework are not cast in stone, and one does not have to collect information on every element. Appendix A lists the segments and their constituent elements for this framework. When reading about an industry, the analyst should use the segments and elements, and include the five forces, as a template for categorizing, sorting, and saving information. This approach is subjective, but useful, because all of the data will be collated and have source documentation.

In summary, the External Environment Model, which encompasses the Five Forces Model, captures the key external factors that influence the profits earned by firms in an industry and the intensity of competition. For our purposes, analysts should be able to use the External Environment Model to form a mental picture of the industry as they perform data collection and analysis. It is important to clarify that, while in business, the Five Forces and External Environment Models provide a basis for strategic planning, we are focusing on identifying and understanding industry interactions with national governments to develop strategic intelligence insights. Once analysts have internalized their understanding of the industry, they can then quickly perform the day-to-day task of reviewing industry information and extracting any strategic intelligence insights.

Value Chain Model

The final model is the Value Chain Model. This model is important because it identifies the fundamental activities in an industry that influence or control the profitability or growth of an industry. These key activities are also frequently the areas where nations exercise export controls for national-security or national-competitiveness reasons.

The Value Chain Model provides a contextual framework for review and evaluation of information. Are there activities that are not only key (hence are on the value chain), but also determine or control growth or profitability in the industry? For example, a country concerned about national competitiveness may focus its attention on those key activities that determine the growth of that industry.

The Value Chain Model was introduced to the broader business community in the 1980s.[32] The value chain, as originally envisioned, is oriented toward

the firm and, in large corporations, the business unit. The example provided in Figure 2.4 is a visualization of the value chain discussed in Porter's book, *The Competitive Advantage of Nations.*

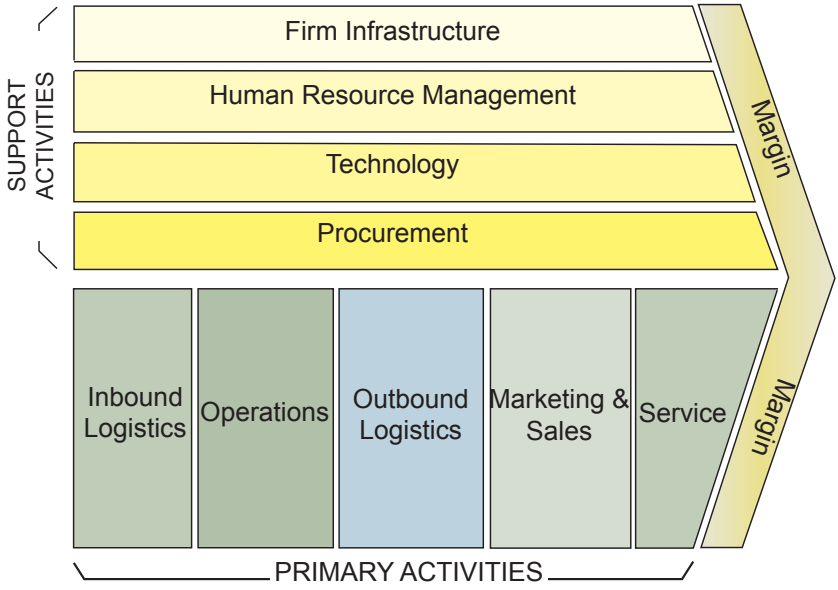


Figure 2.4: Value Chain (© Dinesh Pratap Singh)[33]

A firm using the Value Chain Model will lay out its major activities and then systematically evaluate how each activity adds value to the firm. Business analysts understand that this analysis also includes the relative performance of competitors in executing those activities. This approach supports the firm's strategic planning to achieve competitive advantage.

For Porter's purposes 30 years ago, applying the value chain to anything above the level of the firm (to the industry or sector level) would not shed much light on the unique value that the firm had in creating competitive advantage. Back then, the value chains of U.S. industry were primarily domestic. Multinational firms had overseas subsidiaries in place to deliver products from domestic U.S. value chains. Today, however, multinational corporations base many parts of the value chain, including product development and manufacturing processes,

in many regions and countries. Lifting the value chain to the industry level begins to make sense.

For our purposes, we will exclusively focus on developing the value chain at the industry level. The Intelligence Community is not interested in the competitive advantage of individual firms; our focus is on understanding the structure and conduct of an industry and the strategic intelligence insights its interactions with other nations can provide. Fortunately, there is a body of work in academe that applies the Value Chain Model in describing the scope and scale of globalization, including how industries organize to operate in a global environment.[34] For example, Timothy Sturgeon's work recognizes that development of many products is now the result of global value chains. Academicians seeking to understand the governance of such far-flung industries identify several different types of global value chain governance (Figure 2.5).

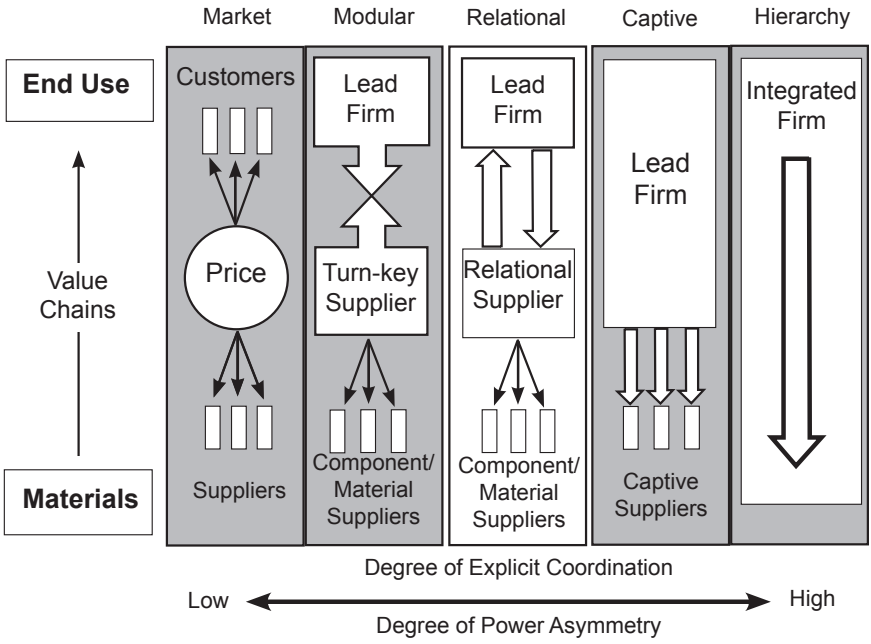


Figure 2.5: Global Value Chain Governance (© Taylor & Francis Group)[35]

Figure 2.5 shows both vertical and horizontal integration by governance type. At the far left, the value chains flow "up" from materials to end use. Arranged horizontally across the bottom is the degree of coordination required between activities and the degree of power asymmetry. Within the value chain examples, the black arrows indicate where price is the only interaction between activities in the value chain, and the solid white arrows indicate where information is included in the interaction. Looking at the far right, the integrated firm maintains competency in all facets of that industries' value chain. At the far left, the most basic value chain, the market, is a price-based market with multiple suppliers and customers communicating only via price. The models in-between show varying complex, symbiotic relationships between suppliers and buyers within the value chain. As one moves from basic to more complex value chains, the development of standards and the ability to exchange information far more complex than pricing information are major facilitators for the development of a global value chain. For now, these global value chain governance models should be kept in the background; they will be of more use when we select and analyze an industry.

In summary, the Value Chain Model captures the key value-added activities of the industry, and the Governance Model shows the level of complexity of the value chain. Developing or being able to interpret the value chain for the industry under analysis is an important early step in understanding the industry. Internalizing an understanding of the industry value chain also contributes to the day-to-day task of reviewing industry information and extracting any strategic intelligence insights.

The firm is the fundamental business unit, and a group of firms that produce similar products are collectively referred to as an industry. This chapter has so far provided three basic models to help the analyst frame the scope of industry analysis. The Porter Five Forces Model helps in understanding the forces influencing the conduct and structure of industry via the power of the buyer and supplier to set prices, the threat of substitution and new entrants to the industry, and the intensity of the existing competition. For our purposes, the analyst can use the Five Forces Model to form a mental picture of the industry. The External Environment Model identifies how and to what extent firms and the industries in which they reside interact with the external environment. For our purposes, the analyst will use the External Environment Model

segments and elements in developing the collection plan (discussed later). The Value Chain Model will become central to the analyst's understanding of the industry under analysis, and also provides a context for reviewing information regarding the industry.

Chapter Three

Putting It All Together—The Five Steps

This chapter discusses how the all-source analyst, covering a region or country desk, includes commercial industry when tasked to provide inputs for an intelligence assessment. There are five steps in the process used by the analyst: (1) select an industry, (2) define the industry, (3) identify sources of information, (4) collect information, and (5) analyze results. The five steps are described below.

Step 1: Select the Industry

For the business analyst, selecting the industry for analysis is straightforward. For the all-source analyst, however, selecting the region or country of strategic interest is even more straightforward. If a nation wants to foster development of an industry with a view toward improving national competitiveness, its domestic firms must become efficient producers of that industry's products. While a nation can subsidize an inefficient industry, that does not mean its segment of the industry will have a comparative advantage over another nation's industrial capability for that product. For the all-source analyst, the policy or resource actions by a nation in fostering development in their industrial capability are of interest for the strategic intelligence insights they may provide.

Criteria for Selecting Industry

Our selection criteria include looking for an industry that is mature, global, and has a large presence in the region or country we are interested in. But first, a couple of new terms—*mature* and *global*—require a brief explanation.

The concept of industry *maturity* is sometimes shown as a stage in the life cycle of an industry. Using the measure of industry sales, the industry life cycle has the following periods: introduction, growth, maturity, and decline.[36] Other industry life-cycle portrayals, using the same measure of industry sales, label the periods of change as fragmentation, shakeout, maturity, and decline.[37] For our analysis, a mature industry is one in which the industry structure is stable and there is little change in the rank of leading firms.

A *global* industry is where an individual firm's competitive position in one country is affected by its position in other countries, and the reverse is also true.[38]

The final criterion, a large presence in the region or country, provides a starting point in selecting and reviewing industry candidates. Potential candidates for industry analysis are available from reviewing the Department of Commerce website for publicly released analysis on U.S. International Trade in Goods and Services. For this example, Department of Commerce International Trade Administration (ITA) publicly released factsheets were used.[39] A March 2009 ITA factsheet states that "capital goods" represent the largest U.S. export category and lists the top capital good export categories as civilian aircraft ($3.8 billion), semiconductors ($2.6 billion), industrial machines ($2.3 billion), telecommunications equipment ($2.3 billion), and medicinal equipment ($2.2 billion).[40] The United States holds a comparative advantage in these industries, where we are the more efficient producer of a product and it is to the advantage of other nations to trade with us to obtain that product or service. Conversely, a list of major U.S. *imports* would indicate where other nations' industries may have a comparative advantage over U.S. industry.

Starting with the ITA export factsheet cited earlier, an Internet search for the worldwide manufacturing rankings for an industry will provide a quick check on that industry's presence in the region or country of interest. This Internet search will also provide initial leads on sources of information regarding the industry.

To illustrate our analysis, the semiconductor industry will be the industry analysis example for the remaining steps. The semiconductor industry is a major export for the United States. It is a *mature* industry with established leaders, and a *global* industry with major outsourcing of manufacturing steps, such that any changes that affect facilities in other countries have an effect throughout a firm's operations. Other countries in the world want to advance in this industry, so industry analysis may yield strategic intelligence insights into another nation's plans and intentions that may affect U.S. comparative advantage in the semiconductor industry and, by extension, U.S. national competitiveness. Finally, the semiconductor industry has a large presence in East Asia, a region of strategic intelligence interest to the United States.

Step 2: Define the Industry

The starting point for the business analyst in formulating industry strategies and plans is to first define the industry and understand its structure. The importance of specifically identifying the industry for analysis is analogous to the task of the all-source analyst in clearly identifying collections requirements. In business, the analyst may have the subject-matter advantage of being in the industry, but there are still limits on the resources available for collection and analysis. The analyst in business may start with the six-digit North American Industry Classification System (NAICS) code for his or her industry and use it to access industry data collected by the U.S. Department of Commerce.[41] While the NAICS code and Department of Commerce data are available to the all-source analyst as well, the ITA factsheet and Internet search results that the previous step provides are more germane to that analyst.

To understand the industry under analysis, the all-source analyst has to research sources of general information on semiconductors and the industry. Appendix B provides the results of open-source Internet research on the basics of semiconductors and their manufacture.

Constructing a Value Chain: Aid to Industry Definition

One way to capture an understanding of this newfound information is to construct a value chain for the industry. The following discussion on developing an industry value chain is based on the information in Appendix B.

An industry value chain is the set of interrelated activities that, taken together, cover the cost of providing the product or service. For the semiconductor industry, the standardization of process steps and information exchange between processing steps led to the globalization of the value chain for this mature industry.[42] The semiconductor or electronic components industry and the term "value chain" are mentioned frequently in academic and industry trade journals. There are even illustrations of value chains for various aspects of the semiconductor industry available on the Internet. For example, in Figure 3.1, the Taiwan Semiconductor Industry Association 2009 Report outlines a semiconductor value chain to indicate the number and distribution of Taiwan firms comprised in its domestic semiconductor industry.

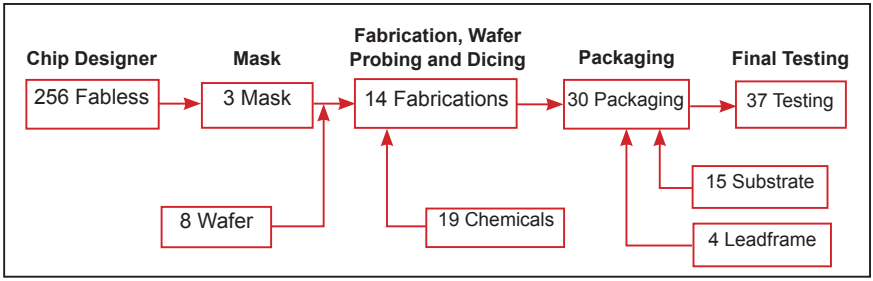


Figure 3.1: Taiwan Semiconductor Industry, 2008 (© Taiwan Semiconductor Industry Association)[43]

The Taiwan semiconductor industry value chain follows the product flow from design to test of the packaged chip. The figure indicates that, in 2008, Taiwan had 256 firms involved in the design of integrated circuits. The term "fabless" denotes firms that create and sell the designs of integrated circuits, but do not fabricate (manufacture) integrated circuits. The figure also indicates 14 firms with fabrication operations and 30 firms with packaging operations.

Academic papers employ value chains to evaluate industries, and those value chains produced in the country of interest can yield insights into how important an industry is to a nation. For example, Figure 3.2 shows a semiconductor value chain reflecting Taiwan's capability in the design of integrated circuits relative to capabilities of other advanced countries. The *Technovation* article from which the figure was derived goes on to discuss the strategy of the Taiwan semiconductor industry and the reasons behind its relative success at that point in time. Although dated, the article still provides background for collection and analysis on the semiconductor industry in Taiwan.

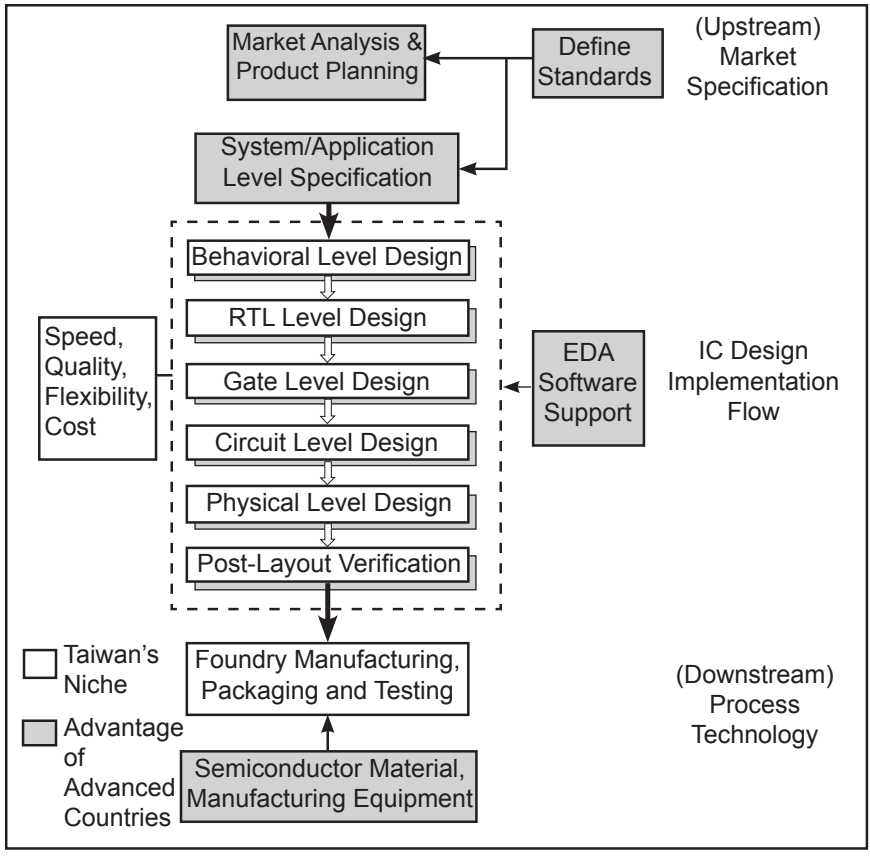


Figure 3.2: Taiwan Integrated Circuit Design Capabilities (© Elsevier)[44]

For our immediate purposes, the value chain in Figure 3.2 confirms the steps and their sequence in the production of semiconductors. The value chain also provides key terms that are encountered in analyzing the semiconductor industry.

Figure 3.3 shows a semiconductor value chain that can be used to illustrate the semiconductor manufacturing process and the globalization of the industry value chain.

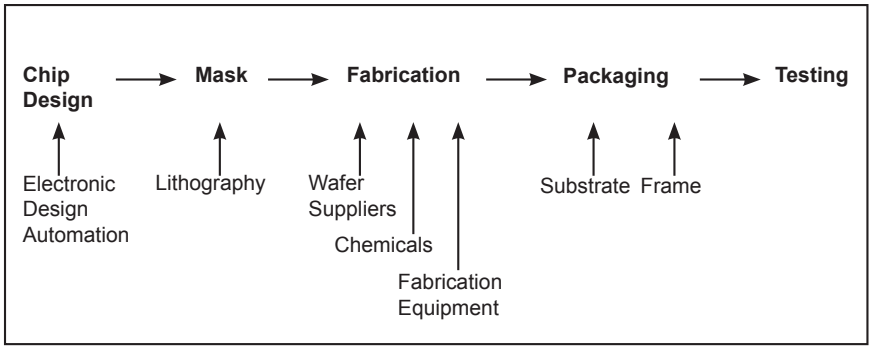


Figure 3.3: Semiconductor Value Chain[45]

Figure 3.3 shows the major value-added activities in the industry (chip design, mask, etc.), as well as the key suppliers to the industry (electronic design automation, lithography, etc.). An important point for analysts to understand is the variation in ownership of the value-chain activities for this mature industry. For example, in Figure 3.4, the top value chain shows the domain of the integrated design manufacturer and refers to a firm that participates in all the steps in the value chain. In terms of global value-chain governance (remember Figure 2.5), this is a hierarchical governance with high degrees of explicit coordination within the firm and power asymmetry over the suppliers. The middle value chain in Figure 3.4 shows the domain of the foundry, and refers to a semiconductor fabrication firm that fabricates the wafers from designs provided by other firms, and then returns the wafers to the customer. Finally, the bottom value chain in Figure 3.4 shows the domain of a fabless firm. This firm creates the integrated circuit design (intellectual property) and sells the design to other companies or subcontracts for fabrication.

In terms of global value-chain governance, both a foundry and a fabless firm are examples of modular value-chain governance. The standardization of design-manufacturing interfaces and information supports a lower degree of explicit coordination and power asymmetry over others. A useful way to think of power asymmetry is in terms of the power of the buyer or supplier in the interchange. The integrated design manufacturer has a lot more power over suppliers than the foundry or fabless firm.

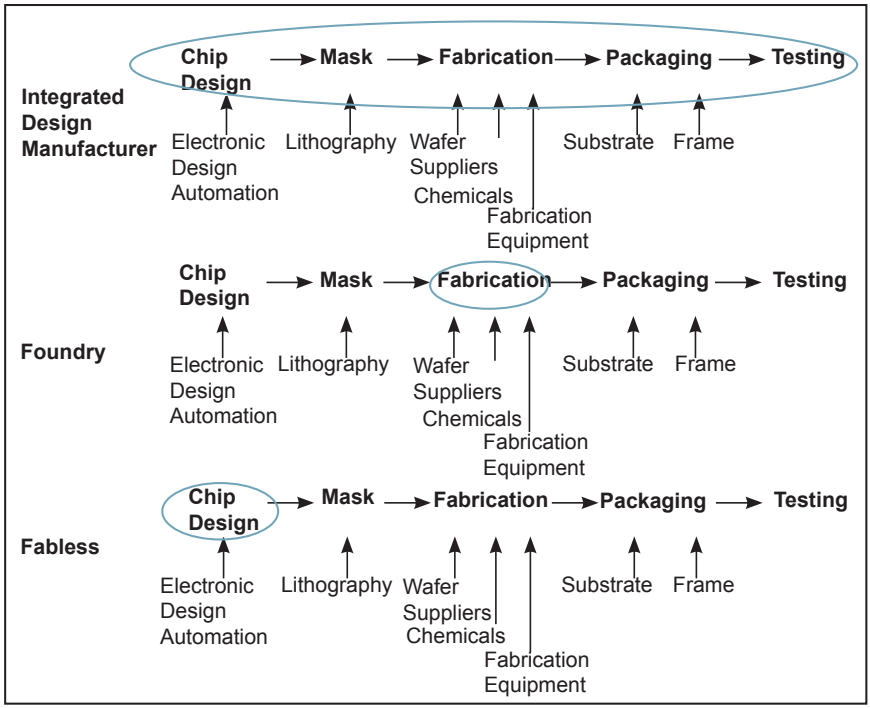


Figure 3.4: Semiconductor Value Chain—Firm Participation[46]

Step 3: Identify Sources of Information

Timothy Sturgeon points out the importance of not focusing on macro-level statistics, such as trade and investment, to understand a country's plans and intentions, because they "cannot help but render invisible the detailed contours of the world economy."[47] Also beware the technophile's focus on "the next big thing" or, at the other end of the spectrum, the engineer's focus on details. Keep these cautions in mind when starting to scan and select topics from the "daily scrape" for further review and analysis.[48]

This section takes the next step of identifying the types of potential open-source data available to support the industry analysis. Appendix C lists, by category, potential data sources specific to the semiconductor industry.

Books

While currency of the data source is a primary consideration, the search should include recent books on the industry.

Reports

The National Academy of Sciences, a nonprofit institution, has a searchable website of its publications, many of which are free to download. While the publication of National Academy reports is unpredictable, you can set e-mail notifications when topics of interest are available. The federal government, particularly within the Department of Commerce, provides a regular stream of trade and industry statistics, but occasionally it will also produce reports on global trade topics that are of interest. For example, the Bureau of Industry and Security (*www.bis.doc.gov/*) provides current news regarding trade issues, and the Defense Industrial Base Programs link provides a list of Defense Industrial Capability and Technology Assessments regarding foreign industrial development that may be of interest.

Trade Associations

Most industries have trade associations, and the associations usually release publications. Trade association websites provide news and documents, although the frequency of their updates and data available can be irregular.

Trade Journals

The most useful sources of current information are the industry trade journals. While there are government policy announcements and occasional analytical articles of use in metropolitan newspapers and business magazines, many of the stories are not much more than news releases from the subject company.

Other Internet Sources

This category concerns the ever-evolving platforms and content of the Internet. A few examples follow.

YouTube

The website YouTube (*www.youtube.com*), although pedestrian to aficionados of social media, can still provide good sources of information.

Blogs

Blogs written by industry analysts, enthusiasts, or employees can be a good source of information.

Twitter

The use of Twitter by the trade journals and even companies is noteworthy, but they typically tweet links to journal or marketing content already accessible via other means.

Webcasts, Virtual Conferences

The increasing use of webcasts and virtual conferences are good real-time sources. Subscriptions to the industry trade journals will lead to announcements of these events. The events offer another avenue for the industry to share information and develop market opportunities. The presenter slides are usually available for download prior to the presentation or the site may allow archival access.

Trade Shows

Trade shows, the best alternative to actually visiting semiconductor companies in other countries, obviously present challenges to the all-source analyst even beyond the requirements of time and funding. Trade association websites and trade journals carry advertisements for upcoming tradeshows. Tradeshows offer sessions in a variety of areas; it pays to read the program beforehand to ensure that the tradeshow is not devoted to a sub-industry topic or technical interchange. Also, unless the analyst is multilingual, it is advisable to ensure that the session is in English or a simultaneous translation is available. A walkthrough of the exhibit halls, including gathering literature, proves useful. One caution is that most corporate booths require a business card or the signing of a register before they provide literature. The purpose of the exhibit hall is to generate business leads for the companies, so the collection of literature may have to be skipped if identification presents a problem.

Step 4: Collect Information

For the purposes of this discussion, data was collected from November 2009 to June 2010, using all of the sources discussed in the preceding subsection. The sources included subscriptions to multiple semiconductor industry trade

journals, two semiconductor industry trade shows (Tokyo and Seoul), and one industry strategy symposium (Half Moon Bay, California). With the Porter Five Forces and the Value Chain Models for context, relevant online information was saved in the program Zotero, organized by folders labeled with the External Environment Model segments. Also available were digital copies of the tradeshow proceedings.

Preparing for Collection

The sources that are included in the "daily scrape" of open-source media require preplanning.

Using E-mail as an Information Portal

For this project, a separate Gmail account was created just to receive industry trade journals and other industry source materials. During the workweek, the trade journals push their content out to subscribers. Via the Gmail account, it was possible to quickly scan the subjects and synopsis of articles in each journal.

Capturing and Sorting Information

There are several ways to capture results. One approach is to use a series of e-mail folders to keep and organize items of interest. The freeware program Zotero was chosen to collect, manage, and cite the source materials.[49] Zotero was active and ready to use whenever the browser was open. Saving a copy of an article entailed clicking the Zotero icon in the toolbar, and selecting "create new item" in the folder designated. Zotero uses a cloud-based storage approach to capture a copy of the specific article, and also puts a copy on the computer. The reviewed trade journal is placed in a folder within the Gmail account that is marked by the name of the journal in case it is necessary to access the journal again. The advantage of Zotero's cloud-based approach is that the analyst can work from multiple computers and keep up with the work. In June 2010, Zotero's annual rate was $20 for 1 GB of storage ($1.67 per month). A plus for Zotero is that it has a plug-in to Microsoft Word, permitting direct transfer of citations from Zotero to a Word document.[50]

Filing Information

The External Environment Model provided the framework for active collection of information on the industry. Folders were created in Zotero and labeled with the names of the segments in the model. Here is the list of virtual folders established in Zotero to capture information:

Demographics
Economic
Global
- *China*
- *Europe*
- *India*
- *Japan*
- *Korea*
- *Singapore*
- *Taiwan*

Political/Legal
Sociocultural
Technological

Note that, within the global element, country-specific folders were also developed for information that pertains only to that country. There is also a folder named Industry Analysis that was used to collect information regarding the structure and conduct of the industry. Figure 3.5 shows a screenshot of the online data collection (Zotero tool) for this industry analysis.

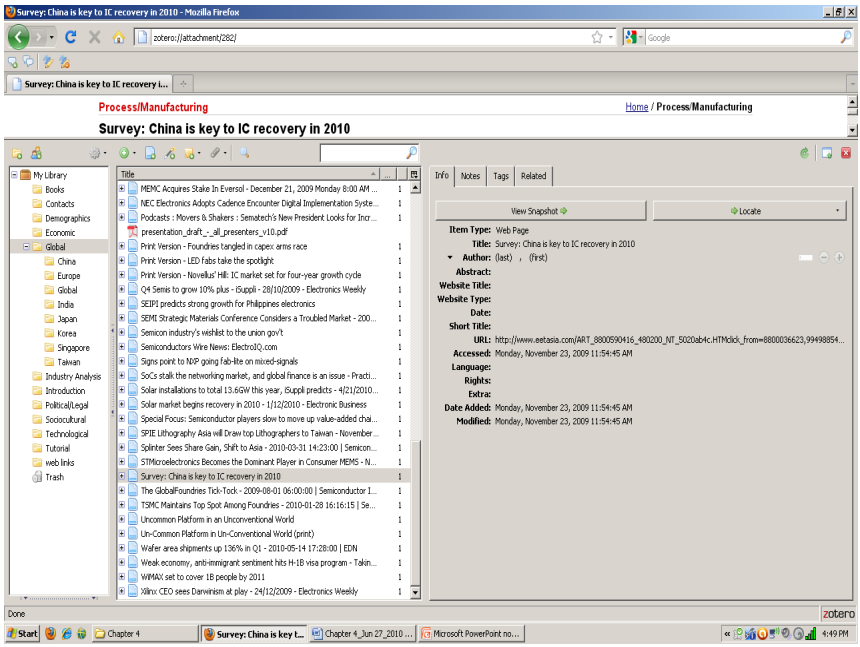


Figure 3.5: Data Collection Using Zotero

In Figure 3.5, the Global folder is highlighted in the far-left column. The middle column lists all the articles saved in that Global folder; highlighted is an article titled "Survey: China is key to IC recovery in 2010." Double-clicking on that title opens up the article in that window for rereading. In the far-right column is a snapshot of the citation, including the date it was accessed and the article's Web address. The review and collection of data in one place with a clear documentation trail will be advantageous during the analysis. Once the data-collection framework is in place, the analyst can start reviewing and collecting information. There will be a large volume of information arriving every day, but it is possible to quickly scan and save information of interest.

Industry Observations from Data Collection

Thus far, we have discussed the first four steps: select the industry; define the industry; identify sources of information; and collect information. In this

subsection, we look at industry observations resulting from the data collection. We summarize observations on the current state of the semiconductor industry based on the results of the open-source collection. The summary will provide a backdrop for step five: analyze results (the following subsection). There, we will review and analyze collection results on East Asia—the focus of our analysis.

At this point, the analyst should be comfortable with reviewing incoming information on the semiconductor industry. The Five Forces Model and the Value Chain Model aid in reading and comprehension during collection. The External Environment Model and the Zotero software tool provide a means to sort and preserve collection results. The observations at this point will be a collection of opinions and facts consistent with how the industry views itself. While the psychology of intelligence analysis is beyond the scope of this discussion, Figure 3.6 provides a conceptual view of applying the industry analysis model for intelligence analysts.[51]

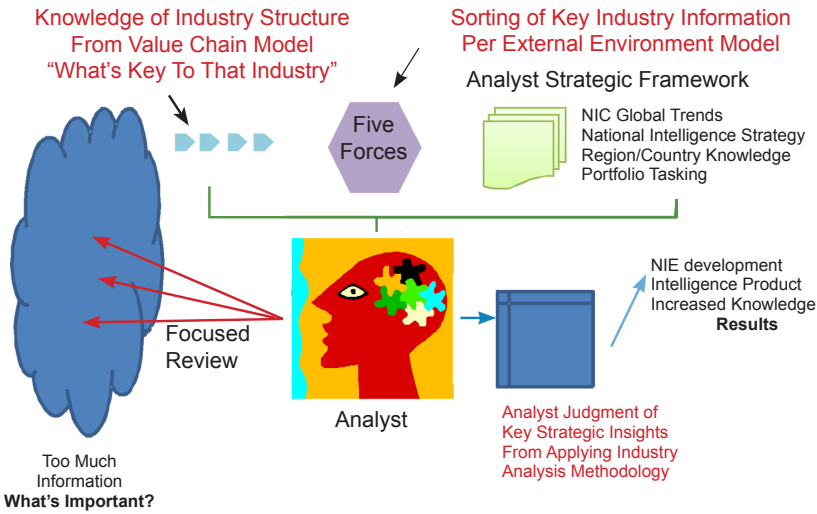


Figure 3.6: Conceptual View of Model Application

Figure 3.6 shows the analyst at the center because he or she is the target audience for this book. On the left side, the blue cloud indicates the large amount of open-source information and the caption "Too Much Information" describes the daily challenge of the all-source analyst. Along the top

are arrayed the various models described in Chapter 2, but it also includes the analyst's strategic perspective and tradecraft experience. The combination of industry analysis models and the strategic framework provides a new lens for the analyst to now perform a "Focused Review" of industry-related data. The "Analyst Judgment of Key Strategic Intelligence Insights" represents the intellectual task of reviewing and assessing the information collected. This is not a serial process; the analyst over time builds a strategic perspective of the industry and draws equally strategic and intelligence insights (or connections) from his or her tradecraft experience. This subsection provides the result of building a strategic perspective on the semiconductor industry. Later in this chapter, under step 5, we describe the result of focusing our newfound perspective on the target region of East Asia and suggest strategic intelligence insights for use in the intelligence products listed in Figure 3.6 as "Results." It is worth stating again that the intellectual process of learning to use the industry analysis models, learning to understand the industry, collecting information, developing observations, and finally generating strategic intelligence insights is not serial.

Summary of Industry Observations

The semiconductor industry faces continuing consumer demand to increase capability and decrease prices. The advances in technology have been impressive; however, achieving each advancement (sometimes referred to as a technology "node") requires enormous amounts of capital, and it is the economics, not the technology, that is becoming the main driver. Four primary observations resulted from the information collection and analysis of the industry:

1. Economics of pursuing the leading edge is in question;
2. "Globalization" of the industry market is not a remedy for profitability concerns;
3. East Asia's emergence as the industry's production center is an outcome of pursuing profitability through globalization; and
4. Industry's active pursuit of alternative markets for avenues of profitability is an outgrowth of the competitiveness within the industry.

Economics of Pursuing Leading Edge Is in Question

A hallmark achievement of this industry has been its ability to regularly deliver increasing capability. However, while there is a lot of discussion of the approaching physical limits of achieving further increases in the number of transistors that can be crammed onto an integrated circuit, industry analysts believe the real barrier may be an economic one. At semiconductor equipment conferences this year, several speakers brought up the point that new technology nodes may not meet the 18-month cycle of delivering new capability per Moore's Law.[52] Figure 3.7 illustrates the industry's fear that the financial hurdles may be too great for delivering new capability.

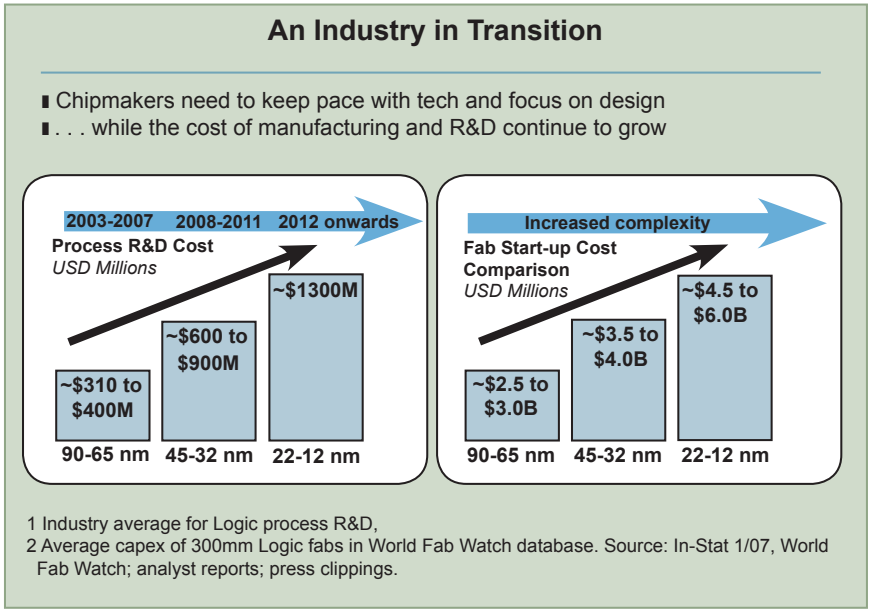


Figure 3.7: Financial Hurdles for Semiconductor Industry (© GLOBALFOUNDRIES)[53]

Figure 3.7 shows the increasing research and development costs required to achieve decreasing feature size. The figure also shows that the industry faces huge costs to build the fabrication facility to render that design into a chip. In terms of Porter's Five Forces Model, both of these factors represent high

barriers to entry for a company interested in joining the industry. These large investments also represent high exit costs for existing firms.

Figures 3.8 and 3.9 illustrate that even the *conceptualization* and *design* of leading-edge chips are becoming cost prohibitive and resulting in fewer new design starts. One result is that many companies within the industry will continue production using older feature dimensions, and will reuse old blocks of design (intellectual property) in order to avoid the enormous costs of leading-edge design and fabrication.

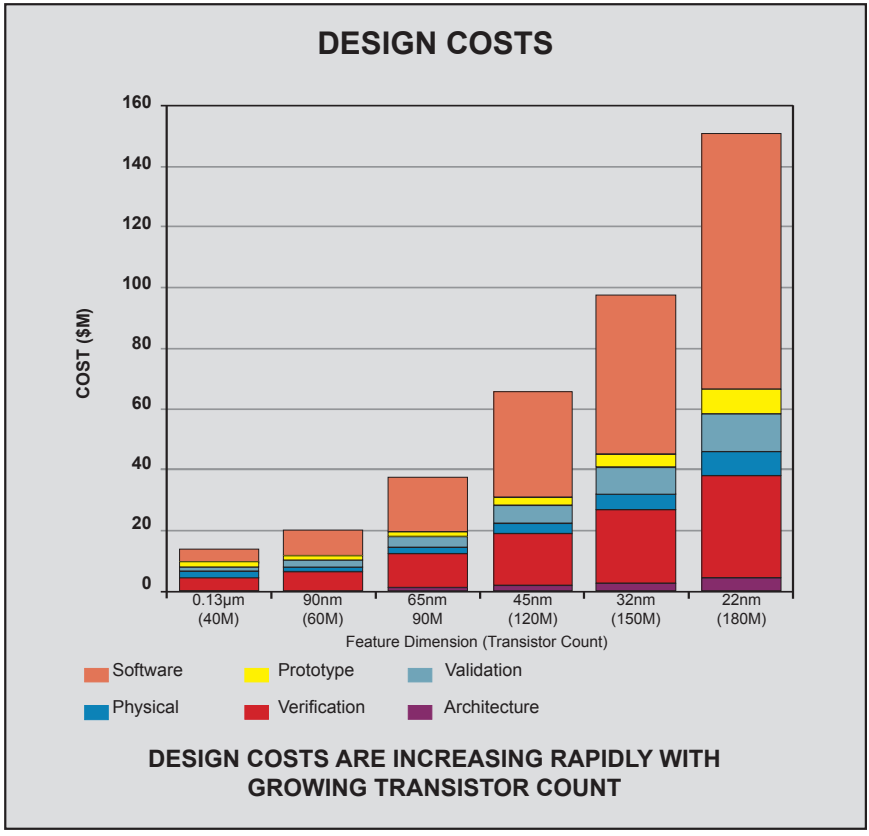


Figure 3.8: Increasing Design Costs (© International Business Strategies, Inc.)[54]

Figure 3.8 illustrates the increasing cost of design in leading-edge integrated circuits. The growing software cost is due to the increase in software required throughout the design process to achieve breakthroughs in the performance of integrated circuits.

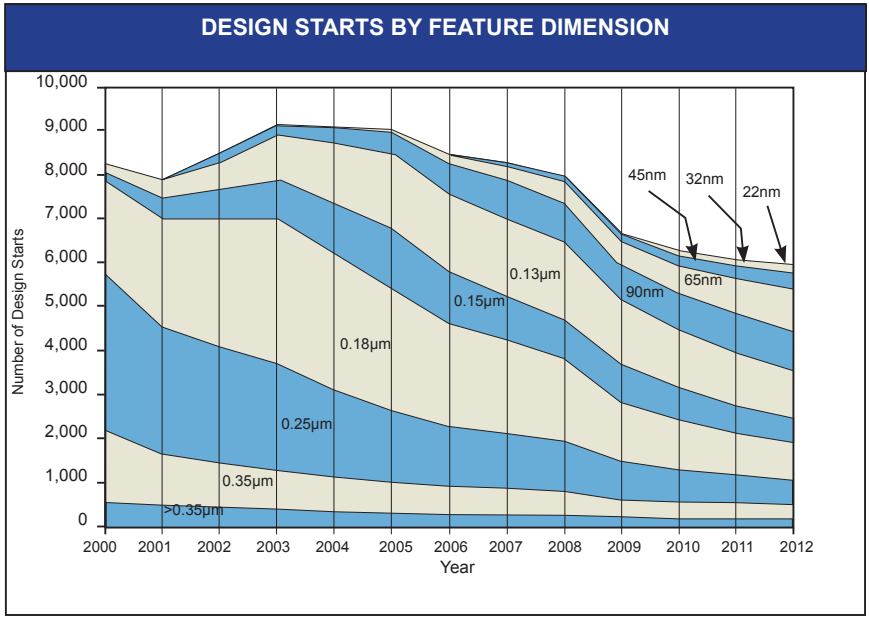


Figure 3.9: Decreasing Design Starts (© International Business Strategies, Inc., 2010)[55]

Figure 3.9 illustrates that increasing costs of pursuing the leading edge in semiconductors are resulting in a slowdown of new starts in leading-edge design. Instead, companies are trying to earn as much revenue as possible from existing designs and fabrication facilities. In terms of the Five Forces Model, the intensity of competition requires a company to commit huge amounts of capital in order to stay at the leading edge of the industry. These capital commitments have led to fewer competitors with clear leaders in each category of the industry. For example, Intel is the world leader in microprocessor units in terms of sales and market share.

When you factor in the huge costs to stay on the leading edge and the industry's claim that the returns on investment are increasingly difficult to find, it is

hard to see why firms even try to pursue the leading edge. Figure 3.10 shows a slide from an industry strategy session that graphically captures this point, but does not provide any answers.

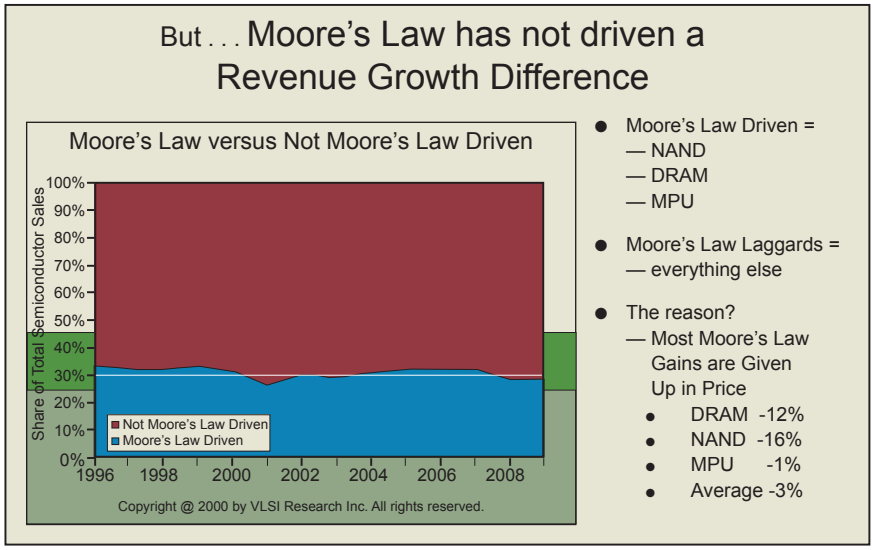


Figure 3.10: Lagging Edge over Leading Edge in Semiconductor Sales (© VLSIresearch. "Economics and Collaboration Panel Discussion" SEMI ISS 2010. Half Moon Bay: SEMI, 2010.)[56]

Figure 3.10 illustrates that, despite all the attention paid to the leading edge (Moore's Law–driven) and the expectation that a leading-edge strategy will result in higher profits, the fact is that the share of total semiconductor sales has remained steady between the leading and lagging edge. The statement "Most Moore's Law Gains are Given Up in Price" illustrates the power of the buyer (in this case, the electronics-equipment manufacturer) in the semiconductor industry. So the semiconductor firm (supplier) has to either find ways to remain competitive or exit the industry, possibly going out of business altogether.

Unfortunately, even if a company steps back from the enormous costs of leading-edge fabrication, it will still face intense price competition in the trailing edge that requires it to carefully select its strategy. Figure 3.11 shows that, while integrated design manufacturers still predominated in the top 20 semiconductor sales leaders (as of 2008), the Taiwan Semiconductor Manufacturing Company, a *pure-play foundry*, is in the top five, and two *fabless*

firms, Qualcomm and Broadcom, registered the highest growth rates. For the remaining integrated design manufacturers to stay at the leading edge, they must continue to leverage their lead in market segments with large amounts of capital investment.

2008 Top 20 Semiconductor Sales Leaders ($M)

2008 Rank	2007 Rank	Company	Headquarters	2007 Tot Semi	2008 Tot Semi	2008/2007 % Change
1	1	Intel	U.S.	35,021	34,490	-2%
2	2	Samsung	South Korea	19,951	20,272	2%
3	3	TI	U.S.	13,309	11,966	-10%
4	4	Toshiba	Japan	11,850	11,059	-7%
5	5	TSMC*	Taiwan	9,813	10,556	8%
6	7	ST**	Europe	8,637	9,052	5%
7	8	Renesas	Japan	8,001	7,017	-12%
8	13	Qualcomm***	U.S.	5,619	6,477	15%
9	9	Sony	Japan	7,203	6,420	-11%
10	6	Hynix	South Korea	9,201	6,182	-33%
11	12	Infineon	Europe	5,772	5,972	3%
12	11	AMD	U.S.	6,013	5,808	-3%
13	14	NEC	Japan	5,593	5,732	2%
14	15	Micron	U.S.	5,520	5,688	3%
15	10	NXP	Europe	6,026	5,318	-12%
16	16	Freescale	U.S.	5,447	4,898	-10%
17	23	Broadcom***	U.S.	3,754	4,509	20%
18	17	Fujitsu	Japan	4,568	4,462	-2%
19	21	Panasonic	Japan	3,810	4,321	13%
20	19	Nvidia***	U.S.	3,979	3,660	-8%
--	--	**Total Top 20**	--	**179,087**	**173,859**	**-3%**

*Foundry **Not incl. flash and ST-NXP Wireless in 2007 & 2008 ***Fabless
Source: Company reports, IC Insights

Figure 3.11: Integrated Design Manufacturers Still Predominate (© IC Insights)[57]

Figure 3.11 not only lists the leaders in the semiconductor industry, it also shows the international makeup of the industry. One notable absence on the list is mainland China, which is usually portrayed in the media as a juggernaut in manufacturing.

"Globalization" of the Industry Market is not a Remedy for Profitability Concerns

Collaboration and Protection of Intellectual Property

The industry understands the technology challenges ahead, but finds it increasingly difficult to find the capital and business model to fund the necessary research and development for pursuit of the next technology node. One possible solution the industry is exploring is collaborations in research and development between semiconductor firms. The International Semiconductor Technology Roadmap is the best example of this type of collaboration. Participating firms are able to share technology and still achieve differentiation in their product.

A few large firms, such as Intel, still choose to fund their own research and development and keep their technology advantage in-house. Other firms also carefully guard their intellectual property, but do so in a surprising way. For example, within weeks of the release of Apple's iPad, the Canadian company Chipworks released an analysis and cross-section images of the core processor chip and correctly identified Samsung as the designer and fabricator.[58] This practice of reverse engineering and publishing the integrated circuit design of another firm is protected by the Semiconductor Chip Protection Act in the United States, which allows reverse engineering "for the purpose of teaching, analyzing, or evaluating the concepts or techniques embodied in the mask work or circuitry."[59] The industry uses this carefully stipulated openness to share achievements and protect its intellectual property.

Expanding Market, Increasing Competition

Another hallmark of this industry is the growth in unit volume, which drives lower cost per unit of semiconductors. One observation in *EE Times India* stated that "the total semiconductor TAM [total available market] grows because of—not in spite of—the 35 percent per year reduction in the unit price of transistors."[60]

During this past decade, electronics consumption has shifted from business use to personal and home use, and this is growing despite the economic downturn. One supporting figure cited is that 55 percent of the world GDP of electronics is now from personal consumption.[61] The $226 billion

semiconductor industry is a key part of the $1.1 trillion electronics industry.[62] Despite the recent economic downturn, the semiconductor content of electronic systems was forecasted to increase about 27 percent for 2010.[63]

A major portent of the future of the semiconductor market lies in the rising awareness of people in other parts of the world to the use of portable electronics such as cell phones. However, a significant portion of these groups only has an annual per capita income of greater than U.S. $3,000.[64] Industry analysts are warning business to be aware of the tipping point, when 50 percent or more of its demand is in emerging markets.[65] Figure 3.12 illustrates the point that, while the majority of this rising consumer class will have high expectations for capability, they will not have the economic means to afford it, thereby exerting further downward pressure on prices.

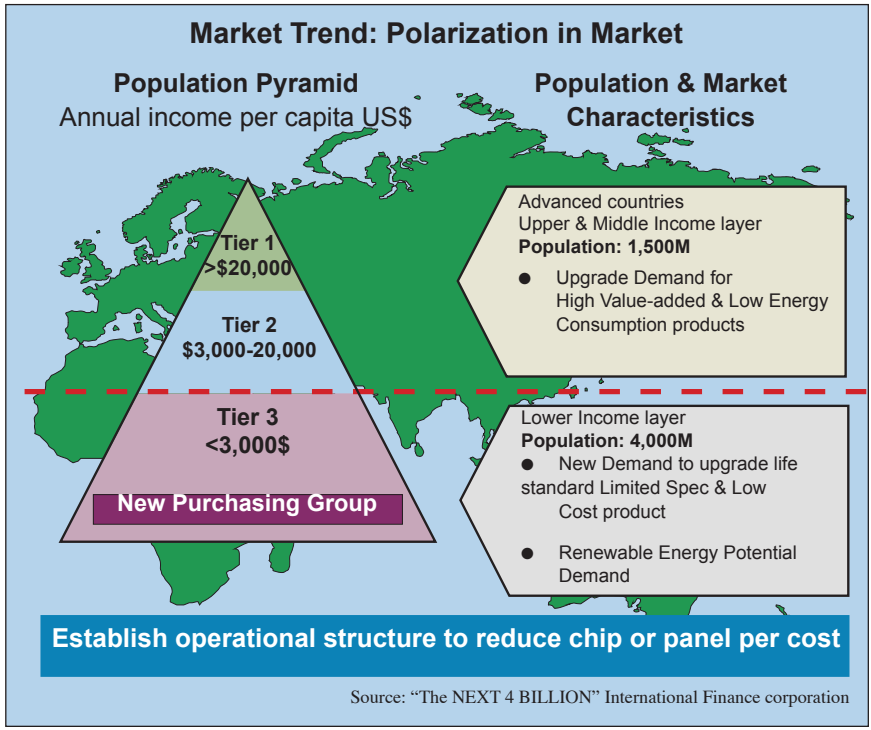


Figure 3.12: Future Market Economics (© Tokyo Electron using information from "The NEXT 4 Billion" International Finance Corporation and "The Fortune at the Bottom of the Pyramid" Strategy + Business, no. 26: 2–14)[66]

Figure 3.12 also provides a sociocultural insight regarding rising living conditions in developing nations around the world. While the industry is struggling with future profitability, demand in developing countries is increasing. This bodes ill for the semiconductor industry, because the power to set prices is still firmly in favor of the consumer.

Ultimately, a semiconductor company has to turn a profit in order to survive in the industry. Turning a profit means being able to sell enough chips over what it cost to develop and produce them. One figure cited at an industry strategy session is that there needs to be a total available market of at least $2 billion in order to justify pursuing a 32 nm advanced chip design.[67] The qualifying 2013 product markets were listed as mobile phones, personal computers, video games, and televisions with set top boxes. The financial community expects that before a semiconductor company invests its capital in a project, the expected value from the project will cover its investment and, in addition, earn a higher return than alternative uses for that capital.

East Asia's Emergence as the Industry's Production Center is an Outcome of Pursuing Profitability through Globalization

It was the drive for profitability that forced U.S. firms to first outsource finished electronic components to Asia for use in producing end items for consumption.[68] The developing standardization of design-to-manufacturing interfaces helped the rise in technical sophistication of Asian countries, and now that region is becoming the fabrication center of this global industry.[69] The global Value Chain "modular" model discussed earlier in this chapter neatly captures the current semiconductor design and fabrication processes.

The establishment of the *dedicated foundry model* in Taiwan is central to understanding the modularity of the industry.[70] While there are variations in scope and organization, in its simplest form, the foundry receives the chip design "intellectual property" from a customer and produces wafers with the integrated circuits. The customer then takes the wafer and either finishes the process or outsources it to yet another firm, so they only handle sales of the finished chip. A pure-play foundry does not fabricate and market its own chips. Sometimes an integrated design manufacturer will contract out its excess production capacity to other firms and produce chips in their fab for them.

The dedicated foundry is a way to transfer portions of the huge costs (and technology risks) of semiconductor fabrication outside of the firm. Some "fab-lite" semiconductor companies are reducing their fabrication capabilities to cover only key technology areas and are relying on foundries for production of the remainder of their product portfolio. Other "fabless" firms have no fabrication capability and are concentrating on generating designs for fabrication or for sale to other companies.

The result of all these changes is a shift in semiconductor manufacturing to Asia, where the majority of the foundries are located. Figure 3.13 shows, by geographic region, the change in installed capacity (use of 200 mm equivalents allows inclusion of all wafer sizes) from 1995 to 2009; it also includes forecasts for 2010 and 2011. The center of gravity for this industry is clearly shifting to East Asia.

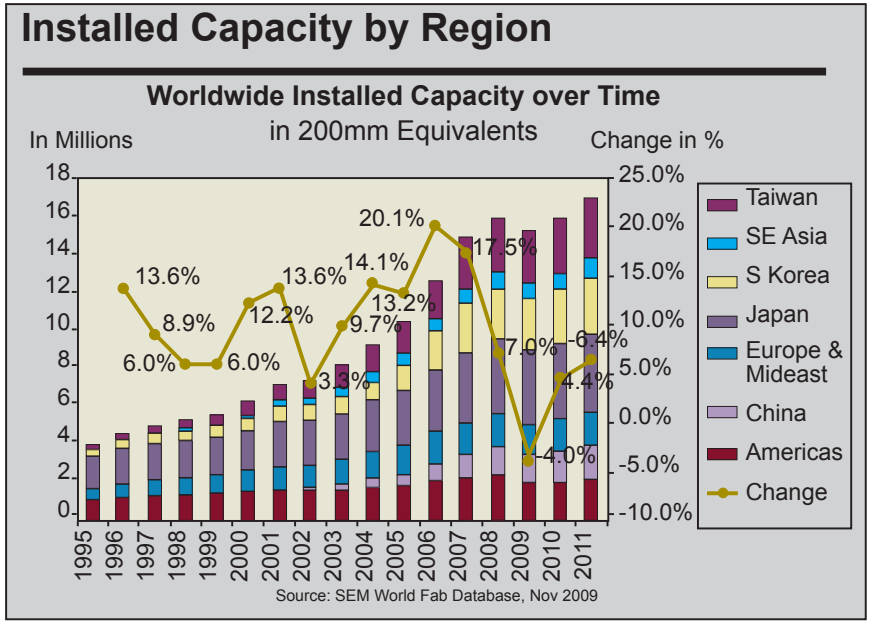


Figure 3.13: Rise of Asia in Semiconductor Manufacturing (© SEMI Industry Research & Statistics)[71]

Industry's Active Pursuit of Alternative Markets for Avenues of Profitability is an Outgrowth of the Competitiveness within the Industry

There are several promising areas for future growth in the semiconductor industry that are not as capital intensive or technologically challenging. These areas are photovoltaic (PV) and light emitting diodes (LED). There is also an emerging and potentially large application area for semiconductors in the biomedical market.

Photovoltaic (PV). Photovoltaic (or solar-cell) fabrication starts with square silicon wafers and uses a simpler—relative to CMOS (complementary metal-oxide-semiconductor)—fabrication process to produce a solar panel. Figure 3.14 shows a simplified version of the process; note the absence of the repeated mask exposures that produce the complex designs of an integrated circuit. The fabrication of the solar cell starts with flat sheets of silicon that are the same size as the finished solar cell. The processing of the silicon into a solar cell is much quicker than the process for fabricating an integrated circuit. While it is important to control the introduction of impurities in the process, solar-cell fabrication does not require the same level of stringent process controls involved in integrated-circuit fabrication.

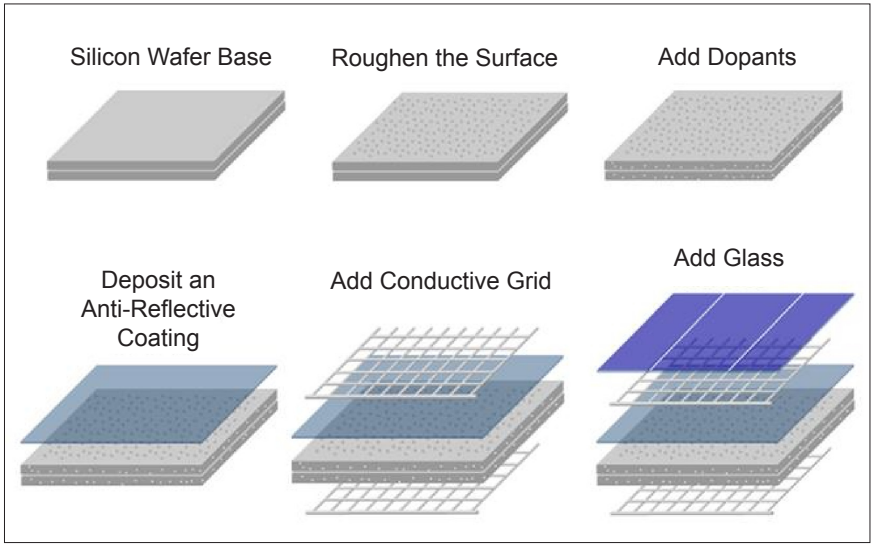


Figure 3.14: Fabrication of a Solar Cell[72]

The PV market is a topic of much discussion, but the business model for widespread adoption is still not in place. As Figure 3.15 indicates, demand in the industry is still heavily dependent on government subsidies for producers and consumers. Until PV can compete economically with conventional power sources, its progress will continue to depend on government subsidies.

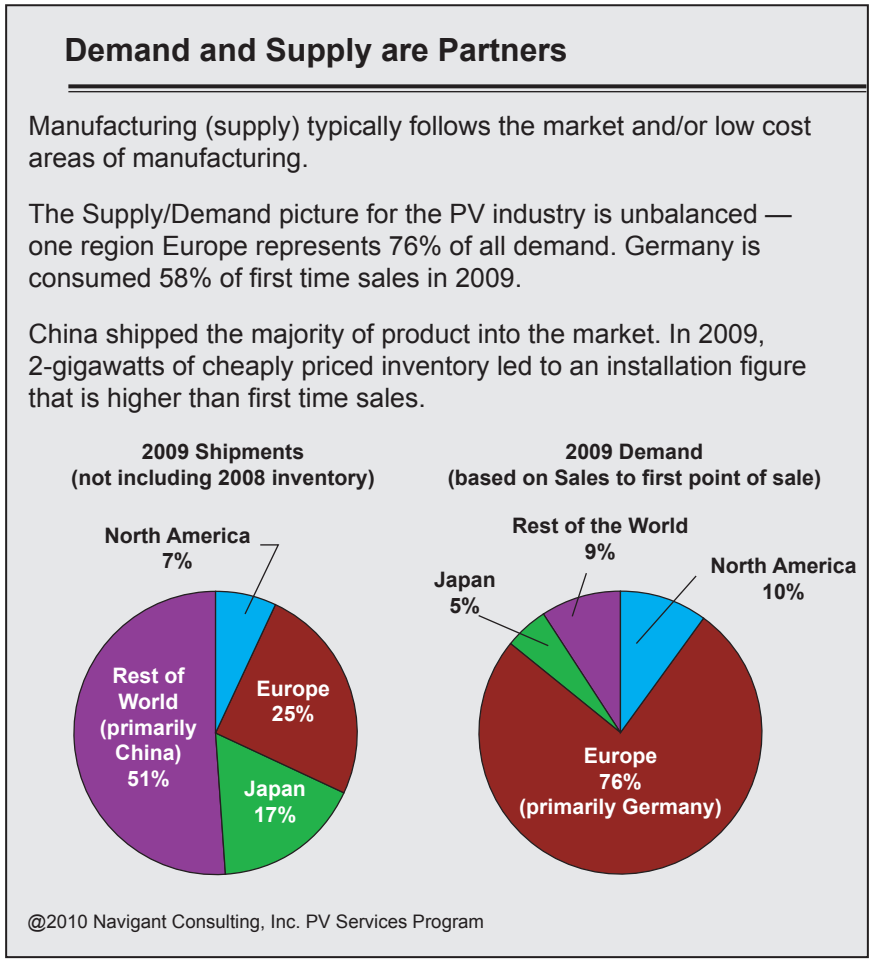


Figure 3.15: PV Market Still Developing (© Navigant Consulting)[73]

It is interesting to note from Figure 3.15 that China is a major producer of photovoltaic devices, but is not a major consumer. The fabrication finding is not surprising, since photovoltaic fabrication is not as complex as integrated circuits, but the future of mainland China as a consumer of photovoltaics remains open to speculation.

Light Emitting Diodes (LEDs). LEDs are another promising growth area. They are based on semiconductor substrates and, in concept, are even simpler than PV cells to produce. The LED industry is characterized as being 10 years behind the semiconductor industry in terms of process control and automation.[74] Figure 3.16 provides a simple view of the fabrication steps.

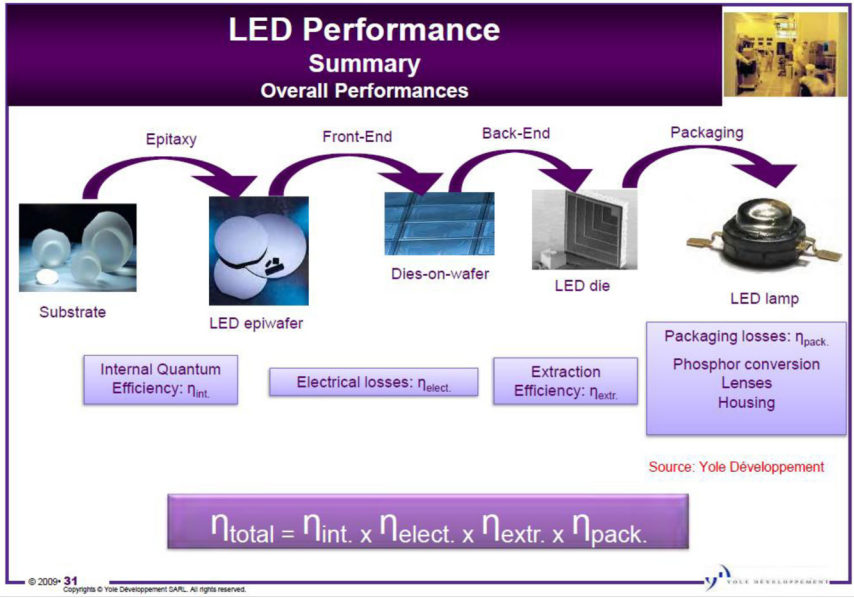


Figure 3.16: LED Fabrication (© Yole Développement)[75]

The fabrication of an LED also begins with silicon substrate. A layer of material is grown on the substrate, and the resulting epiwafer is ready for further processing. The dies are cut out of the epiwafer and packaged in a fixture with electrical connections.

Figure 3.17 shows that the promise of continuing market growth for LEDs is in the consumer-product areas of automobiles, flat-screen televisions and monitors, and energy-efficient applications, such as commercial and residential lighting. These growth projections and low technology barriers are now drawing larger semiconductor companies into this segment. While the consumer will benefit from the increasing competition, only the firms that can quickly scale up production will remain profitable.

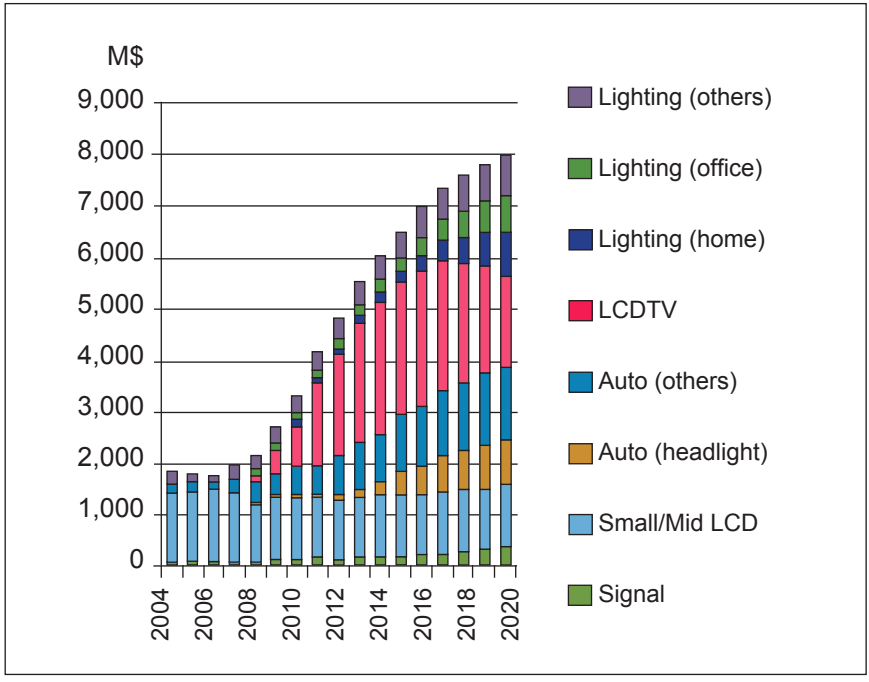


Figure 3.17: LED Market Forecast (© iSuppli)[76]

Figure 3.18 shows that the distribution of LED fabs is the highest in East Asia. The LED fab has a lower barrier to entry, and East Asia is close to the buyer (in this case, electronics and automotive manufacturers).

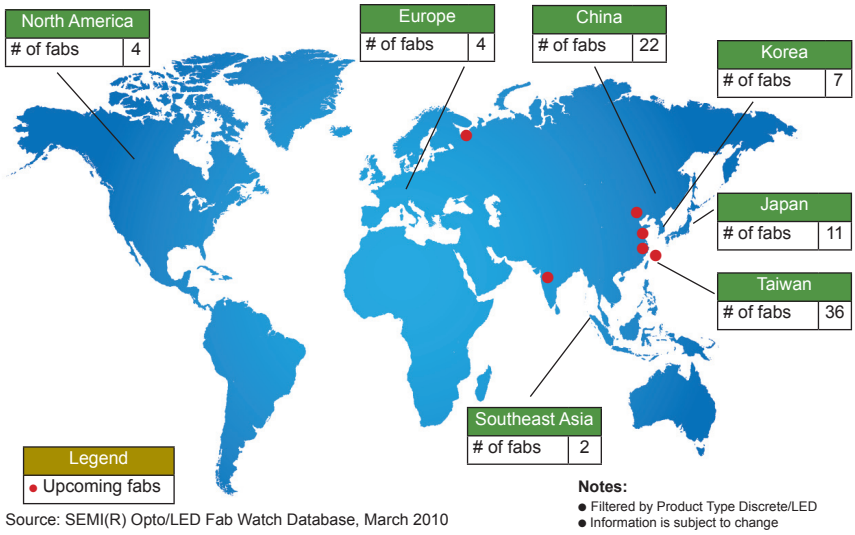


Figure 3.18: LED Fabs Worldwide (© SEMI Industry Research & Statistics)[77]

Biomedical. The semiconductor industry is awakening to the market potential of the application of semiconductors in medicine. During an *EE Times* virtual conference on Medical Systems Design (cited as an example data source in the preceding subsection), the keynote speaker presented a slide (Figure 3.19) listing the drivers and potential for growth in this market segment.

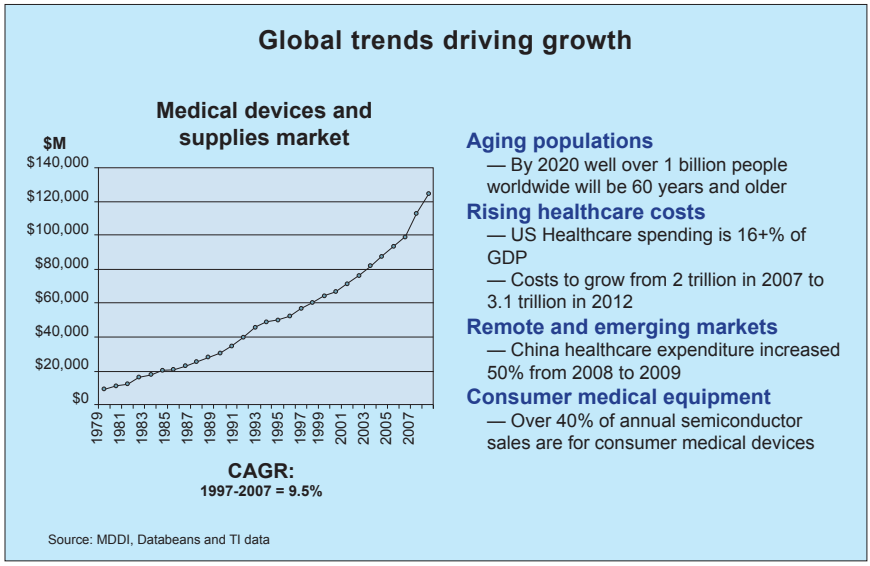


Figure 3.19: Medical Devices Market Potential (© Doug Rasor)[78]

Figure 3.19 provides insights into the drivers for potential demand for semiconductors in medical applications. The aging of populations in developing and developed nations is one driver. Another projected demand driver is rising healthcare costs, even in developing nations.

During a keynote address at SEMICON Korea, Tien Wu, the chief operating officer of ASE (Advanced Semiconductor Engineering), Taiwan (the world's largest provider of semiconductor-manufacturing services in assembly), presented a slide (Figure 3.20) showing that medical applications are part of the next semiconductor life cycle. The speaker went on to say that every single life cycle tends to be larger than the previous one, and champions of one tend to lose in the next life cycle.[79]

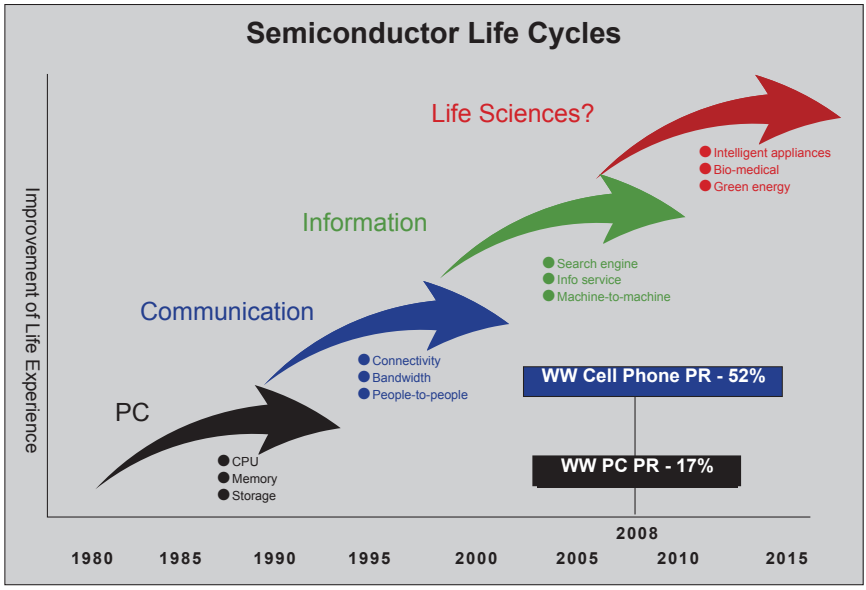


Figure 3.20: Semiconductor Life Cycles (© ASE Group)[80]

The continuing reductions in the size of integrated circuits and power requirements are raising the potential for integration of semiconductors into the human body. As Figure 3.21 illustrates, the applications of semiconductors are poised to become essential to our health and well-being.

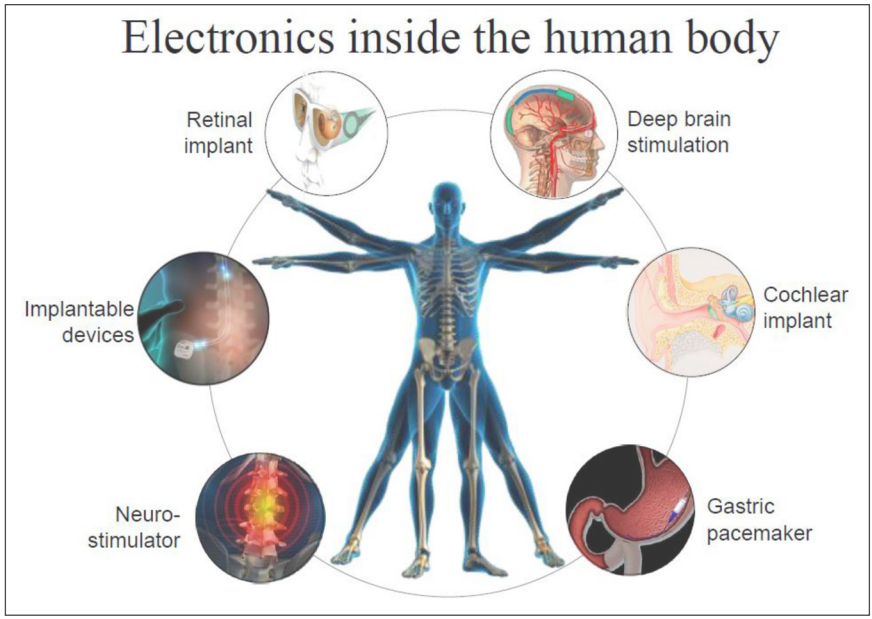


Figure 3.21: Semiconductor Integration into Biomedical Devices (© Doug Rasor)[81]

Summary

This subsection provided the result of building a strategic perspective on the semiconductor industry. The observations are the result of reviewing and evaluating a large body of collected information. The extensive footnoting for each observation provides the means for recalling and verifying the source of these observations. To summarize, particularly with respect to influences on the structure and conduct of relations between this industry and the governments with which they interact: (1) the industry is caught between buyer expectations and skyrocketing development and fabrication costs; (2) this industry-wide challenge at the leading edge is driving a continuing search for funding; and (3) the shakeout in the industry at the leading edge is driving competition in the trailing edge and alternate avenues of profitability (e.g., photovoltaic, LEDs, medical devices).

Step 5: Analyze Results

At this point, the all-source intelligence analyst needs to review the information collected and initial industry insights to make connections beyond the business world to produce strategic intelligence insights. The results of this fifth and final step will round out the all-source analysts' perspective and provide inputs for future intelligence products. We focus our newfound perspective on the target region of East Asia and suggest strategic intelligence insights for use in producing the intelligence products listed in Figure 3.6.

East Asia: Semiconductor Industry

While their approaches vary, the national governments in East Asia all set out to foster the establishment and growth of the industry.[82] But this governmental involvement does not guarantee continuing success. Brown and Linden explain:

> For governments, the years of U.S.-Japan rivalry established the reduced scope for government intervention in an established industry. In the 1970s a range of policy tools such as tariffs and subsidies were available to the Japanese government in its efforts to overtake U.S. chip firms, and international trade agreements forced these to be dropped once Japan's industry was established. The direct policy tools of the past have been sidelined by various agreements under the World Trade Organization (WTO), although developing countries like China are still able to provide subsidies to push their infant industry along.[83]

Figure 3.22 summarizes the state of the semiconductor industry in East Asia. A discussion of each country follows the figure.

	Market Strength	Value Chain Focus	Technology Node	Industry Outlook	Government Involvement	Observation
Japan	Memory	Lithography, Fabrication, Packaging, Testing	Leading Edge	Falling Behind	Minimal, Export Controls	Seeking growth through outsourcing and joint ventures in process R&D
Korea	Memory	Design, Fabrication, Packaging, Testing	Leading Edge	Memory	Trying to Expand Domestic Capability Beyond Memory Sector	One Company dominates. Domestic Industry is still developing.
Singapore	Foundry	Fabrication	TBD	TBD	TBD	Acquisition of Chartered by off-shore investors, outcome still TBD.
Taiwan	Memory, Foundry, PV, LED	Design, Fabrication, Packaging, Testing	Leading Edge	Positive Growth	Decreasing, Export Controls	Strategy emerging to keep Taiwan at leading edge and off-shore trailing edge and associated value chain steps to mainland China.
China	Foundry, PV, LED	Design, Fabrication, Packaging, Testing	Constrained By Export Controls	Positive Growth in Trailing Edge	Very Involved, and Governments at National, State, and Local levels have equity stake in domestic firms.	Chinese government interested in developing capability to address new markets such as PV and LED.

Figure 3.22: Summary of East Asia Semiconductor Industry, 2010

Japan

Japan is still a major competitor in the chip industry, but its domestic economic turmoil and its inability to adapt to the changing semiconductor market have affected its standing.[84] Japan's older established chip firms are pursuing consolidation and are outsourcing design and fabrication outside of Japan.[85] Referencing the semiconductor value chain, Japanese semiconductor-equipment manufacturers (machines that fabricate the chips) are competitive and increasing shipments to China and Taiwan.[86] Japan is home to Nikon and Canon, the number two and number three firms of the top lithography companies in the world.[87] Japanese-headquartered companies are the world leaders in the packaging materials segment of the semiconductor industry, with a 2009 combined market share of 65 percent of an estimated $15.8 billion packaging-materials market.[88] Beyond encouraging energy-saving semiconductor applications, the Japanese government is not playing a major role in their mature domestic semiconductor industry.[89]

Korea

Korea's Samsung is the world leader in memory production and flat-panel displays, but the government is concerned about the concentration of its semiconductor industry in the memory market, continuing dependency on the import of integrated circuits for incorporation into consumer electronics, a slow start in creating a fabless sector, and the rise of China's industrial capability.[90] The Korean news media provides a sociocultural insight into perceptions of China's rise, characterizing Korean workers as avoiding the arduous work in semiconductor and LCD production, while their counterparts in China work at one-fifteenth of the annual salary of a Korean worker. That same article describes Korean firms as seeming to be horrified at the full-fledged efforts of high-ranking China officials to establish a predominant position in the semiconductor industry. The Korean semiconductor industry is concentrated in a few very large companies, of which Samsung is clearly the flagship. Korean-headquartered semiconductor packaging materials companies are increasing their overseas versus domestic sales, but in comparison to Japan, they remain a small player.[91] The remainder of Korea's firms on the semiconductor value chain primarily supply the domestic giants of electronics, LG and Samsung.[92] *EE Times* reports that the Korean government's "System IC 2010" project is an effort to jump-start the nation's fabless community, including analog

start-ups, but it is too early to see the results.[93] Samsung recognizes the risk of the company's concentration in memory and is expanding into the foundry arena, already scoring a significant win by producing the processor for Apple's new iPad.[94] Through its "low carbon, green growth" vision, the Korean government is supporting the industrialization of renewable energy sources as a driver for new employment and economic growth.[95]

Singapore

According to the Economic Development Board of Singapore, there are four 12-inch fabs in operation in Singapore by the world's top three wafer-foundry companies.[96] This island nation is also home to headquarters activities of over 125 electronic companies (including the 50 largest). Recently, U.S.-based Applied Materials opened its first facility in Asia for manufacturing its advanced semiconductor-fabrication equipment, citing that over 70 percent of its business is now in Asia.[97] Singapore's Chartered foundry (once 62 percent owned by the Singapore government's investment agency, Temasek Holdings) struggled to compete with Taiwan foundry's Taiwan Semiconductor Manufacturing Company (TSMC) and United Microelectronics Corporation (UMC), and was acquired in 2009 by the Advanced Technology Investment Company (ATIC), a wholly owned subsidiary of the Abu Dhabi government.[98] This acquisition, folded into the ATIC and AMD Global Foundries venture, creates a first-tier foundry competitor.

Taiwan

Taiwan is home to the world's two largest pure-play chip foundries—Taiwan Semiconductor Manufacturing Company (TSMC) and United Microelectronics Corporation (UMC)—and also has the largest number of LED fabs. Figure 3.23 shows that, in terms of integrated-circuit foundry sales, these two firms are positioned well ahead of their peer competitors.

2009 Major IC Foundries

2009 Rank	Company	Foundry Type	Location	2007 Sales ($M)	2008 Sales ($M)	08/07 Sales %	2009 Sales ($M)	09/08 Sales %
1	TSMC	Pure-Play	Taiwan	9,813	10,556	8%	8,989	-15%
2	UMC	Pure-Play	Taiwan	3,430	3,070	-10%	2,815	-8%

2009 Major IC Foundries continued								
2009 Rank	Company	Foundry Type	Location	2007 Sales ($M)	2008 Sales ($M)	08/07 Sales %	2009 Sales ($M)	09/08 Sales %
3	Chartered*	Pure-Play	U.S.	1,458	1,743	20%	1,540	-12%
4	GlobalFoundries	Pure-Play	U.S.	0	0	N/A	1,101	N/A
5	SMIC	Pure-Play	China	1,550	1,353	-13%	1,075	-21%
6	Dongbu	Pure-Play	South Korea	510	490	-4%	395	-19%
7	Vanguard	Pure-Play	Taiwan	486	511	5%	382	-25%
8	IBM	IDM	U.S.	570	400	-30%	335	-16%
9	Samsung	IDM	South Korea	355	370	4%	325	-12%
10	Grace	Pure-Play	China	310	335	8%	310	-7%
11	He Jian	Pure-Play	China	330	345	5%	305	-12%
12	Tower**	Pure-Play	Europe	231	252	9%	292	16%
13	HHNEC	Pure-Play	China	335	350	4%	290	-17%
14	SSMC	Pure-Play	Singapore	350	340	-3%	280	-18%
15	TI	IDM	U.S.	450	315	-30%	250	-21%
16	X-Fab	Pure-Play	Europe	410	368	-10%	223	-39%
17	MagnaChip	IDM	South Korea	322	290	-10%	220	-24%

Source: IC Insights, company reports

*Purchased by GlobalFoundries in 4Q09.
**Tower bought Jazz in 2008.

Figure 3.23: TSMC Top among Foundries (© IC Insights, Company Reports)[99]

Given our previous discussion of the modularization of the semiconductor value chain and the rise of East Asia, it is not surprising to see the preponderance of foundries located there. The foundry model promises to shield a semiconductor firm from the intense capital costs of fabrication. It remains to be seen how far the fabless or fab-lite model will continue to progress.

Despite its history as the first chipmaker in Taiwan, UMC is seen as now falling behind the technology curve, succumbing to the continuing demands for capital to stay at the leading edge.[100] TSMC continues to grow, and expansion

plans garner most of the news regarding Taiwan's semiconductor industry. At the front end of the value chain, TSMC's Electronic Design Automation plans and offerings have led some analysts to identify TSMC as a new integrated device manufacturer (IDM).[101] Also at the front end, TSMC announced its collaboration with MAPPER Lithography (a Netherlands firm) to incorporate a maskless lithography technology in its manufacturing processes.[102]

Akira Minamika, a speaker at SEMICON Japan, presented a slide (Figure 3.24) that reinforces the view that TSMC is going to grow beyond the business model of a pure-play foundry. TSMC's announcement that it is going to open an R&D center and wafer fab to develop and produce LEDs clearly establishes an IDM role for TSMC, as least in optoelectronics, despite its assurances that it will remain a pure-play foundry in the IC market sector.[103] This is significant, because a key selling point of a pure-play foundry is that it does not compete with its customers by producing its own line of chips.

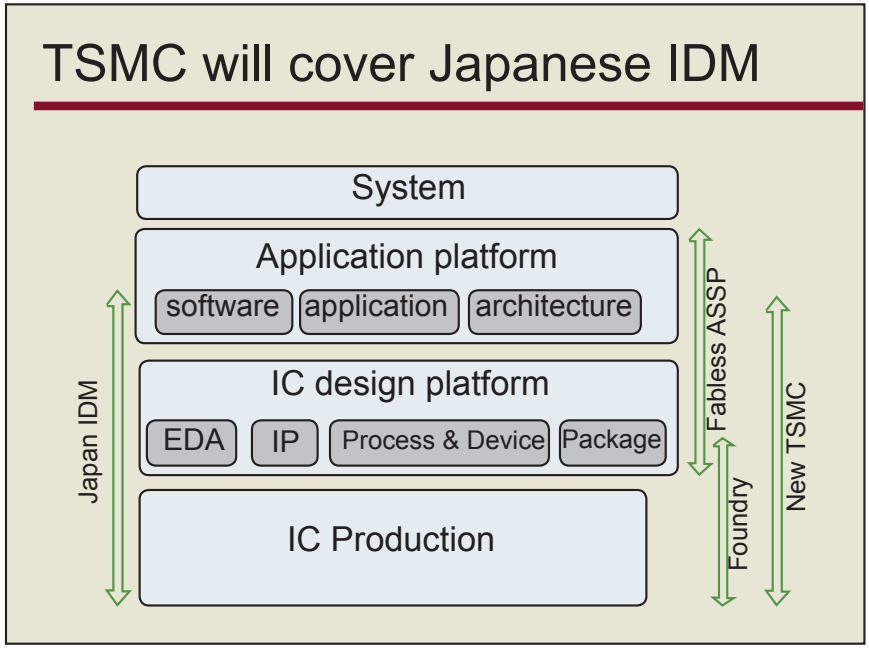


Figure 3.24: TSMC's Expanding Coverage (© IC Insights, Company Reports)[104]

Figure 3.24, provided at an industry tradeshow in Japan, highlights the recognition that TSMC is expanding its coverage of the value chain. This will be an interesting development, since Japanese firms use the foundry capabilities of TSMC and have not viewed TSMC as a competitor.

Although TSMC has a Samsung-like impact in its global stature, Taiwan has a more diverse semiconductor industry, with close ties to domestic and international electronics-manufacturing companies. Reflecting this strength of diversity is a recent legislative resolution that asks the Economics Ministry to discard a restructuring plan for Taiwan's DRAM industry, characterizing it as a waste of resources.[105] However, in the same session, it agreed to cut Taiwan's corporate tax rate from "20 to 17 percent and retain tax breaks targeted at R&D," which will sustain its national competitiveness.[106]

Strategic Intelligence Insight

The most interesting developments from a strategic intelligence perspective are the growing ties between Taiwan's and mainland China's semiconductor industries. In February 2010, Taiwan relaxed restrictions on "high-tech investment in China in another move to help local companies expand their global market shares and competitiveness."[107] The Taiwan Ministry of Economic Affairs will establish a panel to screen proposed investments. Existing regulations still in force prohibit local foundries from setting up 300 mm wafer fabs or foundries capable of processes below 130 nm, but will allow them to invest in or acquire China-based wafer foundries. Taiwan regulations now allow its chip companies to set up a maximum of three wafer fabs in China using processes less advanced than 0.18 micrometers (180 nm). The new rules also apply to low-end IC design and chip set packaging and testing industries, although projects greater than $50 million require screening for approval.[108]

Prior to this announcement, Taiwan's electronic manufacturing firms (the buyers of semiconductor chips) made use of China's labor force and location to build consumer end items. For example, Flextronics International, a Taiwan firm and one of the world's largest electronic manufacturing firms, is expanding its presence in China with a design center and manufacturing facilities in Wuzhong Export Processing Zone. This expansion complements its two existing computing design centers in Shanghai and Wujiang.[109] A government official in Taiwan allowed that the provisions on investments or

acquisitions of Chinese wafer foundries were meant to cover UMC's then-illegal investment in the Chinese foundry firm He Jian in 2006 and TSMC's pending stake in the Chinese foundry SMIC (a result of its successful intellectual property rights dispute with SMIC [Semiconductor Manufacturing International Corporation]).[110] Upon approval, UMC will be able to acquire the remaining 85 percent of He Jian, and TSMC will take a 10 percent stake in SMIC.[111] TSMC's chairman said they have no intent to take any day-to-day role in SMIC, and that they intend to keep their leading-edge fabs in Taiwan in order to take advantage of economies of scale; however, he also said they have submitted a technology-transfer application to produce higher-end circuits on its Shanghai wafer plant (about 200 mm fab).[112]

Smaller companies representing semiconductor value-chain activities are also strengthening ties to mainland firms. Chipbond Technology, a Taiwan firm that provides backend assembly processing for LCD driver ICs (a key component in LCD TVs), is requesting permission from the Taiwan government to increase its current holdings (20 percent) and take a majority share in China-based Chipmore Technology, in order to gain a foothold in China and its growing consumer market.[113] Taiwan's automotive industry, a consumer of ICs, is actively working to establish cross-strait agreements with China's automotive industry. Examples of IC applications include low-cost night vision systems, 360-degree viewing systems, and rain sensors.[114] A final, more conventional indicator of the increasing economic links between the two industries is illustrated by Taiwan's export statistics for May 2010: "[E]lectronics had the largest export value of $6.627B, rising by 47% on year and China (including Hong Kong) represents 43.8% of Taiwan's total export value."[115]

China

China's rise as an economic power is clear, but a subject of continuing debate is China's "openness" to reforms in governance and economics as it continues to develop. A single industry analysis can provide a degree of insight by the nature of its method of inquiry. Using our example of the semiconductor industry, here is the checklist of reasons why strategic insights on China are discoverable:

- The semiconductor industry is a priority for China.
- The technology and manufacturing leadership is centered in companies headquartered outside of China.

- The semiconductor industry has a history of openness in technology roadmaps and achievements.
- Semiconductor companies will not share their intellectual property or relocate manufacturing without openness in how their intellectual property is protected.

These points will be addressed as our analysis of results continues.

Figure 3.25 provides a map of the distribution and types of wafer fabs and foundries in China at the end of 2009.

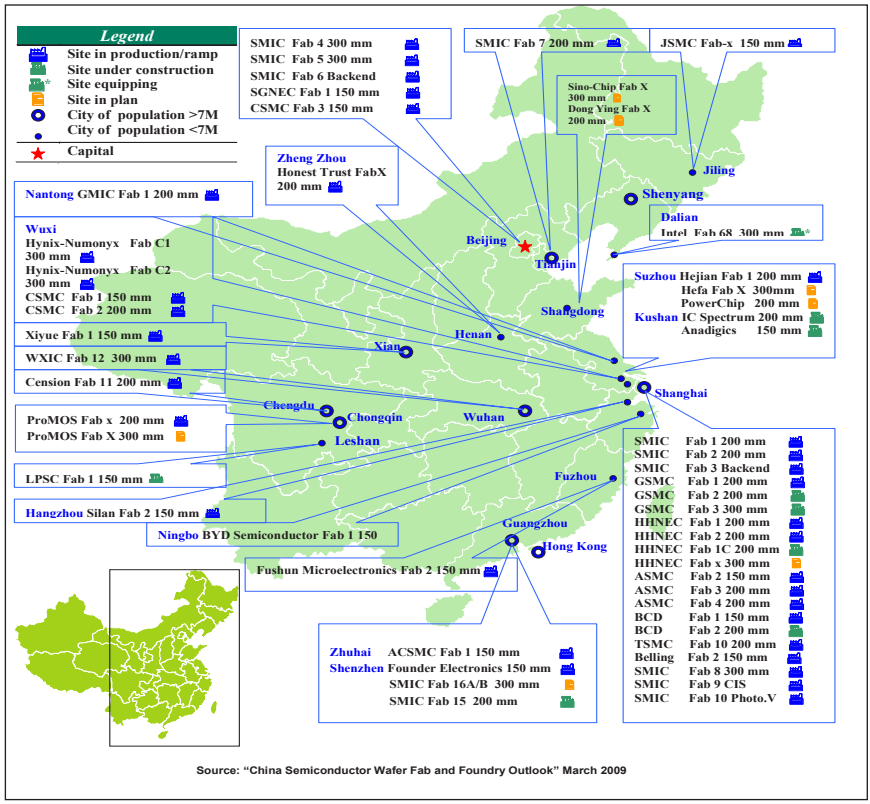


Figure 3.25: China Semiconductor Wafer Fab and Foundry Outlook (© SEMI)[116]

Studying the distribution and wafer-handling size of the semiconductor plants in China reveals several things. First, the majority of their capability cannot process 300 mm wafers, the current state of the art in the industry. Second, the majority of their manufacturing capability is clustered along the coastal areas. One factor driving this is the requirement to have a reliable infrastructure in place to support a semiconductor fab. This infrastructure must include reliable power, water, roads, and suppliers to support the 24/7 demands of a semiconductor fab.

China's government has a great interest in developing indigenous semiconductor fabrication capabilities. SEMI analysis of China includes the following excerpts:

> Since China surpassed Japan and the US in 2007 to become the world's largest consumer of ICs, China policy makers have increasingly voiced concerns about the 'chip gap' between supply and demand. In 2008, China consumed approximately one-quarter of the world's ICs, yet manufactured only $5.6 billion in chips, enough to support only 8% of their domestic requirements. By 2011, the China IC market will grow to $85 billion with domestic production expected to reach $8.2 billion, about 10% (iSupply, IC Insights, CSIA). By 2013, China's share of the global chip market will reach 35%. In the past, in markets such as computers, mobile phones, and automobiles, such an imbalance between supply and demand has prompted increased investments in local production capacity. … [T]he Chinese government also remains the biggest investor in the semiconductor industry in China. In the past five years, the China government influenced the investment of about $7 billion in new fabs. In the next five years, local government will likely continue to be the significant co-investor in strategic IC Fab projects throughout the country. Going forward, the central government may also invest up to $30 billion on semiconductor (semiconductor equipment and material are included), also software and high-end chip hardware industry by 2020.[117]

The profitability of China's leading-edge foundry, SMIC, provides insights into the government's progress. In 2000, the governments of Beijing, Shanghai, Wuhan, Chengdu, and Guangzhou put forward the resources to support SMIC.[118] After 10 years of investment, as Figure 3.26 illustrates, SMIC, China's bid to create a leading-edge foundry, has yet to turn a profit.[119]

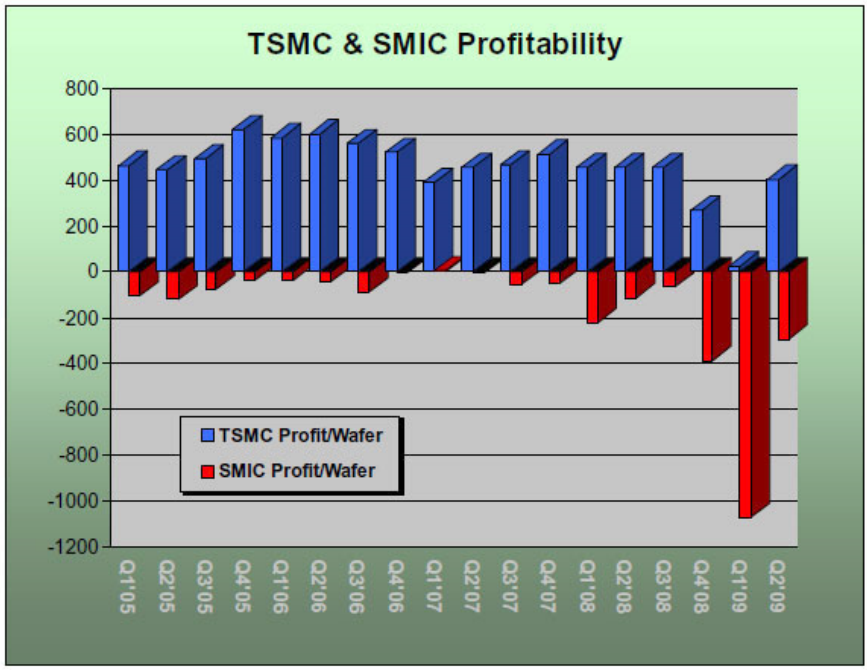


Figure 3.26: Profitability of Taiwan and Mainland China's Leading-Edge Foundries (© VLSIresearch. In "China Leads World Out of Recession, Through Recovery." January 14, 2010, *Semiconductor International*.)[120]

Figure 3.26 shows that, on a profit-per-wafer basis, Taiwan's TSMC has clearly outperformed China's SMIC. In addition to infrastructure requirements, a semiconductor fab has equally demanding process requirements. A high degree of process maturity is required in order to achieve success (both in terms of quality of product and turning a profit) in operating a semiconductor fab. SMIC's profit performance and TSMC's out-of-court settlement with SMIC (due to SMIC's theft of intellectual property belonging to TSMC) led to a turnover in SMIC leadership.[121] All of this indicates

that China's semiconductor industry has not attained the required process maturity required for leading-edge IC fabrication.

Recognizing that the bulk of the semiconductor market is in the trailing edge, taking advantage of the economic downturn, and the migration of the industry to 300 mm equipment, the trade press believes that China will invest billions over the next several years into repurposing and refurbishing 200 mm and 300 mm fabs, and utilizing primarily used and refurbished equipment.[122] Referencing some of the earlier figures showing the relative rankings of semiconductor firms, it is clear that the largest companies still reside outside of China. Also, the research and development expenditures of these industry leaders are much greater than China has been willing or able to invest.

China's intellectual-property laws and their enforcement are still a work in progress. One company characterizes patent enforcement in China as "slightly improved from terrible to bad," and said that China now concentrates enforcement on discovering export items to Europe, Japan, and the United States that illegally use China's intellectual property, recognizing that enforcement within China is not possible.[123] One rationale for TSMC's out-of-court settlement with SMIC is that it did not want to bankrupt SMIC and risk TSMC's intellectual property being acquired or lost entirely.[124] Now, TSMC, with its minority share, can closely monitor SMIC's use of TSMC's technology. The IBM Corporation is very adept at handling intellectual-property licensure for semiconductor processes, only raising eyebrows in the industry by offering technology that may allow Chinese firms to "catch up."[125]

Freescale, a U.S. semiconductor design firm, has five IC design centers in China, and describes its Chengdu center as "the front lines in the development and customization in the networking-chip arena."[126] One approach to protecting intellectual property would appear to be in jointly developing technology with China. Intel Capital, the Intel Corporation's global investment arm, and China Investment Corporation (CIC) announced that they are going to pair CIC's resources with Intel Capital's technology expertise to make strategic investments in pioneering for companies engaged in the next generation of groundbreaking technologies.[127] Although the agreement states that the investments will be outside of China, this is an interesting development to watch in order to understand the extent of the globalization of intellectual property.

As related earlier, many of the largest firms in the industry locate only less important processing or fabrication steps in China, sometimes due to export control laws, but also due to concerns about intellectual-property infringement. For example, Intel continues to run its leading-edge fabs outside of China in order to protect its microprocessor and process technology. Applied Materials operations in China has taken measures to prevent intellectual-property theft, such as "sealing its computers' ports in Xian, to prevent easy use of flash drives"; controlling removal of computers by employees; and maintaining computer passwords and door codes to control technology access.[128] Applied Materials continues to conduct its research and development in laboratories in the United States and Europe, but put its first Asian equipment-manufacturing operation in Singapore, where protection of intellectual property is more developed. Despite the risks of intellectual-property theft, the rising purchasing power of China's population, and governmental trade and tax policies, the semiconductor industry is placing more capability in China.

The example of Applied Materials and the establishment of a laboratory for assembly-line design in Xian illustrate the financial incentives for establishing operations in China. According to an article in the *International Herald Tribune*, first the Xian city government sold a 75-year land lease to Applied Materials at a deep discount, and then it reimbursed the company for about a quarter of the complex's operating costs for five years.[129] Thomas J. Friedman, an op-ed columnist with *The New York Times*, interviewed Paul Otellini, the CEO of Intel, comparing the incentives in the United States with those in China:

> "The things that are not conducive to investments here are [corporate] taxes and capital equipment credits," he said. "A new semiconductor factory at world scale built from scratch is about $4.5 billion—in the United States. If I build that factory in almost any other country in the world, where they have significant incentive programs, I could save $1 billion," because of all the tax breaks these governments throw in. Not surprisingly, the last factory Intel built from scratch was in China. "That comes online in October [2010]," he said. "And it wasn't because the labor costs are lower. Yeah, the construction costs were a little bit lower, but the cost of operating when you look at it after tax was substantially lower and you have local market access."[130]

Incentives to relocate to China are available to many countries, but they are not always financial incentives. An article in *Business Week* stated that Yukio Sakamoto, the president of Elpida Memory Inc., Japan's sole maker of computer-memory chips, announced plans to build factories in Taiwan and China to meet demand and reduce tax payments. Reading further in the article, it is clear Elpida is also relocating to avoid Chinese import tariffs.[131] In the same article, Intel (United States) and Hynix (Korea) set up factories in China "to avoid a 17 percent value-added tax that applies to chips imported into China and used in electronics sold domestically."

Despite China's outwardly successful mix of incentives and tax policies, the original equipment manufacturers (OEMs), assemblers of final end items for consumption, are still very cost conscious and will move to lower-cost areas of the world if it is more profitable. China's rising labor costs, increases in energy prices, quality problems, intellectual-property theft, and a global modular value chain keep other regions of the world as viable alternatives.[132]

When the economic downturn occurred in 2009, many Chinese workers left the coastal area and returned home to inland areas. Now, with the economic recovery and China's stimulus spending, many of these workers find work at home and are not migrating back to the coastal areas—inflating wages in the coastal areas, where electronics manufacturing is centered.[133]

On the environmental-regulatory front, China is planning to implement REACH (Register, Evaluation, and Authorization of Chemicals) regulations similar to the European Union's REACH. The REACH regulations require companies to declare the types and uses of chemicals in production and also include chemicals released during the end products' normal use.[134] The effects and enforcement of these regulations on the semiconductor industry remain to be seen.

China is aggressively pursuing all the new avenues of profitability. As shown earlier, China has a large number of LED fabs in operation. In photovoltaic (PV) production, already noted is Applied Materials' opening of the world's largest solar research center in China. Domestically, China's government is working with their PV Industry Association to assist in setting up a photovoltaic industry alliance for research and standards setting. It might be a strategic insight to say that, in order for China to incorporate the PV industry into its

energy economy, it will need to set standards for PV components and grid connections, improve those grid connections, and resolve the economics of getting PV-generated power (requiring large open areas) to distant population areas.[135] Figure 3.27 illustrates the PV cluster areas in China.

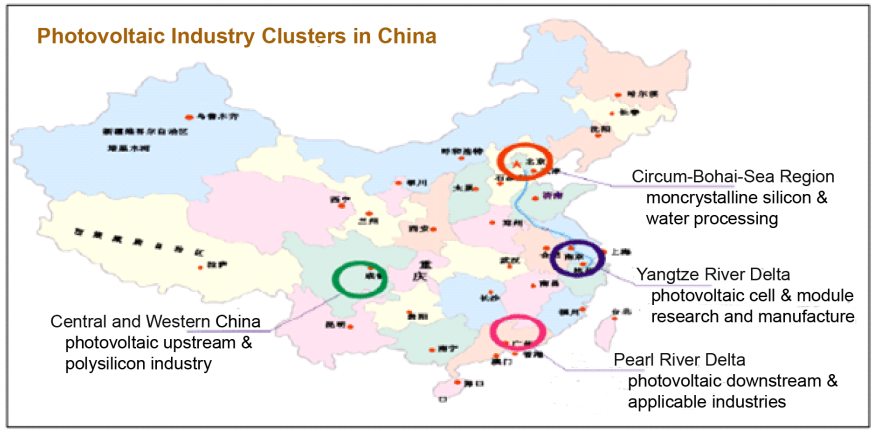


Figure 3.27: China's Photovoltaic Industry (© ResearchinChina)[136]

While Figure 3.27 provides the location of industry clusters for mainland China PV manufacturers, more important is the previous citation that describes the Chinese government's hosting of meetings to set standards and share information among the domestic PV companies.

Medical-device applications provide a sociocultural view into China and why the semiconductor industry is looking at China as a large potential market. An article in *EE Times China* states:

> The portable/home electro-medical device market is enjoying a fast and stable expansion in China due to the government's medical reform, citizens' concern in healthcare, and the unique features the devices are offering.
>
> The CAGR of portable electro-medical device market is expected to go up significantly, with market survey showing rapid expansion from 8 billion yuan ($1.17 billion) in 2006 to 28 billion yuan ($4.1 billion) in 2011. "The market is proven to have a powerful anti-risk capability because the whole

> market is oriented toward China's internal demand and is basically insusceptible to the global financial crises. In China, the market is only in the initial startup phase, so the market demand is huge. In addition, the Chinese have an increasingly high consciousness of health," Zhou Wensheng, senior sales manager of ADI's medical division in Asia-Pacific, said.
>
> Like ADI, the worldwide semiconductor manufacturers cast more eyes on the portable/home electro-medical device market of China. Looking forward to the future, everyone will have multiple portable medical devices rather than just one, making it a more exciting market than the cell phones. After losing the country's huge mobile phone market, numerous Europe and U.S. companies are expected to try their best to get a share of the portable/home electro-medical device market of China. "China and the world have a huge demand for the portable electro-medical devices, and China will enter the list of the largest electro-medical device manufacturers and largest markets," Fan Xujin, chief product marketing engineer of Microchip's medical product division, said.[137]

Summary

While Japan was the leading challenger to the U.S. lead in the semiconductor industry in the 1980s, Japan's domestic economic challenges have slowed the growth of its semiconductor industry. Important is the decline of Japanese firms in manufacturing lithography equipment (the basis for the key value-chain activity, mask creation). Japanese companies Nikon and Canon were the leaders in the lithography-equipment market, but they are now overshadowed by the market leader ASML, headquartered in the Netherlands. If business conditions do not change, ASML will have a virtual monopoly on leading-edge lithography equipment.

The Korean firm Samsung is the world's leader in semiconductor memory, but its enormous size has not translated into development of a broader semiconductor industry in Korea.

Singapore is the leader in hosting the regional headquarters functions of almost all the major semiconductor companies in the world. But Singapore's

divestment of Chartered Semiconductor to outside investors leaves open the question of its future industrial capability.

Taiwan is a success story in joint government and private industry development of an industrial base capability. Taiwan's semiconductor industry is conscious of the challenges of staying at the leading edge and is pursuing cost savings by off-shoring trailing-edge and associated value-chain steps to lower-cost areas, such as mainland China.

Mainland China has a strategy to develop an indigenous capability to supply the chips that they currently must import for both domestic and export industries. Various levels of government in China provide incentives and equity backing to domestic semiconductor firms. After a decade of investing to establish a leading-edge foundry in China, the government is now content to buy up trailing-edge semiconductor fabrication equipment and relocate it to China. In the PV- and LED-fabrication sectors, where there are no leading-edge export controls, China is rapidly building up value-chain elements tailored to these market sectors. Analyzing the semiconductor industry and East Asia provides some strategic insights.

Despite China's juggernaut appearance in technology advancement, the leading edge of semiconductors represents a difficult level to attain and, as a result, China is slowing its indigenous leading-edge development. China's internal market potential, incentives, and tax policies are attracting the placement of semiconductor operations in China, but concerns about intellectual property are still valid. As the foremost consideration, if higher profits can be earned in manufacturing outside of China, then manufacturers will relocate elsewhere, despite China's policies. A sign of China's rising consumer population is forecasted to increase demand for cell phones, LCD TVs, and medical devices within China.

A strategic insight that rises up to the level of strategic intelligence insights is the growing economic ties between mainland China and Taiwan. Taiwan industries are leveraging Chinese industry in pursuit of competitive advantage. China is gaining advanced technology and building its industries through ties to Taiwan and other nations. This insight will be developed and discussed further in the next chapter's concluding discussion and evaluation of the value of industry analysis to the Intelligence Community.

Chapter Four

Conclusion

An all-source intelligence analyst can use the analysis tools of business strategists and competitive intelligence professionals in analyzing an industry in another country or region of the world. By using these tools, an analyst is able to develop strategic intelligence insights about a nation's plans and intentions. The main conclusions to be drawn are as follows: (1) industry analysis is easy to grasp and only a little harder to apply; (2) the results of industry analysis provide a useful lens for intelligence-collection analysis and synthesis; and (3) globalization has become a defining force in the world, and merits more attention from the Intelligence Community.

Applying Industry Analysis

The application of industry analysis is, first and foremost, not a major break with the conduct of all-source analysis. Industry analysis will provide a lens (or frame of reference) that complements the existing repertoire of analysis tools within the Intelligence Community. At a minimum, it offers a better alternative than performing a keyword search on open-source business and industry information.

Follow the Steps

The steps for conducting industry analysis are straightforward and meant to be easily internalized. The first steps of selecting and defining the industry for analysis will be the most difficult. For one thing, selecting an industry that will yield strategic insights automatically excludes countries that, while of interest to the Intelligence Community, do not have a developing industry sector or choose not to participate in the global economy. Second, defining an industry is time-consuming, but its practice (and, concurrently, the exposure to economics and industry structure) will serve the analyst in defining other industries in the future. Using the models described earlier will facilitate a focused review and selection of sources.

The collection and analysis steps are the most straightforward for the all-source analyst. At that point, the analyst will understand the nuances of the

industry information before him or her and have a framework for collection and analysis. The major difference in these steps, between the business analyst and the all-source analyst, is the strategic perspective the all-source analyst brings to the task. In addition, the all-source analyst can synthesize the findings with other Intelligence Community inputs to improve strategic understanding.

Utility of Industry Analysis

In the last chapter, the major strategic-intelligence insight points to the growing economic ties between mainland China and Taiwan. Analysis of the semiconductor industry provides this insight, but also lays the foundation for future analysis of other industries, such as the automotive industry, to see if they are also fostering cross-strait ties.

Another topic for further exploration is mainland China's progress in rebuilding its power-generation infrastructure to handle alternative "green" power generation and applications. The photovoltaic and light-emitting diode industries (subsets of the semiconductor industry) provide a window into a challenge that the United States also faces. It is now clear that mainland China has an interest in developing its indigenous semiconductor industry and is willing to deal with Taiwan in pursuit of that goal. This strategic insight lasers through the unpredictability of nationalism or geopolitical flare-ups.

Utilizing the addition of a new lens for intelligence analysis is achievable at the level of the all-source analyst by examining current national intelligence estimates to see how our strategic insight above "fits" with the prevailing view within the Intelligence Community. The classification of national intelligence estimates leaves this action outside of this book. Ian Bremmer, however, in his book *The End of the Free Market*, offers an interesting strategic assessment independent of our industry analysis in the context of discussing the challenges posed by state-sponsored capitalism:

> Beijing's primary military concern is the risk of a direct or proxy conflict with the United States over Taiwan. But the Chinese leadership is well aware that no U.S. government will support a Taiwanese bid for independence, and why should the Chinese launch a self-defeating invasion of the

> island when it can co-opt most of Taiwan's business elite with privileged access to investment opportunities on the mainland? So far, globalization has been good to China's Communist Party, and wars are bad for business.[138]

It is important to point out that the inclusion of industry analysis is meant to enhance the national-intelligence estimate, not drive startling new conclusions. What is suggested here is that too great a focus on political and military dimensions by the Intelligence Community leads to discounting the influence of economics in international politics.[139] The strategic-intelligence insights we seek come from examining the "contours" of industry interactions with foreign governments, and any contributions to a national-intelligence estimate resulting from these strategic-intelligence insights will be in the "contours" of the estimate. As a result, the final utility or value-added assessment of industry analysis remains within the analysis community.

Increased Attention by the Intelligence Community to Globalization

In the introductory chapter, the background question of the role of the Intelligence Community in assessing the effects of globalization came with a brief historical perspective. A couple of the points from this perspective are worth highlighting. First, the Intelligence Community at one time believed that the way a nation (the Soviet Union) acted in the economic sphere was likely to reveal its intentions. Second, policymakers' interest in the community's industry analysis was motivated by perceptions of the United States potentially being outperformed economically and militarily by the Soviet Union.

The Soviet Union is consigned to the history books, and there is no concern about a renaissance of centralized command economies among the world's nations. But there is a relatively new competitor to the U.S. free-market system, which is a "state-sponsored capitalism" that may spark an interest in reviving industry analysis within the Intelligence Community. State-sponsored capitalism "is a system in which the state dominates markets primarily for political gain."[140] The recent acquisition of Chartered Semiconductor in Singapore highlighted earlier is an example of state-sponsored capitalism at work. The Singapore government's holding company was a major shareholder in Chartered and approved its sale to a joint venture by a holding company of the Abu Dhabi government and the publicly traded semiconductor firm

AMD.[141] This exchange was in part a nation-to-nation business transaction that, in the case of Abu Dhabi, solely benefits the ruling family.

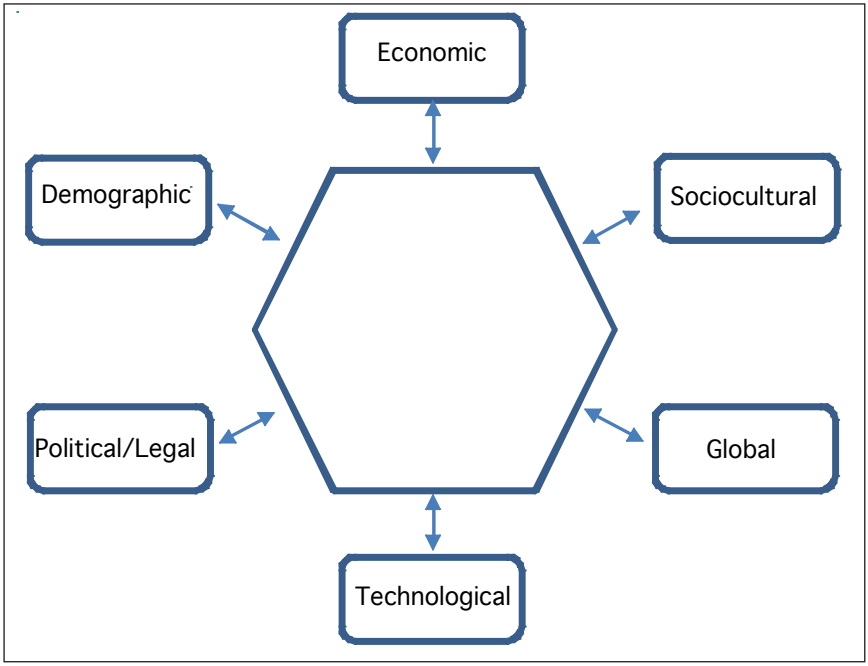
Ian Bremmer notes that state-sponsored capitalism is not protectionism for developing national competitiveness; it is the state "using markets to create wealth that can be directed as political officials see fit."[142] Put another way, the major difference in state-sponsored capitalism vis-à-vis free-market capitalism is that the overriding objective of state-sponsored capitalism is maintaining the party in power, not the prosperity of its people.[143]

The potential for the United States being outperformed economically and militarily is open for debate, but it should not be the threshold for reawakening industry analysis within the Intelligence Community. The global interdependencies between nations are a fact and, in the case of U.S.-China relations, have even earned the catchphrase "mutually assured economic destruction." This play on the Cold War term "'mutually assured destruction' is not to suggest that a new cold war is upon us, but that the battle for the free market is a battle for national competitiveness that must avoid catastrophic outcomes."[144] Even though the current priorities of the Intelligence Community reflect its customers' requirements, there is a need for the community to step up and enhance its intelligence offerings with insights into globalization and its potential effects on national security.

Appendixes

Appendix A

External Environment Model Segments and Elements[145]



Source: Adapted from Hoskisson, Hitt, and Ireland.

Demographic

Population Size, Age/Gender Structure, Geographic Distribution, Ethnic Mix

Economic

Distribution/Uses of Resources, Impact of Global Economy on Domestic Economy/ Markets, Macroeconomic Factors

Sociocultural

Cultural Attitudes, Customs, Values, Education/Skill Levels, Workforce Diversity, Attitudes about Quality of Work Life, Concerns about Environment

Global

Important Political Events, New Markets, Changes to Existing Markets, Different Cultural and Institutional Attributes

Technological

Product Innovations, Focus of Private and Government-Supported R&D Expenditures, New Technologies

Political/Legal

Appendix B

Semiconductor Industry Tutorial

The purpose of this appendix is to provide a brief tutorial on semiconductors, the key activities involved in their development, and the size and composition of their market. Chapter 2 introduces three models to use in industry analysis, and Chapter 3 describes a methodology for selecting an industry for analysis, which, for the purposes of this book, is the semiconductor industry. The next step is to define the selected industry, which in this case requires developing a broad understanding of the semiconductor industry. This understanding will first be put to use in developing a value chain for the industry. The development of a value chain is an iterative process; it reflects and reinforces your understanding of the industry. It is quite possible that a value chain is already available from open sources. If so, it can be used as a guide for sorting out the key activities and processes involved in producing semiconductors. Following the industry definition step, the value chain will be put to further use during the collection and analysis of information on the semiconductor industry.

Since the technology behind semiconductors is over 60 years old, there is a wealth of open-source information on the semiconductor industry, both in print and on the Internet. What will become readily apparent is how far that technology has progressed, especially in process development and applications. There are useful glossaries of industry-related terms available on the Internet. This appendix will cite several for definitions so the analyst has a choice of sources in case a website becomes unavailable.[146] To understand an industry, a basic understanding of its products and markets is necessary. For the semiconductor industry, product knowledge equates to a basic understanding of semiconductors and their development into integrated circuits. Research into the size and composition of the semiconductor market brings into focus the globalization of the industry and its importance to developed and developing nations of the world.

Gain knowledge of semiconductors and their development into integrated circuits.

Devices made from semiconductor materials are the foundation of the computer and communications industries. Also familiar are the multitude of

consumer-oriented electronic devices (such as cell phones) in use in almost every corner of the earth. Semiconductors are also increasingly used in the automotive and medical-devices industries, and form the basis for promising devices for saving or generating energy.[147] One surprising fact is that, although it was the U.S. federal government's funding of basic research and government demand for electronics that fueled the early growth of this industry, today the government constitutes less than 1 percent of the semiconductor market.[148]

The first question to answer is: what are semiconductors? A semiconductor is a material that has the properties of a conductor and an insulator. The exact properties are determined during the production of the silicon crystal and the processing of the wafer that provides the platform for the integrated circuit. The fabrication process described here is referred to as CMOS (complementary metal-oxide semiconductor) and is the industry's main manufacturing platform.[149] Figure B.1 illustrates the process for creating the silicon crystal.

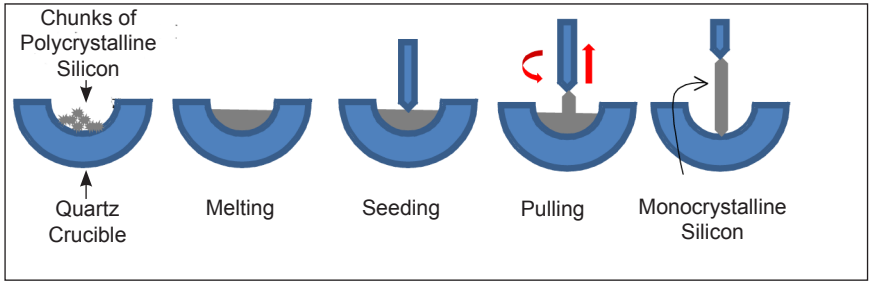


Figure B.1: Crystal Growth[150]

There are several methods for creating the silicon crystal for wafers. The process in Figure B.1 is common and the one most likely to be found in diagrams, pictures, or video on the semiconductor process. The rough silicon material is noteworthy because, while it is a common material, there can be temporary shortages of supply due to the cyclical nature of the semiconductor market. The raw material is melted in a furnace.[151] The next step, called *seeding*, involves lowering a single silicon crystal into the molten material. The molten silicon immediately affixes itself to the seed, forming a single crystal, and while the seed is slowly withdrawn, its simultaneous rotation produces

the resulting cylindrical shape. The cylinder of pure silicon is often referred to as a boule.[152] The process is controlled to produce the desired diameter of the finished wafer. A wafer is defined as "a thin slice with parallel faces cut from a semiconductor crystal."[153] Wafers are produced in a wide variety of sizes and characteristics. The state of the practice now produces up to 300 mm (about 12 inches in diameter) wafers.

To create the wafers, the boule is removed from the furnace and the two ends are sawed off. Figure B.2 shows the entire boule cut into the thin slices referred to as the wafers. Following this, the wafers are run through a lapping process to remove surface irregularities and produce a uniform flat surface. Lapping involves placing the wafer on a revolving surface with a constant stream of a fine abrasive material, and then another surface revolving in the opposite direction placed above. The sandwiching of the wafer between the counter-rotating surfaces and the wet abrasive gradually removes irregularities. The etching step is a chemical process to remove any crystal damage from lapping. Polishing, the final step, smooths the uneven surface left by the lapping and etching and makes the wafer flat and smooth.

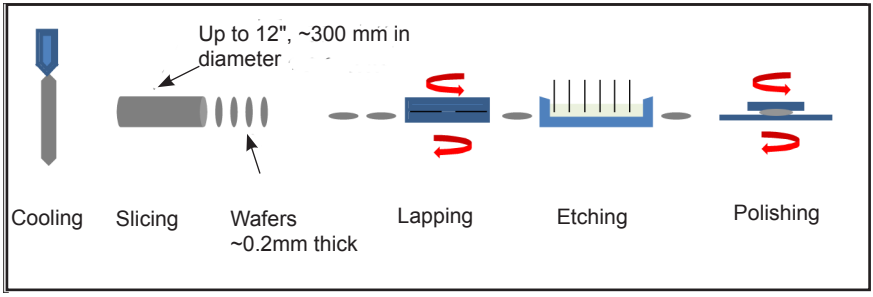


Figure B.2: Wafer Processing

Integrated Circuits

A wafer is composed of a semiconductor material and is the platform for the process that creates integrated circuits, which are then packaged into chips. An integrated circuit, or IC, is created on a wafer, usually made of silicon, and can hold anywhere from hundreds to hundreds of millions of electronic components, such as transistors, resistors, and capacitors.[154]

Transistor Density

The familiar phrase "Moore's Law" is frequently referred to in articles regarding the semiconductor industry. In reality, Moore's Law is not a law at all; it is an observation made by Gordon Moore in the 1960s and later revised in the 1970s. His observation, remarkably prescient, is that the transistor densities on integrated circuits will double every two years.[155] Transistor density is important because more transistors equates to more functions in a smaller space, lower power requirements, and, with economies of scale, lower cost. Figure B.3 provides an example of increasing capability and decreasing price for semiconductor memory.

Reduced Memory Cost Drives New Architecture and Applications

	1979	1984	2001	2005	2007
	SONY WALKMAN	**SONY DISCMAN**	**IPOD ORIGINAL**	**IPOD NANO**	**IPOD TOUCH**
Storage Technology	Cassette Tape	CD	Hard Drive	Flash	Flash
Storage Size	60 MB (20 songs)	700 MB (26 songs)	5 GB (1,000 songs)	4 GB (800 songs)	16 GB (3,200 songs)
Cost	$200	$299	$400	$249	$399
Device Cost per Song	$10	$11.50	$0.40	$0.31	$0.13

Figure B.3: Memory Example (© Mentor Graphics)[156]

All of these are what the industry and its customers have come to expect. Figure B.4 illustrates how Moore's Law is still a driving force in the semiconductor industry:

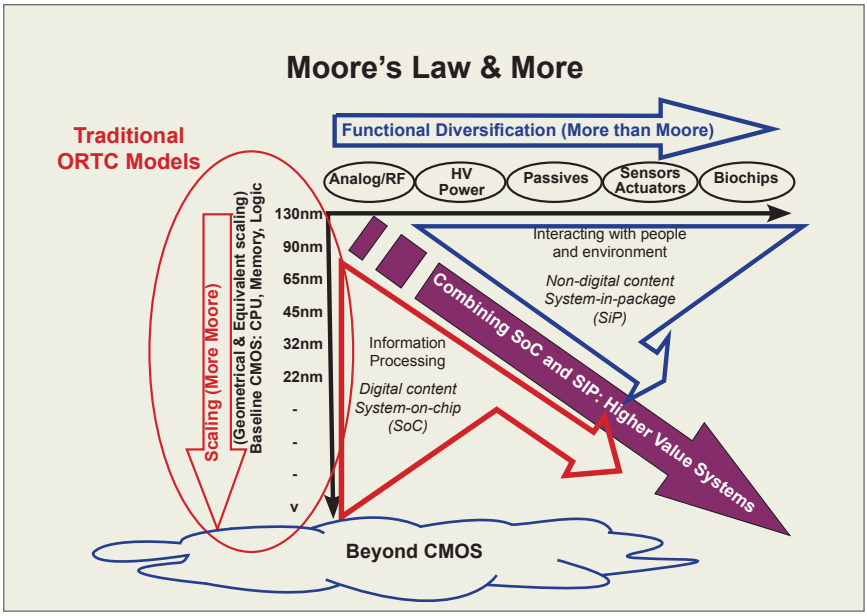


Figure B.4: Beyond Moore's Law (© Semiconductor Industry Association)[157]

Note that the y-axis scale shows decreasing numbers, with "nm"—nanometers, or a billionth of a meter—appended to each. The numbers refer to the width of the smallest feature—"feature size"—on an integrated circuit.

Feature Size

Almost all trade journal issues bring up the topic of feature size, typically by using the shorthand of providing the scale of the integrated circuits in nanometers. Figure B.5 provides a pictorial representation of the comparative size of objects on a nanometer scale.

How many nanometers is ...	Approximately
The width of a hair	100,000 nanometers
The width of a red blood cell	10,000 nanometers
The length of a typical bacterium	1,000 nanometers
The width of a dust particle	800 nanometers
The wavelength of red light	650 nanometers
The wavelength of ultraviolet light	300 nanometers
The length of a typical virus	100 nanometers
The size of a membrane enzyme	10 nanometers
The width of a carbon atom	1 nanometer
The distance between carbon atoms	0.15 nanometers

Figure B.5: Size Comparison (© Northwestern University Nanoscale Science and Engineering Center); Images in Nanoscale (© Dennis Kunkel Microscopy, Inc.); Table by Waldron and Batt (© McNeil-Lehrer Productions)[158]

Referring to Figure B.5, feature sizes below 25 nm are now going into production. This means the size of an individual circuit path on a chip is smaller than the length of a virus and a little larger than a strand of DNA. A topic of much discussion is: what comes after the limits of scaling are reached?

Chip Design

The process for creating chips starts with the design. The software used in designing chips is an entire industry unto itself. It is called the electronic design automation (EDA) industry, and this industry develops and sustains integrated circuit design tools. EDA Consortium, the electronic design automation industry trade association, also has a web-accessible video that quickly describes the entire semiconductor design and fabrication process.[159] The design for

an integrated circuit is captured on digital files that are used throughout the manufacturing process.[160] These digital files are representative of the information exchange that characterizes a modularized value chain.

Chip Fabrication

Figure B.6 provides a simplified view of this process. The design information is first used to create a mask. In simple terms, the mask is a clear piece of quartz, referred to as a reticle, which is etched with one level of the integrated circuits' design. Today's integrated circuits may have many layers, so there would be a reticle for each layer. Using lithography, a process similar to processing photographs, the wafer is coated in a material referred to as "photoresist"; then a light is projected through the reticle, and that layer of the design is transferred via exposure to the wafer. A key step in process planning is maximizing the number of copies of the design layer that can be placed on the wafer. Each of those copies on the wafer is referred to as a "die." Per the design files, the wafer is then sent off to additional processing; one step removes the exposed photoresist, leaving the design of the integrated circuit behind. The wafer is then recoated with photoresist and is exposed using the reticle containing the next level of the design.

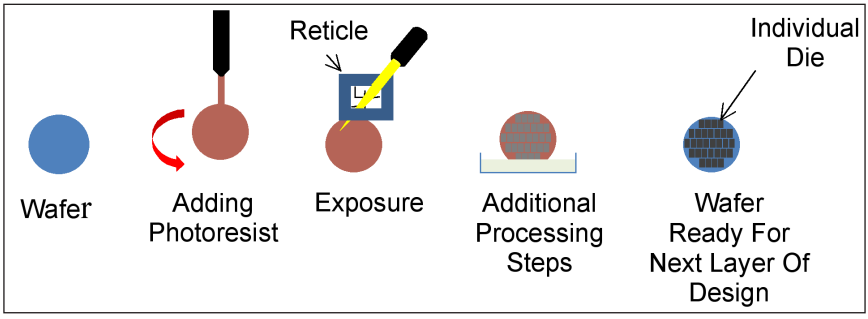


Figure B.6: Fabrication Steps

Referring to Figure B.6, the bare wafer on the left is ready to start the fabrication process. The wafer is coated with photoresist and then moved to the lithography station, where it is exposed to light. The reticle (also referred to as the mask) is a thin piece of quartz that is etched with one level of the integrated circuits' design. The mask holds a layer of the design and, when the wafer coated with photoresist is exposed to a light source, the areas of the

wafer not obscured by the design pattern on the mask are exposed. This wafer is then put through a series of chemical baths that strip away the exposed photoresist on the wafer, leaving the layer of the design untouched. The wafer is then re-covered with photoresist and run through the lithography station, and then put through a series of chemical baths to strip away the photoresist and leave the second layer of the design on the wafer.

To process the wafer with multiple mask sets (one mask for each layer on the individual chip) takes weeks. Since the processing steps for a typical forty-layer chip design take so long, and it is cost-prohibitive to build an additional line, semiconductor companies pursue other options, such as increasing the number of chips they produce on each pass through the process.

One approach for increasing the number of chips produced is to increase the wafer size. The industry standard is currently a 300 mm wafer (roughly 12 inches in diameter). The industry movement from 200 mm to 300 mm wafers provided an increase of 125 percent in surface area on which to produce integrated circuits (dies). For example, this transition means that for a die size of 161.3 square millimeters (approximately ¼ square inches), the fabrication line is processing 376 dies per wafer on a 300 mm wafer versus 148 dies on a 200 mm wafer.[161]

The industries' nine-year transition from 200 mm to 300 mm and the cost of developing an entirely new process line are not lost on the equipment manufacturers. While 300 mm wafer processing continues to deliver productivity improvements, that transition did not translate into higher profit margins for the semiconductor-equipment industry. The industry is currently debating a move to a 450 mm wafer (a 125 percent increase over 300 mm), but only a few of the industry leaders are showing interest, and there is no agreed-to business model that shows funding for the transition and also provides a reasonable return on investment for the semiconductor-equipment manufacturers.[162]

Chip Packaging

Figure B.7 shows the continuation of the fabrication process once all of the integrated circuit design is on the wafer. When all of the design is processed into the wafer, each die on the wafer is tested, and any defective dies are marked. The individual dies are then cut from the wafer and undergo further testing.

The usable dies are attached to frames and, after wire bonding and encapsulation, they are chips ready for placement in their intended application.

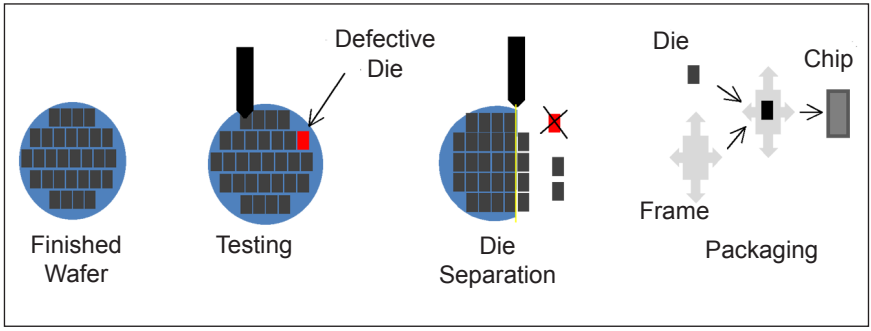


Figure B.7: Die Testing and Packaging

The semiconductor industry is technology driven and requires a continuing investment in research and development to produce the advances observed by Moore's Law. Equipment to produce a leading-edge computer chip costs hundreds of millions of dollars.[163] A basic understanding of the fabrication of semiconductors is possible in a short amount of time. The fact that global industry is trying to figure out how to reduce feature size so it can deliver increased performance in ever-smaller packages is readily apparent without requiring a technical degree or know-how.

Understand the size and composition of the semiconductor market.

Industry trade associations, industry trade press, international trade organizations, market research firms, and government documents are just a few of the available sources for market information. For the semiconductor industry, the World Semiconductor Trade Statistics, a nonprofit corporation, compiles industry trade statistics and provides market forecasts.[164] The data is provided by the member semiconductor companies and is considered to be a reliable source of information. The top-level forecasts are provided free via their website. For 2008, the world semiconductor market was $248.6 billion, and Figure B.8 shows the major market segments and their relative percentage of the total market.

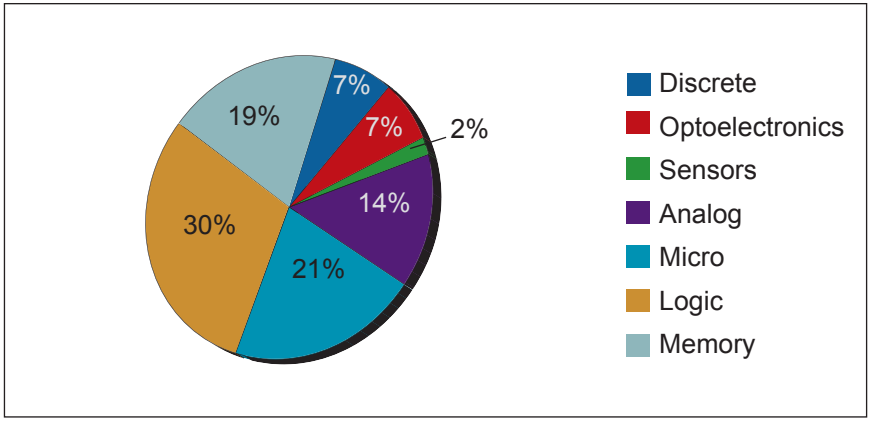


Figure B.8: Total World Semiconductor Market, 2008—$248.6 Billion[165]

A look at the composition of the semiconductor market segments reveals that logic, memory, and micro devices are the largest segments. The IC Insights glossary cited earlier and the Semiconductor Glossary provide the following definitions for the semiconductor market segments shown in the figure:[166]

- **Discrete**—A class of electronic components that includes power transistors and rectifiers, each of which contains one active element. In contrast, ICs typically contain hundreds, thousands, or millions of active elements in a single die.
- **Optoelectronics**—A device that is responsive to or that emits or modifies light waves; for example, LEDs, optical couplers, laser diodes, and photo detectors.
- **Sensors**—A component that provides an electrical signal in response to a specific physical or chemical stimulus, such as heat, pressure, magnetic field, or a particular chemical vapor.
- **Analog**—Integrated circuit realizing analog functions; in analog systems, output signal follows continuously input signal.
- **Micro**—Integrated circuits that are microcomputer related. This category contains three subcategories, that is, microprocessor (MPU), microcontroller (MCU), and digital signal processor (DSP).

- **Microprocessor**—(1) A central processing unit (CPU) fabricated on one or more chips, containing the basic arithmetic, logic, and control elements of a computer that are required for processing data; or (2) an IC that accepts coded instruction, executes the instructions received, and delivers signals that describe its internal status. The instructions may be entered or stored internally.
- **Microcontroller**—A single-chip microcomputer with onboard program ROM and I/O that can be programmed for various control functions.
- **Digital Signal Processor**—Digital circuits used to enhance, analyze, filter, modulate, or otherwise manipulate standard real-world (i.e., analog) functions, such as images, sounds, radar pulses, and other such signals in real-time.

- **Logic**—Integrated circuit performing switching functions; implements logic functions, such as AND, OR, and NOT. Also includes Application Specific Integrated Circuits and Field Programmable Gate Arrays.
- **Memory**—Integrated circuit consisting of memory cells and usually including associated circuits such as those for address selection and amplification. A class of integrated circuits that store digital information, for example, ROM, EPROM, EEPROM, Flash memory, DRAM, and SRAM.

The industry trade press is also a good source of market information. For example, in Figure B.9, *EE Times India* reports the change in semiconductor revenue by end-use from 1995 to 2009. As the figure's title indicates, the only major change in the total available market (TAM) is the incorporation of handheld wireless. The market sectors and percentages have remained relatively steady, which reflects a mature industry. Remember, during this step of building understanding, we are not trying to analyze the semiconductor market and what the above market allocations portend for the industry. It is enough that we understand what major product areas are the buyers of semiconductors.

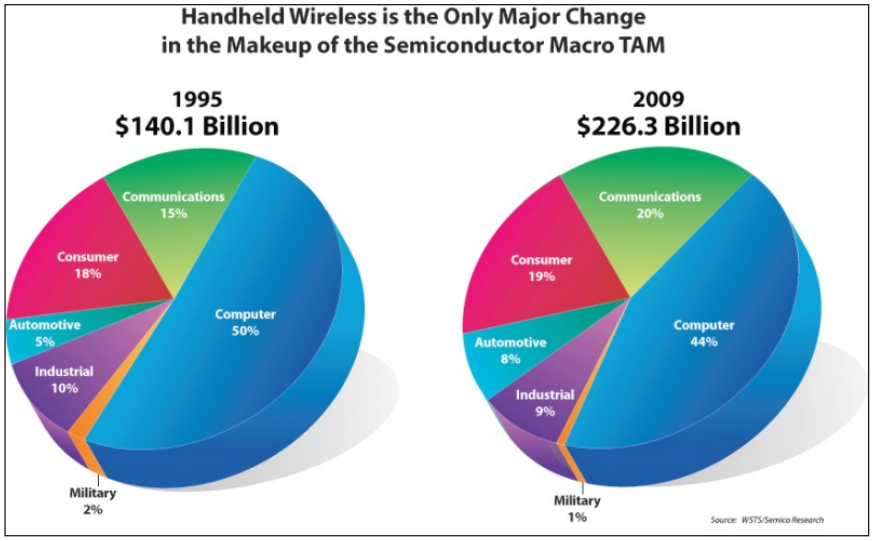


Figure B.9: Semiconductor Total Available Market (TAM) (© Semico Research)[167]

Now that we have looked at the market for semiconductors (power of the buyer), it is also important to understand who are the major producers of semiconductors (intensity of competition). Figure B.10, reported in *EE Times Asia*, shows the top semiconductor vendors ranked by revenue estimates for 2009. These companies will become familiar as information is collected. It is readily apparent that Intel is by far the leading semiconductor producer, with Samsung a distant second, and the remaining companies trailing behind it.

Top 10 Semiconductor Vendors by Revenue Estimates, 2009 (Millions of U.S. Dollars)						
2009 Rank	2008 Rank	Vendor	2008 Revenue	2009 Revenue	2008–2009 Growth (%)	2009 Market Share (%)
1	1	Intel	34,814	33,253	-4.5	14.6
2	2	Samsung Electronics	17,391	17,686	1.7	7.7
3	3	Toshiba	10,601	9,604	-9.4	4.2
4	4	Texas Instruments	10,593	9,142	-13.7	4.0
5	5	STMicroelectronics	10,270	8,510	-17.1	3.7

Top 10 Semiconductor Vendors by Revenue Estimates, 2009 (Millions of U.S. Dollars) continued						
2009 Rank	2008 Rank	Vendor	2008 Revenue	2009 Revenue	2008–2009 Growth (%)	2009 Market Share (%)
6	8	Qualcomm	6,477	6,409	-1.0	2.8
7	9	Hynix Semiconductor	6,010	6,035	0.4	2.6
8	7	Renesas Technology	7,081	5,670	-19.9	2.5
9	11	Advanced Micro Devices	5,298	5,157	-2.7	2.3
10	6	Infineon Technologies (incl. Qimonda)	8,224	4,682	-43.1	2.1
		Others	138,375	122,223	-11.7	53.5
		Total Market	**255,134**	**228,371**	**-10.5**	**100.0**

Source: Gartner (March 2010)

Figure B.10: Top 10 Semiconductor Vendors, 2009 (© Gartner, Inc.)[168]

Figure B.11 shows the top ten semiconductor companies projected by 2010 capital investment; the inclusion of the major product line for each company is also useful. For example, Intel is listed as having the largest revenue of semiconductor companies in 2009, and its major product area is listed as MPU, or microprocessor unit. The microprocessor is the main component in the computers that now come in so many forms and sizes. The large revenue numbers reported by Intel are also consistent with the computer sector of the semiconductor market being the largest of the various sectors. Samsung reported the second-largest revenues, and its major product area is memory. While memory is important to the computer sector, memory applications are also present in the consumer, communications, and automotive sectors. There is also a major product category, foundry, which appears on the list. Referring to the value-chain examples in Chapter 2, a foundry is a firm that does not design and produce its own line of semiconductors. The foundry receives the design information and masks from a customer and fabricates the individual die. In some cases, they do not even separate the die from the wafer, and the customer will either complete the packaging of the die or outsource the task to another vendor. The value chain helps to visualize what activities are being discussed in the trade press.

Top 10 Semiconductor Industry Capital Spenders*										
2010 Rank	Company	2007 ($M)	07/06 % Change	2008 ($M)	08/07 % Change	2009 ($M)	09/08 % Change	2010F ($M)	10/09 % Change	Major Product
1	Samsung	7,964	16%	6,750	-15%	3,518	-48%	5,000	42%	Memory
2	Intel	5,000	-13%	5,197	4%	4,515	-13%	4,900	9%	MPU
3	TSMC	2,557	6%	1,877	-27%	2,687	43%	4,800	79%	Foundry
4	Toshiba	3,595	18%	2,210	-39%	950	-57%	1,950	105%	Memory
5	AMD/ GlobalFoundries**	1,683	-9%	621	-63%	466	-25%	1,900	308%	MPU/ Foundry
6	Hynix	5,145	8%	2,900	-44%	855	-71%	1,840	115%	Memory
7	Micron	3,700	23%	2,300	-38%	800	-65%	1,715	114%	Memory
8	Nanya	2,098	131%	695	-67%	640	-8%	1,415	121%	Memory
9	UMC	850	-15%	349	-59%	551	58%	1,350	145%	Foundry
10	Elpida	2,111	59%	890	-58%	535	-40%	1,000	87%	Memory
	Total	**34,703**	**12%**	**23,789**	**-31%**	**15,517**	**-35%**	**25,870**	**67%**	

*Includes company's share of joint-venture spending **Includes Chartered in 2010
Source: IC Insights, Company Reports

Figure B.11: Top 10 Semiconductor Industry Capital Spenders (© IC Insights, Company Reports)[169]

Understanding the size and scope of the market makes it apparent that the semiconductor industry, although mature, is still experiencing growth. It may seem counterintuitive that a mature industry continues to spend large amounts on research and development, but that is because, while the semiconductor process steps are easy to understand, the actual achievement of producing the design is intellectually and capitally intensive. To bring it up to a strategic level, it is also important to note where the leading companies are headquartered and where they are producing their product. This will become apparent as collection begins and will be important in our analysis task. For now, having a list of the key competitors will be useful in the collection and analysis of industry information.

This appendix provides a basic background in the industry we want to analyze. At this point, we have a general overview of semiconductors and the processing of semiconductors into integrated circuits, and insight into the size and composition of the semiconductor market. A test of our understanding is to construct a value chain for the industry. If you have already found one for the industry, use it as a contextual template for the collection and analysis of industry information.

Appendix C

Data Sources Specific to Semiconductor Industry

Books

Since getting the latest data is a primary consideration, it is important to search for recent books on the industry. For example, at the start of research for this study, a 2009 book by Claire Brown and Greg Linden, *Chips and Change*, turned out to be an excellent data source for understanding the origin, development, and future of the semiconductor industry.[170] The book even provides a value chain for the semiconductor industry. A 2008 book on China's high-technology industry, *China's Science and Technology Sector and the Forces of Globalization*, provides an interesting perspective on the prospects and problems for development of China's semiconductor industry.[171]

Reports

The National Academy of Sciences, a nonprofit institution, has a searchable website of its publications, and many are free to download.[172] While the publication dates of National Academy reports are unpredictable, you can request e-mail notifications when topics of interest are available. The federal government, particularly within the Department of Commerce, provides a regular stream of trade and industry statistics, but occasionally they will also produce reports on global trade topics that are of interest. For example, the Bureau of Industry and Security provides current news reports regarding trade issues, and its Defense Industrial Base Programs link provides a list of Defense Industrial Capability and Technology Assessments regarding foreign industrial development that may be of interest.[173]

Trade Associations

The major semiconductor trade association websites provide news and documents, although the frequency of their updates and data available are irregular. The major semiconductor industry trade associations are

- Semiconductor Industry Association (SIA): *www.sia-online.org*.

  They provide an updated factsheet with basic statistics on the worldwide

semiconductor market and also provide issue papers regarding global competition.

- Taiwan Semiconductor Industry Association (TSIA): *www.tsia.org.tw/Eng*.
- Japan Electronics and Information Technology Industries Association (JEITA): *www.jeita.or.jp/english*.
- Korea Semiconductor Industry Association (KSIA): *www.ksia.or.kr/eng/main.*
- China Semiconductor Industry Association (CSIA): *www.csia.net.cn*. (Note: website's language is not translated into English.)
- Singapore Semiconductor Industry Association (SSIA): *http://www.ssia.org.sg*.
- Electronic Design Automation Consortium (EDAC): *www.edac.org.*
- Semiconductor Equipment and Materials International (SEMI): *www.semi.org*. SEMI is an international trade association that represents the suppliers to the semiconductor industry. It also includes suppliers to the display and photovoltaic (solar-cell) industries. The SEMI trade shows are held around the world, with each providing insight into the host country's semiconductor industry. The SEMI international standards forum invites members to collaborate on developing standards. The SEMI industry statistics group presents industry forecasts and invites other organizations to also share their forecasts at SEMI events.

Trade Journals

The most useful sources of current information on the semiconductor industry are the industry trade journals. Trade journals are much better sources than government policy announcements and the occasional analytical articles in metropolitan newspapers and business magazines, because many of those stories are not much more than news releases from the subject company. The industry trade journals, on the other hand, are reflective of the global evolution of this industry, and not only carry articles of interest to the technical community, they also provide analysis and forecasts on industry-wide

issues. The semiconductor trade press is not immune to industry competition, though. For example, during this book's preparation, the parent company for the trade journal *Semiconductor International* ceased operations and removed its content from the Internet. The reality of publishing these days makes it important to capture hardcopies of source articles in order to document the sources of analysis. In the semiconductor industry, most of the trade journals are available as Web subscriptions, some without charge, while others charge a small fee for subscribing or downloading full text articles:

- *EE Times Asia*: *www.eetasia.com.*
- *EE Times India*: *www.eetindia.co.in.*
- *Electronic Design News*: *www.edn.com.*
    - *Electronic Business*—separate subscription available from EDN.
    - *ElectronicNewsToday*—separate subscription available from EDN.
- ElectroIQ—portal for electronics manufacturing: *http://www10.giscafe.com/nbc/articles/1/737191/%3Cem%3Ewww.ElectroIQ.com%3C/em%3E.*
    - *Solid State Technology*—digital edition available from ElectroIQ.
- SEMI Newsletters: *www.semi.org.*
    - *SEMI Global Update*
    - *Semiconductor Manufacturing Newsletter* (simplified Chinese)
- *DigiTimes*, *www.digitimes.com*—provides news summaries free of charge, but to access full articles requires a subscription.

Other Internet Sources

This category concerns the Internet and its ever-evolving platforms and content. The website YouTube (*www.youtube.com*), although pedestrian to aficionados of social media, still provides good sources of information. Using search terms gained from your study of the industry can yield video clips from news organizations, trade associations, and even companies within the industry.[174]

Blogs and Twitter

The blogs by industry analysts, enthusiasts, or employees are embedded or linked into many of the industry trade journals, and can be a good source of information. The EDA Consortium website has a publications page (*www.edac.org/news_publications.jsp*) that provides a list of links to trade journals, but also provides links to news and blog sites, such as EDACafé (*http://www.edacafe.com*), or individual bloggers, such as EDA Confidential (*www.aycinena.com*).

The use of Twitter by the trade journal *Semiconductor International* is noteworthy, but it only Tweeted links to its journal content. This trial experiment went offline with the demise of that trade journal.

Webcasts and Virtual Conferences

The increasing use of webcasts and virtual conferences provide good real-time sources. Subscriptions to the industry trade journals will lead to announcements of these events. These events offer another avenue for the industry to share information and develop market opportunities. The presenter slides are usually available for download prior to the presentation, or the site allows archival access. Figure C.1 shows a recent *EE Times* virtual conference portal that provides all the trappings of a conference with spaces for the auditorium, exhibition, and business meetings.[175]

Figure C.1: Virtual Conference Portal (© UBM Electronics)

Referencing Figure C.1, in a six-hour conference, the listeners can choose the sessions they want and even interact with the presenter via the portal interface. A visit to the exhibit hall provides a view of kiosks for each company exhibiting. Entering the kiosks, the visitor sees a list of company content, such as product presentations and white papers. The virtual conference remains as an archive on the *EE Times* website, but, as with other Internet sources, it is advisable to download the information before it disappears.

Trade Shows

Trade shows are the best alternative to actually visiting semiconductor companies in other countries. Tradeshows will offer sessions in a variety of areas, and it pays to read the program beforehand to ensure it is not devoted to a sub-industry topic or technical interchange. Also, unless you are multilingual, make sure the session is in English or that simultaneous translation is available. Be sure also to take the time to walk through the exhibit halls and gather literature of interest. One caution is that most corporate booths will require a business card or the signing of a register before they will give out literature. The purpose of the exhibit hall is to generate business leads for the companies, so bring appropriate identification if you want to collect

information. As a final note, in the absence of attending the trade show, the trade press usually reports from the show and provides their perspective via the Internet. By way of an example of what is available, the SEMI tradeshows are scheduled a year in advance and occur in a different country each quarter. The SEMI tradeshows provide market forecast presentations, and also offer a copy of the proceedings. The shows provide an outsider's perspective of semiconductor companies (SEMI represents the suppliers to the industry), as well as insight into the future outlook for the industry.

Bibliography

Applied Materials. "What Is Solar Electric Power?" Applied Materials video, 6:33. *http://www.appliedmaterials.com/media-resources/wisep*.

Armour, Norm. "The Innovation Imperative: Toward a New Model for Semiconductor Manufacturing." Presentation at SEMI ISS, Half Moon Bay, CA, January 2010.

ASE Group. "Semi Business Evolution." Presentation by Tien Wu, SEMICON Korea 2010, Seoul, Korea, February 2010.

Aycinena, Peggy. *TSMC: The New Pax Romana*. May 26, 2010. *http://www.aycinena.com/index2/index3/tsmc%20pax%20romana%202010.html.*

Baumol, William J., and Alan S. Blinder. *Economics Principles and Policy*. 7th Edition. Orlando, FL: Dryden Press, 1998.

Berger, Suzanne. *How We Compete: What Companies around the World Are Doing to Make It in Today's Global Economy*. New York: Doubleday, 2006.

Birnbaum, Mark D. *Essential Electronic Design Automation (EDA)*. Upper Saddle River, NJ: Prentice Hall, 2004.

Bitran, Gabriel R., Suri Gurumurthi, and Shiou Lin Sam. "The Need for Third-Party Coordination in Supply Chain Governance." *MIT Sloan Management Review* 48, no. 3 (Spring 2007): 30–37.

Bogdanski, Jack. "Obsolescence Management: Another Perspective." *Military Embedded Systems* (January/February 2009). *http://www.mil-embedded.com/articles/id/?3747.*

Boundless. "Overview of Types of Plans and Tools for Planning." May 20, 2014. *https://www.boundless.com/management/strategic-management/the-planning-process/overview-of-types-of-plans-and-tools-for-planning/.*

Bradsher, Keith. "China Drawing High-Tech Research from U.S." *New York Times.* March 17, 2010. *http://www.nytimes.com/2010/03/18/business/global/18research.html?sq=Applied%20Materials%20&st=nyt&adxnnl=1&scp=2&adxnnlx=1309464261-clRhmw1kjIyyEagvJFAo7A.*

Bremmer, Ian. *The End of the Free Market*. New York: Portfolio, 2010.

Britton, Phil. *"Integrating Web 2.0 Tools in Your Intelligence Process."* Washington: Strategic and Competitive Intelligence Professionals Professionals Conference, 2010. Comment during lecture.

Brown, Clair, and Greg Linden. *Chips and Change: How Crisis Reshapes the Semiconductor Industry*. Cambridge, MA: MIT Press, 2009.

Bruck, Bob. "Economics and Collaboration Panel." Presentation at SEMI ISS, Half Moon Bay, CA, January 2010.

Business Dictionary. "Industry Analysis." *http://www.businessdictionary.com/definition/industry-analysis.html.*

Caves, Richard E. *American Industry. Structure, Conduct, Performance*. 7th Edition. Edited by Otto Eckstein. Vol. Foundation of Modern Economics Series. Englewood Cliffs, NJ: Prentice Hall, 1992.

Center for History and New Media, George Mason University. Zotero. *http://www.zotero.org/.*

Chang, Pao-Lang, and Chien-Tzu Tsai. "Finding the niche position-competition strategy of Taiwan's IC design industry." *Technovation* 22, no. 2 (February 2002): 101–11.

Chul-ho, Lee. "[Viewpoint] In China, a Giant Stirs." Korea JoongAng Daily. February 1, 2010. *http://joongangdaily.joins.com/article/view.asp?aid=2916001.*

Clarke, Peter. "TSMC breaks ground on LED lighting wafer fab." *EE Times.* March 25, 2010. *http://www.eetimes.com/electronics-news/4088182/TSMC-breaks-ground-on-LED-lighting-wafer-fab*.

———. "Winners, losers in 2009 chip vendor ranking." *EE Times Asia*. March 31, 2010. *http://www.eetasia.com/ART_8800602399_480200_NT_72aebd89.HTM.*

Conner, Margery. "Protecting your hardware IP in China: Practical experience." EDN. February 4, 2010. *http://www.edn.com/blog/1470000147/post/650052465.html?nid=2431&rid=16641388.*

Council On Competitiveness. *http://www.compete.org.*

Danne, John. "Semiconductor State of the Industry." Semiconductor Industry Association, March 17, 2010. *http://www.choosetocompete.org/downloads/2010_SOI.pdf.*

Dennis Kunkel Microscopy, Inc. In Northwestern University. "How Small Is Small?" DiscoverNano. *http://www.discovernano.northwestern.edu/whatis/index_html/howsmall_html.*

Dertouzos, Michael L., Richard K. Lester, and Robert M. Solow. *Made in America*. New York: HarperPerennial, 1989.

Economic Development Board. "Facts and Figures." *EDB Singapore*. June 28, 2010. *http://www.edb.gov.sg/edb/sg/en_uk/index/industry_sectors/electronics/facts_and_figures.html*.

Economist. "Economics A–Z." March 25, 2010. *http://www.economist.com/research/economics/alphabetic.cfm?term=economics#economics.*

Economy Watch. *http://www.economywatch.com/world-industries/global-industry.html.*

EDA Consortium. *Where Electronics Begin™*. *http://www.edac.org/Video/ElectronicsBegins/electronics_begins.jsp.*

EE Times. "Medical System Design Conference." May 20, 2010. *http://vshow.on24.com/vshow/medical?l=en#home.*

EE Times Asia. "Flextronics to build design center in Wuzhong." October 20, 2009. *http://www.eetasia.com/ART_8800587191_480100_NT_d705de31.HTM?8800033984&8800587191&click_from=8800033984,9949885433,2009-10-20,EEOL,ARTICLE_ALERT.*

EE Times China. "Portable medical electronics see big market in China." January 18, 2010. *http://www.eetasia.com/RT_8800595589_499495_NT_d3e66dac.HTM*.

EE Times India. "Barriers restrict China PV market growth." March 10, 2010. *http://www.eetindia.co.in/ART_8800600232_1800008_NT_5347451b.HTM.*

EE Times Korea. "South Korea bets on renewable energy." January 19, 2010. *http://www.eetasia.com/ART_8800595704_765245_NT_32db61a9.HTMclick_from=8800040880,9949885433,2010-01-19,EEOL,ARTICLE_ALERT*.

Fleisher, Craig E., and Babette E. Bensoussan. *Business and Competitive Analysis*. Upper Saddle River, NJ: FT Press, 2007.

———. *Strategic and Competitive Analysis*. Upper Saddle River, NJ: Prentice Hall, 2003.

Friedman, Thomas L. *The World Is Flat.* New York: Farrar, Straus and Giroux, 2005.

———. "A Word from the Wise." *New York Times*. March 2, 2010. *http://www.nytimes.com/2010/03/03/opinion/03friedman.html?ref=intelcorporation.*

Gartner, Inc. "Top 10 Semiconductor Vendors by Revenue Estimates, 2009." In Peter Clarke. "Winners, Losers in 2009 Chip Vendor Ranking." *EE Times Asia*. March 31, 2010. *http://www.eetasia.com/ART_8800602399_480200_NT_72aebd89.HTM*.

George, Roger Z., and James B. Bruce. *Analyzing Intelligence: Origins, Obstacles, and Innovations*. Washington, DC: Georgetown University Press, 2008.

Gereffi, Gary, John Humphrey, and Timothy Sturgeon. "The Governance of Global Value Chains." *Review of International Political Economy* 12, no. 1 (February 2005): 78–104. *http://www.global-production.com/scoreboard/resources/sturgeon_2005_governance-of-value-chains.pdf.*

Grant, Robert M. *Contemporary Strategy Analysis*. 5th Edition. Malden, MA: Blackwell Publishing Ltd., 2005.

Haines, Gerald K., and Robert E. Leggett. *Watching the Bear: Essays on CIA's Analysis of the Soviet Union*. Pittsburgh: Government Printing Office, 2003.

Heuer, Richard J. Jr. *Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence, 1999.

Hoskisson, Robert E., Michael A. Hitt, and R. Duane Ireland. *Competing for Advantage*. Mason, OH: Thomson South-Western, 2004.

Howe, Charles L. "Semiconductor Value Chain." Industrial College of the Armed Forces. Washington DC, January 2006.

Hwang, Adam. "Taiwan exports hit record in May." *DigiTimes*, June 8, 2010. *http://www.digitimes.com/NewsShow/MailHome.asp?datePublish=2010/6/8&pages=VL&seq=200.*

IC Insights. *Glossary of Terms*. 2002–2008. *http://www.icinsights.com/search/?q=Glossary+of+Terms+2002-2008.*

Integrated Circuit Engineering Corporation. "Cost Effective IC Manufacturing 1998–1999." *Smithsonian the Chip Collection*. 1997. *http://smithsonianchips.si.edu/ice/cd/CEICM/TITLE.pdf.*

Intel. *From Sand to Circuits: How Intel makes integrated circuit chips*. May 21, 2010. *http://www.intel.com/Assets/PDF/General/308301003.pdf.*

———. *Moore's Law: Raising the Bar.* 2005. *http://download.intel.com/museum/Moores_Law/Printed_Materials/Moores_Law_Backgrounder.pdf.*

International Business Strategies, Inc. "Cost of Participation in Semiconductor Industry Increasing: Impact after 32/28nm." Presentation at SEMI ISS, Half Moon Bay, CA, January 2010.

International Technology Roadmap for Semiconductors. "ITRS 2009 Edition." May 19, 2010. *http://www.itrs.net/Links/2009ITRS/Home2009.htm.*

International Trade Administration. *http://www.trade.gov*.

INVESTOPEDIA. *Economics Basics*. A Forbes Digital Company. March 25, 2010. *http://www.investopedia.com/university/economics/default.asp.*

iSuppli. "New phase of electronics market in 2010s." Presentation by Akira Minamika at SEMICON Japan 2009, SEMI Market Seminar, Chiba, Japan, December 2009.

Johnson, Bob. "The Changing Economics of Moore's Law." Presentation at SEMI ISS, Half Moon Bay, CA, January 2010.

Kogut, Bruce. "Designing Global Strategies: Comparative and Competitive Value-Added Chains." *Sloan Management Review* 26, no. 4 (Summer 1985): 15–28.

Kyodo News International. "Toshiba to set up joint venture in China for chip assembly." November 20, 2009. *http://www.healthtechzone.com/news/2009/11/20/4493943.htm.*

LaPedus, Mark. "Analysis: Change is in the wind at SMIC." *EE Times Asia*. November 12, 2009. *http://www.eetasia.com/ART_8800589303_480100_NT_5bba5b55.HTMclick_from=8800035720,9949885433,2009-11-12,EEOL,ARTICLE_ALERT.*

———. "Analysis: Is IBM turning over key IC tech to China?" *EE Times Asia*. October 21, 2009. *http://www.eetasia.com/ART_8800587281_480200_NT_55620e65.HTM*.

———. "Analysis: UMC needs new strategy." *EE Times Asia*. May 26, 2010. *http://www.eetasia.com/ARTP_8800607794_480200.HTM*.

———. "Freescale expands Chengdu design center." *EE Times Asia*. June 7, 2010. *http://www.eetimes.com/electronics-news/4199969/Freescale-expands-Chengdu-design-center.*

———. "Korea lags in analog, experts warn." *EE Times*. October 16, 2009. *http://www.eetimes.com/news/latest/showArticle.jhtml;jsessionid=NKWPPGLPF1RW1QE1GHOSKHWATMY32JVN?articleID=220601073.*

———. "Korea's IC industry seen on shaky ground." *EE Times Asia*. October 20, 2009. *http://www.eetimes.com/news/latest/showArticle.jhtml;jsessionid=HCFRU2WD32O4BQE1GHRSKH4ATMY32JVN?articleID=220700489.*

———."Six reasons why Samsung will succeed in foundry biz." *EE Times Asia*. March 3, 2010. *http://www.eetasia.com/ART_8800599719_480200_NT_9f869000.HTMclick_from=8800044080,9949885433,2010-03-05,EEOL,ARTICLE_ALERT*.

Lee, Ingrid, and Jessie Shen. "Chipbond to raise stake in China affiliate." *DigiTimes.* June 7, 2010. *http://www.digitimes.com/NewsShow/MailHome.asp?datePublish=2010/6/7&pages=PD&seq=219*.

Liang, Quincy. "Taiwan Courts Chinese Automakers—Possibilities of cross-strait synergy in the automobile industry." CENS.com—Taiwan Economic News. April 6, 2010. *http://www.cens.com/cens/html/en/news/news_inner_31883.html.*

Lowenthal, Mark M. *Intelligence: From Secrets to Policy*, 4th Edition. Washington, DC: CQ Press, 2009.

Maxfield, Clive "Max," and Kuhoo Goyal Edson. *EDA: Where electronics begins.* Cupertino, CA: KuhooZ, Inc., 2001.

Maxfield, Clive. *Bebop to the Boolean Boogie*. 2nd Edition. Boston, MA: Newnes, 2003.

McGahan, Anita M. *How Industries Evolve*. Boston, MA: Harvard Business School Press, 2004.

McGrath, Dylan. "Canon litho dreams hinge on nanoimprint." *EE Times Asia*. March 16, 2010. *http://www.eetasia.com/ART_8800600815_480200_NT_982140e7.HTMclick_from=8800044799,9949885433,2010-03-16,EEOL,ARTICLE_ALERT.*

Mentor Graphics. "Reduced Memory Cost Drives New Architecture and Applications." In Rhines, Walden. "Is consolidation the new game for the IC industry?" *EE Times India*. April 7, 2010. *http://www.eetindia.co.in/ART_8800603040_1800007_NT_b69fec09.HTM.*

Microwave Encyclopedia. Growing Semiconductor Boules. July 3, 2005. *http://www.microwaves101.com/encyclopedia/boules.cfm.*

Minamika, Akira. "New phase of electronics market in 2010s." Presentation at SEMICON Japan 2009, SEMI Market Seminar. Chiba, Japan. December 2009.

Mutschler, Ann Steffora. "IC Insights ups ww IC market forecast to 27%." *EDN*. March 9, 2010. *http://www.edn.com/article/457768-IC_Insights_ups_ww_IC_market_forecast_to_27_.php*.

National Intelligence Council. "Global Trends 2025: The National Intelligence Council's 2025 Project." Vers. NIC 2008-003. November 2008. *http://www.dni.gov/nic/NIC_2025_project.html.*

Navigant Consulting. "Solar in the New Decade: How Far Can We Go?" Presentation by Paula Mints at SEMI ISS, Half Moon Bay, CA, January 2010.

Nevison, Gary. "China REACH to take effect in October." *EDN*. February 26, 2010. *http://www.edn.com/blog/570000257/post/1300052930.html?nid=3351&rid=16641388*.

Northwestern University, Nanoscale Science and Engineering Center. "How Small Is Small?" Discover Nano. 2005. *http://www.discovernano.northwestern.edu/whatis/index_html/howsmall_html.*

NOVA Electronic Materials. Common Wafer Terminology. May 20, 2010. *http://www.novawafers.com/resources-wafer-terminology.html.*

Office of the Director of National Intelligence. "National Intelligence Strategy of the United States of America." August 2009. *http://www.dni.gov/reports/2009_NIS.pdf.*

Oster, Sharon M. *Modern Competitive Analysis.* New York: Oxford University Press, 1999.

Peng, April. "SMIC Beijing 300mm Fab Reported to Be Planning for Expansion." SEMI. June 1, 2010. *http://www.semi.org/en/MarketInfo/CTR_037308?id=sguna0610.*

PingQing, Liu, Gao Yonghui, and Gu Qiang. "Study on the Upgrading of China Integrated Circuit (IC) Industry Up to the Global Value Chain: A Case Study." *Management Science and Engineering* 1, no. 2 (December 2007): 14–21.

Porter, Michael E. *Competitive Advantage*. New York: Free Press, 1985.

———. *The Competitive Advantage of Nations*. New York: Free Press, 1990.

———. *Competitive Strategy.* New York: Free Press, 1980.

———. "The Five Competitive Forces That Shape Strategy." *Harvard Business Review* (January 2008). *http://hbr.org/2008/01/the-five-competitive-forces-that-shape-strategy/ar/1*.

Rasor, Douglas. "Convergence of Technology and Healthcare." Virtual presentation, *EE Times*, Virtual Conference: Medical System Design, May 20, 2010, *http://www.eetimes.com/medical/.*

Rhines, Walden. "Is consolidation the new game for the IC industry?" *EE Times India*, April 7, 2010. *http://www.eetindia.co.in/ART_8800603040_1800007_NT_b69fec09.HTM.*

Ross, Stephen A., Randolph W. Westerfield, and Jeffrey Jaffe. *Corporate Finance*, 7th Edition. New York: McGraw-Hill, 2005.

Ruzyllo, Jerzy. "Semiconductor Glossary." 2001–2009. *http://www.semi1source.com/glossary/default.asp?whichpage=default.*

SEMATECH. "Acronyms and Abbreviations." 2010. *http://www.sematech.org/publications/acronyms/index.htm.*

SEMI. "Can Government Help High Tech and Spur Economic Growth?" February 2, 2010. *http://www.semi.org/en/MarketInfo/ctr_034251?id=sguna0210.*

———. "Closing the China 'Chip Gap' Creates Long-Term Opportunities for Equipment and Materials Suppliers." June 14, 2010. *http://www.semi.org/en/marketinfo/ctr_033668.*

———. SEMI Industry Research & Statistics. "World Fab Forecast and the Trend of Taiwan Foundry and DRAM Fabs." Presentation by Clark Teng at SEMICON Japan exhibition, Chiba, Japan, December 2009.

Semico Research. "Handheld Wireless Is the Only Major Change in the Makeup of the Semiconductor Macro TAM." In Rhines, Walden. "Is consolidation the New Game for the IC industry?" *EE Times India*. April 7, 2010. *http://www.eetindia.co.in/ART_8800603040_1800007_NT_b69fec09.HTM.*

Semiconductor Industry Association. *The International Technology Roadmap for Semiconductors.* 2009 Edition. Austin, TX: International SEMATECH, 2009. *http://www.itrs.net/Links/2009ITRS/Home2009.htm.*

———. "What is a Semiconductor?" May 20, 2014. *http://semiconductors.org/faq/questions/.*

Siam-Heng, Michael H. "Development of China's Semiconductor Industry: Prospects and Problems." Vol. 13. In Elspeth Thompson and Jon Sigurdson. *China's Science and Technology Sector and the Forces of Globalization,* 219. Singapore: World Scientific Publishing, 2008.

Singh, Dinesh Pratap. "Dinesh Pratap Singh's Visualization for Porter's Value Chain." August 5, 2009. *http://commons.wikimedia.org/wiki/File:Porter_Value_Chain.png.*

Shu-yuan, Lin and Wu, Sofia. "Taiwan Conditionally Broadens High-tech Investment in China." Central News Agency (CNA). February 10, 2010. *http://www.etaiwannews.com/etn/news_content.php?id=1177917&lang=eng_news&cate_img=35.jpg&cate_rss=news_Business.*

Song, Young S., Nghis Nguyen, Kei Wong, Eyad Fanous, Eyad Wong, Hanna Kimj, and Steven Hsu. "Silicon Manufacturing." *EE 4345—Semiconductor Electronics Design Project. 2002. www.uta.edu/ronc/4345sp02/lectures/L09a_4345_Sp02.ppt.*

Sperling, Ed. "Why the Chartered Semiconductor Acquisition Matters." System-Level Design. October 16, 2009. *http://chipdesignmag.com/sld/sperling/2009/09/11/why-the-chartered-semiconductor-acquisition-matters/.*

Spiegel, Rob. "Manufacturing trending away from China." *EDN*. October 13, 2009. *http://www.edn.com/article/CA6701633.html.*

Strategic and Competitive Intelligence Professionals. FAQ. *http://www.scip.org/resources/content.cfm?itemnumber=601&navItemNumber=533.*

Sturgeon, Timothy J. "Exploring the Risks of Value Chain Modularity: Electronics Outsourcing during the Industry Cycle of 1992–2002." MIT Industrial Performance Center Working Paper Series. May 2003. *http://web.mit.edu/ipc/publications/pdf/03-002.pdf.*

———. "From Commodity Chains to Value Chains: Interdisciplinary Theory Building in an Age of Globalization." MIT Industrial Performance Center Working Paper Series. January 2008. *http://web.mit.edu/ipc/publications/pdf/08-001.pdf* .

———. "How Do We Define Value Chains and Production Networks?" MIT Industrial Performance Center Working Paper Series. April 2001. *http://www.inti.gob.ar/cadenasdevalor/Sturgeon.pdf.*

———. "How Globalization Drives Institutional Diversity: The Japanese Electronics Industry's Response to Value Chain Modularity." *Journal of East Asian Studies* 7 (2007): 1–34.

Suutari, Raymond. *Understanding Industry Structure*. CMA Management. January 2000. *http://findarticles.com/p/articles/mi_hb6419/is_11_73/ai_n28765036/?tag=content;col1*.

Taiwan Semiconductor Industry Association. "Overview on Taiwan IC Industry—2009 Edition." *http://www.tsia.org.tw/Eng/service/publication_more.asp?zvpWnp.*

T@iwan Today. "Ban List for Mainland-Bound Investment Revised." Taiwan's Government Information Office e-publication. February 10, 2010. *http://www.taiwantoday.tw/ct.asp?xitem=94165&CtNode=415.*

TechTerms.Com. "Integrated Circuit." May 21, 2010. *http://www.techterms.com/definition/integratedcircuit.*

Tokyo Electron. "TEL's Views on Equipment Maker Future Business." Presentation by Ken Sato at SEMI ISS, Half Moon Bay, CA, January 2010.

Top-Alternative-energy-sources.com. "The Czochralski Process." May 20, 2014. *http://www.top-alternative-energy-sources.com/Czochralski-process.html.*

Torrance, Randy. "IC reverse engineering—a design team perspective." *EDN*. March 11, 2010. *http://www.edn.com/design/integrated-circuit-design/4312346/IC-reverse-engineering-a-design-team-perspective*.

Tseng, Clark. "LED Industry Set to Enter Fast Growth Stage in 2010: New Investments, New Market Entrants." SEMI. *http://www.semi.org/en/IndustrySegments/LED/CTR_035763?id=sguna0410.*

UBM Electronics. "Enjoy the Show." Image screenshot. *EE Times* Virtual Conference: Medical System Design. May 20, 2010. *http://www.eetimes.com/medical/.*

Van Opstal, Debra. *The Resilient Economy: Integrating Competitiveness and Security.* Council on Competitiveness. July 2007. *http://www.compete.org/publications/detail/31/the-resilient-economy-integrating-competitiveness-and-security/.*

Vardaman, Jan, and Dan Tracy. "Japanese Companies Continue to Dominate the Packaging Materials Market." SEMI. January 5, 2010. *http://www.semi.org/en/MarketInfo/PackagingMarket/ctr_033627?id=sgurow0110*.

VLSI Research. "Economics and Collaboration Panel Discussion." Panel presentation at SEMI ISS, Half Moon Bay, CA, January 2010.

Waldron, Anna M., and Carl A. Batt. "How Small Am I? The Science of Nanotechnology." *PBS NewsHour Extra*. 2010. *http://www.pbs.org/newshour/extra/teachers/lessonplans/science/nanotechnology.html.*

Wang, Hsiao-wen. "Why TSMC Showed Mercy." *CommonWealth Magazine*. February 4, 2010. *http://english.cw.com.tw/article.do?action =show&id=11727.*

Wilson, Ron. "Semiconductors, emerging markets, and self-interest of survival." *EDN*. November 20, 2009. *http://www.edn.com/blog/1690000169/post/1770050777.html?nid=3357&rid=16641388.*

World Semiconductor Trade Statistics. "WSTS Semiconductor Market Forecast Autumn 2009." November 17, 2009. *http://www.wsts.org/PRESS/PRESS-ARCHIVE/WSTS-Semiconductor-Market-Forecast-Autumn-2009.*

Yoshida, Junko. "New Renesas chief shares renaissance roadmap." *EE Times Asia*. May 24, 2010. http://www.eetasia.com/ARTP_8800607528_499495. HTM.

Zakaria, Fareed. *The Post-American World*. New York: W. W. Norton & Company Inc., 2008.

NOTES

1 While the Council on Competitiveness is not the only voice on these issues, it provides an open-source forum on national competitiveness and concomitant issues.

2 Thomas L. Friedman's books, including *The World Is Flat* (New York: Farrar, Straus and Giroux, 2005) and its follow-on editions, provide a good overview of the impact of global Internet connectivity and the diffusion of knowledge it enables.

3 Based on my reading of "The National Intelligence Strategy," Director of National Intelligence (DNI), August 2009.

4 Suzanne Berger, *How We Compete: What Companies around the World Are Doing to Make It in Today's Global Economy* (New York: Doubleday, 2006), 9.

5 Gerald K. Haines and Robert E. Leggett, *Watching the Bear: Essays on CIA's Analysis of the Soviet Union* (Pittsburgh: Government Printing Office, 2003), 17.

6 Ibid., 18.

7 Ibid., 21.

8 Ibid., 17.

9 Dertouzos et al., *Made in America*, 1.

10 Mark M. Lowenthal, *Intelligence: From Secrets to Policy*, 4th Edition (Washington, DC: CQ Press, 2009), 267. (Since this observation was made, the source was released in a 5th edition.) The compelling questions can be synopsized as protecting intelligence sources and methods, determining distribution rules for intelligence gathered, and whether there was an implicit quid pro quo from the government providing intelligence to business.

11 Berger, *How We Compete*, 290–91.

12 Based on my reading of the "National Intelligence Strategy," DNI, August 2009.

13 Fareed Zakaria, *The Post-American World* (New York: W. W. Norton & Company, 2008), 4.

14 DNI, "National Intelligence Strategy," 5.

15 Ibid.

16 DNI, "National Intelligence Strategy," 3–4.

17 National Intelligence Council. *Global Trends 2025: A Transformed World*, November 2008, iv. This observation was listed under the heading "Relative Certainty."

18 Timothy J. Sturgeon, "How Do We Define Value Chains and Production Networks?" MIT Industrial Performance Center Working Paper Series, April 2001, *http://www.inti.gob.ar/cadenasdevalor/Sturgeon.pdf*.

19 Industry analysis definition adapted from *Business Dictionary, http://www.businessdictionary.com/definition/industry-analysis.html*.

20 Anita M. McGahan, *How Industries Evolve* (Boston, MA: Harvard Business School Press, 2004), 7.

21 Adapted (with permission) from Stephen A. Ross, Ronald W. Westerfield, and Jeffrey Jaffe, *Corporate Finance*, 7th ed. (New York: McGraw-Hill, 2005), Figure 1.4.

22 Strategic and Competitive Intelligence Professionals, a leading industry nonprofit organization, defines competitive intelligence "as a necessary, ethical business discipline for decision making based on understanding the competitive environment." Strategic and Competitive Intelligence Professionals FAQ, *http://www.scip.org/re_pdfs/1395928684_pdf_FrequentlyAskedQuestions.pdf.*

23 Robert M. Grant, *Contemporary Strategy Analysis*, 5th ed. (Malden, MA: Blackwell Publishing Ltd., 2005), 113.

24 Michael E. Porter, *Competitive Strategy* (New York: Free Press, 1980).

25 Robert E. Hoskisson, Michael A. Hitt, and R. Duane Ireland, *Competing for Advantage* (Mason, OH: Thomson South-Western, 2004), 82.

26 Adapted (with permission) from Michael E. Porter, "The Five Competitive Forces That Shape Strategy," *Harvard Business Review* (January 2008), *http://hbr.org/2008/01/the-five-competitive-forces-that-shape-strategy/ar/1*.

27 The word *environment* is not meant to connote a focus on the impact of "green" or "eco-friendly" factors on an industry.

28 Craig S. Fleisher and Babette E. Bensoussan, *Business and Competitive Analysis* (Upper Saddle River, NJ: FT Press, 2007), 88.

29 Boundless, "Overview of Types of Plans and Tools for Planning," May 20, 2014, *https://www.boundless.com/management/strategic-management/the-planning-process/overview-of-types-of-plans-and-tools-for-planning/*.

30 Fleisher and Bensoussan, *Business and Competitive Analysis*, 88.

31 Adapted (with permission) from Robert E. Hoskisson, Michael A. Hitt, and R. Duane Ireland, *Competing for Advantage* (Mason, OH: Thomson South-Western, 2004), Figure 3.1.

32 Michael E. Porter, *Competitive Advantage* (New York: Free Press, 1985).

33 Dinesh Pratap Singh, "Dinesh Pratap Singh's Visualization for Porter's Value Chain," August 5, 2009, *http://commons.wikimedia.org/wiki/File:Porter_Value_Chain.png.*

34 Timothy Sturgeon, "How Do We Define Value Chains and Production Networks?," MIT Industrial Performance Center Working Paper Series, April 2001, *http://www.inti.gob.ar/cadenasdevalor/Sturgeon.pdf.*

35 Gary Gereffi, John Humphrey, and Timothy Sturgeon, "The Governance of Global Value Chains," *Review of International Political Economy* 12, no. 1 (February 2005): Figure 1. Reprinted with permission of the authors and Taylor & Francis Group, *http://www.global-production. com/scoreboard/resources/sturgeon_2005_governance-of-value-chains.pdf.*

36 Michael E. Porter, *Competitive Strategy* (New York: Free Press, 1980), 158.

37 Anita M. McGahan, *How Industries Evolve* (Boston, MA: Harvard Business School Press, 2004), 67.

38 "Global Industry," *Economy Watch, http://www.economywatch.com/world-industries/global-industry.html.*

39 International Trade Administration, *http://www.trade.gov/.*

40 International Trade Administration, "U.S. Export Fact Sheet," *http://trade.gov/press/press_releases/2009/export-factsheet_031309.pdf.*

41 The NAICS code specifies industries by the type of product or service they produce.

42 Berger, *How We Compete*, 78–79.

43 Adapted (with permission) based on graphic provided by the Taiwan Semiconductor Industry Association. For more information, see "Overview on Taiwan IC Industry—2009 Edition," *http://www.tsia.org.tw/Uploads/Publications/2012%20Overview-Final.pdf.*

44 Adapted (with permission) from Pao-Lang Chang and Chien-Tzu Tsai, "Finding the niche position-competition strategy of Taiwan's IC design industry," Technovation 22, no. 2 (February 2002): Figure 1.

45 Charles L. Howe, "Semiconductor Value Chain," Industrial College of the Armed Forces, Washington, DC, January 2006.

46 Ibid.

47 Timothy Sturgeon, "How Do We Define Value Chains and Production Networks?" MIT Industrial Performance Center Working Paper Series. April 2001, *http://www.inti.gob.ar/cadenasdevalor/Sturgeon.pdf.*

48 The term "daily scrape" comes from an open-source analyst who shared his method for reviewing and saving articles of interest from the daily newspapers from the target country.

49 Zotero was developed by the Center for History and New Media at George Mason University. The program is available for download at: *http://www.zotero.org/.*

50 Zotero supports many citation formats.

51 Richard J. Heuer's book, *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999), is an excellent source for this topic.

52 Personal notes from "SEMI ISS Blue Chip Panel," SEMI Industry Strategic Symposium, Half Moon Bay, CA, January 2010.

53 Adapted (with permission) from Norm Armour, "The Innovation Imperative: Toward a New Model for Semiconductor Manufacturing," presentation at the SEMI Industry Strategic Symposium, Half Moon Bay, CA, January 2010, slide 20.

54 International Business Strategies, Inc., "Cost of Participation in Semiconductor Industry Increasing: Impact after 32/28nm," presentation at SEMI Industry Strategic Symposium, Half Moon Bay, CA, January 2010, slide 17 (reprinted with permission).

55 Ibid., slide 11.

56 VLSI Research, "Economics and Collaboration Panel Discussion," SEMI Industry Strategic Symposium, Half Moon Bay, CA, January 2010, slide 7 (adapted and reprinted with permission).

57 "Fabless Companies Gain in Top 20 Ranking," Semiconductor International, March 3, 2009 (adapted and reprinted with permission).

58 Dick James, "Apple's A4 iPad chip is Samsung 45-nm," *Semiconductor International*, April 12, 2010.

59 Randy Torrance and Dick James, "IC reverse engineering—a design team perspective," *Electronics Design Network,* March 11, 2010, *http://www.edn.com/design/integrated-circuit-design/4312346/IC-reverse-engineering-a-design-team-perspective.*

60 Walden Rhines, "Is Consolidation the New Game for the IC Industry?" *EE Times India*, April 7, 2010, *http://www.eetindia.co.in/ART_8800603040_1800007_NT_b69fec09.HTM.*

61 Akira Minamika, "New phase of electronics market in 2010s" presentation, market seminar, SEMICON Japan 2009, Tokyo, Japan, December 2009, slide 30.

62 John Daane, "Semiconductor State of the Industry," Semiconductor Industry

Association, March 17, 2010, *http://www.choosetocompete.org/downloads/2010_SOI.pdf.*

63 Ann Steffora Mutschler, "IC Insights ups ww IC market forecast to 27%," *Electronics Design Network*, March 9, 2010, *http://www.edn.com/article/457768-IC_Insights_ups_ww_IC_market_forecast_to_27_.php.*

64 Tokyo Electron, "TEL's Views on Equipment Maker Future Business," presentation by Ken Sato, SEMI Industry Strategic Symposium, Half Moon Bay, CA, January 2010, slide 9.

65 Ron Wilson, "Semiconductors, emerging markets, and self-interest of survival," *Electronics Design Network*, November 20, 2009, *http://www.edn.com/blog/1690000169/post/1770050777.html?nid=3357&rid=16641388.*

66 Tokyo Electron, "TEL's Views on Equipment Maker Future Business."

67 Bob Johnson, "The Changing Economics of Moore's Law," presentation at SEMI Industry Strategic Symposium, Half Moon Bay, CA, January 2010, slide 8.

68 Clair Brown and Greg Linden, *Chips and Change: How Crisis Reshapes the Semiconductor Industry* (Cambridge, MA: MIT Press, 2009), 44.

69 Berger, *How We Compete*, 78–82. Berger provides a good description of modularity in the semiconductor industry.

70 Brown and Linden, *Chips and Change*, 45.

71 SEMI Industry Research & Statistics, "World Fab Forecast and the Trend of Taiwan Foundry and DRAM Fabs," presentation by Clark Teng, SEMICON Japan, Chiba, Japan, December 2009, slide 23 (adapted and reprinted with permission).

72 Adapted (with permission) from Applied Materials, "What Is Solar Electric Power," Applied Materials video, 6:33, *http://www.appliedmaterials.com/media-resources/wisep.*

73 Navigant Consulting, "Solar in the New Decade: How Far Can We Go?" presentation by Paula Mints, SEMI Industry Strategic Symposium, Half Moon Bay, CA, January 2010, slide 15 (adapted and reprinted with permission).

74 David Lammers, "LED Manufacturing Tools Gain Attention," *Semiconductor International*, January 26, 2010.

75 Yole Développement, "HB LED & LED Packaging 2009," October 2009: also, "LED Manufacturing Steps," reprinted in David Lammers, "LED Manufacturing Tools Gain Attention," *Semiconductor International*, January 26, 2010 (reprinted here with permission).

76 iSuppli, "New phase of electronics market in 2010s," presentation by Akira Minamika, SEMICON Japan, SEMI market seminar, Chiba, Japan, December 2009, slide 30 (adapted and reprinted with permission).

77 Clark Tseng, "LED Industry Set to Enter Fast Growth Stage in 2010: New Investments, New Market Entrants," SEMI, April 6, 2010, *http://www.semi.org/en/IndustrySegments/LED/CTR_035763?id=sguna0410* (adapted and reprinted with permission).

78 Douglas Rasor, "Convergence of Technology and Healthcare," virtual presentation, EE Times, Medical System Design Virtual Conference, May 20, 2010, http://www.eetimes.com/medical/, slide 3 (adapted and reprinted with permission).

79 Personal notes from SEMICON Korea, Seoul, Korea, February 4, 2010.

80 ASE Group, "Semi Business Evolution," presentation by Tien Wu, SEMICON Korea 2010, Seoul, Korea, February 2010, slide 20 (reprinted with permission).

81 Douglas Rasor, "Convergence of Technology and Healthcare," virtual presentation, *EE Times*, Medical System Design Virtual Conference, May 20, 2010, *http://www.eetimes.com/medical/,* slide 23 (reprinted with permission).

82 See Berger, *How We Compete*, 78–79; also, Brown and Linden, *Chips and Change*, 197. Mark LaPedus, "Korea's IC industry seen on shaky ground," *EE Times*, October 20, 2009, *http://www.eetimes.com/news/latest/showArticle.jhtml;jsessionid=HCFRU2WD32O4BQE1GHRSKH4ATMY32JVN?articleID=220700489.* Ed Sperling, "Why the Chartered Semiconductor Acquisition Matters," System-Level Design, October 16, 2009, *http://chipdesignmag.com/sld/sperling/2009/09/11/why-the-chartered-semiconductor-acquisition-matters/*; SEMI, "Can Government Help High Tech and Spur Economic Growth?" February 2, 2010, *http://www.semi.org/en/MarketInfo/ctr_034251?id=sguna0210.*

83 Brown and Linden, *Chips and Change*, 37.

84 Brown and Linden, *Chips and Change*, 27; Junko Yoshida, "New Renesas chief shares renaissance roadmap," *EE Times Asia*, May 24, 2010, *http://www.eetasia.com/ARTP_8800607528_499495.HTM.*

85 Kenji Tsuda, "Japan's IC Makers to Consolidate Fabs," *Semiconductor International*, February 2, 2009; "Toshiba to Set Up Joint Venture in China for Chip Assembly," Kyodo News International, Kyodo, November 20, 2009, *http://satellite.tmcnet.com/news/2009/11/20/4493943.htm.*

86 "Pretax Earnings Improve at 7 Japan Chipmaking Gear Makers," *Semiconductor International*, February 15, 2010.

87 Dylan McGrath, "Canon Litho Dreams Hinge on Nanoimprint," *EE Times Asia*, March 16, 2010, *http://www.eetasia.com/ART_8800600815_480200_NT_982140e7.HTMclick_from=8800044799,9949885433,2010-03-16,EEOL,ARTICLE_ALERT*. The world's largest lithography company is AML Holding NV of the Netherlands.

88 Jan Vardaman and Dan Tracy, "Japanese Companies Continue to Dominate the Packaging Materials Market," SEMI, January 5, 2010, *http://www.semi.org/en/MarketInfo/PackagingMarket/ctr_033627?id=sgurow0110.*

89 Akira Minamika, "New phase of electronics market in 2010s," presentation at SEMICON Japan 2009, SEMI Market Seminar, Chiba, Japan, December 2009, 30.

90 Mark LaPedus, "Korea's IC industry seen on shaky ground," October 20, 2009; Mark LaPedus, "Korea lags in analog, experts warn," *EE Times*, October 16, 2009, *http://www.eetimes.com/news/latest/showArticle.jhtml;jsessionid=NKWPPGLPF1RW1QE1GHOSKHWATMY32JVN?articleID=220601073*; Lee Chul-ho, "[Viewpoint] In China, a Giant Stirs," Korea JoongAng Daily, February 1, 2010, *http://joongangdaily.joins.com/article/view.asp?aid=2916001.*

91 Vardaman and Tracy, "Japanese Companies Continue to Dominate the Packaging Materials Market," SEMI, January 5, 2010.

92 LaPedus, "Korea's IC industry seen on shaky ground," October 20, 2009.

93 LaPedus, "Korea lags in analog, experts warn," October 16, 2009.

94 Dick James, "Apple's A4 iPad chip is Samsung 45-nm," *Semiconductor International*, April 12, 2010; Mark LaPedus, "Six reasons why Samsung will succeed in foundry biz," *EE Times Asia*, March 3, 2010, *http://www.eetasia.com/ART_8800599719_480200_NT_9f869000.HTMclick_from=8800044080,9949885433,2010-03-05,EEOL,ARTICLE_ALERT.*

95 "South Korea bets on renewable energy," *EE Times Asia*, January 19, 2010, *http://www.eetasia.com/ART_8800595704_765245_NT_32db61a9.HTMclick_from=8800040880,9949885433,2010-01-19,EEOL,ARTICLE_ALERT.*

96 Economic Development Board, "EDB Singapore," June 28, 2010, *http://www.edb.gov.sg/edb/sg/en_uk/index/industry_sectors/electronics/facts_and_figures.html.*

97 Business Wire, "Applied Materials Opens Global Hub in Singapore for Manufacturing Semiconductor Equipment," *Semiconductor International*, April 13, 2010.

98 Ed Sperling, "Why the Chartered Semiconductor Acquisition Matters," System-Level Design, October 16, 2009, *http://chipdesignmag.com/sld/sperling/2009/09/11/why-the-chartered-semiconductor-acquisition-matters/.*

99 IC Insights, "2009 Major IC Foundries," in "TSMC Maintains Top Spot Among Foundries," Semiconductor International. January 28, 2010 (adapted and reprinted with permission).

100 Mark LaPedus, "UMC needs new strategy," *EE Times Asia*, May 26, 2010, *http://www.eetasia.com/ARTP_8800607794_480200.HTM.*

101 Peggy Aycinena, "TSMC: The New Pax Romana," EDA Confidential, May 26, 2010, *http://www.aycinena.com/index2/index3/tsmc%20pax%20romana%20 2010.html.*

102 Market News Publishing, "And MAPPER Reached Joint Development Milestone," *Semiconductor International*, February 19, 2010.

103 Peter Clarke, "TSMC breaks ground on LED lighting wafer fab," *EE Times*, March 25, 2010, *http://www.eetimes.com/electronics-news/4088182/TSMC-breaks-ground-on-LED-lighting-wafer-fab.*

104 Akira Minamika, "New phase of electronics market in 2010s," presentation at SEMICON Japan 2009 SEMI, Market Seminar, Chiba, Japan, December 2009, slide 30 (adapted and reprinted with permission).

105 "Taiwan Legislature Rejects DRAM Industry Restructuring Plan," *Semiconductor International*, November 12, 2009.

106 "Taiwan Tax Cut Agreement Expected to Benefit Businesses," Osc Seoul Yonhap in English, January 14, 2010.

107 Lin Shu-yuan and Sofia Wu, "Taiwan Conditionally Broadens High-tech Investment In China," *Central News Agency* (CNA), February 10, 2010, *http://www.etaiwannews.com/etn/news_content.php?id=1177917&lang=eng_news&cate_img=35.jpg&cate_rss=news_Business;* "Ban List for Mainland-Bound Investment Revised," T@iwan Today, February 10, 2010*, http://www.taiwantoday.tw/ct.asp?xitem =94165&CtNode=415.*

108 Ibid.

109 "Flextronics to build design center in Wuzhong," *EE Times Asia*, October 20, 2009, *http://www.eetasia.com/ART_8800587191_480100_NT_d705de31. HTM?8800033984&8800587191&click_from=8800033984,9949885433,2009-10-20,EEOL,ARTICLE_ALERT.*

110 Lin Shu-yuan and Sofia Wu, "Taiwan Conditionally Broadens High-tech Investment In China," *CAN*, October 20, 2009.

111 Asia Pulse, "Taiwanese Chip Foundries Investing in Chinese Firms," *Semiconductor International*, April 5, 2010.

112 David Lammers, "TSMC to Take No Day-to-Day Role in SMIC," *Semiconductor International*, November 11, 2009; China Knowledge Newswire, "TSMC says no plans to move advanced plants to mainland," *Semiconductor International*, April 7, 2010.

113 Ingrid Lee and Jessie Shen, "Chipbond to raise stake in China affiliate," *DigiTimes*, June 7, 2010, *http://www.digitimes.com/NewsShow/MailHome.asp?datePublish=2010/6/7&pages=PD&seq=219.*

114 Quincy Liang, "Taiwan Courts Chinese Automakers—Possibilities of cross-strait synergy in the automobile industry," CENS.com—The Taiwan Economic News, April 6, 2010, *http://www.cens.com/cens/html/en/news/news_inner_31883.html.*

115 Adam Hwang, "Taiwan exports hit record in May," *DigiTimes*, June 8, 2010, *http://www.digitimes.com/NewsShow/MailHome.asp?datePublish=2010/6/8&pages=VL&seq=200.*

116 April Peng, "SMIC Beijing 300mm Fab Reported to Be Planning for Expansion," SEMI, June 1, 2010, available at *http://www.semi.org/en/MarketInfo/CTR_037308?id=sguna0610* (reprinted with permission from SEMI).

117 "Closing the China 'Chip Gap' Creates Long-Term Opportunities for Equipment and Materials Suppliers," SEMI, June 14, 2010, *http://www.semi.org/en/marketinfo/ctr_033668.*

118 Hsiao-wen Wang, "Why TSMC Showed Mercy," *CommonWealth Magazine*, February 4, 2010, *http://english.cw.com.tw/article.do?action=show&id=11727.*

119 Mark LaPedus, "Analysis: Change is in the wind at SMIC," *EE Times Asia*, November 12, 2009, *http://www.eetasia.com/ART_8800589303_480100_NT_5bba5b55.HTMclick_from=8800035720,9949885433,2009-11-12,EEOL,ARTICLE_ALERT.*

120 VLSI Research, "TSMC & SMIC Profitability," in "China Leads World Out of Recession, Through Recovery," *Semiconductor International*, January 14, 2010.

121 LaPedus, "Analysis: Change is in the wind at SMIC," November 12, 2009.

122 "China IC Industry Development Targets Renewed and Repurposed Fabs," Targeted News Service, March 8, 2010.

123 Margery Conner, "Protecting your hardware IP in China: Practical experience," *Electronics Design Network*, February 4, 2010, *http://www.edn.com/blog/1470000147/post/650052465.html?nid=2431&rid=16641388.*

124 Hsiao-wen Wang, "Why TSMC Showed Mercy," *CommonWealth Magazine*, February 4, 2010.

125 Mark LaPedus, "Analysis: Is IBM turning over key IC tech to China?" *EE Times Asia*, October 21, 2009, *http://www.eetasia.com/ART_8800587281_480200_NT_55620e65.HTM.*

126 Mark LaPedus, "Freescale expands Chengdu design center," *EE Times Asia*, June 7, 2010, *http://www.eetimes.com/electronics-news/4199969/Freescale-expands-Chengdu-design-center.*

127 "Intel Capital and China Investment Corporation Announce Collaboration Agreement," *Semiconductor International*, February 12, 2010.

128 Keith Bradsher, "China Drawing High-Tech Research from U.S.," *New York Times*, March 17, 2010, *http://www.nytimes.com/2010/03/18/business/global/18research.html?sq=Applied%20Materials%2 &st=nyt&adxnnl=1&scp=2&adxnnlx=1309464261-clRhmw1kjIyyEagvJFAo7A.*

129 Ibid.

130 Thomas L. Friedman, "A Word from the Wise," *New York Times*, March 2, 2010, *http://www.nytimes.com/2010/03/03/opinion/03friedman.html?ref=intelcorporation.*

131 "Elpida Plans China, Taiwan Factories to Meet Demand," *Business Week*, June 7, 2010.

132 Rob Spiegel, "Manufacturing trending away from China," *Electronics Design Network*, October 13, 2009, *http://www.edn.com/article/CA6701633.html.*

133 Personal notes from SEMI ISS Blue Chip Panel, SEMI Industry Strategic Symposium, Half Moon Bay, CA, January 2010.

134 Gary Nevison, "China REACH to take effect in October," *Electronics Design Network*, February 26, 2010, *http://www.edn.com/blog/570000257/post/1300052930.html?nid=3351&rid=16641388.*

135 "Barriers restrict China PV market growth," *EE Times India*, March 10, 2010, *http://www.eetindia.co.in/ART_8800600232_1800008_NT_5347451b.HTM.*

136 Research in China, "China Polysilicon Industry Report, 2009" in "China Looks to Control Polysilicon Oversupply, Quality," PV Society, December 3, 2009 (reprinted with permission).

137 "Portable medical electronics see big market in China," *EE Times Asia*, January 18, 2010, *http://www.eetasia.com/ART_8800595589_499495_NT_d3e66dac.HTM.*

138 Ian Bremmer, *The End of the Free Market* (New York: Portfolio, 2010), 149.

139 The economics of industry is being highlighted here; based on the 2009 NIS, the intelligence community is adept at analyzing monetary policy, exchange rates, capital flows, and other major macroeconomic trends.

140 Bremmer, *The End of the Free Market*, 23.

141 Sperling, "Why the Chartered Semiconductor Acquisition Matters."

142 Bremmer, *The End of the Free Market*, 5.

143 Ibid., 175.

144 Ibid., 199.

145 Adapted from Robert E. Hoskisson, Michael A. Hitt, and R. Duane Ireland, *Competing for Advantage* (Mason, OH: Thomson South-Western, 2004), Figure 3.1 (adapted with permission).

146 IC Insights, "Glossary of Terms, 2002–2008," *http://www.icinsights.com/search/?q=Glossary+of+Terms+2002-2008.*

147 Semiconductor Industry Association, "What is a Semiconductor?," May 20, 2014, *http://semiconductors.org/faq/questions/.*

148 Jack Bogdanski, "Obsolescence Management: Another Perspective," Military Embedded Systems, January/February 2009, *http://www.mil-embedded.com/articles/id/?3747.*

149 Brown and Linden, *Chips and Change*, 9.

150 Visualizations of this common industry process can be found in Top-Alternative-energy-sources.com, "The Czochralski Process," May 20, 2014, *http://www.top-alternative-energy-sources.com/Czochralski-process.html*; and in corporate websites, for example, SUMCO Corporation, "The Next Generation Wafer," May 17, 2010, *http://www.sumcosi.com/english/products/next_generation/breakthrough.html.*

151 NOVA Electronic Materials, "Common Wafer Terminology," May 20, 2010, *http://www.novawafers.com/resources-wafer-terminology.html.*

152 Microwave Encyclopedia, "Growing Semiconductor Boules," July 3, 2005, *http://www.microwaves101.com/encyclopedia/boules.cfm.*

153 SEMATECH, "Acronyms and Abbreviations," *http://www.sematech.org/publications/acronyms/index.htm.*

154 Definition of integrated circuit is adapted from TechTerms.Com, May 21, 2010, *http://www.techterms.com/definition/integratedcircuit.*

155 Intel, "Moore's Law: Raising the Bar," 2005, *http://www.bandwidthco.com/whitepapers/hardware/cpu/moore/Moores%20Law%20-%20Raising%20the%20Bar.pdf?.*

156 Adapted (with permission) from Mentor Graphics, "Reduced Memory Cost Drives New Architecture and Applications," in "Is consolidation the new game

for the IC industry?," *EE Times India*, April 7, 2010, *http://www.eetindia.co.in/ART_8800603040_1800007_NT_b69fec09.HTM.*

157 Semiconductor Industry Association, The International Technology Roadmap for Semiconductors, 2009 Edition. International SEMATECH: Austin, TX (2009). *http://www.itrs.net/Links/2009ITRS/Home2009.htm* (adapted and reprinted with permission).

158 Northwestern University, Nanoscale Science and Engineering Center, "How Small Is Small?," DiscoverNano, 2005, *http://www.discovernano.northwestern.edu/whatis/index_html/howsmall_html* (reprinted with permission from Northwestern University and Dennis Kunkel Microscopy, Inc.); Anna M. Waldron and Carl A. Batt, "How Small Am I? The Science of Nanotechnology," PBS NewsHour Extra, 2010, *http://www.pbs.org/newshour/extra/teachers/lessonplans/science/nanotechnology.html* (reprinted with permission from PBS NewsHour/MacNeil-Lehrer Productions).

159 "Where Electronics Begin," EDA Consortium, *http://www.edac.org/Video/ElectronicsBegins/electronics_begins.jsp.*

160 For a good overview of the process, see "From Sand to Circuits: How Intel makes integrated circuit chips," Intel, May 21, 2010, *http://www.intel.com/Assets/PDF/General/308301003.pdf.*

161 Integrated Circuit Engineering Corporation, "Cost Effective IC Manufacturing 1998–1999," Smithsonian Chip Collection, 1997, 7-4, *http://smithsonianchips.si.edu/ice/cd/CEICM/TITLE.pdf.*

162 Personal notes from SEMI Industry Strategic Symposium Blue Chip Panel, Half Moon Bay, CA, January 12, 2010.

163 Bob Bruck, "Economics and Collaboration Panel," presentation at SEMI Industry Strategic Symposium, Half Moon Bay, CA, January 2010.

164 World Semiconductor Trade Statistics, *http://www.wsts.org.*

165 Graphic based on data from World Semiconductor Trade Statistics, "WSTS Semiconductor Market Forecast Autumn 2009," November 17, 2009, *http://www.wsts.org/PRESS/PRESS-ARCHIVE/WSTS-Semiconductor-Market-Forecast-Autumn-2009* (adapted and data used with permission).

166 IC Insights, "Glossary of Terms," 2002–2008, *http://www.icinsights.com/search/?q=Glossary+of+Terms+2002-2008*; Jerzy Ruzyllo, "Semiconductor Glossary," 2001–2009, *http://www.semi1source.com/glossary/default.asp?whichpage=default.*

167 Semico Research, "Is consolidation the new game for the IC industry?," *EE Times India*, April 7, 2010, *http://www.eetindia.co.in/ART_8800603040_1800007_NT_b69fec09.HTM* (reprinted with permission).

168 Gartner, Inc., "Top 10 Semiconductor Vendors by Revenue Estimates, 2009," in Peter Clarke, "Winners, Losers in 2009 Chip Vendor Ranking," EE Times Asia, March 31, 2010, *http://www.eetasia.com/ART_8800602399_480200_NT_72aebd89.HTM* (adapted and reprinted with permission).

169 IC Insights, Company Reports, "Top 10 Semiconductor Industry Capital Spenders," in "IC Insights: Top 10 to Spend Aggressively in 2010," Semiconductor International, February 24, 2010 (adapted and reprinted with permission from IC Insights).

170 Clair Brown and Greg Linden, *Chips and Change: How Crisis Reshapes the Semiconductor Industry* (Cambridge, MA: MIT Press, 2009).

171 Michael H. Siam-Heng, "Development of China's Semiconductor Industry: Prospects and Problems," in Elspeth Thomson and Jon Sigurdson, *China's Science and Technology Sector and the Forces of Globalization* (Singapore: World Scientific Publishing, 2008), 219.

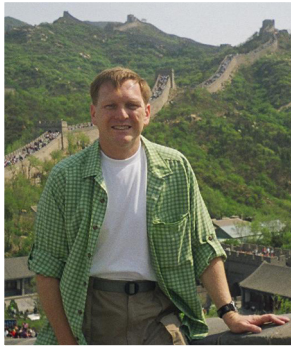
172 National Academies, *http://www.nationalacademies.org/*.

173 U.S. Bureau of Industry and Security, *www.bis.doc.gov/*.

174 As a side note, many companies are using file names with random hexadecimal code on YouTube, thereby allowing their video clips to "hide in plain sight." Source: Phil Britton, "Integrating Web 2.0 Tools in Your Intelligence Process," Washington, DC: Strategic and Competitive Intelligence Professionals Conference, 2010. Comment during lecture.

175 UBM Electronics, "Enjoy the Show," image screenshot, *EE Times* Virtual Conference: Medical System Design, May 20, 2010, *http://www.eetimes.com/medical/* (reprinted with permission).

ABOUT THE AUTHOR



Charles (Chuck) Howe serves as Deputy Director to the Assistant Deputy Director of National Intelligence Acquisition organization, which is part of the Acquisition, Technology & Facilities organization within the Office of the Director of National Intelligence. Before joining the Intelligence Community, Mr. Howe served in the United States Air Force for 27 years, retiring with the rank of Colonel. He has a long association with the aerospace industry, and capped off his military career teaching at the Industrial College of the Armed Forces (now Dwight D. Eisenhower School for National Security).

National Intelligence Press
National Intelligence University

www.NI-U.edu

ISBN: 978-1-932946-32-1

PCN 45645

This Page Is Intentionally Left Blank

NATIONAL DEFENSE INTELLIGENCE COLLEGE

SENSEMAKING

A STRUCTURE FOR AN INTELLIGENCE REVOLUTION

DAVID T. MOORE

CLIFT SERIES
on the Intelligence Profession

Sensemaking

A Structure for an Intelligence Revolution

David T. Moore

NATIONAL DEFENSE INTELLIGENCE COLLEGE
WASHINGTON, DC

March 2011

The views expressed here are those of the author and do not reflect the official policy or position of any branch of the U.S. Government.

Sensemaking is the inaugural book in our new series, titled The A. Denis Clift Series on the Intelligence Profession. The *Clift Series* will present original research on intelligence analysis and the teaching of intelligence.

In 2009, A. Denis Clift concluded a 50-year career with the federal government. Clift was president of the National Defense Intelligence College from 1994 to 2009 and was instrumental in creating the Center for Strategic Intelligence Research, which houses the NDIC Press.

Sensemaking: A Structure for an Intelligence Revolution, by David T. Moore

Sensemaking, whereby intelligence professionals would work with executive decisionmakers to explain data that are "sparse, noisy, and uncertain," requires an interpreter and experienced champion to bring about a practicable understanding and acceptance of the concept among intelligence practitioners. David Moore has accomplished that feat. Further, he, along with collaborators in chapters 5 and 7, demonstrate how sensemaking can be accomplished as a collaborative enterprise.

The manuscript for this publication was reviewed and cleared for public release by the Department of Defense's Office of Security Review. Clearance does not imply endorsement of opinion nor of factual accuracy. This volume is subject to Title 17, United States Code, Sections 101 and 105. It is in the public domain and may not be copyrighted.

How to order this book. *Everyone* may download a free electronic copy from our website at *www.ndic.edu. U.S. government employees* may request a complimentary copy by contacting us at: *press@ndic.edu*. The *general public* may purchase a copy from the Government Printing Office (GPO) at *http://bookstore.gpo.gov.*

Cathryn Quantic Thurston, PhD
Editor, NDIC Press

Library of Congress Control Number 2011924457
ISBN 978-1-932946-28-4

CONTENTS

Foreword ..... **ix**
Gregory F. Treverton

Commentary ..... **xiii**
Anthony Olcott, PhD

Commentary ..... **xvii**
Emily S. Patterson, PhD

Commentary ..... **xix**
Christian P. Westermann

Commentary ..... **xxi**
Phil Williams, PhD

Preface: On Being Mindful ..... **xxiii**
What is Mindlessness? ..... **xxiii**
Attaining Mindfulness ..... **xxv**

Acknowledgments ..... **xxxiii**

Definitions ..... **xxxv**

Chapter 1: Introduction **1**
Where We Are **1**
A Roadmap **4**
Kent's Imperative **6**

Chapter 2: The Failure of "Normal Intelligence" **11**
Intelligence Challenges **11**
Errors and Failures **12**
Considering Standard Models **16**
Types of Problems **17**
A Wicked Look at Wicked Problems in Intelligence **20**
An Intelligence Example: Pandemics as Wicked Problems **29**
Complexity **33**

Chapter 3: From Normal to Revolutionary Intelligence **37**
Evidence-Based Intelligence Creation **37**
Considering the Normal **44**
Paradigm Shift **47**

CONTENTS (Continued)

Chapter 4: The Shape of Intelligence Sensemaking 51
Planning for Tame and Wicked Intelligence Problems. 51
Foraging 54
Marshaling 62
Understanding. 62
Communicating 64
Chapter 5: A Practice of Understanding 69
Intuition 69
Types of Judgment 74
Thinking About Anticipating 79
The Roles of Intuitive Thinking in Intelligence Sensemaking 88
Does More Information Improve Anticipation? 90
Future Vision: Red Brains, Blue Brains? 92
Looking Ahead 93
Chapter 6: Considering Validation 95
Analogies from Other Fields. 95
Replication in Intelligence. 98
Validation in Foresight and Hindsight 99
Validating the Practice of Intelligence Sensemaking. 100
Seeking Validation: Toward Multiple Methods 103
Chapter 7: Making Sense of Non-State Actors: A Multimethod Case Study of a Wicked Problem 105
Introduction. 105
Introducing the Wicked Problem of Non-State Actors 106
Three Approaches to Making Sense of Non-State Actors. 108
Approaches and Methodologies 114
Critical Assessment: Lessons Learned from the Study of Non-State Actors 122
Changes in the Roles of Non-State Actors: An Alternative View 123
Moving Beyond a Proto-Revolution 129

CONTENTS (Continued)

Chapter 8: Establishing Metrics of Rigor 133
Defining Intelligence Rigor 133
Assessing Sensemaking Rigor in Studies of Non-State Actors 138
Observations and Discussion 144
Chapter 9: Implications, Limitations, and Conclusions 149
Considering Foresight 149
Implications 152
Limitations 153
Conclusions 154
References 157
About the Author 181
About the Contributors 183
Index 185
Colophon 195

CONTENTS (Continued)

Tables

1. Characteristics of Wicked Problems. **19**
2. Cooper's Analytic Pathologies **26**
3. Classical Planning and Execution Versus Flexecution **53**
4. Comparing NIC and LSS Critical Thinking Perspectives **115**
5. Advantages and Disadvantages of Each Method **118**
6. Attributes of the The Rigor Metric **136**
7. Comparative Scores of the Three Efforts Examining the Roles of Non-State Actors **138**

CONTENTS (Continued)

Figures

1. Types of Intelligence and the Phenomena They Characterize 39
2. Changes in Predictive Accuracy and Confidence as Available Information Increases. 57
3. Space-Time Envelope of Indeterminate Causality 82
4. A Notional Example of Causality Across the Space-Time Envelope 84
5. A Space-Time Envelope of Anticipation Regarding the Authenticity of the Documents Recovered at Huelva, Spain, 1943 86
6. Drivers for the Rise and Growth of Violent Non-State Actors (vNSAs). 107
7. Composite Non-State Actor Role Scores for Africa. 110
8. Non-State Actor Potential Spectra for Botswana and the Central African Republic 112
9. Kenyan Non-State Actor Potential Spectra 113
10. Iraqi Points of Segmentation 121
11. A Metric for Rigor 135
12. The Rigor of the NIC-Eurasia Group Study of Non-State Actors 140
13. The Rigor of the Mercyhurst College Students' Study of Non-State Actors 142
14. The Rigor of the Least Squares Social Science Study of Non-State Actors 143
15. The Composite Rigor of the Three Studies of Non-State Actors 145
16. Conceptual Comparison of Kent and Kendall 150

FOREWORD

Gregory F. Treverton
Director
RAND Corporation Center for Global Risk and Security

Recently, I had the opportunity to work with some very impressive young analysts at David Moore's recent home-away-from-home, the National Geospatial-Intelligence Agency (NGA). Assisting U.S. operations in Iraq and Afghanistan, they understood how much the world of what we still call "imagery" had changed. As they put it: We at NGA used to look for things and know what we were looking for. If we saw a Soviet T-72 tank, we knew we'd find a number of its brethren nearby. Now, though, we're not looking for things. Instead, we're looking for activities or transactions. And we don't know what we're looking for.

In fancier language, the paradigm of intelligence and intelligence analysis has changed, driven primarily by the shift in targets from the primacy of nation-states to trans-national groups or irregular forces. In the world of the national-state, I and others divided intelligence problems into puzzles and mysteries (or variants of those words).[1] Puzzles are those questions that have a definitive answer in principle. How many nuclear missiles the Soviet Union had was a puzzle. So is whether Al Qaeda possesses fissile material. By contrast, mysteries are questions that cannot be answered with certainty. They are future and contingent. Will North Korea reach agreement to cease its nuclear program? No one knows the answer, not even North Korean leader Kim Jong Il. It depends. The question is a mystery, not a puzzle.

For puzzles, intelligence tried to produce *the* answer. In solving puzzles about the Soviet Union, the United States spent billions of dollars, primarily on the technical systems whose fruits were and are analyzed at David's home institution, the National Security Agency (NSA) and at NGA, along with espionage collected by the CIA. For mysteries there was no answer. Instead, analysts sought to frame the mystery by providing a best estimate, along, perhaps, with excursions or scenarios to test the sensitivity of critical factors. If intelligence failed to understand the full picture of Soviet missiles,

[1] For my version of the distinction, see Gregory F. Treverton, "Estimating Beyond the Cold War," *Defense Intelligence Journal* 3, no. 2 (Fall 1994): 5-20. Cited hereafter as Treverton, "Estimating."

and puzzle became mystery, it at least knew something about where to look: there was experience and theory about missile building, plus historical experience of Soviet programs. The mystery came with some shape.

However, today's transnational threats confront us with something more than mysteries. I call these shapeless mysteries-plus "complexities," borrowing Dave Snowden's term. They are sometimes called, as Moore notes, "wicked problems" or simply "messes." The come without history or shape. Large numbers of relatively small actors respond to a shifting set of situational factors. Thus, they do not necessarily repeat in any established pattern and are not amenable to predictive analysis in the same way as mysteries. Those characteristics describe many transnational targets, like terrorists—small groups forming and reforming, seeking to find vulnerabilities, thus adapting constantly, and interacting in ways that may be new.

For complexities, especially, the challenge is to employ sensemaking—the term is from Michigan psychologist, Karl Weick. Exactly how to accomplish sensemaking is a task that still mostly lies before us, which makes this book such an important contribution. Sensemaking departs, as Moore notes, from the postwar tradition of Sherman Kent, in which analysis meant, in the dictionary's language, "the process of separating something into its constituent elements." Sensemaking also blurs America's bright white line between intelligence and policy, for, ideally, the two would try to make sense together, sometimes disaggregating events, sometimes aggregating multiple perspectives, always entertaining new hypotheses, all against the recognition that dramatic failure (or success) might occur at any moment.

Sensemaking is a tall order, but there is no better sherpa for the unfamiliar terrain of this new paradigm than David Moore. He almost uniquely embodies both practice and academic scholarship. Indeed, one of the tantalizing aspects of his academic work is that, as a careful intelligence professional (and one from NSA to boot), he is very careful about classification. That means the visible trails of his practice in his scholarship are sparse, and his cases are mostly familiar ones, albeit ones often spun in new directions.

His approach to sensemaking takes us from information foraging, harvesting and marshalling into understanding. He looks at various forms of tacit knowledge, and he and the contributors report on some intriguing tests of sensemaking. Several of us who looked around the Intelligence Community in the years after September 11th noted how little use it made

of formal methods or machines other than computers for sorting.[2] Worse, in some sense the Cold War practice of analysis sought to turn humans into machines by rooting out judgment, bias, hunch, stereotyping—all the things humans do best. The new paradigm makes the use of machines and method imperative, letting machines do what they do best—searching large amounts of data, remembering old patterns, and the like—while letting humans use the judgment they alone can apply. Yet the tests by Moore and his colleagues remind us that methods are critical but only if they have been tested. It turns out, for instance, that ACH, analysis of competing hypotheses, a method more frequently used now and one that has been tested, isn't all that valuable, at least not for analysts beyond the novice level.

For years I've had at hand a bumper sticker for which I lacked the car. The bumper sticker is: Intelligence cannot truly be reshaped until it reshapes its products. So long as it thinks of products primarily as words on paper (or bytes on a screen) produced by relevant experts and stovepiped by agency it is stuck in the old paradigm. Moore should not be blamed for my bumper stickers, but his emphasis on communication echoes the concern underlying it. I'd be happy if the Intelligence Community began a number of pilot projects trying to develop sensemaking, but Moore is much more ambitious: while recognizing its limitations, he'd make sensemaking the basis of intelligence. It should be.

2 Most striking is the work of anthropologist Rob Johnston, now on the inside: Rob Johnston, *The Culture of Analytic Tradecraft: An Ethnography of the Intelligence Community* (Washington, DC: Center for the Study of Intelligence, Central Intelligence Agency, 2005). My own version is *Assessing the Tradecraft of Intelligence Analysis* (with C. Bryan Gabbard), TR-293 (Santa Monica, CA: RAND Corporation, 2008).

COMMENTARY

Anthony Olcott, PhD
Associate, Institute for the Study of Diplomacy
Georgetown University

David Moore is right to talk of the need for an intelligence revolution. However, as Lenin learned in the 18 years that passed between publication of *The Development of Capitalism in Russia* and taking over the Winter Palace, it takes more than a diagnosis and a prescription to make a revolution. Although his is among the best, Moore's book is also but the latest addition to a groaning shelf of books devoted to intelligence and analytic reform while the companion shelf, for books on how to improve the policy process, sits dusty and all but empty. In that regard, even though Moore's discussion of the processes of analysis and how the ways we answer questions might be improved is one of the strongest in recent memory, the most valuable part of the book could well be the somewhat smaller amount of attention it devotes to the problem of how we formulate our questions in the first place.

As Moore points out, Sherman Kent and the other *ur*-fathers of intelligence took for granted that the "intelligence questions" are self-evident—foreign policy is (Walter Lippmann's words) "the shield of the republic" and strategic intelligence is (Kent's addition to Lippmann) what "gets the shield to the right place at the right time" and what "stands ready to guide the sword."[3] In that metaphor there is no room for doubt about what is threat, what defense, or indeed what receives the thrust of the sword. Even as Kent's book appeared, however, other voices were arguing that policy formation is not so self-evident or straightforward.

Moore quotes one of these voices, that of Kent's contemporary and, for a time, IC colleague, Willmoore Kendall. Kendall did not share Kent's conviction that the job of the analyst was "to stand behind [the policymakers] with the book opened at the right page, to call their attention to the stubborn fact they may be neglecting."[4] Unlike Kent, who was an unabashed elitist, Kendall was a "majoritarian," who believed that, in a democracy, all policy, foreign and domestic, could only be set by the wishes of the "50 percent plus 1" who vote

3 Sherman Kent, *Strategic Intelligence for American World Policy* (Princeton NJ: Princeton University Press, 1949), p. viii. Cited hereafter as Kent, *Strategic Intelligence*.

4 Sherman Kent, *Strategic Intelligence*, p. 182.

for a particular person, platform, or party—and the job of the analyst, therefore, was to help the "politically responsible laymen" whom that majority had elected to bring those policies into being. Although "majoritarianism" led Kendall into some positions which today seem deeply repugnant —for example, he defended racial segregation, on the grounds that this was the wish of the majority—his argument that policy is determined by beliefs, not "objective facts," is one that, had it prevailed, could probably have helped us to avoid a good number of the familiar "intelligence failures" that Moore's book enumerates.

Moore moves some way toward Kendall's position when he describes the potential that sensemaking offers as a means precisely for helping policymakers to improve how they think about policy. The collaborative processes he outlines would help analysts and policymakers alike move from the present fixation on "how things work" (the provenance of analysis) to imaginative exploration of the ways in which things *could* work (the purpose, it would seem, of policy).

It is here particularly that I would encourage Moore's readers to think about how to move this sense-making revolution closer to reality. As philosopher Denis Hilton has remarked, there is a profound difference between "causal attribution" and "causal explanation"—in his words, "attributing the 9/11 attacks to someone is not the same as explaining them to him."[5] Moore has done a deep and convincing job of diagnosing the ills of the IC, and has proposed a rich and promising cure. This, as Hilton points out, is an extended act of cognition. What lies between this book and Moore's revolution, however, is the need to have others come to the same conclusion—which, as Hilton points out, requires *communication*, not cognition.

Sixty years ago a small group of analysts—dubbed "Talmudists" for their pains—worked out a complex, sophisticated method of deriving actionable intelligence from the tightly controlled propaganda outlets of the USSR and Mao's China. This let IC sinologists spot the first signs of the Sino-Soviet split as early as April 1952, and by 1955 Khrushchev had been tagged as the likely winner in the struggle to consolidate power in the Kremlin after Stalin's death. Those early indicators, however, remained scoffed at and un-acted upon precisely because the methodology—which a colleague in the CIA compared to studying "invisible writing on slugs"[6]—was too complex and too weird to

5 Denis Hilton, "Causality vs. Explanation: Objective Relations vs. Subjective Interests," *Interdisciplines*, Institute of Cognitive Sciences, University of Geneva, URL: <http://www.interdisciplines.org/causality/papers/14>, accessed 1 November 2010.

6 Richard Shryock, "For An Eclectic Sovietology," *Studies in Intelligence*, vol. 8, no. 1 (Winter 1964).

be easily explained to policymakers—*who, in any case, already believed other hypotheses, and had their own "facts."*[7]

The challenge we face is the same as that which faced those Talmudists. Moore has convinced himself, and he is highly likely to convince all the analysts who read his book, that sensemaking is indeed the intelligence revolution we need. The challenge now is to communicate that to policymakers, so that they too will be willing to join David Moore's sensemaking revolution.

7 Harold P. Ford, "The CIA and Double Demonology: Calling the Sino-Soviet Split," *Studies in Intelligence*, vol. 42, no. 5 (Winter 1988-1989).

COMMENTARY

Emily S. Patterson, PhD
Assistant Professor
College of Medicine
The Ohio State University

A colleague once said that he was dedicated to the vision of having decisionmaking be directly informed by evidence rather than the popularity of the latest fad or pet projects of powerful leaders. The context for his comment was for deciding what innovations to implement in hundreds of Intensive Care Units to reduce risk-adjusted patient mortality. Nevertheless, I believe that this lofty goal could easily apply to United States policymaking. In my opinion, it is an achievable goal for the vast majority of United States policy to be directly informed by evidence that is systematically validated, collated, and synthesized by teams of professional intelligence analysts.

This book is a critical milestone in attaining the goal of analysis directly supporting evidence-based policymaking. This book's primary contribution is to conduct sensemaking on the label sensemaking. Decades of relevant academic literatures have been synthesized into one framework that illustrates how disparate research streams relate to each other and to the framework. Until now, there has not been such an extensive effort to pull together related research on sensemaking from such diverse disciplines as psychology, political science, philosophy, organizational science, business, education, economics, design, human-computer interaction, naturalistic decisionmaking, and macrocognition.

The contributions of this book go beyond a literature review, however, in that an action-oriented stance is taken toward capturing nuggets of insight on how to improve aspects of analysis. The categories themselves are useful in putting some shape and structure to the amorphous value that expertise brings to creating a solid analytic product in an uncertain world: planning, foraging, marshaling, understanding, and communicating. Of particular value is describing different aspects of validation that are relevant to intelligence sensemaking, and distinguishing processes for predicting future events (foresight) from processes for describing past events and assessing their impacts (hindsight).

Another colleague once said that she looks at what is measured operationally to determine how people truly define a concept. Chapter 8, Establishing Metrics of Rigor, is therefore critically important to any discussion of how to encourage improved sensemaking in the Intelligence Community. As David Moore notes, although we believe our rigor metric to be a promising first step, much more needs to be done to ensure that all of the important aspects of rigorous analysis are captured. The application of the rigor metric to a face valid case study in this book is the first such application in intelligence analysis to compare processes by different analytic teams. Whether or not high rigor on all of these inter-related dimensions is possible to achieve under the working conditions for intelligence analysts today is an unresolved debate. Even if high rigor is not possible under extreme time pressure, data overload, and workload conditions, the measure has potential value in supporting negotiations for what aspects are most important to do well for a given task, as well as communicating the strengths and weaknesses of the process behind an analytic conclusion.

COMMENTARY

Christian P. Westermann
Senior Analyst
Bureau of Intelligence and Research
U.S. Department of State

History will tell us if current intelligence reforms are evolutionary or revolutionary, but the Intelligence Community is responding to mandated change brought about by the 2004 Intelligence Reform and Terrorism Prevention Act (IRTPA).[8] In particular, the analytic and collector communities are adjusting to one of IRTPA's pillars—improved information sharing. As reforms unfold, the collector and analyst must adapt to new rules and new analytic standards, and incorporate more methodologies, techniques, and alternatives in their analysis, in collaboration with managers and tradecraft cells in the national intelligence organizations. These new structures and guidelines present an intellectual challenge as well as a bureaucratic maze for the collector and analyst struggling not only to "produce" intelligence in a timely fashion but also to improve their product. This is not easy for the intelligence professional because time is not on their side. This is why improving the way in which all analysts think is so important and why an understanding of sensemaking will help advance the profession beyond the "established analytic paradigm" for complex problems and create greater possibilities for the application of imagination in the IC. The failure to properly assess Saddam Hussein's WMD programs during the lead-up to Operation Iraqi Freedom is the preferred example of this failure to imagine alternatives. The corporate solution to this problem is increased collaboration and information sharing; David Moore is not in disagreement but has suggested that it must go beyond new methodologies or techniques—it must be done with a strong sense of rigor and individualism in one's thinking.

David Moore has written for the Intelligence Community a revolutionary epistemology. His novel construct for intelligence professionals is the foundation for a philosophy of intelligence. He has started where he left off in his work on *Critical Thinking and Intelligence Analysis* with a path forward for analysts and how they can improve their capacity and move beyond the

8 United States Congress, *Intelligence Reform and Terrorism Prevention Act of 2004*, 108th Congress, 2nd Session, 20 January 2004. Cited hereafter as U.S. Congress, IRTPA, 2004.

methods they learn as "good" tradecraft.[9] Moore's prescription is to take the disaggregation of data, commonly referred to as analysis, synthesize it, and then apply to it one's interpretation and communication skills to make sense of the information. Sensemaking therefore is a theory of knowledge for the intelligence professional and also a practice to aid the difficult art of intelligence reasoning.

Current "total" intelligence reform, as described by Director of National Intelligence James Clapper in late 2010, is reform that is focused on "integration, the merging of collection and analysis—particularly at the ODNI level—analytic transformation, analytic integrity, acquisition reform, counterintelligence—and information sharing."[10] This involves a great deal of uncertainty for organizations and analysts, in light of the formation of new intelligence fusion centers reminiscent of Defense intelligence reform of the 1990s—which saw the rise of Joint Intelligence Centers—and presents a challenge to make sense of new security challenges in the post-9/11 world. The time is therefore ripe for analysts to transform their thinking and tradecraft and Moore's new paradigm offers real improvements to their practice of intelligence. His attention to revolutionary change in the art of intelligence thinking grows from his recognition that organizational reform has been ongoing for decades and despite those changes attendant failures have occurred and continue to occur. Therefore the only hope for achieving positive reform rests with changing the practice of intelligence whereby the individual collector and analyst, working together, and accepting the responsibility to think critically but also independently and across the Community, make sense of the 21st century national security environment.

9 David T. Moore, *Critical Thinking and Intelligence Analysis* (Washington, DC: NDIC Press, 2007). Cited hereafter as Moore, *Critical Thinking*.

10 James Clapper, "Remarks and Q & A by Director of National Intelligence Mr. James Clapper," Bipartisan Policy Center (BPC)—The State of Domestic Intelligence Reform, 6 October 2010, URL: <http://www.dni.gov/speeches/20101006_speech_clapper.pdf>, accessed 29 October 2010.

COMMENTARY

Phil Williams, PhD
Director, Matthew B. Ridgway Center for International Security Studies
Wesley W. Posvar Chair of International Security
Graduate School of Public and International Affairs
University of Pittsburgh

Moore's Law for Intelligence

Any book that discusses amongst other things, red brains and blue brains, kayaking, information foraging, flashlights as blindfolds, space-time envelopes, and intellectual audit trails, is out of the ordinary. When you throw in the contention by the author that intelligence as currently practiced is akin to medicine in the 14th Century you have a book that will raise hackles, blood pressure, and voices. David Moore's provocative and stimulating analysis of critical thinking and sensemaking for intelligence does all of the above.

This is not an easy read. But the overall thesis is straightforward and compelling: the environment within which the U.S. intelligence community now finds itself is not only highly complex but also full of wicked problems. To provide the kind of intelligence that is useful, relevant, and helpful to policy makers who have to anticipate and respond to these problems and challenges, Moore argues that the traditional paradigm developed largely by Sherman Kent has to be superseded by a new paradigm based largely on ideas initially outlined by Willmoore Kendall, a contemporary critic of Kent. The original Moore's Law[11] was narrowly technical; David Moore in contrast argues that a complex environment full of mysteries, not puzzles, requires holistic thinking (as opposed to simply disaggregation of problems), mindfulness (as opposed to mindlessness which he also elucidates), and a dynamic willingness to change paradigms, shift perspectives, and abandon strongly held perceptions. The book also develops the notion of sensemaking rigor and shows how metrics of rigor can be applied to several studies examining the rise and impact of non-state actors.

David Moore's analysis is important and deserves to be widely read in the intelligence community and in the academic world. Yet, the volume—as

11 Gordon E. Moore, "Cramming More Components onto Integrated Circuits," *Electronics*, vol. 38, no. 8 (19 April 1965), URL: <ftp://download.intel.com/museum/Moores_Law/Articles-Press_Releases/Gordon_Moore_1965_Article.pdf>, accessed 7 November 2010.

he would be the first to acknowledge—is intended as an early word on sensemaking and intelligence, rather than the last word. Indeed, it would have been helpful, for example, if David Moore had considered more explicitly the argument by David Snowden that making sense of a complex environment requires probing the environment. Further thought about this suggests that law enforcement is particularly good at this form of knowledge elicitation and sensemaking: sting operations, controlled deliveries, infiltration of criminal organizations, are all probing mechanisms that can contribute significantly to an increased level of understanding and, concomitantly, to an enhanced capacity for effective action. For many intelligence professionals, especially those who have had a dismissive view of law enforcement, the idea that law enforcement approaches to sensemaking might be ahead of those in the intelligence community, is likely to be as uncomfortable as most of the arguments in David Moore's book. Certainly Moore's volume is designed to shake and to stir. It is a manifesto for an intellectual revolution in the approach to intelligence and, as such, is likely to be both acclaimed and reviled. One suspects that the author will measure his own success by the depth of opposition as well as the levels of support for the revolution he is proposing.

PREFACE
On Being Mindful

What Is Mindlessness?

We are surrounded by errors and they are ours. Intelligence officials at the national level repeatedly use the same excuses for professional errors and for the systemic failures that follow. Despite directives to "fix" the structures, and most recently the means, by which intelligence is created, we insistently fail at our obligation to make early sense of vital threats and opportunities. What is our problem?

We may begin by examining the concept of *mindlessness*. Ellen Langer, summarizing her pioneering social psychology research, finds mindlessness to arise from an over-reliance on "categories and distinctions created in the past."[12] She holds that such categories "take on a life of their own."[13] Seen in this context, the failure to recognize in foresight that an American or a Nigerian man could be a member of Al Qaeda arises from a rigid deductive categorization of who is a member of Al Qaeda and is a case of mindlessness.

Langer also sees mindlessness arising from "automatic behavior." Here, people rely on automatic responses as the basis for their behavior, as when one writes "a check in January with the previous year's date."[14] By extension, intelligence professionals, in assessing sources, may develop a habit of discounting human intelligence sources because some are untrustworthy. As a result, they may miss novel insights because they use certain sources to the exclusion of others.

Finally, mindlessness can result from a failure to take into account alternative information that transcends our comfortable worldview. Langer observes that "[highly] specific instructions…encourage mindlessness" because they define what is acceptable and limit the viability of alternative signals that could lead to more accurate understanding of a phenomenon.[15] During the summer of 1962, CIA and DIA intelligence professionals at the Refugee

12 Ellen J. Langer, *Mindfulness* (Cambridge, MA: Da Capo Press, 1989), 11. Cited hereafter as Langer, *Mindfulness*.

13 Langer, *Mindfulness*, 11.

14 Langer, *Mindfulness*, 12.

15 Langer, *Mindfulness*, 17-18.

Processing Center (RPC) in Miami discounted the validity of refugee reports of nuclear missiles on the island because some refugees also went beyond the pale by concocting "farfetched tales of African troops with rings in their noses, lurking Mongolians, and even Chinese troops."[16] There were in fact 100 nuclear-tipped *tactical* missiles deployed on the island months before the arrival of the more infamous strategic missiles.[17] A rigid notion of what constituted a nuclear missile, usually conceived as an offensive weapon, appears to have contributed to the case officers' mindless disregard of the witnesses.

Not only intelligence practitioners, but also those with whom they communicate their understandings, remain subject to the dangers of mindlessness. With respect to intelligence consumers, two faculty members at the International Institute of Management Development (IMD), corporate strategy expert Cyril Bouquet and corporate leadership and organization expert Ben Bryant, suggest that "decision makers often suffer from poor attention management, being obsessed with the wrong types of signals and ignoring possibilities that could significantly improve the fate of their undertakings."[18] They characterize these behaviors as *fixation* and *relaxation*. People who fixate "become so preoccupied with a few central signals that they largely ignore things at the periphery."[19] A deadly example of fixation occurred in 1977, when the KLM 747 flight crew on Tenerife failed to avoid a collision with a Pan Am 747: "they didn't give sufficient attention to the presumably very important communications coming in from air traffic controllers."[20] Naval aviators engaged in night landings on aircraft carriers also fixate and this leads to pilots' ignoring "the obvious and doing the inexplicable" (and

16 James H. Hansen, "Soviet Deception in the Cuban Missile Crisis," *Studies in Intelligence,* 46, no. 1 (2002), 56. The author referred to this incident in his book on critical thinking and intelligence. See Moore, *Critical Thinking*, 20.

17 Raymond L. Garthoff, "US Intelligence in the Cuban Missile Crisis," in James G. Blight and David A. Welch, eds., *Intelligence and the Cuban Missile Crisis* (London, UK: Frank Cass, 1998), 22.

18 Cyril Bouquet and Ben Bryant, "The Crisis Is Here To Stay. Do You Have The Key To Coping?" *Forbes*, 21 April 2009, Online Edition, URL: <http://www.forbes.com/2009/04/21/stress-coping-mindfulness-leadership-managing-fixation.html>, accessed 13 January 2010. Cited hereafter as Bouquet and Bryant, "Key to Coping." IMD is not well known within the Intelligence Community. Its Executive Education program has been rated the number two program worldwide by the *Financial Times* for the past three years; *The Economist* rates its MBA Program as the second best in the world. See *Financial Times*, "Executive Education—open—2009, URL: <http://rankings.ft.com/businessschoolrankings/executive-education—open>, accessed 15 January 2010; and *The Economist*, "Which MBA? 2009 Full-time MBA Ranking," URL: <http://www.economist.com/business-education/whichmba/>, accessed 15 January 2010.

19 Bouquet and Bryant, "Key to Coping."

20 Bouquet and Bryant, "Key to Coping." The accident occurred when KLM 747 collided with the Pan Am 747 as the former took off over the latter. In the crash 583 passengers and crew were killed although miraculously, 65 passengers and crew on the Pan Am flight survived.

often dying).[21] Such fixations are goal-oriented—taking off in the former example and landing in the second. The pilots know intellectually what to do but their fixation on an emotional goal mis-focuses them: "knowing [is] no match for emotion."[22] While they are fixated, they are not truly aware. Nor are they living in the moment; instead, they are inadvisably envisioning themselves already in the air or on the deck and expecting the resulting emotional sense of relief.

Bouquet and Bryant identify relaxation as when, after a "sustained period of high concentration," people become unfocused on the task at hand and look to the ultimate goal.[23] A case in point involves the deaths of three climbers on Oregon's Mount Hood in 2002: they were distracted from the matter at hand—that of completing a difficult descent; they took shortcuts.[24]

Both fixation and relaxation contribute to intelligence failures. For intelligence practitioners, focusing on the wrong factors and failing to recognize the significance of novel indicators are examples of fixation that may have been at work in the December 2009 failure to anticipate the attempted bombing of Northwest Airlines flight 253 over Detroit. Sometimes ascribed to intelligence professionals' and national consumers' falling prey to "creeping normalcy," relaxation was also a contributor to Israel's failure to anticipate the attacks by Egypt and Syria in 1973.

In sum, mindlessness too often guides the assessment of affairs in too many domains, leading to errors, failures, and catastrophes. Mindlessness is deemed unacceptable within the larger American society only when the resulting errors do lead to accidents and disasters. However, mindlessness is completely unacceptable within the domain of intelligence. One can never be certain in foresight whether errors will occur, so intelligence professionals must seek to anticipate, recognize and avoid them at all costs.

Attaining Mindfulness

The antithesis of mindlessness is mindfulness.[25] For Langer, a mindful state corresponds with: "(1) [aptitude for the] creation of new categories;

---

21 Laurence Gonzales, *Deep Survival: Who Lives, Who Dies, and Why* (New York, NY: W.W. Norton, 2003), 26. Cited hereafter as Gonzales, *Deep Survival*.

22 Gonzales, *Deep Survival*, 35.

23 Bouquet and Bryant, "Key to Coping."

24 Gonzales, *Deep Survival*, 97-123.

25 One of the origins of the concept of mindfulness lies in the work of the 19th-century U.S. philosopher Charles Sanders Peirce, whose notion of "thirdness" relates to present connotations of "mindfulness" by recognizing thirdness as an observer's self-referenced content of an interpretation. See: Charles Sanders Peirce, "Lowell Lectures (1903)," *Collected Papers of Charles Sanders Peirce*, Volume 1, Charles Hartshorne and Paul Weiss, eds. (Cambridge, MA: Harvard University Press, 1958), para 331-332.

(2) openness to new information; and (3) awareness of more than one perspective."[26] For example, as an intelligence professional considers who might be a member of Al Qaeda, a *mindful* attitude would involve constant reassessment and categorization of who might hold such membership—leaving the path open to new information for making sense of the organization and its membership. Thus, as we apply the idea that "[a] steer is a steak to a rancher, a sacred object to a Hindu, and a collection of genes and proteins to a molecular biologist,"[27] the notion of a Nigerian male or even a blonde woman from Pennsylvania as a possible Al Qaeda affiliate would emerge from a mindful perspective.

Leadership scholar Deepak Sethi sees mindfulness as a "form of meditation" teaching "three simple-on-the-surface yet revolutionary skills: Focus, Awareness, and Living in the Moment."[28] This definition descends from millennia of Buddhist tradition. He argues that rather than an esoteric method it is "very practical, action oriented, and transformational." Sethi believes that one practical way to bring about mindfulness is through the use of daily meditation, first using one's breathing as a focus, and then using "specific daily activities such as meetings with another colleague." However, the "real challenge [of employing mindfulness] is to take it from the meditation chair to the office chair and the real world."[29] Intelligence journeymen face this dilemma from a different perspective. They confront the real world and are challenged to contemplate their own thought processes as they engage it.

Australian expert on argumentation Tim Van Gelder distinguishes mindfulness from critical thinking (which he calls "metacognition"): "Metacognition is concerned with what you are thinking about. Mindfulness is concerned with *how* you think as you go about what you are doing."[30] While Van Gelder accepts Ellen Langer's definition, he argues that metacognition and mindfulness can bear an inverse relationship to one another. As an individual masters one, the need for the other diminishes. To illustrate this point, he asserts that "[in metacognitive terms, a novice] driver needs to pay lots of attention to even the most mundane aspects of driving, such as where the gearshift is. The experienced [mindful] driver pays very little attention to

---

26 Langer, *Mindfulness*, 62.

27 Langer, *Mindfulness*, 69.

28 Deepak Sethi, "Mindful Leadership," *Leader to Leader*, no. 51 (Winter 2009), 7. Cited hereafter as Sethi, "Mindful Leadership."

29 Sethi, "Mindful Leadership," 10.

30 Tim Van Gelder, "Mindfulness Versus Metacognition, and Critical Thinking," [Weblog Entry] *Bringing Visual Clarity to Complex Issues*, 27 May 2009, URL: <http://timvangelder.com/2009/05/27/mindfulness-versus-metacognition-and-critical-thinking/>, accessed 13 January 2010. Emphasis in original. Cited hereafter as Van Gelder, "Mindfulness."

driving, and can carry on a lively conversation instead."[31] Van Gelder's viewpoint—which derives from his definition of critical thinking—holds a serious implication for the intelligence professional: if one learns to be mindful, and is good at it, the risk of a lapse in critical thinking will have increased.

For example, empirical studies of the level of distraction among drivers who are using cell phones reveal an associated, *diminished* driver capacity.[32] Non-distracted drivers are receiving information—without conscious awareness—from: traffic changes ahead, behind, and along side; various mirrors in and on the car; and weather and light conditions. All these inputs factor into their decisions on how to proceed. They are intuitively "in the moment," that is, *mindful* of what they are doing and what is going on around them. They are, as Sethi notes, focused, aware, and living in the moment. But if, as experienced drivers, they are at ease in carrying on a telephone conversation, are they not more accident-prone as a result of operating with a reduced capability or likelihood to be thinking critically?

Van Gelder notes that novice drivers likely monitor their thinking and actions closely—at least intermittently.[33] The amount of metacognitive monitoring that occurs as they become more skilled probably diminishes under normal circumstances. However, it is the author's experience, drawn from office and classroom observation, that people who are skilled critical thinkers still tend to be able to question what is occurring around them even as they are aware of how they are thinking about it. They are thinking critically, even if it is not obvious that they are doing so.

Drivers who employ critical thinking skills to ensure they remain mindful of the appropriate stimuli continually make sense of the environment in which they find themselves. Being metacognitively aware of their likely diminished capacity to drive safely while engaging in cell phone conversations (as well as texting), they are likely to engage in these dangerous acts less often than one who is mindlessly fixated on the cell phone conversation and not mindfully aware of the environment inside and outside their vehicles. To use Gelder's definitions, they are thinking about what to do as well as how to do it; critical thinking and mindful thinking inform each other.

Ben Bryant and IMD research associate Jeanny Wildi write that mindfulness "involves the ability to accurately recognize where one is in one's

---

31 Van Gelder, "Mindfulness."

32 For more information on diminished driver capacity see Transportation Research Board of the National Academies, "Selected References on Distracted Driving: 2005-2009," URL: <http://pubsindex.trb.org/DOCs/Publications from TRIS on Distracted Driving.pdf>, accessed 9 December 2009.

33 Van Gelder, "Mindfulness."

emotional landscape and allows…understanding, empathy, and capacity for accurate analysis and problem-solving."[34] They identify a process of detaching, noticing, and developing "here and now awareness."[35] Detachment, for example, allows a viewer to remember that a movie is really merely a "beam of light passing through a piece of moving celluloid projecting onto a screen with some sound and music that are designed to generate particular emotions."[36]

In intelligence work, detachment involves stepping back from the full sensual experience of an issue to consider the actors involved, their motives, the larger context. Critical thinking as it is taught in the Intelligence Community attempts to make sense of the overall purpose or goal of a phenomenon, the points of view and assumptions of the actors involved, the implications of their acting in certain fashions, and other aspects of the larger context surrounding the issue.[37] Questioning the available evidence and the inferences arising from it brings further detachment from the issue.

Noticing involves remaining open to both internal and external stimuli. Ultimately, situational information is conveyed from external sources through sight, sound, touch, smell, and taste. People can think consciously about these but they tend to process them using more autonomic brain structures, often without noticing they are doing so. The unease one feels about getting into a taxi or onto an elevator in an unfamiliar setting are examples of such input. In intelligence work this might be represented as a hunch about what an adversary will do. As Daniel Kahneman and Gary Klein note, in certain environments—where one can learn the cues—these intuitions may be quite accurate.[38] However, in domains where one has not developed expertise, such intuitions can be *inaccurate*.[39] The challenge is determining which of these situations one is in. This brings us back to the imperative of applying mindful detachment from the situation.

---

34 Ben Bryant and Jeanny Wildi, "Mindfulness," *Perspectives for Managers*, no. 162 (September 2008), 1, URL: <http://www.imd.ch/research/publications/upload/PFM162_LR_Bryant_Wildi.pdf>, accessed 14 January 2010. Cited hereafter as Bryant and Wildi, "Mindfulness."

35 Bryant and Wildi, "Mindfulness," 2-3.

36 Bryant and Wildi, "Mindfulness," 3.

37 These are some of the "Elements of Thought" developed by Linda Elder, Richard Paul, and Gerald Nosich of the Foundation for Critical Thinking. This author operationalized the Foundation's critical thinking paradigm for intelligence work. See Moore, *Critical Thinking*, 8-9; and Gerald M. Nosich, *Learning to Think Things Through: A Guide to Critical Thinking Across the Curriculum*, 3rd edition (Upper Saddle River, NJ: Pearson-Prentice Hall, 2009), 50-67. Cited hereafter as Nosich, *Learning to Think Things Through*.

38 Daniel Kahneman and Gary Klein, "Conditions for Intuitive Expertise: A Failure to Disagree," *American Psychologist*, vol. 64, no. 6 (September 2009), 520. Cited hereafter as Kahneman and Klein, "Intuitive Expertise."

39 Kahneman and Klein, "Intuitive Expertise," 521-522.

Critical thinking assists noticing as well. Bryant and Wildi observe that because people tend to make immediate sense of stimuli, "We all too often contaminate our perceptions with unexamined assumptions we have already internalized."[40] In other words, from the time when we have already decided what something means, everything we notice tends to confirm that interpretation. However, by challenging critically our assumptions and choices of evidence (and their interpretations) and asking about alternative explanations, we may bring our noticing back to a state where it "contributes to mindfulness by keeping us open to our experiences of the external."[41]

Bryant and Wildi consider "here and now awareness" to involve paying attention to immediate experience—as it happens. Clausewitz observes this phenomenon when he distinguishes between a commander's plan for war and the friction of war.[42] The former must be adapted in light of the latter. Knowing how to do this, and when, requires the situational awareness found in the here and now. As has been noted, critical thinking allows questioning of both what one is doing and how one is doing it. Here again, one can challenge whether one is focused in the present or dwelling in the past or imagining a future. One can ask whether one is relaxed or fixated on a goal; we can also reflect on whether we are acting mindlessly or mindfully. The key is remaining vigilant, as Warren Fishbein and Gregory Treverton note, as "[mindfulness] is the result of a never-ending effort to challenge expectations and to consider alternative possibilities."[43]

Such mindful vigilance can be a lifesaver, as *Foreign Policy* columnist and blogger Thomas Ricks notes about its absence among troops serving in Afghanistan, where Marines wearing iPods while on patrol can (and apparently do) fail to notice changes in the environment they have previously patrolled, and get hit by improvised explosive devices.[44] If they were mindful, they could have noticed that a hole in the road when they went out on patrol has been filled in before their return. Instead, the "turret gunner [is]

---

40 Bryant and Wildi, "Mindfulness," 3.

41 Bryant and Wildi, "Mindfulness," 3.

42 Carl von Clausewitz, *On War,* COL James J. Graham, trans. (London, UK: Keegan Paul, Trench, Truebner & Co., Ltd.: 1908), 80.

43 Warren Fishbein and Gregory Treverton, "Making Sense of Transnational Threats," *Sherman Kent Center Occasional Papers*, vol. 3, no. 1 (October 2004), 17, URL: <https://www.cia.gov/library/kent-center-occasional-papers/pdf/OPV3No1.pdf>, accessed 8 November 2010. Cited hereafter as Fishbein and Treverton, "Making Sense."

44 Thomas E. Ricks, "A Marine's Afghan AAR (XIV): Get Rid of the iPods on Patrol," Web Log, Foreign Policy. URL: <http://ricks.foreignpolicy.com/posts/2010/01/20/a_marine_s_afghan_aar_xiv_get_rid_of_ the_ipods_on_patrol>, accessed 26 January 2009. Ricks quotes a Marine Corps source, referred to in the web log as "CWO2/Gunner Keith Marine." Cited hereafter as Ricks, "Get Rid of the iPods." iPod is a registered trademark of Apple Computer.

watching a movie on an iPod…[and] the back seater [is] listening to music on his [iPod]."[45] Not only are they not mindful, but no one is paying attention. According to Rick's Marine informant, ensuing and repeated iPod-wearing-induced mindlessness led to the unit's losing "15 out of 20 vehicles in about a month."[46] Clearly, the cost of not being mindful is high. However, becoming mindful is not difficult; that cost is relatively low.

Developing mindfulness is not—as Bouquet and Bryant, as well as Sethi, observe—an arcane spiritual practice. The process certainly involves self-reflection—meditation to some—but in fact self-reflection has become a central facet of professional practice in "real-world" security and defense planning.[47] However, mindfulness in operations or in intelligence is neither a panacea nor a formula: Bouquet and Wildi observe that "executives need to meditate in their own way, find ways to step back and reflect on their thoughts, actions, and motivations, and decide which ones are really supportive of their strategic agendas."[48] One of the benefits of such meditation, according to recent experimental findings, is that perceptual sensitivity and vigilance improve in situations requiring sustained visual attention.[49] While perceptual sensitivity and increased vigilance could also be attained, as in the case cited by Ricks, by simply leaving the iPods turned off and actually conducting reconnaissance and surveillance of one's surroundings, the problem of sustained-attention failure remains. Simply put, mindfulness declines over time. However, as MacLean *et alia* have demonstrated, sustained-attention failure can be reduced through formal meditation training.[50] In this case, formal

45 Ricks, "Get Rid of the iPods."

46 Ricks, "Get Rid of the iPods."

47 For an example of a "how-to" guide to reflective practice, see Faculty of the School for Advanced Military Studies, *The Art of Design*, vol. 2 (Fort Leavenworth, KS, 2010). Available at URL: <http://www.cgsc.edu/events/sams/ArtofDesign_v2.pdf>, accessed 20 May 2010. This student text, which aims to prepare senior military officials for leadership roles in overseas operations, employs "reflective practice [to construct] a cognitive framework for how to reason through complexity." The doctrinal publication develops and applies reflective thinking ideas originated by Donald Schön. See URL: <http://www.infed.org/thinkers/et-schon.htm>, accessed 20 May 2010.

48 Bouquet and Bryant, "Key to Coping."

49 Katherine A. MacLean and others, "Intensive Meditation Training Improves Perceptual Discrimination and Sustained Attention," *Psychological Science*, vol. 21, no. 6 (2010), 829. Cited hereafter as MacLean et al., "Intensive Meditation." See also, John Cloud, "Losing Focus? Studies Say Meditation May Help," *Time*, online edition, 6 August 2010, URL: <http://www.time.com/time/health/article/0,8599,2008914,00.html>, accessed, 11 August 2010. Cited hereafter as Cloud, "Meditation."

50 MacLean et al., "Intensive Meditation," 829.

meditation practices appear to sustain longer-term mindfulness—something the U.S. Army hopes will enhance the capabilities of its soldiers.[51]

While the U.S. Military and the Intelligence Community (like business enterprises) can provide environments conducive to developing mindfulness, Bouquet and Bryant remind us that developing mindfulness is "the responsibility of individuals, not companies."[52] The simple expedient of not engaging in mindfulness-reducing activities is one means of enhancing mindfulness; there are many others.[53] Critical thinking provides one self-reflective or *metacognitive* means to ascertain what surrounding phenomena are or are not taken into account.[54] Such mindfulness in turn supports the larger objective of intelligence sensemaking, the subject of this book. The author is aware of the confounding problem that intelligence may need to give attention to the entire domain of human behavior because every sphere of human practice and knowledge can be of interest and of use in the process of sensemaking. To limit this challenge, this book focuses on those areas that in the author's observation and experience appear most germane to the successful practice of national intelligence. The author intends for this book to generate beneficial discussion and further consideration of exactly what it means to engage in intelligence sensemaking and how one can go about it effectively.

---

51 Bonnie Rochman, "Samurai Mind Training for Modern American Warriors," *Time*, online edition, 6 September 2009, URL: <http://www.time.com/time/nation/article/0,8599,1920753,00.html>, accessed 4 August 2010.

52 Bouquet and Bryant, "Key to Coping."

53 Cloud, "Meditation."

54 "Metacognitive" as used here refers to a process of critically monitoring one's reasoning about an issue while one is engaged in that reasoning or critical thinking. This makes explicit the process of reasoning. However, the term "metacognitive" refers to much more as will be developed further in the paper that follows.

ACKNOWLEDGMENTS

The author's first notes about what 21st Century intelligence would look like as well as how it might be accomplished were crafted at a 2001 conference on the future of intelligence in Italy. The intervening years brought work on what it takes to be a successful intelligence professional and how critical thinking could aid the consideration of strategic issues and the creation of intelligence knowledge for decisionmakers. These steps, it turned out, led to a larger vision of what the practice of intelligence could be: a process of sensemaking.

Few projects are created without substantial assistance from others. This book is no exception. Elizabeth Moore offered valuable ideas and challenged my thinking. She also once again put up with a distracted husband who worked (very) late into the night and on the weekends. Colleagues and peers read and commented on various drafts, criticizing and offering valuable suggestions that sent the author in new directions. Among them are James Bruce, Science Applications International Corporation (SAIC); Stu Card, Palo Alto Research Center; Steven Carey, NDIC; Bruce Chew, Monitor Group; Jeffrey Cooper, SAIC; Linda Elder, Enoch Hale, Gerald Nosich, and Richard Paul, Foundation for Critical Thinking; Norman Endlich, University of Maryland; Warren Fishbein, Department of State; Robert Heibel, Mercyhurst College Institute for Intelligence Studies (MCIIS); Noel Hendrickson, James Madison University; Richards J. Heuer, Jr., Central Intelligence Agency (retired); Robert Horn, Stanford University; Francis J. Hughes, NDIC; Gary Klein, Klein Associates; Lisa Krizan, National Security Agency (NSA); Martin Krizan, NSA; Mark Lowenthal, president of the Intelligence and Security Academy, LLC; Brandon S. Minnery, IARPA (Intelligence Advanced Research Projects Activity); Esther Neckere, National Geospatial-Intelligence Agency; William Nolte, University of Maryland; Anthony Olcott, Georgetown University; Emily S. Patterson, Ohio State University; Randy Pherson, Pherson Associates; Peter Pirolli, Palo Alto Research Center; Timothy Smith, Office of Naval Intelligence; David Snowden, Cognitive Edge; Mark Stefik, Palo Alto Research Center; Kenneth Stringer, Booze Allen Hamilton; Cathryn Thurston, NDIC Press; Gregory Treverton, RAND; Kristan J. Wheaton, MCIIS; Phil Williams, University of Pittsburgh; Chris Westermann, Department of State; David Woods, Ohio State University; and Daniel Zelik, Ohio State University.

The participants in a number of workshops sponsored by IARPA, the Office of the Director of National Intelligence (ODNI), NSA, and the ODNI Global Futures Forum also provided input and ideas. The staff of the Foreign Denial and Deception Committee's denial and deception program at the National Defense Intelligence College (NDIC) invited the author to defend an early version of the text as part of an advanced studies program.

Contributors Robert Hoffman (Chapter 5) and Elizabeth Moore, William Reynolds, and Marta Weber (Chapter 7) graciously agreed to share their ideas in collaborative efforts to bring those chapters about. Without their assistance those two chapters would have been far less rich. Colleagues of Dr. Reynolds as well as Kristan Wheaton and his students in the MCIIS (acknowledged separately in Chapter 7) provided much of the "heavy lifting" that made the conclusions derived possible.

Russell Swenson, under contract to the NDIC's Center for Strategic Intelligence Research, once again provided the essential input of a good editor. His reviews tightened arguments and focused what follows. He also provided a wealth of new ideas that sent the author off in new directions and enriched the book significantly. William Spracher once more provided the skills of a technical editor. Cathryn Thurston, the Director of the NDIC Center for Strategic Intelligence Research and NDIC Press editor, supported the creation of this project as part of her advocacy that intelligence needs to be recast for this century.

While the author was privileged to receive the assistance of others, this remains his work and any errors are his. The author may be reached via electronic mail at *david.t.moore@ugov.gov*.

Definitions for Making Sense of Sensemaking

Intelligence is a "specialized form of knowledge…[that] informs leaders, uniquely aiding their judgment and decision-making." It is a type of knowledge created through organized activity that adds unique value to the policy- or decisionmaker's deliberations. In the U.S. context, it makes sense of phenomena of interest to national leaders, warfighters, and those that directly and indirectly support them. Intelligence makes sense of phenomena related to the social behaviors of others. It reflects interest in what anyone will do to, and with, others that could affect the national interests of the United States as well as the prosperity and security of its citizens. Intelligence maintains an interest in external phenomena, such as epidemic or pandemic diseases, that impact U.S. national interests. In contrast to some popular portrayals, it really is not voyeuristic: what others do privately and alone is generally of little interest or value except as it affects how they relate to, and behave toward others. In other words, when private behaviors reveal either vulnerabilities or preferences, they may become of value to intelligence practitioners.

Sources: David T. Moore, *Critical Thinking and Intelligence Analysis, Occasional Paper Number Fourteen* (Washington, DC: National Defense Intelligence College, 2006), 2. Cited hereafter as Moore, *Critical Thinking.* Intelligence also refers to activity and organization: See Kent, *Strategic Intelligence.*

Sensemaking as it is used here refers to "a set of philosophical assumptions, substantive propositions, methodological framings, and methods." As Mark Stefik notes (referring to work done with colleagues Stuart Card and Peter Pirolli), it "is how we gain a necessary understanding of relevant parts of our world. Everyone does it." Sensemaking goes beyond analysis, a disaggregative process, and also beyond synthesis, which meaningfully integrates factors relevant to an issue. It includes an interpretation of the results of that analysis and synthesis. It is sometimes referred to as an approach to creating situational awareness "in situations of uncertainty." Gary Klein, Brian Moon, and Robert Hoffman consider the elements of sensemaking and conclude that it "is a motivated, continuous effort to understand connections (which can be among people, places, and events) in order to anticipate their trajectories and act effectively."

These authors conclude that "the phenomena of sensemaking remain ripe for further empirical investigation and [warn] that the common view of sensemaking might suffer from the tendency toward reductive explanation." By reductive explanation Klein, Moon, and Hoffman refer to a tendency to overly simplify explanations—to "reduce" complex phenomena to simplistic models facilitating an apparently needed but shallow understanding.

Sources: Brenda Dervin, "Sense-Making Methodology Site", URL: <http://communication.sbs.ohio-state.edu/sense-making/>, accessed 12 September 2007; Mark Stefik, "The New Sensemakers: The Next Thing Beyond Search Is Sensemaking," *Innovation Pipeline* (15 October 2004), URL: <http://www.parc.com/research/publications/files/5367.pdf>, accessed 11 March 2009; Dennis K. Leedom, *Final Report: Sensemaking Symposium*, 23-25 October 2001, Command and Control Research Program Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence. Gary Klein, Brian Moon, and Robert R. Hoffman, "Making Sense of Sensemaking 1: Alternative Perspectives," *IEEE Intelligent Systems* vol. 21, no. 4 (July/August 2006), 71, 72. Cited hereafter as Klein, Moon, and Hoffman, "Making Sense of Sensemaking 1." Paul J. Feltovich, Robert R. Hoffman, Axel Roesler, and David Woods, "Keeping It Too Simple: How the Reductive Tendency Affects Cognitive Engineering," *IEEE Intelligent Systems* vol. 19, no. 3 (May/June 2004).

Intelligence sensemaking encompasses the processes by which specialized knowledge about ambiguous, complex, and uncertain issues is created. This knowledge is generated by professionals who in this context become known as Intelligence Sensemakers.

These terms are used as defined here throughout this book.

Sensemaking: A Structure for an Intelligence Revolution[55]

David T. Moore

Knowledge welcomes challenges.

— Peter Kosso

Venture boldly into nonsense. Nonsense is nonsense only when we have not yet found that point of view from which it makes sense.

— Gary Zukav

CHAPTER 1
Introduction

Where We Are

How people notice and make sense of phenomena are core issues in assessing intelligence successes and failures. Members of the U.S. Intelligence Community (IC) became adept at responding to certain sets of phenomena and "analyzing" their significance (not always correctly) during the Cold War. The paradigm was one of "hard, formalized and centralized processes, involving planned searches, scrupulously sticking with a cycle of gathering, analyzing, estimating and disseminating supposed enriched information."[56] The paradigm did not stop within the IC, either. As Pierre Baumard notes, it was also imported, unchanged, by corporations.[57] However, the range

55 The opinions expressed are those of the author and do not represent those of the National Security Agency, the Department of Defense, or the Office of the Director of National Intelligence.

56 Philippe Baumard, "From Noticing to Making Sense: Using Intelligence to Develop Strategy," *International Journal of Intelligence and CounterIntelligence*, vol. 7, no. 1 (Spring, 1994), 30. Cited hereafter as Baumard, "From Noticing to Making Sense."

57 Baumard, "From Noticing to Making Sense," 30.

of phenomena noticed by intelligence professionals has broadened from a focus on largely static issues to encompass highly dynamic topics over the two decades since the end of the Cold War. Intelligence professionals are challenged to stay abreast. A growing professional literature by intelligence practitioners discusses these trends and their implications for advising and warning policymakers.[58]

The literature by practitioners embodies a trust that national intelligence producers can overcome the "inherent" enemies of intelligence to prevent strategic intelligence failure.[59] The disparity between this approach and accepting the inevitability of intelligence failure has grown sharp enough to warrant the identification of separate camps or schools of "skeptics" and "meliorists."[60] As a leading skeptic, Richard Betts charitably plants the hopeful note that in ambiguous situations, "the intelligence officer may perform most usefully by not offering the answer sought by authorities but by forcing questions on them, acting as a Socratic agnostic."[61] However, he completes this thought by declaring, fatalistically, that most leaders will neither appreciate nor accept this approach.

Robert Jervis resurrects a colorful quote from former President Lyndon Johnson, who epitomized the skeptical policymaker:

> Let me tell you about these intelligence guys. When I was growing up in Texas we had a cow named Bessie. I'd go out early and milk her. I'd get her in the stanchion, seat myself and squeeze out a pail of fresh milk. One day I'd worked hard and gotten a full pail of milk, but I wasn't paying attention, and old Bessie swung her s[..]t-smeared tail through the bucket of milk. Now, you know

---

58 The author previously explored this topic in David T. Moore, *Creating Intelligence: Evidence and Inference in the Analysis Process*, MSSI Thesis chaired by Francis J. Hughes (Washington, DC: Joint Military Intelligence College, July 2002) and David T. Moore, *Critical Thinking and Intelligence Analysis*, Occasional Paper Number Fourteen (Washington, DC: National Defense Intelligence College, 2006). Earlier work completed with coauthor Lisa Krizan also included such an examination. See, for example David T. Moore and Lisa Krizan, "Core Competencies for Intelligence Analysis at the National Security Agency," in Russell G. Swenson, ed., *Bringing Intelligence About: Practitioners Reflect on Best Practices* (Washington, DC: Joint Intelligence Military College, 2003), 95-132. Other recent work includes the writings of a number of Intelligence Community practitioners collected by Roger Z. George and James B. Bruce in *Analyzing Intelligence: Origins, Obstacles, and Innovations* (Washington, DC: Georgetown University Press, 2008).

59 Richard K. Betts, *Enemies of Intelligence: Knowledge and Power in American National Security* (New York: Columbia University Press, 2007). Cited hereafter as Betts, *Enemies of Intelligence*.

60 Tamas Meszerics and Levente Littvay, "Pseudo-Wisdom and Intelligence Failures, *International Journal of Intelligence and Counterintelligence* vol. 23, no. 1 (December 2009), 134, 135.

61 Betts, *Enemies of Intelligence*, 51.

> that's what these intelligence guys do. You work hard and get a good program or policy going, and they swing a s[..]t-smeared tail through it.[62]

Jervis asserts that policymakers and decisionmakers "need confidence and political support, and honest intelligence unfortunately often diminishes rather than increases these goods by pointing to ambiguities, uncertainties, and the costs and risks of policies."[63] The antagonism is exacerbated when policy is revealed to be flawed and to have ignored intelligence knowledge. For example, in the case of the Bush administration's handling of the Iraq War, intelligence challenges to policy were seen as "being disloyal and furthering its own agenda."[64] Jervis adds that the Bush administration is only the most recent one to exhibit such behavior. He finds that the administrations of Presidents Clinton, Johnson, Kennedy, and Eisenhower also browbeat and ignored intelligence.[65]

Betts, Jervis, and other *skeptics* believe that potential improvements to intelligence processes are limited. Jervis' article on intelligence and policy relations, while it correctly notes the tensions arising from the differing roles of intelligence and policy, over-generalizes the homogeneity of the policy community. It is the author's experience that outside of the highest levels, there are many levels of policymaking that both encourage and welcome the contributions of intelligence. Indeed, some parts of the policy community, beyond the Department of Defense (DoD) where it is the norm to do so, rely strongly on intelligence. Further, disagreements (which Jervis consistently labels conflict) are inherent and typically welcome in the process. Hard questions about the accuracy of judgments must be asked. If we are doomed to such "disagreements," then it is a doom we should be eager to embrace.[66]

The other perspective is that of the *meliorists*—those who feel intelligence processes can be improved. The present authors reside in this camp, preferring to believe that the application of well-informed, mindful expertise, as developed in the present work, can bring positive and substantive value to the fulfillment of the IC's obligations.

---

62 President Lyndon Johnson quoted by Robert Jervis, "Why Intelligence and Policymakers Clash," *Political Science Quarterly*, vol. 125, no. 2 (Summer 2010), 185. Cited hereafter as Jervis, "Why Intelligence and Policymakers Clash."

63 Jervis, "Why Intelligence and Policymakers Clash," 187.

64 Jervis, "Why Intelligence and Policymakers Clash," 190.

65 Jervis, "Why Intelligence and Policymakers Clash," 190.

66 Jervis, "Why Intelligence and Policymakers Clash," 204.

Much of the community and its supporting contractors have adopted the meliorist position.[67] As a result, intense attention within and outside the IC has focused on the means by which pertinent phenomena are to be understood. So-called intelligence "analytic" methods are being unshelved or developed and taught to novice and experienced intelligence professionals alike. However, less fully considered are the appropriateness and validity of these methods as well as the underlying assumptions they enshrine. Even less well understood is what happens when specific methods are combined and how those combinations may be made. Several ways exist to characterize these methods in terms of their purpose. However, to date, there is no readily available way to characterize methodological appropriateness or effectiveness, nor the limitations of individual methods. We also lack sound guidance on the use of combined methodologies, despite some recent, promising literature.[68]

A Roadmap

Before these deficiencies can be remedied, however, we need to reframe the way in which intelligence is created. Such a re-conceptualization involves critically examining what intelligence practitioners actually do, and why. The examination demands methodological rigor with particular attention to how we might ensure the validity of our approach to the work of intelligence. If the examination indicates that the existing paradigm for intelligence creation is inadequate, then a revolutionary shift in IC habits will be justified.

Despite the existence of legislative mandates for change, the intelligence-creation process remains largely a product of Cold War-era institutions

---

67 It should be observed that it is in the interest of IC contractors to adopt this position. As they lobby IC leadership, their sales pitch rests on the idea that their products are best suited for "fixing" the IC's problems. A contractor who is (honestly) skeptical of the possibility that intelligence can be improved is thus likely to see little IC business.

68 The human species likes to organize knowledge and intelligence professionals are no exception. The list of proposed organizational strategies or taxonomies for intelligence analysis is growing: Morgan Jones developed one such system fifteen years ago in conjunction with his book, *The Thinker's Toolkit: 14 Powerful Methods for Problem Solving* (New York, NY: Random House, Inc., 1995). Babette Bensoussan and Craig Fleisher include taxonomic elements in their catalog of competitive intelligence methods. See for instance, Craig S. Fleisher and Babette Bensoussan, *Strategic and Competitive Analysis: Methods and Techniques for Analyzing Business Competition* (Upper Saddle River, NJ: Prentice Hall, 2002) and *Business and Competitive Analysis: Effective Application of New and Classic Methods* (Upper Saddle River, NJ: FT Press, 2007). The faculty of Mercyhurst College's Institute for Intelligence Studies has issued a taxonomy of methods. Richards Heuer, Jr. developed one on a subcontract to support work performed by Least Squares Software under a contract to IARPA. Another former IC practitioner, Randy Pherson, developed a taxonomy for use in his training programs and subsequently combined his taxonomy with that of Heuer. See Richards J. Heuer, Jr. and Randolph H. Pherson, *Structured Analytic Techniques for Intelligence* (Washington, DC: CQ Press, 2010). To date, none of the taxonomies use cases nor do they ontologize the techniques, that is, show how they are interrelated in process.

and thinking, using the same cognitive frameworks that have been employed for decades. Some argue that what worked in the past is still appropriate. However, as numerous executive and legislative reports confirm, intelligence targets have in fact evolved: adversaries' goals have changed, and their methods have evolved, even if the threats they pose seem very familiar. In sum, the old national intelligence paradigm is woefully out of date.

What is needed now is a discussion of how intelligence can be adjusted to deal with its "traditional" issues as well as new and evolving ones. This book begins that discussion by challenging the standard view of how intelligence professionals do their work. First, as will become clear, intelligence professionals ought *not* be characterized as "analysts." The term is imprecise and inaccurate. If real improvement in intelligence practice is to occur, precision and accuracy in terminology, and thereby in how we think about what we do, are essential first steps.

Intelligence issues are not the same as the issues framed separately by policymakers. To partner successfully with policymakers, intelligence professionals must consider issues from multiple perspectives. This is the role of sensemaking. Yes, the sensemaking process includes "analysis" or attacking issues by "taking them apart." The process also includes synthesis—putting the pieces back together; interpretation—making sense of what the evidence means; and communication—sharing the findings with interested consumers. Essential to these processes is another, that of sound planning or "design."[69] While it could be said that this is what intelligence analysts do, such a statement is epistemologically false. Strictly speaking, intelligence analysts only take issues apart.

So what? Why should we be concerned with a matter of semantics? In short, because the terms we use within the Intelligence Community shape and reflect our practice. If we are to change the culture of intelligence, and be changed by it, our practice of intelligence must also change. New language encourages a new paradigm, and paradigm shifts are revolutionary, not evolutionary. Such a revolution in intelligence is implied in the reform legislation arising out of the 9/11 attacks and the failures to accurately assess the state of Saddam Hussein's programs of weapons of mass destruction.

---

69 Here, the term "design" mirrors the reflective re-conceptualization of the operational planning process being put in place, as noted earlier, by the School of Advanced Military Studies at Fort Leavenworth.

Kent's Imperative[70]

When much of the tradecraft of intelligence was put in place sixty or more years ago, the dominant framework was that of the historian as scientist. The primary intellectual framework for Cold War intelligence at the national level grew from Sherman Kent's seminal work, *Strategic Intelligence for American World Policy*.[71] Kent's legacy remains active in the National Intelligence Council and the Community at large.[72] Although decision theory and other social science thinking began to influence the creation of intelligence in the 1960s and 1970s, these inputs languished until the reform efforts of recent years. More recently, advances in cognitive science, anthropology, decision theory, knowledge theory, and methods and operations research have brought us to the brink of informed, mindful intelligence sensemaking.

Sherman Kent argues that in creating predictive intelligence about its adversaries "the United States should know two things. These are: (1)…*strategic stature*, (2)…*specific vulnerabilities*."[73] These objectives focus on capabilities and draw heavily from the "descriptive and reportorial elements" of intelligence for basic data.[74] In this way, knowledge about what an adversary ought to do is created. The method by which this is accomplished, according to Kent, is "the one which students reared in the Western tradition have found to be best adapted to the search for truth. It is the classical method of the natural sciences."[75] It involves advice from experts but sees as superfluous to these experts the use of designated red teams—which Kent considers "a new high in human fatuity."[76] If estimates developed from expert judgments are erroneous, he sees the remedy simply in getting more and better information to shed more light on foreign decisionmaking.[77]

---

70 This phrase was originally adopted by an anonymous blogger as the name for a web log of musings on intelligence that ran from 1 January 2006 to 15 October 2008. URL: <http://kentsimperative.blogspot.com>, accessed 6 October, 2010.

71 Kent, *Strategic Intelligence*.

72 Anthony Olcott, "Revisiting the Legacy: Sherman Kent, Willmoore Kendall, and George Pettee—Strategic Intelligence in the Digital Age, *Studies in Intelligence*, vol. 53, no. 2 (June 2009): 21-32.

73 Kent, *Strategic Intelligence*, 40.

74 Kent, *Strategic Intelligence*, 56.

75 Sherman Kent, "Cuban Missile Crisis: A Crucial Estimate Relived," *Studies in Intelligence*, vol. 8, no. 2 (1964), reprint, URL: <https://www.cia.gov/library/center-for-the-study-of-intelligence/kent-csi/vol8no2/pdf/v08i2a01p.pdf>, accessed 27 May 2010, 113. Cited hereafter as Kent, "Crucial Estimate."

76 Kent, "Crucial Estimate," 118.

77 Kent, "Crucial Estimate," 119.

The Failure of an Analytic Paradigm…

Kent's preference for gathering and disaggregating more and more data to find answers fails today in the face of information volume, velocity, and volatility. Marshaling and disaggregating ever more data does not equate to contextual understanding. Further, the assumption that larger pipes to collect data and larger arrays to store it will then allow us to uncover the hidden, clarifying nuggets, is misleading.

Consider what actually happens when intelligence professionals look for an answer to a problem or question. They do not just disaggregate data. Instead, people inquisitively (and selectively) interpret patterns by comparing observed, newly emergent phenomena to what they already "understand." They make sense of phenomena by asking questions; foraging for information; marshaling it into evidence; analyzing, synthesizing, and interpreting that evidence, and communicating their evidence-based understanding of issues to others. Something makes sense because, based on their experience, its pattern is similar to something they previously have seen and that made sense to them. They may even employ a new, self-generated pattern based on previously learned and remembered patterns if they do not get a good match to an ostensible pattern.[78]

Doing so accurately requires making judgments that correlate, according to Air Force thinker William Brei, to the "external world, as it actually exists, regardless of [one's] desires."[79] In other words, one must be able to convincingly correlate ostensible patterns to the data or information for which one is attempting to "make sense." This is not always possible, especially if the phenomenon or issue is broad, novel, or poorly understood; that is, not easily subject to confirmation by universal human sensory apparatii. Brei invokes Ayn Rand on this point:

> To define the meaning of the color "blue," for instance, one must point to some blue objects to signify, in effect: "I mean this."…To define "existence," one would have to sweep one's arms around and say: "I mean this."[80]

---

78 Dr. David Snowden, conversation with the author, 22 January 2008. Snowden, formerly director of IBM's Institute for Knowledge Management, writes and teaches on complexity and how organizations can leverage it to their advantage. Cited hereafter as Snowden, conversation.

79 Capt William S. Brei, USAF, *Getting intelligence Right: The Power of Logical Procedure,* Occasional Paper Number Two (Washington, DC: Joint Military Intelligence College, 1996), 17. Cited hereafter as Brei, *Logical Procedure.*

80 Ayn Rand, *Introduction to Objectivist Epistemology* (New York, NY: Mentor, 1979), 53. Referenced in Brei, *Logical Procedure*, 18.

The social, economic and political relationships that characterize the government intelligence milieu mean that severe uncertainty will often remain part of the practitioner's conclusions; telling patterns are at best elusive.

…And a Remedy in Sensemaking

For practitioners to create intelligence knowledge—even with an acknowledged degree of uncertainty—therefore requires much more than mere "analysis." One alternative framework is embodied in the concept of sensemaking. Sensemaking begins with a mindful planning and questioning that leads to foraging for answers. It is true that along the way the resulting relevant assemblage of information—or evidence—is disaggregated into its constituent elements. However, it is also synthesized or combined to form a theory or systematic interpretation of the issue that subsequently must be explained, and convincingly. Throughout sensemaking, a continuous assessment is demanded of both the processes by which the intelligence is created and of the intelligence knowledge itself.[81] Mindfulness—as discussed above in the Preface—coupled with a critical thinking-based approach, provide the vigilance, awareness, and self-reflection needed to assess an issue rigorously. This is a central point: Intelligence does not exist in a vacuum. It must contribute to the understanding of an issue by informing the concerned parties of a perspective or information they did not already know. Ultimately, if no one is concerned about the knowledge sensemakers create, it is not intelligence.[82]

Karl Weick sees sensemaking as a multiple-step process by which someone goes from becoming aware of "something, in an ongoing flow of events, something in the form of a surprise, a discrepant set of cues, [or] something that does not fit," to a useful understanding of the phenomenon.[83] This definition, which allows for a focus on the social and political environments in which sensemaking takes place, applies to the concept as developed in the present book.

---

81 For a further discussion of assessing both the process and product of intelligence, see David T. Moore and Lisa Krizan, "Core Competencies for Intelligence Analysis at the National Security Agency," in *Bringing Intelligence About: Practitioners Reflect on Best Practices*, Russell Swenson, ed. (2004), 95-131; and David T. Moore, Lisa Krizan, and Elizabeth J. Moore, "Evaluating Intelligence: A Competency-Based Approach," in the *International Journal of Intelligence and CounterIntelligence*, vol. 18, no. 2 (Summer 2005): 204-220. Cited hereafter as Moore, Krizan, Moore, "Evaluating."

82 See Lois Foreman-Wernet, "Rethinking Communication: Introducing the Sense-Making Methodology," in Brenda Dervin, Lois Foreman-Wernet, and Eric Lauterbach, *Sense-Making Methodology Reader: Selected Writings of Brenda Dervin* (Cresskill, NJ: Hampton Press, Inc., 2003), 1-10. The authors consider communicating an essential part of sensemaking.

83 Karl E. Weick, *Sensemaking in Organizations* (Thousand Oaks, CA: Sage Publications, Inc., 1995), 2. Cited hereafter as Weick, *Sensemaking*.

Building on Weick's definition and work he did with Kathleen Sutcliffe, Warren Fishbein and Gregory Treverton observe that sensemaking is about anticipating uncertainty as opposed to reacting to it.[84] This means that the processes of sensemaking, and particularly collaborative sensemaking, are never satisfied with the status quo. Rather, sensemaking institutions constantly admit and raise doubts about what they believe. Because threats—as typified by many 21st century issues—can emerge "at any time, anywhere, and in a variety of forms, analysts need to think more in terms of a broad mental readiness to perceive early warning signs."[85]

IARPA, the Intelligence Advanced Research Projects Activity, employs a definition of sensemaking that is complementary to that developed here.[86] They propose that sensemaking is "a core human cognitive ability [that] underlies intelligence analysts' ability to recognize and explain relationships among sparse and ambiguous data."[87] This book accepts that perspective and develops the psychological, behavioral, and social levels of sensemaking as they apply to intelligence creation. By contrast, IARPA's own program on sensemaking seeks to build upon advances in computational cognitive neuroscience that reveal "the underlying neuro-cognitive mechanisms of sensemaking."[88]

As characterized by Peter Pirolli, the process of sensemaking is highly iterative, involving a foraging loop and a sensemaking loop.[89] In the former the sensemaker seeks information, "searching and filtering it," while in the

---

84 Fishbein and Treverton, "Making Sense," 17. See also, Karl E. Weick and Kathleen M. Sutcliffe, *Managing the Unexpected: Assuring High Performance in an Age of Complexity* (San Francisco, CA: Jossey-Bass, 2001).

85 Fishbein and Treverton, "Making Sense," 18.

86 See IARPA Broad-Agency Announcement IARPA-BAA-10-04, *Integrated Cognitive-Neuroscience Architectures for Understanding Sensemaking* (ICArUS) Program, 1 April 2010. URL: <http://www.iarpa.gov/solicitations_icarus.html>, accessed 1 June 2010. Cited hereafter as IARPA, BAA-10-04.

87 IARPA, BAA-10-04, 4.

88 IARPA, BAA-10-04, 4. On the emerging discipline of cognitive neuroscience, see The 4th Computational Cognitive Neuroscience Conference, URL: <http://ccnconference.org/>, accessed 7 June 2010.

89 Peter Pirolli and Stuart Card, "The Sensemaking Process and Leverage Points for Analyst Technology as Identified Through Cognitive Task Analysis," *2005 International Conference on Intelligence Analysis*, McLean, VA, 2-6 May, 2005, URL: <https://analysis.mitre.org/proceedings/Final_Papers_Files/206_Camera_Ready_Paper.pdf>, accessed 18 August 2010. Cited hereafter as Pirolli and Card, "Sensemaking." Pirolli and Card's work here builds on earlier work. See particularly Peter Pirolli and Stuart Card, "Information Foraging," *Psychological Review*, vol. 106, no. 4 (October 1999): 643-675; and Dennis M. Russell, Mark J. Stefik, Peter Pirolli, and Stuart Card, "The Cost Structure of Sensemaking," paper presented at the INTERCHI '93 Conference on Human Factors in Computing Systems, Amsterdam, NL, 24-25 April 1993, URL: <http://www2.parc.com/istl/groups/uir/publications/items/UIR-1993-10-Russell.pdf>, accessed 18 August 2010.

latter an iteratively developed mental model or schema is developed "that best fits the evidence."[90] While the overall flow is "from raw information to reportable results," top-down and bottom-up processes act in concert to reframe issues: information either does or does not fit the hypotheses being considered; hypotheses are refuted or refined, and the larger issue and its context are also reframed, as it comes to be more thoroughly understood.[91] How this can occur within the context of intelligence creation is developed in the following chapters.

To sum up, this book argues that intelligence built around a model of disaggregation as it originated with and developed under Kent, and is still largely practiced today, is at best insufficient. A paradigm based on the concept of sensemaking and employing insights from other knowledge-creation disciplines provides a more appropriate means of skillfully creating intelligence. This book draws a general picture of 21st Century intelligence under a revolutionary paradigm, although it does not explain how all its contours can be fleshed out. We believe that intelligence could be a true profession and moving toward that goal is our desire.[92]

90 Pirolli and Card, "Sensemaking," 3.

91 Pirolli and Card, "Sensemaking," 3.

92 In 1960, the Office of Personnel Management (OPM) defined the role of an "intelligence research specialist" as administrative work, not professional work. As it stands, professionals with "state of the discipline knowledge" are by definition excluded from intelligence work. See United States Office of Personnel Management, Workforce Compensation and Performance Service, *Introduction to the Position Classification Standards*, TS-107 August 1991, URL: <http://www.opm.gov/fedclass/gshbkocc.pdf>, accessed 11 December 2009; and United States Office of Personnel Management, *Position Classification Standard for Intelligence Series*, GS-0132 TS-28 June 1960, TS-27 April 1960, URL: <http://www.opm.gov/fedclass/html/gsseries.asp>, last accessed 11 December 2009.

CHAPTER 2
The Failure of "Normal Intelligence"

Intelligence Challenges

Our understanding of everyday phenomena is confounded by everyday strategies employed to mitigate cognitive dissonance, a stressful condition arising when reality clashes with one's perceptions. Two broad strategies, selective exposure and selective perception, can prevent dissonance, but at the expense of sound, mindful reasoning. Through the former, we limit the evidence to that which agrees with or otherwise supports our positions; in the latter, we interpret what we experience in terms of our pre-existing world-view.[93] Examples abound, for these strategies are inherent to the human species. A non-intelligence example appeared in a 2008 broadcast of National Public Radio's *This American Life*, in the story "What Part of 'Bomb' Don't You Understand?" In the broadcast, BBC commentator Jon Ronson juxtaposes the stories of London subway bomb survivor Rachel North and conspiracy theorists who claimed the entire event was fabricated by the British government. The conspiracy theorists even claimed that Rachel North was not an actual person despite her well-documented reality.[94]

Instructive accounts of 9/11 conspiracies and others appear in Farhad Manjoo's *True Enough: Learning to Live in a Post-Fact Society*. One example, related to 9/11, is a belief by some that the second plane that struck the World Trade Center first launched a missile into the building.[95] In both of the above cases, the conspiracy theorists only selected evidence consistent with their conspiracy world-views. What of the situation within intelligence sense-making circles? If the phenomena of both selective exposure and selective

93 For a highly readable discussion of cognitive dissonance, see Carol Tavris and Elliot Aronson, *Mistakes Were Made (But Not by Me): Why We Justify Foolish Beliefs, Bad Decisions, and Hurtful Acts* (Orlando, FL: Harcourt, 2007). For more on selective exposure and selective perception see Farhad Manjoo, *True Enough: Learning to Live in a Post-Fact Society* (Hoboken, NJ: John Wiley & Sons, 2008), especially Chapters 2 and 3. Cited hereafter as Manjoo, *True Enough*.

94 Jon Ronson, "What Part of 'Bomb' Don't You Understand?" *This American Life*, episode 338, 3 August 2008, URL: <http://www.thislife.org/Radio_Episode.aspx?episode=338>, accessed 4 August 2008.

95 Manjoo, *True Enough*, 74-80. Its proponents do not adequately explain the logic of such a claim. One key question is "What purpose would such a missile serve?" The proponents of this notion fail to answer this and a number of other important questions.

perception are common, then their effects on intelligence professionals deserve fuller study. It is not understood, for example, how much selective use of evidence typically occurs in the creation of intelligence assessments and estimates.

However, intelligence professionals cannot afford to consider only information that conforms to their own pre-existing worldview or agreed-upon, collective perspective. It is likely that selective exposure and selective perception contributed to the "failures of imagination" noted by the authors of the 9/11 Commission Report: U.S. intelligence professionals and policymakers in two U.S. administrations failed to make sense of the events leading up to the 11 September 2001 disaster.[96] Failure of imagination was so pervasive a factor that the 9/11 Commission Report found that even those who were oriented toward the threat, such as Richard Clarke, failed to adequately imagine the events of that tragic day.[97]

Errors and Failures

A first step in understanding the lack of sensemaking prior to the 11 September 2001 attacks and other similar events is to understand the differences between "intelligence error" and "intelligence failure." Anthropologist Rob Johnston defines intelligence error in terms of "factual inaccuracies in analysis resulting from poor or missing data."[98] Conversely, intelligence failures are "systemic organizational surprise resulting from incorrect, missing, discarded, or inadequate hypotheses."[99] Thus, the term "failure of imagination" makes sense as a synonym for intelligence failure, where members of an intelligence creating organization fail to imagine in advance the essential outlines of an incident that subsequently occurs.

Additionally, one must consider policy failures. Characterized simply, this failure is seen as the failure to act on intelligence received, and it occurs at many levels. Bruce Berkowitz argues that these errors arise when policymakers "blindside themselves by how they perceive intelligence, by

---

96 National Commission on Terrorist Attacks Upon the United States, *The 9/11 Commission Report* (Washington, DC: Government Printing Office, 2004), 339-360. Cited hereafter as *The 9/11 Report*.

97 *The 9/11 Report*, 344. Richard Clarke's memo to Condoleezza Rice warning of the aftermath of such an attack understates the consequences. Clarke considers hundreds dead, not thousands. See Dan Eggen and Walter Pincus, "Ex-Aide Recounts Terror Warnings: Clarke Says Bush Didn't Consider Al Qaeda Threat a Priority Before 9/11," *The Washington Post*, 25 March 2004, A01.

98 Rob Johnston, *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study* (Washington, DC: Center for the Study of Intelligence, 2005), 6. Cited hereafter as Johnston, *Analytic Culture*.

99 Johnston, *Analytic Culture*, 6.

the mental hurdles intelligence must surmount before it can change their perceptions, and in the constraints that limit their ability to act on information…deep down, officials seem to want intelligence to make decisions for them, when in reality, it rarely can."[100] Thus Admiral Husband Kimmel's failure to anticipate the Japanese attack on Pearl Harbor can be attributed (in part) to an inability to overcome a preexisting view about the (in)vulnerability of U.S. forces in Hawaii and particularly at the Pacific Fleet headquarters of which he was in charge.[101] This was exacerbated presumably by a degree of uncertainty in the intelligence. In order to take preventative measures, Kimmel had to *act* based on intelligence reporting, not *react* to it. In considering intelligence-based policy failures, one must consider that despite these explanations, it is the job of intelligence to make sure policy "gets it" and therefore intelligence (or at least its presenters) must also share in the blame. Thus the briefer of a senior policymaker bears a degree of responsibility if the message is not effectively transmitted and acted upon. That this is a difficult task at best must be noted. Policymakers—as is widely noted—often have their own agendas. Would they use intelligence to further them? Fen Osler Hampson argues this was the case in (at least) three separate crises involving Cuba (1962, 1973, and 1979).[102]

Intelligence failures, policy failures and their resulting crises are a regularly recurring theme in U.S. intelligence and policy from at least the mid-20th Century, and likely earlier, to the present. A list of such failures includes:

- Japan's attack on Pearl Harbor (intelligence failure, policy failure).[103]

---

100 Bruce Berkowitz, "U.S. Intelligence Estimates of Soviet Collapse: Reality and Perception," in Francis Fukuyama, ed., *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics* (Washington, DC: Brookings Institution Press, 2007), 30. Cited hereafter as Berkowitz, "Soviet Collapse."

101 See Francis Fukuyama, "The Challenges of Uncertainty: An Introduction," in Francis Fukuyama, ed., *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics* (Washington, DC: Brookings Institution Press, 2007), 1.

102 Fen Osler Hampson, "The Divided Decision-Maker: American Domestic Politics and the Cuban Crises," *International Security*, vol. 9, no. 3 (Winter, 1984-1985), 130. Cited hereafter as Hampson, "The Divided Decision-Maker." The ODNI issued *Intelligence Community Directive Number 203: Analytic Standards* (June 21, 2007), URL: <http://www.fas.org/irp/dni/icd/icd-203.pdf>, accessed 16 October 2010. The second standard is "Independent of Political Considerations" (p. 2).

103 This failure consisted of intelligence policy and errors, as well as intelligence and policy failures. However, hindsight consideration of the events clouds the fact that it was not clear until just before the Japanese attack that an attack was indeed likely. That it was a possibility was, however, discussed. At Pearl Harbor, however, no measures were taken to mitigate the impact of such an attack: Aircraft remained tightly packed on landing areas and ships lacked torpedo nets. The result was strategic surprise at all levels. The best account remains Roberta Wohlstetter, *Pearl Harbor: Warning and Decision* (Stanford, CA: Stanford University Press, 1962).

- North Korea's invasion of the South and China's involvement in the subsequent war (policy failure, intelligence failure);[104]
- The Soviet Union's deployment of IRBM and MRBM nuclear missiles in Cuba (intelligence failure);[105]
- The Vietnamese' Tet Offensive (policy failure, intelligence error);[106]
- The fall of the Shah of Iran (intelligence failure);[107]
- The Soviet Union's invasion of Afghanistan (intelligence failure);[108]

---

104 There is controversy as to whether the invasion of South Korea by North Korea was predicted in advance. Common wisdom considers that no prediction was made. However, Major General Charles A. Willoughby's Korean Liaison Office (KLO) did predict the likelihood of invasion in the spring of 1950 (Kenneth J. Campbell, "Major General Charles A. Willoughby: A Mixed Performance," unpublished paper, URL: <http://intellit.muskingum.edu/wwii_folder/wwiifepac_folder/wwiifepacwilloughby.html>, accessed 5 January 2010). However, according to D. Clayton James, Willoughby had so alienated himself from the CIA and the State Department's intelligence bureau that his warnings apparently were ignored by the civilian intelligence components. The Army's G-2 apparently ignored his warning as well, possibly because the United States Military Advisory Group to the Republic of Korea, and not the KLO, was tasked with such estimating. See also, D. Clayton James, *Years of MacArthur, 1945-1964* (Boston, MA: Houghton Mifflin, 1985), 416. The fact that warnings were issued but ignored adds the policy failure component.

105 DCI John McCone was at first skeptical and then was convinced that there were missiles in Cuba. Refugee reports during the summer of 1962 suggested that the missiles were based in Cuba. However, the Office of National Estimates under the leadership of Sherman Kent predicted the Soviets would not deploy missiles in Cuba. U-2 overflights did not detect the presence of the missiles until mid October, although they had earlier detected the presence of defensive Surface to Air Missiles. Lacking confirmatory technical corroboration, the State Department and the White House were not willing to act based on refugee reports (which had been received since 1960 and up to this point apparently had been incorrect). See Linda K. Miller and Mary McAuliffe, "The Cuban Missile Crisis," *Magazine of History*, vol.8 (Winter 1994), URL: <http://www.oah.org/pubs/magazine/coldwar/miller.html>, accessed 5 January 2010.

106 According to Harold Ford, despite analyses to the contrary, wishful thinking by key policymakers and their political pressure on the Intelligence Community to concur led to an underestimation of the Viet Cong and North Vietnam's military capabilities. Such a view precluded the possibility of a Tet-like offensive. Thus systemic surprise from a policy failure is associated with the Tet Offensive. See Harold Ford, *CIA and Vietnam Policymakers: Three Episodes 1962-1968* (Washington, DC: Center for the Study of Intelligence, 1998), 85-138.

107 In writing about failure, Bruce Berkowitz quotes the CIA August 1978 assessment that "Iran is not in a revolutionary or even pre-revolutionary state." See Bruce Berkowitz, "U.S. Intelligence Estimates of Soviet Collapse: Reality and Perception," in Francis Fukuyama, ed., *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics* (Washington, DC: Brookings Institution Press, 2007), XX. Cited hereafter as Berkowitz, "Soviet Collapse."

108 Doug MacEachin writes that the failure to predict the Soviet invasion of Afghanistan "illustrates probably the most recurrent trap for analysts...One part of it might be called the 'model cage.' Once having constructed an intellectual model of how the variables are likely to play out, each new piece of information is weighed in accordance with the components of that model. Evidence that does not fit is far more likely to be explained away than used to question the model's validity. In this case, the actions taken (military preparations) were not used to interpret intentions so much as the conclusions about intentions were used to interpret the actions." See Douglas MacEachin, *Predicting the Soviet Invasion of Afghanistan: the Intelligence Community's Record* (Washington, DC: Center for the Study of Intelligence, 2002), URL: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/predicting-the-soviet-invasion-of-afghanistan-the-intelligence-communitys-record/predicting-the-soviet-invasion-of-afghanistan-the-intelligence-communitys-record.html>, accessed 5 January 2010.

- The collapse of the Soviet Union (intelligence failure?, policy failure?);[109] and
- Iraq's 1990 invasion of Kuwait (intelligence failure, policy failure).[110]

Similarly, professionals apparently failed to make sense of the precursors of the 25 December 2009 attempt to bring down a U.S. airliner over Detroit. Here again, failures of imagination that accompanied the centrifugal disaggregation of data gathering and evaluation on the "underwear bomber" contributed to the scenario of not performing early cross-checking of no-fly lists and other terrorist-related databases, as well as not accepting the father of a motivated Islamic radical as a credible source.[111]

These intelligence errors and failures have occurred as the IC has continued in the Kent vein of seeking more and better data, but without framing the issues in a way that allows the national intelligence process to use its special capabilities to apply deductive or even abductive logic to foraging for, marshaling and evaluating data. At the same time, intelligence oversight reports by Congressional committees and Special Commissions

---

109 There is considerable disagreement about whether the Community failed to predict the collapse of the Soviet empire. For a summary of both sides of the issue with references, see Gerald K. Haines and Robert E. Leggett, ed., "Introduction and Overview of the Conference Papers" in *Watching The Bear: Essays on CIA's Analysis of the Soviet Union* (Washington, DC: Center for the Study of Intelligence, 2003), URL: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/watching-the-bear-essays-on-cias-analysis-of-the-soviet-union/index.html>, accessed 5 January 2010. In taking the position that the community *did* warn, Bruce Berkowitz argues the "record suggests that U.S. intelligence provided about as good a product as one could reasonably expect...[It] stipulated a set of conditions...and it notified top U.S. leaders when these conditions were met." If not an intelligence failure, then what? Berkowitz offers clues to this question in noting that leaders blindside themselves by failing to understand intelligence—in this case their failing to "get it" about the intelligence coming out of the IC leads one to conclude the failure was theirs—a policy failure. Additionally, he notes that popular belief in the failure, an example of selective perception, was also the result of key documents remaining classified, a sort of selective exposure. See Berkowitz, "Soviet Collapse," 29-30, xx.

110 Don Oberdorfer, writing in *The Washington Post*, notes that policymakers admitted to being "guilty of a kind of mind-set or framework about Iraq." They failed to consider that the Iraqis would go beyond saber rattling to invade Kuwait. Oberdorfer also quotes administration officials as admitting that they did not focus on Iraq because the "didn't have the time." See Don Oberdorfer, "Missed Signals in the Middle East, *The Washington Post Magazine*, 17 March 1991, 40.

111 The Senate Select Committee on Intelligence released its report on the "underwear bomber" incident on 18 May 2010 (see *http://intelligence.senate.gov/100518/1225report.pdf*). Of 14 points of failure identified, 12 were failures of intelligence process, including interpretation. Failures to correctly interpret source information are a part of the other failures cited above. For example, such failures also occurred in the case of the Cuban Missile crisis where (as we discovered some 40 years later) the refugees were telling us the truth: there were nuclear missiles in Cuba during the summer of 1962; they simply were not strategic missiles. Rather they were tactical, nuclear-tipped cruise missiles. See Raymond L. Garthoff, "US Intelligence in the Cuban Missile Crisis," in James G. Blight and David A. Welch, eds., *Intelligence and the Cuban Missile Crisis* (London, UK: Frank Cass, 1998), 29. Cited hereafter as Garthoff, "US Intelligence."

have repeatedly faulted the Community for its lack of imagination in anticipating at least the grand design of events that, instead, surprised or shocked nearly everyone associated with this Community. This unhappy situation suggests that there are flaws in Kent's model of disaggregating significant amounts of data in order to predict specific events. The etymology of "imagination"—generating images—reminds us of the contemporary critic of Kent, Willmoore Kendall, who suggested that the job of national intelligence is to communicate with decisionmakers in a "holistic" way so as to generate the "pictures [mental models] that they have in their heads of the world to which their decisions relate."[112]

Considering Standard Models

Intelligence failures occur as practitioners employ a "standard model"[113] of intelligence: In it, analysts "separate something into its constituent elements[114] so as to find out their nature, proportion, function, relationship, etc.[115] and "produce reports" based on "collected" information and data. There is a definitional presumption that disaggregation will lead to answers. However, this model *incompletely* describes what the intelligence professional does and its underlying presumption about finding answers may be false.

One problem is that in Kent's data-based analytic framework, analysts need to have all the data available so they can be marshaled into a coherent account. "Dots"—if they exist at all—can be connected in more than one way.[116] In foresight it is difficult at best to determine which combination and order is valid. Such determinations can be further complicated by the fact that adversaries may change their actions if they suspect we have arrived at a certain conclusion.

An additional problem is that with an increased number of signals there is also an increased level of noise. Which signals, which facts, or which inferences the intelligence professional should consider valid becomes a very important consideration. At best, warning of a pending incident is a problem of assembling and making sense of the details of a specific incident in advance. However, many intelligence problems inherently defy such linear

---

112 Willmoore Kendall, "The Function of Intelligence," *World Politics*, vol. 1, no. 4 (July 1949), 550. Cited hereafter as Kendall, "Function of Intelligence."

113 A standard model is one that is widely accepted to be justified and true. It is—in day-to-day considerations—sufficient and therefore its validity is not questioned.

114 *New Oxford American Dictionary*, Apple Computer Edition, entry under "analysis."

115 Webster's New Universal Unabridged Dictionary, 2nd ed. 1983, entry under "Analysis."

116 Robert Horn prefers to refer to dots as "smudges," suggesting that they are at best imprecise in both existential and contextual frameworks. Robert Horn, conversation with the author, 6 October 2010.

characterization. They are in fact "wicked" problems—a formal designation of a complex issue with myriad linkages. We turn next to an exploration of problem types to see how their nature directs our making sense of them.

Types of Problems

In order to understand "wicked problems," one must first understand the nature of "tame problems."

Tame Problems

In a tame problem there is general agreement as to what or who an adversary is, what the "battlefield area" is, and what an attack is. Such problems, while difficult, exhibit specific characteristics: They are clearly defined and it is obvious when they are solved. Solutions to these problems arise from a limited set of alternatives that can be tested; the correct solution can be objectively assessed. Finally, solving one tame problem can facilitate creating valid solutions to other, similar tame problems.[117]

It is important to note that analysis protocols for tame problems contain little or no room for "emergent" properties. One may not know that the analytic protocol is insufficient until the puzzle has been incorrectly defined, characterized, and solved, if it is in fact solvable. One arrives at one solution that at first appears to have resolved the issue, but in fact, the issue reemerges elsewhere. For example, the implementation of a linear, intelligence-driven solution to crack down on insurgents and their improvised explosive devices (IEDs) in one area may lead to an emergence of IED-caused explosions somewhere else. In such a case, the application of "tame problem protocols" may in fact have been inappropriate—the problem is in fact not tame.

Admittedly, many 21st Century intelligence issues remain puzzles or tame problems. This occurs when the events surrounding the issues have already occurred, appropriate questions are readily identifiable, and answers exist, even if they are difficult to find. For example, in a weapons proliferation puzzle, if we know that missiles have been built, the nature of their warheads and their accuracy "may remain unknown even though they are knowable."[118] Solution is a process of discovery and sensemaking.

Seen in this light, even the attacks on the United States by Al Qaeda on 11 September 2001 could be considered a puzzle or tame problem. Plans

---

117 Jeff Conklin, *Dialogue Mapping: Building Shared Understanding of Wicked Problems* (Hoboken, NJ: John Wiley and Sons, Ltd., 2005), 9.

118 Gregory F. Treverton, *Reshaping National Intelligence for An Age of Information* (Cambridge, UK: Cambridge University Press, 2001), 12. Cited hereafter as Treverton, *Reshaping National Intelligence*.

had been made, necessary skills (flying airplanes) learned, surveillance conducted, targets selected, weapons acquired, and terrorists positioned. The issue faced by intelligence professionals—and where we failed—was to sense and then figure out all (or at least enough) of the pieces before the events of that day occurred. We also had to figure out what the "event" was. The difficulty of doing so at both a theoretical and practical level points out how difficult tame problems can be to solve. As noted, in the end we failed, although some pieces of the puzzle—such as the flying skills necessary—at least had been sensed. In this case, the essence of the puzzle itself—the intention to deliberately fly passenger airplanes into structures in the U.S.—remained unidentified.

Wicked Problems

However, seen in a larger context, are such puzzles truly tame? Or are they components—as Russell Ackoff suggests—of something larger: a mystery in Treverton's terms, or a "mess" according to Ackoff.[119] Treverton's intelligence mysteries defy easy definition. They belong to a class of problems defined by social researchers Horst Rittel and Melvin Webber as "Wicked Problems." In describing this domain Rittel and Webber note that in considering wicked problems and systems there are a great many barriers to sensemaking:

> [Theory] is inadequate for decent forecasting; our intelligence is insufficient to our tasks; plurality of objectives held by pluralities of politics makes it impossible to pursue unitary aims; and so on. The difficulties attached to rationality are tenacious, and we have so far been unable to get untangled from their web. This is partly because the classical paradigm of science and engineering—the paradigm that has underlain modern professionalism—is not applicable to the problems of open societal systems.[120]

The adaptive nature of adversaries makes seemingly tame puzzles wicked, moving them into the realm of "unknown unknowables."

By definition, wicked problems are "incomplete, contradictory, and changing."[121] They do not have single answers and in fact, are never truly

---

119 Treverton, *Reshaping National Intelligence*, 11-13; Russell A. Ackoff, *Redesigning the Future: A Systems Approach to Societal Problems* (New York, NY: John Wiley and Sons, 1974), 11.

120 Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences*, vol. 4 (1973), 157. Cited hereafter as Horst and Webber, "Dilemmas." The term "men" refers to people.

121 Wikipedia, Entry under "Wicked Problem," accessed 28 March 2007. Cited hereafter as Wikipedia, "Wicked Problem."

answered. In the context of intelligence, the sensemaker may never realize a problem has been resolved. This is because "the solution of one of its aspects may reveal or create another, even more complex problem."[122] The emergent complexity of the problem itself, its adaptive nature, efforts at denial and deception by adversarial actors, as well as cognitive frailties on the part of sensemakers, compound the problem, confounding sensemaking, leading in some cases to disastrous courses of action or consequences.

Table 1. Characteristics of Wicked Problems
Wicked problems have no definite formulation.
Wicked problems have no clear end-point.
Solutions to wicked problems are at best good or bad.
Tests of solutions to wicked problems may not demonstrate their validity and may provoke undesired consequences.
Implementing solutions to wicked problems changes the problem.
Sensemakers can never know if they have determined all the solutions to wicked problems.
Each wicked problem is essentially unique.
Every wicked problem is embodied in another one.
How wicked problems are resolved is determined by the means and methods used to make sense of them.
Sensemakers have no right to be wrong.

Source: Derived from Horst W. J. Rittel and Melvin M. Webber, "Dilemmas in a General Theory of Planning," *Policy Sciences* 4 (1973), 155-169.

Rittel and Webber note that all wicked problems share at least 10 characteristics in common (summarized in table 1). Wicked problems so framed allow us to proceed with discussions into their nature. The two men argue, however, that our standard "basis for confronting problems of social policy is bound to fail, because of the nature of these problems." The means that we typically have at hand for cognitive handling of these problems "is not applicable."[123]

122 Wikipedia, "Wicked Problem."

123 Rittel and Webber, "Dilemmas," 162.

A Wicked Look at Wicked Problems in Intelligence

Characterizing intelligence issues in terms of their problem type—admittedly somewhat vaguely (in keeping with their nature)—reveals just how prevalent wicked problems are within the domains of intelligence.

Wicked problems have no definite formulation. To Rittel and Webber, "the process of solving the problem is identical with the process of understanding its nature, because there are no criteria for sufficient understanding."[124] In other words, making sense of problems deemed sufficiently complex so as to be considered wicked is equivalent to characterizing them in the first place; the description encompasses all possible solutions.

For example, one wicked problem could be "how best to stem the growth of terrorism in the Middle East." An assumption in considering this problem is that if intelligence professionals can understand what motivates people to become terrorists in the first place, intervention might be possible. Mitigating the creation of new terrorists could aid in reducing both their numbers and by extension, their attacks. Do people become terrorists because they are dissatisfied with what they see as contradictions and hypocrisies in their lives? If so, what then are the specific roots of dissatisfaction and contradiction? One commonly cited is a lack of economic opportunity for males within societies. In that light, Rittel and Webber ask, "where within the…system does the real problem lie? Is it deficiency of the national and regional economies, or is it deficiencies of cognitive and occupational skills within the labor force?"[125] The possible solutions to this problem extend the domain of questions, spreading ever outward.[126]

Our ignoring domains that seem irrelevant (either for practical or political reasons) is a strategy of selective exposure and perception. Admittedly, some domains may be inconsequential. On the other hand, one of the interesting features of complex systems is that small perturbations can produce large impacts. So, a decision to eliminate factors from consideration may result in discarding seemingly inconsequential elements, with as yet unknown but major impacts. Such possible impacts cannot be known in advance, as they are a part of the noise surrounding the issue. Indeed, as Nicholas Taleb notes,

> [Our] track record in predicting those events is dismal; yet by some mechanism called the hindsight bias we think that we understand

124 Rittel and Webber, "Dilemmas," 162.

125 Rittel and Webber, "Dilemmas," 161.

126 Such domains include (among others) economics, culture, history, geography, roles of language, religion, or law, singly or in combinations.

> them. We have a bad habit of finding "laws" in history (by fitting stories to events and detecting false patterns); we are drivers looking through the rear view mirror while convinced we are looking ahead.[127]

Seemingly unimportant factors also are not considered by sensemakers due to a failure to adequately address assumptions about the issue at hand, as noted in official reviews of recent "intelligence failures." For example, the Senate's report on the prewar assessment of weapons of mass destruction in Iraq specifically notes that analysts' assumptions were not challenged in the creation of the estimate.[128]

Even with the addressal of major assumptions, there remain additional underlying factors that do not get questioned—almost an endless succession of assumptions that must be peeled off the problem much as one peels layers off an onion. There is an added complication that individual layers are not sequential and in fact may lead (to continue the analogy) to other onions or other vegetables, or even fruit. In intelligence, such assumptions are themselves a *mess*: a complex system of interrelated experience, knowledge, and even ignorance that affects reasoning at multiple levels sequentially and simultaneously. There is an old English children's nursery rhyme that neatly characterizes this: "For want of a nail the shoe was lost. For want of a shoe the horse was lost. For want of a horse the rider was lost. For want of a rider the battle was lost. For want of a battle the kingdom was lost. And all for the want of a horseshoe nail."[129] Clearly, such a sequence implies a logical progression, whereas in dealing with wicked problems, the order may be mixed up. Some of the links may even be unknown—either missing or unknowable.

Wicked problems have no clear end-point. With tame and well-structured problems one knows when the solution is reached. In wicked problems this is not so, as Rittel and Webber make clear:

> There are no criteria for sufficient understanding and because there are no ends to the causal chains that link interacting open systems, the would-be planner can always try to do better. Some additional investment of effort might increase the chances of finding a better solution.[130]

---

127 Nicholas Nassim Taleb, "Learning to Expect the Unexpected," *Edge*, 19 April 2004, URL: <http://www.edge.org/3rd_culture/taleb04/taleb_indexx.html>, accessed 1 March 2007.

128 United States Senate, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*, Select Senate Committee on Intelligence, 108th Congress, 7 July 2004, 18.

129 Anonymous, *For Want of a Nail Rhyme*, URL: <http://www.rhymes.org.uk/for_want_of_a_nail.htm>, accessed 10 September 2007.

130 Rittel and Webber, "Dilemmas," 162.

This is not a new consideration. Writing in the 1930s, John Dewey observed that "the 'settlement' of a particular situation by a particular inquiry is no guarantee that *that* settled conclusion will always remain settled. The attainment of settled beliefs is a progressive matter; there is no belief so settled as not to be exposed to further inquiry."[131] Intelligence sensemakers routinely confront this challenge. Reports and assessments often update or revise previous conclusions. Often the previous reporting is consulted *before* the new report is written so that the author can determine the preexisting point of view on the issue. Such consultations at best determine whether the current situation deviates from the norm. Unfortunately, sometimes such consultations lead to the rejection of the new evidence, opening the way to intelligence errors and failures. One goal of an adversary's denial and deception activities is to facilitate rejection of the novel deviation. It was in this way that the possibility of nuclear missiles deployed to Cuba was rejected amid outlandish noise during the summer of 1962, and military exercises along the Suez Canal lulled Israel into a sense of creeping normalcy prior to October 1973.

Solutions to problems may be implemented for "considerations that are external to the problem" itself: problem solvers "run out of time, or money, or patience."[132] In intelligence, sensemakers may only be able to work for a given time on a problem before they have to issue their report. Changes in funding may mean that an effort to understand a phenomenon has to be discontinued. The practicalities of resource limitations force changes in sensemakers' foci. However, this does not mean that the problem does not continue to exist and perhaps, threaten. Rather, an answer has been developed to a distilled problem, communicated, and now other things must be done.

Solutions to wicked problems are at best good or bad. Some problems have true or false, yes or no answers. These are not wicked problems. Wicked problems have no such answers. Differing perspectives applied by different problem solvers, differing sets of assumptions, and differing sources of evidence are several of the factors that lead separate groups to come to different judgments about wicked problems. The impossibility of exhaustively considering all the factors and solutions of the problem also contributes to a multiplicity of solutions. At best these can be ranked as good or bad solutions. In most cases, according to Rittel and Webber, the solutions are expressed as "better or worse" or "satisfying" or "good enough."[133]

---

131 John Dewey, *Logic: The Theory of Inquiry* (New York, NY: Henry Holt, 1938), 8-9. Emphasis (italics) in the original.

132 Rittel and Webber, "Dilemmas," 162.

133 Rittel and Webber, "Dilemmas," 163.

Given, for example, the problem of stemming the growth of terrorism, there is no one simple solution that suffices. Instead, a number of differing solutions exist, depending upon (among other things) the perspectives about the domains at work in the problem. Focusing on the economics surrounding the growth of terrorism leads to different proposed solutions than does focusing on the demographics involved in the issue. Religious considerations or broader cultural considerations also create different solutions. Each of these perspectives in turn optimizes multiple points of view with differing, good and bad solutions. Overlap is possible and even desired. Good solutions encompass multiple domains.

Tests of solutions to wicked problems may not demonstrate their validity and may provoke undesired consequences. Implemented solutions to wicked problems "generate waves of consequences over an extended—virtually an unbounded—period of time."[134] Further, these consequences may themselves prove so undesirable as to negate any and all benefits of the original decision—*and this cannot be determined in advance*. Thus an intelligence-based decision to invade a country's possessions may create circumstances that offset any gains initially won, as the Argentineans discovered in 1982 when they—unwisely in retrospect—seized the British-owned Falkland Islands. From the perspective of the Argentine regime, the initial "victory" was offset when Britain forcibly retook the islands. The Argentine Navy lost a capital ship and many died; the regime lost power and was ultimately ousted. Seen from the perspective of the Argentine people this was, in the long term, of benefit. The government-condoned disappearances (torture and murder) of its foes ceased. Democratic processes were restored. However, things could easily have gone in another direction. One repressive regime could have been replaced by another. None of these outcomes was knowable in advance.

Implementing solutions to wicked problems can change the problem. In intelligence problems, real solutions cannot be practiced; there are no "dry runs." True, sensemakers and their policy-making customers can (and should) consider what *might* happen or the "implications" of the decisions or solutions of the problem at hand. Doing so might increase the likelihood that the decision selected is the best or the less bad of a set of bad alternatives.

Modeling the situation is one common means of assessing the implications of a potential action. However, models must by their very nature limit the factors considered. This raises the question of how one might know in advance if the eliminated factors are in fact significant. Further, modeling or any other means of generating solutions does not guarantee that the selected

134 Rittel and Webber, "Dilemmas," 163.

decision is the right decision. Once implemented it cannot be undone. It is noteworthy that at this point "implications" that do arise are actually "consequences" and hopefully they have been considered. But additional consequences and responses to those consequences by the actors in the problem as they respond to the "solution" will change, transform and evolve the problem. Taking down a terrorist's "safe house" may not reduce the threat, but does change where and how the remaining terrorists operate. This applies as well to attempts to reverse decisions. As Rittel and Webber note, "every attempt to reverse a decision or to correct for…undesired consequences poses another set of wicked problems,"[135] as sensemakers and planners involved in the U.S.-led "war on terror" have discovered. Actions, once taken, may mitigate the threat, or may not, which leads to the next facet of wicked problems.

Sensemakers can never know if they have determined all the solutions to wicked problems. They can expect, however, that they almost certainly *have not* determined all the solutions. In developing the range of alternatives within scenarios, two goals predominate: mutual exclusivity and collective exhaustion. In other words, each alternative must preclude the simultaneous possibility of the others, *and* the entire set of known alternatives must be considered. In practical terms, this is much more difficult to achieve than it sounds. Intellectual frameworks and so-called "biases" such as vividness, anchoring, confirmation, and others combine to prevent people from being able to consider all the alternatives. Adding to this is the fact that issues evolve in unpredictable ways. All the solutions simply are not knowable because they lie in the future. This does not justify not trying to completely assess the alternatives but rather provides recognition that some alternatives elude consideration.

Each wicked problem is unique. While it is true that common elements can be found between problems, there remain additional and unique properties of "overriding importance."[136] In other words, wicked problems cannot be characterized into "*classes*…in the sense that principles of solution can be developed to fit *all* members of a class."[137] For example, there are common elements or patterns in proliferation that allow recognition by sensemakers: acquisition of certain materials, construction of facilities, and the like. However, denial and deception—if applied—may obscure these commonalities. Knowing specific details of a weapons development program can be elusive. Another element, the *intentions* of the proliferators or the

135 Rittel and Webber, "Dilemmas," 163.
136 Rittel and Webber, "Dilemmas," 164.
137 Rittel and Webber, "Dilemmas," 164.

recipients of the proliferated systems are also of critical importance; they may be unique, and perhaps intractable. What Rittel and Webber have to say about this consideration is germane to intelligence: "Despite seeming similarities…one can never be *certain* that the particulars of a problem do not override its commonalities with other problems already dealt with."[138]

Every wicked problem is embodied in another one. Rittel and Webber describe problems as

> [discrepancies] between the state of affairs as it is and the state as it ought to be. The process of resolving the problem starts with the search for causal explanation of the discrepancy. Removal of that cause poses another problem of which the original problem is a "symptom." In turn, it can be considered the symptom of still another, "higher level" problem.[139]

What policies and actions, for example, are necessary to "fix intelligence?" Answering this involves asking what is causing intelligence to fail. One place to start is to consider why analysts are wrong and how intelligence errors lead to intelligence failure.[140] Yet such considerations lead one to consider how consumers may ignore intelligence, and how adversaries may in fact be "more capable" than expected. These in turn lead to what Jeffrey Cooper considers "analytic pathologies" that decrement both individual and corporate efforts to make sense of issues (table 2). Each of Cooper's specific pathologies is furthermore at least partially embodied in the others, giving rise to error-producing systems.[141] For example, Cooper argues that intelligence professionals' pathological focus on both "the 'dots' analogy and the model of 'evidence-based' analysis…understate significantly the need for imagination and curiosity."[142] Related to this is what he calls the myth of "Scientific Methodology." Analysis is *not* [hard] science and is *not* about proof. Rather it is about discovery.[143] These are embodied in the protocols he refers to as the flawed "Tradecraft Culture,"—a guild system of potential sensemakers and their historically unchanging ways of working.[144]

---

138 Rittel and Webber, "Dilemmas," 165. Emphasis in original.

139 Rittel and Webber, "Dilemmas," 165.

140 Johnston develops this distinction. Johnston, *Analytic Culture*, 64-66.

141 See Jeffrey R. Cooper, *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis* (Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 2005). Cited hereafter as Cooper, *Analytic Pathologies*.

142 Cooper, *Analytic Pathologies*, 28.

143 Cooper, *Analytic Pathologies*, 28-29.

144 Cooper, *Analytic Pathologies*, 30.

Table 2. Cooper's Analytic Pathologies
An intelligence account system whereby institutions and individuals "own" issues is inefficient. The return on investment for having accountability is too low when compared to the lack of cooperation, collaboration, and sharing such a system promotes. (30-31)
A cultural "evidence-based scientism" that prevents anticipatory consideration of policy and military intelligence consumers' needs. (31)
An overemphasis on current intelligence to the detriment of the "long view" resulting from a chaotic post-Cold War environment of emergent issues and crises. (32)
A production-oriented model that focuses on collecting, and processing massive quantities of data, and producing routine reports without the capability to adroitly refocus resources for ad hoc reports. (32)
A use of previous judgments as the starting point for all subsequent reporting. A corollary is a belief that "finished intelligence" is anything more than a snapshot in time, that it conveys larger "truth." (33)
A neglect of deep research about issues brought about by short-term tasks. (34)
A neglect of anticipatory intelligence arising from attempts by intelligence sensemakers to emulate the other (current) intelligence sources—such as news networks—on which their consumers also rely. (35)
A loss of "keynote species," mid-level sensemakers with deep domain expertise who create the in-depth assessments that convey what specific issues are all about. (36-37)
An inaccurate focus on results instead of processes leads to a failure to develop, validate, and promulgate methods of intelligence sensemaking. (37)
A security mindset leads to a lack of cooperation between intelligence sensemakers, and domain experts and their knowledge regardless of who and where they are. (38)

Source: Derived from Jeffrey Cooper, *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis* (Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 2005), 30-38.

Rittel and Webber posit "incrementalism" as a not uncommon approach to mitigating these effects. Related to Kuhn's concept of "normal science," incrementalism may actually compound the specific problem further because incrementalism

> [advertises] a policy of small steps, in the hope of contributing systematically to overall improvement. If, however, the problem is attacked on too low a level (an increment), then success or resolution may result in making things worse, because it may become more difficult to deal with the higher problems. Marginal improvement does not guarantee overall improvement.[145]

In considering Cooper's pathologies, summarized in table 2, fixing selective individual pathologies—insofar as possible—produces organizational changes that may inhibit further "fixes" by making them monetarily or organizationally too expensive. For instance, "solving" technological problems associated with Cooper's identified pathologies imposes infrastructures that may inhibit other necessary transformations such as developing a more agile workforce.

How wicked problems are resolved is determined by the means and methods used to make sense of them. In other words, how problems are perceived determines the kinds of solutions that are proposed. Point of view becomes essential in defining what a problem is and how it is to be resolved. Complex, wicked problems (as well as many "tame" ones) cannot be defined from one point of view. Defining the causes of terrorism is a case in point. As considered by the participants at the 2005 International Summit on Democracy, Terrorism, and Security, sponsored by the *Club de Madrid*, terrorism's causes lie in five broad domains: psychology, politics, economics, religion, and culture. Yet, as Martha Crenshaw notes in the conference report on the causes of terrorism, such considerations may be invalid:

> Explaining terrorism in terms of background conditions (social, economic, demographic, political, or cultural) is insufficient at best, and wrong at worst. Focusing exclusively on underlying structures provides little predictive capacity. "Root causes" may, in fact, influence the subsequent trajectory of terrorism more than its onset since they determine the extent of social support for violence by justifying grievances.[146]

---

145 Rittel and Webber, "Dilemmas," 165.

146 Martha Crenshaw, "Political Explanations," in Kim Campbell, ed., *Addressing the Causes of Terrorism: The Club de Madrid Series on Democracy*, vol. 1 (Madrid, SP: Club de Madrid, 2005), 13.

Yet these considerations are used to develop "solutions" to terrorism. Methods that consider and "solve" underlying economic or demographic issues, we may discover, only partly explain the phenomena.

How Are Wicked Problems Disruptive?

Disruption, as developed by Clayton Christensen, emerges from technologies that, while they may under-perform established technologies, open new markets and change the ways people do things. Enlarging the definition, disruptive intelligence problems threaten to change the way people interact. They proffer or impose new paradigms—both "good" and "bad"—for non-governments and governments alike. The disruption occurs because the incumbent is doing the *most rational thing it can do* given its circumstances. Doing the right thing generates the opportunity for disruption. For example, among the disruptions arising from a pandemic could be an easing of population pressures (if enough people die). This could lead to a freeing-up of energy resources for the survivors. Alternately, such a population die-off might cause a breakdown of societal infrastructures leading to riots and chaos. Both outcomes (and others)—as seen in anticipation—share likelihoods: all are likely. None of them can be reliably calculated (and therefore predicted) with any certainty.

See Clayton Christensen, *The Innovator's Dilemma* (Cambridge, MA: Harvard University Press, 1997).

Sensemakers have no right to be wrong. One of the first things many visitors to the CIA first see is the aphorism, "You shall know the truth, and the truth shall set you free."[147] As retired CIA veteran Ray McGovern comments,

> [T]he primary function of the Central Intelligence Agency is to seek the truth regarding what is going on abroad and be able to report that truth without fear or favor. In other words, the CIA at its best is the one place in Washington that a President can turn to for an unvarnished truthful answer to a delicate policy problem.[148]

This aphorism may have validity in the domain of tame problems where the truth is known or knowable. However, it has much less (if any) validity in the world of wicked problems where many truths can coexist,

147 John, 8:32 (King James' Version).

148 Will Pitt, "Interview: 27-Year CIA Veteran," *Truthout*, 26 June 2003, URL: <http://www.truthout.org/docs_03/ 062603B.shtml>, accessed 12 March 2007.

depending on the point of view expressed, the context can be simultaneously true and contradictory, and may in fact be unknowable.

The goal of assessing wicked problems may be to "improve some characteristics of the world where people live. Planners are liable for the consequences of the actions they generate; the effects can matter a great deal to those people that are touched by those actions."[149] Intelligence error, regardless of what causes it, is considered intolerable as U.S. policymakers and Intelligence Community sensemakers most recently discovered with their inaccurate estimate on the state of Iraq's programs to develop WMD. Earlier policymakers and sensemakers faced similar situations regarding the intentions of Japan, North Korea, China, Cuba, the Soviet Union (repeatedly), and India. In other words, restating part of Rittel and Webber's quote above yields this guideline: "*intelligence professionals* are liable for the consequences of the intelligence they generate."

An Intelligence Example: Pandemics as Wicked Problems

One of the threats faced by intelligence organizations and their professionals is that of an emergent global pandemic. What kind of a threat is a pandemic? Is it a tame or wicked problem, or something in between? Such considerations matter because they define what approaches are suitable for alleviating or mitigating the threats to national security that pandemics pose.

Historically, pandemic infectious diseases disrupted societies over wide regions of the world. Of these, the bubonic plague pandemic of the mid 14th Century, also called the "Black Death," is perhaps the best known. By killing off approximately one-third of Europe's population, it is credited with ending serfdom in most of the region. There was tremendous disruption, with both good and bad effects, and it is no coincidence that the Renaissance arose in its aftermath.[150] According to Norman Cantor, "[the] Black Death was the trauma that liberated the new."[151] The rational things to do in the

149 Rittel and Webber, "Dilemmas," 167.

150 Other developments such as the invention and use of the legal contract (by the Italians), which spurred trade; and a widening use of water wheels, which facilitated manufacturing, also were significant factors.

151 Norman F. Cantor, *In the Wake of the Plague: The Black Death & the World it Made* (New York, NY: The Free Press, 2001), 202. Cantor observes that this idea is controversial, citing work by Medieval historian Dom David Knowles arguing that the Black Death had little or no impact on Europe, and that of historian David Herlihy, which argues that it was highly significant. See David Knowles, *Great Historical Enterprises and Problems in Monastic History* (London, UK: Thomas Nelson and Sons, 1962); and David Herlihy, *The Black Death and the Transformation of the West*, Samuel K. Cohn, Jr., ed. (Cambridge, MA: Harvard University Press, 1995).

14th Century were to join concentrated populations in cities with regular inter-city trade routes to move goods. These conditions provided the disruptive opportunity for the pathogen.

Pandemics are by their nature adaptive and possibly recurring. Seen in hindsight, pandemics may appear to be tame problems, seemingly clearly defined and understood. But the requirement to deal with pandemics (and other wicked problems) is not to address them merely in hindsight—rather our well-being depends on foresight. This is, after all, how intelligence enterprises and their professionals work their issues. Rittel and Webber's criteria for a wicked problem provide a means of characterizing pandemics?[152]

- *Wicked problems have no definite formulation*. Ninety years after it occurred, the 1918 influenza pandemic remains only partially understood. As Edwin Kilbourne notes, "the origin of this pandemic has always been disputed and may never be resolved."[153] Seen as it emerged, the pandemic was even less clearly understood. While germ theory was known in some places, we did not know how to apply it to the pandemic nor how to protect ourselves. Similarly, while today the causes of Avian Flu are known to be the H5N1 virus, if, when, how, and where it (or some other as yet unknown virus) mutates from an animal-to-animal (and occasionally an animal-to-human form) to a human-to-human form remains unknown. Further, the exact nature of the mutation—necessary for the formulation of a vaccine—is and remains unknown. Most recently the difficulty in determining these factors with regard to the 2009-2010 H1N1 "Swine Flu" pandemic may have led to an overestimation of the severity of the pandemic by the U.S. Centers for Disease Control.[154] While this is a problem for epidemiologists and others tasked to create vaccines, it is also a problem for the sensemakers—who have to estimate the impact of having or not having a vaccine—and the policymaker who has to consider the implications of various courses of action (with or without a vaccine).
- *Wicked problems have no clear end-point*. Specific pandemics do have an end. The disease, having run through the population,

152 It is germane to note that if pandemics truly are a wicked problem (as is argued here) then characterizing them as such only partially and inexactly describes them.

153 Edwin D. Kilbourne, "Influenza Pandemics of the 20th Century" *Emerging Infectious Diseases*, vol. 2, no. 1 (January 2006), 9. URL: <www.cdc.gov/eid>, accessed 28 March 2007. Cited hereafter as Kilbourne, "Influenza."

154 Carl Bialki, "Swine Flu Count Plagued by Flawed Data," *Wall Street Journal*, online edition, 23 January 2010, URL: <http://online.wsj.com/article/SB10001424052748704509704575019313435804 60.html>, accessed 2 February 2010.

dissipates or abates. However, the diseases recur as the viruses evolve and mutate. In the case of the 1918 pandemic, the second wave of the virus apparently was more lethal than the first. Yet, similar, less deadly influenza occurs annually and subsequent pandemics are repeating phenomena.

- *Solutions to wicked problems are at best good or bad*. Vaccines are typically the solution to the annual influenza epidemic. In some years they are good—they are effective against the specific strains of the virus—and in some years they are not good (bad)—they are less effective against the specific strains.
- *Tests of solutions to wicked problems may not demonstrate their validity and may provoke undesired consequences*. Tests of pandemic plans and preparedness for cities and even countries provide a degree of comfort but no guarantee they will be effective against either the pandemic against which they were developed or another unexpected pandemic (such as that of the 2009-2010 H1N1 pandemic). It simply is not known nor knowable in foresight whether the measures will work, or the degree to which they will work until they are tested by the actual event. Furthermore, the proposed measures—once made—close off governments, corporations, and people from considering other options. If major adjustments are needed against the actual pandemic, it will take time to overcome the understandable resistance. Thus, testing and planning may have undesirable consequences in a real pandemic emergency.
- *Implementing solutions to wicked problems can change the problem*. One means of dealing with a pandemic in its early stages is quarantine. At the national level, this means closing international borders, preventing people as well as goods from entering or leaving the country. Doing so compounds the pandemic problem by adding economic issues. Companies relying on imported goods or on the ability to export goods may fail. Essential food items may not be available. Entire sectors of an economy may fail. The effectiveness of closing the borders depends (in part) on timing. Fewer people may die in the short-term but the longer-term economic disruptions may in fact increase mortality from other causes. The "problem" is no longer (just) the pandemic itself. Sometimes highly beneficial consequences arise out of catastrophes brought about by wicked problems. For example, as related by David Morens and Jeffrey Taubenberger, the Phillips Collection of Art in Washington, DC, owes its creation to the response of Duncan Phillips to the deaths

of his father and especially to the death of his brother James.[155] Phillips "as a direct consequence of the death of his brother James from influenza…dedicated his life…to establishing one of the finest public museums of modern art in the world."[156]

- *Sensemakers can never know if they have determined all the solutions to wicked problems.* Developing a collectively exhaustive list of options is difficult even when a complex issue is well understood. When the issue is not well understood, or is emerging, such lists become almost impossible to complete. In the case at hand, vaccinations, quarantines, and border closings all are suggested as means of mitigating a pandemic. However, it remains unknown what else is necessary to prevent or stem the spread of viruses and their impact on populations. While steps such as closing the borders, closing the schools, curfews, and ensuring that people wash their hands can be put in place, they can easily reach a point of unmanageability.
- *Each wicked problem is essentially unique*. While there are some commonalities between them, each influenza pandemic of the 20th Century essentially was unique. As Kilbourne notes, "Each differed from the others with respect to etiologic agents, epidemiology, and disease severity."[157]
- *Every wicked problem can be embodied in another one*. Influenza typically arises from close contact among animals and humans in agrarian settings. Thus, the influenza problem overlaps social problems that overlap economic problems and so on…
- *How wicked problems are resolved is determined by the means and methods used to make sense of them*. Means and methods of problem solving carry embedded assumptions about their appropriateness, the degree to which they are suited to the problem at hand, and of what they actually attempt to make sense. In examining a pandemic, vaccination strategies lead to certain results, whereas border closures lead to other ones.
- *Sensemakers have no right to be wrong.* Nor, in the case of pandemics or other global threats, do their policymaking consumers. When the stakes are the lives of many people, sensemakers

155 David M. Morens and Jeffery K. Taubenberger, "Influenza and the Origins of The Phillips Collection, Washington, DC," *Emerging Infectious Diseases*, vol. 2, no. 1 (January 2006), 79. URL: <www.cdc.gov/eid>, accessed 28 March 2007. Cited hereafter as Morens and Taubenberger, "The Phillips Collection."

156 Morens and Taubenberger, "The Phillips Collection," 79.

157 Kilbourne, "Influenza," 9.

and policymakers who miscalculate or underestimate or are otherwise wrong about a pandemic and its impact on their countries or region can expect vilification at best. A fear of such vilification from the public and the media might contribute to the situation whereby pandemic-tracking organizations such as the U.N. World Health Organization or the CDC *overestimate* the severity and threat posed by a pandemic such as the 2009-2010 Swine Flu pandemic.[158] For intelligence professionals this phenomenon is not unknown. Common wisdom among intelligence sensemakers is that it is far better to warn and be mistaken (and nothing happens) than to not warn and be mistaken (something happens).

Complexity

Rittel and Webber's notions of wicked problems can also be characterized through the lens of complexity theory. As developed by Jonathan Rosenhead, "systems of interest to complexity theory, under certain conditions, perform in regular, predictable ways; under other conditions, they exhibit behaviour [sic] in which regularity and predictability is lost."[159] This is exceptionally true of intelligence. Certain kinds of issues, including the interpretable indications of a build-up to armed conflict, can be extremely predictable. For example, if one observes a mass of troops approaching a national border and knows that the means by which these troops were trained includes a doctrine of "mass and attack," then one might legitimately adduce that an attack is likely and imminent. One could even use the past as a means of prognosticating the future with some degree of legitimate confidence.

However, in other situations, there may be a number of unknowable, unpredictable, and unanticipatable outcomes. Thus, reliable prognostication is simply not possible.[160] For instance, if a coalition of nations removes an oligarch in another nation from power, the specific outcomes of that action cannot be known in foresight. While alternative outcomes can be modeled

158 Whether overestimation occurred was argued in the European Parliamentary Assembly, although the WHO denied that it occurred. See "WHO Rejects Accusations It Mishandled H1N1, Updates Worldwide Stats," Kaiser Family Foundation, URL: <http://globalhealth.kff.org/Daily-Reports/2010/January/25/GH-012510-Swine-Flu.aspx?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+kff%2Fkdghpr+%28Kaiser+Daily+Global+Health+Policy+Report%29>, accessed 2 February 2010.

159 Jonathan Rosenhead, "Complexity Theory and Management Practice," URL: <http://www.human-nature.com/science-as-culture/rosenhead.html>, accessed 23 December 2008. Cited hereafter as Rosenhead, "Complexity Theory." See also, Jonathan Rosenhead, ed., *Rational Analysis for a Problematic World: Problem Structuring Methods for Complexity, Uncertainty and Conflict*, 2nd Edition (Hoboken, NJ: John Wiley & Sons, 2001).

160 More on this below.

and simulated, they remain valuable only as discussion points: there is no guarantee in advance that they have captured the reality that will occur. Modeling and simulation are feasible because complexity science shows that the "indeterminate meanderings of these systems, plotted over time, show there is pattern in the movements…the pattern stays within a pattern, a family of trajectories."[161] Unfortunately, because intelligence must address the "real" world, rather than its modeled or simulated semblance, events often are unique and therefore their patterns also are unique.[162] Thus, there exists an inability to guarantee a future reality; even probabilities may be suspect.

Analysis as here defined is insufficient to address complexity. Disaggregation simply does not reveal future alternatives. That this is so becomes obvious if one finds that it is the emergence of unique and novel behaviors arising from different and minutely differing initial conditions that characterize many 21st Century intelligence issues. In these circumstances, the whole of an issue is *greater* than its parts. But, in analysis, the issue is by definition and practice the *sum* of its parts.

Given these complex issues, the concept of "analysis" is simply insufficient for sensemaking. Instead, greater conceptual accuracy and precision of terminology is required. To achieve the needed accuracy and precision requires more than semantic invention. It also demands that underlying concepts, known as assumptions or premises, be identified and accounted for. Therefore, in developing the case for considering new paradigms for intelligence, certain terms require explicit (re)definition.

Implications of Complexity

Viewed from a larger context, complexity stymies the entire "standard model" of intelligence creation. With regard to Kent's concept of knowledge, or how intelligence is created, complexity—as viewed from the framework of wicked problems—confounds the consideration and mitigation of such problems. Kent's model of predictive and specific warning seems more miss than hit. Complexity further confounds the collaborative processes contained

161 Rosenhead, "Complexity Theory."

162 It should be noted that some intelligence-associated phenomena do exhibit general patterns that may be indicative. Observations of military preparations are an example, although caution is necessary when one extrapolates what those observations mean. For example, while one may make certain conclusions about a massing of troops on a border in light of who trained those troops (as was the case with Iraqi troops massed along the Kuwaiti border in 1990), what the indicator means may be subject to error. This latter point is illustrated by CIA Director John McCone's conclusion that SA-2 deployments in Cuba indicated strategic nuclear missiles were also being deployed. McCone's conclusion—although it turned out to be correct in the Cuban case—ignored the deployment of SA-2s without (presumably) the accompanying strategic nuclear-armed missiles to Egypt and Syria that was taking place at the same time. See Moore, *Critical Thinking*.

within Kent's notions of Activity and Organization, by which intelligence professionals are tasked to interact. How does the intelligence professional know in advance whose imagination will be most helpful in making sense of the problem at hand in time to prevent a catastrophe or even imagine one? For example, viewed in hindsight, the Drug Enforcement Administration (DEA) might have had a key piece of knowledge that would have been useful in the early apprehension of the December 2009 "underwear bomber." Certain illegal drugs—marijuana is one—are often "stashed" in a traveler's underwear.[163] In retrospect, one question becomes, "what else could be carried in this fashion?"

Asking such questions in retrospect is irrelevant. The question should have been asked in foresight—but how does an intelligence professional or even an airline security official know to ask the question in advance? Here again, complexity confounds the necessary collaboration. An intelligence professional might ask, "Which agency or agencies can help me make sense of this issue?" With 17 intelligence agency partners, there are up to 131,071 possible collaborative combinations—any of which (in various combinations) might be valuable.[164] This number presumes the searching intelligence professional knows which person—and there is only one person—in each agency who can help. The number grows at least exponentially when more than one individual at each agency might be helpful. While this situation presumes that the intelligence professional does not know who that person is in advance, in fact the professional does have a likely list of contacts, reducing the number of possible combinations dramatically. Still, this collaboration exercise may be a wicked problem. There may be sets of better collaborative combinations. The key imagination—as characterized by the DEA in the example above—may not be part of the collaborating group. One challenge is to determine a best collaborative combination prior to the event and develop believeable scenarios of what might transpire.[165] Finally, it

---

163 The author presumes the DEA is aware of this practice and would think of it if asked "how might one transport something without its being detected." The author's youthful observations while growing up in the American Southwest as well as discussions with state and local law enforcement officials engaged in intelligence-led policing training suggest the practice is fairly widespread.

164 The formula for such calculations is 2 raised to the power of the number of variables, in this case intelligence agencies, or 17, minus 1 ($2^n - 1$). See David T. Moore and William N. Reynolds, "So Many Ways To Lie: The Complexity of Denial and Deception," *Defense Intelligence Journal*, vol. 15, no. 2 (Fall 2006): 95-116. While the author and William Reynolds discuss complexity calculations in the context of denial and deception, the same notions apply to collaboration.

165 Peter Schwartz and Doug Randall, "Ahead of the Curve: Anticipating Strategic Surprise," in Francis Fukuyama, ed., *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics* (Washington, DC: Brookings Institution Press, 2007), 94. Cited hereafter as Schwartz and Randall, "Ahead of the Curve."

must lead to an action. As Peter Schwartz and Doug Randall write, "Achieving believability and action requires a depth of insight and understanding that is rare."[166]

Given the challenges of both tame and wicked 21st Century intelligence problems and their inherent complexity, what are intelligence professionals to do? One avenue open to them, and presented below, is the development and validation of methods of reasoning about key evidence.

166 Schwartz and Randall, "Ahead of the Curve," 94.

CHAPTER 3
From Normal to Revolutionary Intelligence

Evidence-Based Intelligence Creation

Intelligence sensemakers use more than context-less data and information. They employ assemblages of *evidence*—at a minimum, collections of data and information determined through marshaling to be relevant to the issue under consideration—in other words, contextualized to specific issues. Evidence reveals alternative explanations through pattern-primed, induced inferences about what is going to happen or what has happened already in the past.[167] While the inferences are typically uncertain, they do justify beliefs about phenomena. Justifying beliefs (or theories or hypotheses) presents a case for their accuracy but does not guarantee ground (or any other) "truth." Rather, as Peter Kosso notes, justifying beliefs is "about meeting the standards of evidence and reason [to] indicate [the] likelihood of accuracy."[168] Sensemakers go further and seek to demonstrate that the knowledge of tendencies they establish provides for "a correlation between being more justified and being true."[169] For example, during a recent exercise in which the author was a participant, one team reached an inferential conclusion about a likely explanation of the phenomenon being examined. The participants were presented with a set of previously determined alternative conclusions and a set of supposedly relevant evidence and asked to assess which (if any) conclusions were justified and true. After reaching an initial position they then were required to consider an alternative conclusion that presumed their original conclusion was false. In so doing they found that while the original conclusion initially

167 Reasoning about past events remains easier than reasoning about the future. In the former case, the evidence may be contradictory, deceptive, and subject to more than one interpretation. However, it tends to be more complete and marshaled (or at least discoverable). When looking to the future the important consideration is that much of the evidence does not yet exist. The events described by precursor information may not have occurred. Additionally, the tests of the information that transform it into evidence necessarily remain incomplete.

168 Peter Kosso, "Introduction: The Epistemology of Archaeology," in Garrett G. Fagan, *Archaeological Fantasies: How Pseudoarchaeology Misrepresents the Past and Misleads the Public* (London, UK: Routledge, 2006), 4. Cited hereafter as Kosso, "Epistemology."

169 Kosso, "Epistemology," 4.

appeared more accurate, the latter one was in fact "true." This was in part because they made wishful assumptions about the evidence they used to justify their conclusions. As Kosso observes, "more justification is better, since it raises the likelihood of accuracy. But it is certainly possible for a well-justified belief to be false."[170] This realization on the part of the participants subsequently led to a more critical assessment of the evidence, much of which was found to be false. They discovered that "justification comes in degrees, but truth does not."[171]

It is arguable whether greater evidentiary justification demonstrates the likelihood of a strongly accurate correlation with truth. As Kosso makes clear, even with abundant justification, there is no certainty of truth. Therefore, according to Kosso, it "is the task of the systematic disciplines…to refine carefully the content of justification, the evidence and the network of theoretical beliefs, to bring justification into ever closer correlation with truth."[172] If intelligence is to "speak truth to power" it must first ensure its words are well and critically justified.[173]

As figure 1 illustrates, intelligence sensemaking is conducted in service of a number of goals, including describing states of affairs, explaining phenomena, interpreting events and actions, and estimating the likelihood and impact of a foe's future actions As intelligence professionals move from describing events, explaining patterns of behavior, and grasping underlying factors and intentions, ever more justification of beliefs about the phenomena under scrutiny is required. Yet, as intelligence professionals attempt to apply greater scrutiny in this sequence, their capability to do so decreases as they face greater ambiguity.

Additionally, we may expect that sensemakers will more often be wrong in offering *estimations* about phenomena than when they are merely describing them. This is in part because of an interesting reality characterized by Taleb: To predict the future we must already know the future.[174] What Taleb means is that one has to already have visualized what the future will be in order to estimate it. Kosso, in writing about epistemic science, elaborates:

---

170 Kosso, "Epistemology," 4.

171 Kosso, "Epistemology," 4.

172 Kosso, "Epistemology," 5.

173 The aphorism "speak truth to power" is variously (and wishfully) ascribed to Sherman Kent. Research by the author and discussions with former intelligence officers who knew and worked with Kent fails to reveal this to be the case. Intelligence strives to ensure its findings are factual and—to the best knowledge of its creators—"true."

174 Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable* (New York, NY: Random House, 2007), 173. Cited hereafter as Taleb, *The Black Swan*.

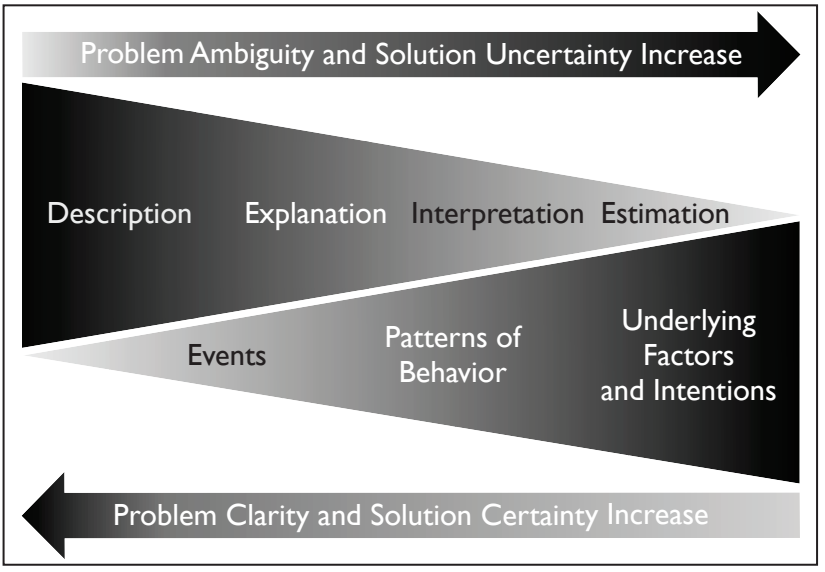


Figure 1. Types of Intelligence and the Phenomena They Characterize. Complexity, ambiguity, and uncertainty increase as one moves from Descriptive to Estimative Intelligence.

Source: Author.

> [The] knowledge claims are more ambitious in that they stray further from what is immediately observed…The theoretical descriptions are based on observation and evidence…But it is important to note that the observations themselves are based on theory. Scientific evidence, after all, is neither haphazard nor uninterpreted, and some prior conceptual understanding of nature will inform decisions about what to observe, which observations are credible, what the observation means, and how what is observed is causally (and hence intentionally) linked to what is not observed. Theory is necessary to turn mindless sensations into meaningful evidence.[175]

While Kosso writes in the language of science, his argument applies as well to Manjoo's "post-fact" world of which intelligence often attempts to make sense.[176] Intelligence is created ultimately from human, sensory-mediated observations of phenomena. Further, intelligence evidence, while

175 Kosso, "Epistemology," 5.

176 By "post-fact" Manjoo refers to a tendency to ignore evidence in favor of predetermined conclusions. Common examples include the arguments of pseudosciences such as astrology or intelligent design. A more serious example is manifested by parents who refuse—due to pseudoscientific (and disproved) conclusions—to vaccinate their children. Within the IC this tendency manifests itself when intelligence professionals let predetermined conclusions drive their intelligence creation efforts rather than let evidence go in search of hypotheses.

it may appear to remain "haphazard," is the result of systematic foraging, gathering and interpretation. The past tells intelligence practitioners what to look for in the future. This poses dangers when those indicators are no longer (if indeed they ever were) valid. As Baruch Fischoff suggests, "searching for wisdom in historic events requires an act of faith—a belief in the existence of recurrent patterns waiting to be discovered."[177] Yet, while general patterns may exist, "the past never repeats itself in detail."[178] In other words one might detect indicators suggesting that an upcoming event similar to one in the past is possible, likely, or even reasonable. On this basis, one could, for example, have anticipated that sooner or later foreign terrorists would again attack the United States by targeting some high-value building or event, such as the World Trade Center.[179] This is a far cry from predicting that Al Qaeda terrorists would fly airplanes into the World Trade Center and the Pentagon on the morning of 11 September 2001.[180] Finally, intelligence practitioners making sense of issues rely heavily on theories, which if unacknowledged, essentially are unexamined assumptions.

If using the past to gain wisdom about what the future holds is not feasible, what about studying the past to avoid folly? Tversky and Kahneman's work on *availability* leads one to suspect (as Fischoff also notes) that focusing on misfortunes "disproportionately enhance[s] their perceived frequency."[181] Another challenge to considering the past as a teacher of what not to do is that one may not properly understand the problem. While understanding may be possible (or even easier) when dealing with Tame Problems—as has been discussed above, when considering Wicked Problems, such understanding is elusive at best and is dependent on the methods chosen to deal with the problem; in other words, woefully incomplete.

---

177 Baruch Fischoff, "For Those Condemned to Study the Past: Heuristics and Biases in Hindsight," in Daniel Kahneman, Paul Slovic, and Amos Tversky, *Judgment Under Uncertainty: Heuristics and Biases* (Cambridge, UK: Cambridge University Press, 1982), 338. Cited hereafter as Fischoff, "Condemned to Study the Past."

178 Fischoff, "Condemned to Study the Past," 336.

179 On 26 February 1993, a truck bomb placed by Islamic terrorists exploded below one of the buildings of the World Trade Center and was apparently intended to topple both towers. For a discussion of the security implications, see Laurie Mylroie, "Who is Ramzi Yousef? And Why It Matters," *The National Interest*, 22 December 1995. Available at URL: <http://www.fas.org/irp/world/iraq/956-tni.htm>, accessed 12 October 2010.

180 Such an attack had been *anticipated*. As Schwartz and Randall comment, "many people did anticipate the terrorist attacks of September 11 [2001]...Yet most Americans, as well as officials in both the Clinton and Bush administrations, focused their attention elsewhere while the inevitable grew imminent." Schwartz and Randall, "Ahead of the Curve," 94.

181 Fischoff, "Condemned to Study the Past," 339. See also Amos Tversky and Daniel Kahneman, "Availability: A Heuristic for Judging Frequency and Probability," *Cognitive Psychology*, vol. 5 (1973): 207-232.

With the intention to improve evidence-based intelligence creation, recent legislation "reforming" intelligence goes so far as to require that "alternative analysis" be conducted.[182] The IC, at least through its schools, interprets this to mean that *multiple* hypotheses be considered. The relevant act mentions "red teaming: a means by which another group of intelligence professionals consider alternative explanations for an issue being scrutinized.[183] The legislation leaves unexamined the question of whether the criteria for sensemaking will be met in examining tame problems and especially wicked problems arising from consideration of adversarial intentions.

If, for example, one estimates that a particular country whose policies one's own government generally opposes will develop both a long-range missile capability and a nuclear weapons capability and then marry the two together, one has to have already imagined, in the context of the target country's political and technological environment, what a long-range missile capability is, what a nuclear weapon is, what a weapon of mass destruction is, and a strong sense of the will to combine these threat elements. Policymakers may challenge the target country's actions, making their leaders more adversarial. Thus, at a minimum, intelligence and policy create the future—or a version of it. Done poorly, this can lead to unintended and dangerous implications.

Emerging from this mélange are hypotheses that are ripe for disconfirmation, although a tendency to compound uncertainties on the part of intelligence professionals and their consumers my serve to prevent this from occurring. If in fact, in the example above the assessment is wrong, and the nuclear capability assessed to be for weapons really is intended to provide an alternative to the nation's dependency on a dwindling supply of increasingly more expensive petroleum as a source of energy, and the missiles support a nascent space program designed to orbit telecommunications satellites that can fulfill the country's needs and those of their neighbors as well as generate income for the government, then sensemakers and policymakers on all sides will have extrapolated inappropriate patterns arising from a misunderstood present. In a tense bilateral or even multilateral environment, rhetoric and actions can precipitate events so as to create a future consistent with those pattern-derived conclusions, driving the target country to produce the weapons. Each side then blames the other nation's government for having "caused" the crisis.

182 U.S. Congress, IRTPA, 2004, 33.

183 U.S. Congress, IRTPA 2004, 33.

There are a number reasons why such faulty causal networks occur. Honest evidentiary considerations demand a degree of agnosticism about the theories being justified. Evidence-based knowledge, as Peter Kosso's epigraph at the beginning of this book acknowledges, is not absolute; justified evidence *changes* theories and not the other way around. In other words, when interpretations of the evidence lead to coherent alternative inferential conclusions, then the existing or accepted theories require changing. What must not happen is to reinterpret the evidence to support the prevailing preexisting theory, as is the case in the above example.

However, this is exactly what happens all too often. People are often unwilling to abandon their cherished positions. This occurs in part because they are not dispassionate as they reason about evidence. In other words, positions are influenced by various worldviews or cognitive approaches, particularly selective perception and selective exposure. These combine to steer how people recognize issues, the phenomena that comprise them, and how they go about making sense of them.[184] These influences or theoretical frameworks shape the patterns people use to interpret new phenomena. The benefit is that these frameworks make people smart and do so quickly.[185] However, this benefit depends on the existence of a repetition of observed phenomena. In order to work successfully, an intuitive framework for understanding requires at least a similar situation, a condition that may not occur with intelligence phenomena.

In an information-rich environment brought about by technical collection, intelligence professionals can select inappropriate patterns to use in making sense of new phenomena. In intelligence work, if such patterns conspire to affect the search for and the selection of the evidence sensemakers use, and that they and their consumers then accept, selective perception and selective exposure set the stage for intelligence error and failure.

Evidence always requires a context, and as the missile example illustrates, there may be more than one explanatory context that makes sense. In intelligence, "evidence is [particularly] rarely self-sufficient in information or credibility."[186] Additionally, the dispassionate nature of evidence itself, when

184 For more information on frameworks or "heuristics" that people employ to cope with judgments about which they are uncertain, the reader should consult the works of Daniel Kahneman, Paul Slovic, and Amos Tversky, *Judgment Under Uncertainty: Heuristics and Biases* (Cambridge, UK: Cambridge University Press, 1982) and Thomas Gilovich, Dale Griffin, Daniel Kahneman, *Heuristics and Biases* (Cambridge, UK: Cambridge University Press, 2002).

185 This is the premise of Gerd Gigerenzer's book *Simple Heuristics That Make Us Smart* (Oxford, UK: Oxford University Press, 1999). These patterns of behavior evolved as survival mechanisms and by and large they have sufficed—the human species survives to the present.

186 Kosso, "Epistemology," 8.

viewed outside its political and social context, contributes to a failure to adequately explore issues. In other words, unless the correct context is known, evidence—if its constituent information can even meet that threshold—is subject to many different interpretations. Without context the person assessing the evidence has no way of knowing which interpretation is correct. Multiple contexts further confound the situation, for different contexts often lead to alternative conclusions as was illustrated in the missile development scenario just described. Finally, as Hampson's essay reveals, the political context of the policymaker may skew the actual context conveyed by intelligence.[187]

What is occurring in the contextual consideration of evidence is a process of epistemological justification and as Kosso notes the "key concern is to distinguish knowledge, on the one hand, from mere belief, opinion, dogma, and wishful thinking, on the other."[188] In relation to intelligence, knowledge depends on contextual justification of evidence and, as noted earlier, the "business of epistemology is to show that there is a correlation between being more justified and being more likely to be true."[189]

Despite their inherently greater inaccuracy, predictions seem to garner more interest from consumers than do explanations. In biology, predictive hypotheses require accommodation to valid background information in order to be useful.[190] Is this true in intelligence? As illustrated by two National intelligence Estimates (NIE's) dealing with weapons of mass destruction (WMD) that were subsequently found to be wrong, *incorrect* predictions certainly garner considerable attention. In these cases, the incorrect predictions perhaps resulted in part from a lack of time available for their preparation. In the first case, the estimate on whether or not the Soviets would place strategic nuclear missiles in Cuba in 1962 was written in a week.[191] In the case of Saddam Hussein's WMD programs, the preparation time was three weeks. Such short time frames for preparation would seem to prevent new information and data

187 Hampson, "The Divided Decision-Maker."

188 Kosso, "Epistemology," 4.

189 Kosso, "Epistemology," 4.

190 Kathrin Stanger-Hall and others, "Accommodation or Prediction?" Letter in response to Peter Lipton, "Testing Hypotheses: Prediction and Prejudice," *Science*, vol. 308, no. 5727 (3 June 2005), 1409.

191 Admittedly this is hindsight analysis. Sherman Kent, writing in 1964, asserts that in retrospect the authors *did* have sufficient time to assess the evidence. See Kent, "A Crucial Estimate Relived," *Studies in Intelligence*, vol. 8, no. 2 (Spring 1964):1-18. Originally classified SECRET, it was declassified and reprinted in *Studies in Intelligence*, vol. 36, no. 5 (1992): 111-119. Kent carefully considers the reasons why the estimate was wrong and why it was not revised. Among the reasons cited was the presumption that past precedents of Soviet foreign policy would continue into the future. Thus, no offensive missiles would be deployed in Cuba.

from being collected and made relevant to the issues (i.e. marshaled as evidence), and prevented alternative perspectives from being fully explored.[192]

A lack of time typifies one context of intelligence sensemaking. This context in which intelligence professionals work and the constraints imposed upon them facilitate their successes but also their failures. As the above examples demonstrate, intelligence sensemakers are often under pressure to consider massive amounts of data and information in a short time. These same professionals must marshal the data and information into evidence even as they attempt to understand, and then explain, the associated complex issues to policy- and decisionmaking consumers.

Finally, the current and past practice of intelligence in the U.S. is consistent with a focus on prediction rather than explanation as its ultimate purpose. This has not been without critique. Willmoore Kendall, in reviewing Kent's book in 1949 for *World Politics*, criticized Kent's "compulsive preoccupation with *prediction*."[193] Given the experience of Kent and others during World War II, it is not surprising that the desire to prevent another Pearl Harbor dominated their practices; such a desire naturally would have led to an activity organized around the creation of surprise-preventing predictive knowledge.[194]

Considering the Normal

The process described in the preceding section can be thought of as "normal intelligence." As conceived by Thomas Kuhn, "normal" refers to "the relatively routine work…within a paradigm, slowly accumulating detail in accord with established broad theory, not actually challenging or attempting to test the underlying assumptions of that theory."[195] We can thus see that "normal intelligence" is an activity of expanding knowledge in which most intelligence professionals engage and which incrementally increases knowledge about targeted phenomena.[196] The professionals work within a model

---

192 The Senate report on the Iraqi WMD noted that alternatives were not explored although this is not the case with the aluminum tubes alternately argued to be for centrifuges and rockets. In this case a groupthink framework seems to have shaped the results. See United States Senate, *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*, Select Senate Committee on Intelligence, 108th Congress, 7 July 2004, 18, 21.

193 Kendall, "Function of Intelligence," 549.

194 Given a "worst-case" perspective about WMD such a perspective perhaps also partially explains points of view about Iraq's alleged WMD programs leading up to the 2002 estimate. It does not, however, explain the apparent 9/11 "failures of imagination."

195 Wikipedia, entry under "Normal Science," URL: <http://en.wikipedia.org/wiki/Normal_science>, accessed 26 September 2007.

196 Thomas Kuhn, *The Structure of Scientific Revolutions* (Chicago, IL: University of Chicago Press, 1962), 10-42, Cited hereafter as Kuhn, *Structure*.

or "paradigm" of reality forged during the Second World War and reinforced throughout the ensuing Cold War. The perceived and recalled successes of the past contribute to the repeat use of unvalidated tradecraft. The paradigm presumes state-level adversaries — eventually with mutually destructive capabilities.

As used in this context, "normal intelligence" is to "intelligence" as Thomas Kuhn's "normal science" is to "science." In both domains newly created knowledge incrementally adds to an increasingly established paradigm; new knowledge does not easily redefine the paradigm. Even the anomalous and truly unknown are only considered in terms of what is known. Normal science or normal intelligence does not seek to revise significantly the paradigm by which new phenomena are known and understood. This may be seen in the way new intelligence personnel adopt existing job accounts. A common practice involves their reviewing previous reporting on the account, with a tendency for new reporting to stay within the conceptual boundaries of what has gone before. Knowledge increases only incrementally.

Intelligence practitioners working within the paradigm of normal intelligence attempt to describe, explain, or predict phenomena *coherently*. In this case, the term refers to another concept developed by Kuhn: A common framework for understanding the phenomena is sought or presumed. New knowledge is understood in the context of the dominant paradigm. For example, normal intelligence of the latter half of the 20th century understood events in relation to the missions and goals of U.S. adversaries, principally the former Soviet Union and to a lesser degree, China. World affairs were understood in the context of the state-based adversaries' hegemonic competition with the United States.

Normal paradigms prevail until previously unnoticed and unnoticeable discrepancies create sufficient inconsistencies in explaining and understanding phenomena so as to cause errors that cannot be ignored. For Kuhn this means a necessary change in scientists' perception of the realities as characterized by science. Kuhn illustrates this with an example of the

> transition from Ptolemaic to Copernican astronomy. Before it occurred, the sun and moon were planets, the earth was not. After it, the earth was a planet, like Mars and Jupiter; the sun was a star, and the moon was a new sort of body, a satellite. Changes of that sort were not simply corrections of individual mistakes embedded in the Ptolemaic system…they involved not only changes in laws of nature but also changes in the criteria by which some terms in those laws are attached to nature. These criteria, furthermore,

were in part dependent upon the theory with which they were introduced.[197]

In the physical sciences, the phenomena themselves do not change (although newly noticed phenomena could make it appear so). In the cultural environment of human interaction, the *new perceptions* of reality can be enough to force a reconsideration of the *old*. In social scientific terms, a new paradigm not only explains the new, it does *better* at explaining the old. Further, even the language previously employed to describe a phenomenon is inadequate because—as Kuhn notes—"scientific development cannot be quite cumulative. One cannot get from the old to the new simply by an addition to what was already known."[198]

Failures to consider discrepancies lead prospective intelligence sensemakers to retain an invalid understanding of phenomena even as the phenomena themselves change. This larger discrepancy leads either to intelligence error or intelligence failure. Once again, within the Kentian paradigm, intelligence errors derive from "factual inaccuracies in analysis resulting from poor or missing data."[199] Conversely, as has been noted, intelligence failures refer to "systemic organizational surprise resulting from incorrect, missing, discarded, or inadequate hypotheses."[200] Within the former concept there is a presumption that if more data are available or better understood, errors can be prevented. In the latter, intelligence practitioners or their policymaking customers have misunderstood the issue and its context.

The existence of particular intelligence errors *does not* necessarily indicate a paradigm has changed. However, repeated intelligence errors *do*. As is the case with science, small errors in adequately characterizing phenomena lead to the emergence of "corrective constants." The sensemaker may have made a perceptual or interpretive error. However, left unchecked, errors eventually combine to cause systemic failures. Intelligence practitioners and policymakers repeatedly may come to incorrect conclusions from faulty sensemaking, leading to policy failures, defined by Rob Johnston as "systemic organizational surprise" resulting from a mixture of practitioners' lapses and policymakers' ignoring proffered intelligence.[201] The more

197 Thomas S. Kuhn, *Thomas S. Kuhn, The Road Since Structure: Philosophical Essays, 1970-1993, with an Autobiographical Interview*, James Conant and John Haugeland, eds. (Chicago, IL: University of Chicago Press, 2000), 15. Cited hereafter as Kuhn, *The Road Since Structure*.

198 Kuhn, *The Road Since Structure*, 15.

199 Johnston, *Analytic Culture*, 6.

200 Johnston, *Analytic Culture*, 6.

201 Johnston, *Analytic Culture*, 6.

germane interpretation offered in the present work is that intelligence failure stems from inadequacies on the part of both policymaker and intelligence professionals to recognize a fundamental, revolutionary shift of the intelligence context.

The state-as-adversary paradigm for intelligence creation is obsolete. Two decades now separate the interpretable intelligence context from that of the Cold War: the adversaries and issues are now strikingly different.[202] The power of the Soviet Union waned dramatically after 1990 as that of China increased. But even more central to the intelligence context, novel phenomena also appeared that were non-state based: emerging non-state actors posed new challenges by threatening traditional state structures. Emerging phenomena such as disease and climate change imposed new complexities. The anomalies these new phenomena have created illustrate how and why normal intelligence is no longer adequate: it could no longer characterize these phenomena within the threat and opportunity framework of strategic intelligence. The "normal" means by which error is explained remain inadequate. As documented in the various Congressional and independent commission reports, intelligence no longer adequately describes, explains, or predicts with respect to the phenomena its consumers need to understand. Thus, intelligence change is necessary—revolutionary change.

Paradigm Shift

Revolutions in science, politics, and military affairs occur because crises reveal the insufficiency of the reigning paradigm. As Kuhn notes, an existing paradigm can "cease to function adequately in the exploration of an aspect of nature to which the paradigm itself [has] previously led the way."[203] Kuhn argues further that science does not evolve smoothly. Rather, periodic revolutions change how phenomena are perceived and understood.[204] Crises are a precursor of such paradigm shifts. Analogously to Kuhn's notions, the (officially) serious failures of the Intelligence Community to predict the attacks of 11 September 2001 and the state of Saddam Hussein's programs of

202 It should be noted that the traditional adversaries of the Cold War remain threats. While an argument can be made that other issues overshadow the dangers they pose, it can also be claimed that emerging threats simply compound the traditional ones. 21st Century dangers are complex; one of their dangers *is* their complexity.

203 Kuhn, *Structure*, 92.

204 Kuhn, *Structure*, 92-110.

WMD (both in 1990 and prior to the 2003 invasion of Iraq) are examples of systemic reframing crises.[205]

If we review these failures through their official re-examinations, certain phrases recur: mind-sets, politicization, and faulty analysis. Across the same period, there are repeated attempts to impose methods of "[social] scientific study…to analysis of complex ongoing situations and estimates of likely future events."[206] What is lacking is any sort of a systematic approach across the Intelligence Community. As long-time practitioner and observer Jack Davis noted a decade ago, no corporate standards for how intelligence is created, including the methods employed, exist.[207] Although sound practice does not ensure that intelligence assessments will be correct, its absence, by definition, contributes to flawed conclusions. Contributing to this scenario is the fact, as Aris Pappas and James Simon observe, that "[potential] opponents [are] often…driven by emotional agendas that [make] them unpredictable."[208] While effective practice might not drive the production of sound estimates from ambiguous evidence, it would routinely alert practitioners to the prospect that these same opponents' actions are unpredictable or at best, that they are predictable within a range of behaviors.

In short, U.S. intelligence professionals operate in an environment similar to an unfolding Kuhnian revolution: the epistemology of normal intelligence is insufficient and new knowledge is needed. The recent failures highlight the necessity for change, as does the graying of the intelligence sensemaking workforce—new people faced with new and emerging issues should be comfortable with finding new ways to systematize their work. The changed contexts and data, once they confront practitioners with problems that are

---

205 The argument that these were crises in reframing rests on the observation that intelligence practitioners were as shocked at the inaccuracy of their estimates as were the surprised policymakers. In the case of the 2000 estimates of Iraqi WMD, the CIA *underestimated* the state of Iraqi WMD, leading to a claim that the apparent overestimation in the 2002 estimate was compensation for that earlier error. While admitting to the underestimation, a CIA press release adds, "in no case were any of the judgments [in the 2002 estimate] 'hyped' to compensate for earlier underestimates." See, Central Intelligence Agency, "Iraq's WMD Programs: Culling Hard Facts from Soft Myths," *Press Release*, 28 November 2003, URL: <https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2003/pr11282003.html>, accessed 9 December 2009.

206 Jack Davis, "Introduction—Improving Intelligence Analysis at CIA: Dick Heuer's Contribution to Intelligence Analysis," in Richards J. Heuer, Jr., *Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999), xv. Cited hereafter as Davis, "Improving Intelligence."

207 Davis, "Improving Intelligence," xxv.

208 Aris A. Pappas and James M. Simon, Jr., "The Intelligence Community: 2001-2015: Daunting Challenges, Hard Decisions," *Studies in Intelligence*, vol. 46, no. 1 (2002), URL: <http://www.cia.gov/csi/studies/vol46no1/article05.html>, last accessed 10 January 2006.

unintelligible in normal intelligence, will reflect the idea that a Kuhnian-style revolution in intelligence is underway.

However, a caveat is necessary. Not all "old school" intelligence practices are without continuing value. Several significant state-level adversaries remain as threats to the security of the American nation although they too are challenged by the new non-state actors and issues that populate the paradigm of the new intelligence—something that compounds any estimate of how they are likely to engage the United States. Further, in many circumstances and in dealing with certain issues, the tacit expertise of highly experienced intelligence professionals is appropriately tapped for "recognition-primed" sensemaking.[209] These "old hands" possess both current knowledge and a highly evolved skill set. Years of innovative and critical thinking mean they are skilled in looking at issues from a variety of perspectives and have the wisdom of deep context. It is no accident, therefore that the contributors to Roger George and James Bruce's recent book, *Analyzing Intelligence*, are very senior intelligence practitioners.[210] The challenges involve *knowing* when such expertise is valuable and needed in the first place, and encouraging the intelligence enterprise to *develop* and *retain* the cognitive and organizational flexibility that such thinking requires.

Indeed, a part of successful and revolutionized intelligence work involves gleaning new meanings from old patterns that have remained hidden to those who have stopped short of sensemaking. One challenge is that the "fresh" eyes lack the knowledge of potentially relevant patterns while the "old" eyes cannot see things as new. Each lacks the other's strength. Experience acquired by newer professionals who engage in the practice of traditional "analysis" jaundices their once-fresh viewpoints even as they start to acquire the relevant and necessary experience.

One solution may be to adopt a model of core competencies broken out according to task analyses of existing intelligence missions and functions. Such a model identifies what is needed and has been at least partially implemented in the IC's Analytic Resource Catalog developed during the tenure of former Director of Central Intelligence George Tenet.[211] Rewarding the successful use of some of the most important competencies may also encourage

---

209 Robert Hoffman, conversation with the author, 4 October 2007.

210 Roger Z. George and James B. Bruce, *Analyzing Intelligence: Origins, Obstacles, and Innovations* (Washington, DC: Georgetown University Press, 2008).

211 Mark M. Lowenthal, "Foreword," in Moore, *Critical Thinking*, xi.

their retention in the catalog. Among these are curiosity, perseverance, and pattern recognition.[212]

A necessary first step in a revolution in intelligence work is looking in depth at what it is intelligence professionals do, must do, and how they do it. Simply put, intelligence practitioners create knowledge to support their customers. As used here, intelligence practitioners are presumed to be contributors to government plans and policies at a variety of levels where they have the opportunity to share broad strategic perspectives with national leaders as well as ensure that deployed warfighters have at hand the fruits of technical collection and marshaling of tactical data.

Finally, it should be noted that intelligence *Knowledge* is only one component of a strategic, operational, and tactical intelligence triumvirate.[213] *Activity* and *Organization* are the other two. It is the author's belief that Activity and Organization also are in need of new paradigms. However, such a discussion hinges on what intelligence Knowledge is and how it is created—in short, the sensemaking involved. Insofar as Activity describes how the precursors of intelligence are hunted, gathered, made sense of, and transformed into knowledge, it is considered here. However, the uses of intelligence (also an activity) and how intelligence professionals are grouped, led, and managed to act and create knowledge—the realm of Organization—lie beyond the scope of this book.

212 For more on core competencies for successful intelligence work see David T. Moore and Lisa Krizan, "Core Competencies for Intelligence Analysis at the National Security Agency," in Russell G. Swenson, ed., *Bringing Intelligence About: Practitioners Reflect on Best Practices* (Washington, DC: Joint Intelligence Military College, 2003): 95-132. Cited hereafter as Moore and Krizan, "Core Competencies."

213 Kent identified and developed three concepts related to strategic intelligence: Knowledge or what is produced and disseminated; Activity, or how such knowledge is produced and disseminated; and Organization, or how people are grouped to produce and disseminate such knowledge. Kent, *Strategic Intelligence*. Moore and Krizan advocated this approach in their competency work. See Moore and Krizan, "Core Competencies" and David T. Moore, Lisa Krizan, and Elizabeth J. Moore, "Evaluating Intelligence: A Competency-Based Approach," *International Journal of Intelligence and CounterIntelligence*, vol. 18, no. 2 (Summer 2005).

CHAPTER 4:
The Shape of Intelligence Sensemaking

Intelligence Sensemaking involves a number of overlapping high-level activities. First, intelligence professionals engage in planning or design and then hunt for and gather the materials they require in order to understand issues, answer questions, or explore new ideas. They can be externally motivated by the needs of a customer or they can be self-motivated as a result of an observation, or both. Second, these professionals disaggregate and then reassemble relevant information, trying to determine what it means. At every stage in their work they assess critically their processes and results, seeking to validate both how they are engaged and the outcomes of their engagements. These overlapping activities can be characterized as Planning, Foraging, Marshaling, Understanding, and Communication. They are supported by Questioning and Assessing. Although these elements are discussed separately, it is of course only through their applied interaction that they describe sensemaking.

Planning for Tame and Wicked Intelligence Problems

Making sense of either tame or wicked problems is predicated upon planning. Plans, according to Gary Klein, are "prescriptions or roadmaps for procedures that can be followed to reach some goal, with perhaps some modification based on monitoring outcomes."[214] Creating plans requires "choosing and organizing courses of action on the basis of assumptions about what will happen in the future."[215] Known as *planning*, this process characterizes the "contingencies and interdependencies such as actions that must occur first as a precondition for later actions."[216] When we add the concept that practitioners—through critical thinking—also engage in reflective thinking and learning, both singularly and collaboratively, we may similarly label this process "the art of intelligence design."

214 Gary Klein, "Flexecution as a Paradigm for Replanning, Part 1," *IEEE Intelligent Systems*, vol. 22, no. 5 (September/October 2007), 79. Cited hereafter as Klein, "Flexecution 1."

215 Klein, "Flexecution 1," 79.

216 Klein, "Flexecution 1," 79.

With tame problems, where answers and solutions can be anticipated, algorithms can calculate actionable probabilities and repeatedly make sense of the problem.[217] The design of useful algorithms may be complex and they operate well only in finite and specific environments. How, on the other hand does one plan or design for wicked problems? One answer is to re-imagine the wicked problem as a tame one. However, the repeated occurrence of "unintended consequences" in past scenarios suggests that this is not a good option. Disaggregating what are assumed to be tame problems into their component parts, regardless of the actual problem type, often proves inadequate, as unintended and unforeseen consequences make clear.

Yet planning must occur regardless of problem type. Otherwise, dealing with problems becomes a process of trial and error with no means of agreement on assessing the solutions or even on what are the solutions. Klein considers—along with Rittel and Webber—that planning is an emergent process: Goals are clarified and revised as understanding of the problem grows.[218] He notes,

> Goals can be dynamic and can change completely as a function of changing circumstances. Goals can conflict with other goals in ways we can't anticipate or resolve in advance. Goals can carry implications we can't perceive or anticipate until events transpire.[219]

In terms of intelligence creation, this means that larger, strategic goals can—and perhaps must—emerge as sense is made of the problems under scrutiny. Thus, a tasking from an intelligence consumer changes as mindful sense is made of the tasking itself, of the resources that are available for understanding it, and the mix of actors involved.

Klein refers to this reflective problem planning as "flexible execution" or "Flexecution."[220] Within the framework of intelligence sensemaking, it provides a self-reflective process—at the individual and organizational levels—that monitors the goals and whether what is understood or being done is consistent with those goals, modifying those goals as understanding emerges. For example, in examining the situation in Cuba during the summer of 1962, the understanding of the intelligence professionals at the Refugee Processing Center in Miami developed as the summer progressed. A new understanding emerged of what the Soviet forces deployed to the island might be doing.

---

217 Gary Klein, "Flexecution as a Paradigm for Replanning, Part 2," *IEEE Intelligent Systems*, vol. 22, no. 5 (November/December 2007), 112. Cited hereafter as Klein, "Flexecution 2."

218 Klein, "Flexecution 1," 81.

219 Klein, "Flexecution 1," 81.

220 Klein, "Flexecution 2, 108.

Table 3. Classical Planning and Execution Versus Flexecution		
	Classical Planning/ Execution	Flexecution
End state	Known	Unknown
Preparation	Alternative courses of action Contingencies	Alternative goals and priorities Potential actions
Mode	Increase constraints and control	Fix/flex cycles
Prior plans	Useful	Often obsolete
Commander's intent	Fixed	Continually adjusted Shows goal priorities Shows trade-offs
Strategy	Management by Objectives	Management by Discovery
Accountability	Clear	Unclear

Source: Gary Klein, "Flexecution as a Paradigm for Replanning, Part 2," *IEEE Intelligent Systems*, vol. 22, no. 5 (November/December 2007), 112.

Intelligence planning took place as sense was being made of the situation, (finally) monitoring what they were observing and what it meant. Such deliberations apparently led two analysts to conclude that the indicators for strategic nuclear missiles deployed in Cuba might be valid, resulting in the U-2 overflight of 14 October 1962 and the "discovery" of the missiles.[221] Unfortunately, as has been noted, the intelligence professionals were not sufficiently flexible in their planning to consider that other types of nuclear missiles also might be (and in fact were) deployed on the island.

As summarized in table 3, flexecutive planning seems ideally structured for making sense of wicked problems and taking advantage of the peculiar capability that intelligence has to initiate information actions and then clandestinely determine the adversary's reactions to it. Intelligence professionals are well placed to learn of changes in planning or strategy on the part of adversaries as well as of their own decisionmakers. One can never be certain that all potential planning options are known, but by focusing on "alternative goals and priorities" to which an adversary might migrate, and the potential actions both at the onset of the sensemaking process and as

221 Garthoff, "US Intelligence," 23.

a part of an ongoing, mindful critical reflection, one comes to understand the alternative goals and priorities of one's own actors as well as those of the adversary.[222]

Foraging

Hunting and Gathering

If, as Baumard asserts, "Intelligence, a continuous human activity, gives sense to the stimuli received from the environment [then] these stimuli [must] be passively or actively sought."[223] This requires hunting and gathering. They comprise foraging, which in turn refers to "a wide search over an area in order to obtain something."[224] Whether it describes birds seeking life-sustaining berries, bees scouting for pollen, or people searching for information, foraging describes how animals go about satisfying their needs. For intelligence professionals, foraging describes the means by which the raw materials needed to notice and make sense of phenomena are acquired.

An apt analogy for the foraging activities of intelligence professionals can be drawn from anthropology, where the activities of the hunter-gatherer have been immortalized. In nonagricultural societies people both hunt for specific game and take advantage of what the local environment provides.[225] Similarly, intelligence professionals may seek specific information, often tasking collection systems as part of the search. They also take advantage of existing repositories of information. Neither approach is wholly satisfying nor provides for all of the sensemaker's needs all of the time. However, without the basic act of foraging there can be no sensemaking as there is nothing from which to make sense.

Information foraging is a rich subject about which Peter Pirolli has done extensive work, some of it sponsored by the Intelligence Community's Novel Intelligence from Massive Data research project funded by IARPA's predecessor, ARDA (Advanced Research and Development Activity). Known

---

222 Within the domain of wicked problem consideration there is a means, known as morphological analysis, that may come close to at least identifying all possible planning options. Invented and developed by astrophysicist Fritz Zwicky, the paradigm has been further developed by the Swedish Morphological Society (URL: <www.swemorph.com>, accessed 10 October 2010), and for the U.S. Government by William N. Reynolds, Least Squares Software. Combined with a model of Flexecution, it seems a promising approach for intelligence (re)planning.

223 Baumard, "From Noticing to Making Sense," 31.

224 *New Oxford American Dictionary*, Apple Computer Edition, 2005, entry under "foraging." Cited hereafter as *New Oxford American Dictionary*.

225 This remains such a culturally (and perhaps psychologically) essential human activity that the practice remains part of seasonal life in modern post-industrial societies.

as "Information Foraging Theory," Pirolli's work makes use of the optimum foraging strategies of animals as a basis for assessing the human acquisition of information. Underlying information foraging theory is the idea that "humans actively seek, gather, share, and consume information to a degree unapproached by other organisms" and therefore, "when feasible, natural information systems evolve toward stable states that maximize gains of valuable information per unit cost."[226]

Pirolli's research and experimentation devotes special attention to foraging efficiency. Efficiency derives from optimizing the time necessary to achieve a goal, the quality of the achievement, and the satisfaction obtained in doing so.[227] In application to the human information foraging scene, the theory becomes "a rational analysis of the task and information environment that draws on optimal foraging theory from biology and…a production system model of the cognitive structure of [the] task."[228]

Toward a Practice of Intelligence Foraging

Developing an optimal foraging model for information acquisition requires the subject to consider whether to remain at a source that provides a superabundance of information of questionable value, or to seek another, more valuable, source.[229] Pirolli and colleague Stuart Card observe that for human foragers, this involves "a tradeoff among three kinds of processes": exploring, enriching, and exploiting.[230]

These three foraging steps will not seem foreign to traditional intelligence practitioners. "Exploring" is a breadth activity whereby a sensemaker broadly examines a wide variety of information that may or may not be relevant to the issue. The premise is that when one considers a broad variety and volume of data, there is less opportunity to miss "something novel in

---

226 Peter Pirolli and Stuart Card, "Information Foraging," *Psychological Review*, vol. 106, no. 4 (October 1999), 643. Cited hereafter as Pirolli and Card, "Information Foraging."

227 Peter Pirolli, *Information Foraging Theory: Adaptive Interaction with Information* (Oxford, UK: Oxford University Press, 2007), 5. Cited hereafter as Pirolli, *Information Foraging Theory*.

228 Pirolli, *Information Foraging Theory*, 5.

229 In the animal kingdom this quantifiable function is known as the "Conventional Patch Model." It was developed by David W. Stephens and John R. Krebs, *Foraging Theory* (Princeton, NJ: Princeton University Press, 1986); and based on work by Eric L. Charnov, "Optimal Foraging: The Marginal Value Theorem," *Theoretical Population Biology*, 9, no 2 (April 1976): 129-136. Referenced in Pirolli, *Information Foraging Theory*, 7-8.

230 Peter Pirolli and Stuart Card, "The Sensemaking Process and Leverage Points for Analyst Technology as Identified Through Cognitive Task Analysis," paper presented at the 2005 International Conference on Intelligence Analysis, Vienna, Virginia, 2-6 May 2005, URL: <https://analysis.mitre.org/proceedings_agenda.htm#papers>, accessed 11 March 2009. Cited hereafter as Pirolli and Card, "Sensemaking Process."

the data."[231] Speaking in traditional intelligence terms, exploring is like reconnaissance. By contrast, "enriching" is a depth activity. Here the sensemaker identifies areas of interest and focuses attention on those areas. As Pirolli and Card note, this is "a process in which smaller, higher-precision sets of documents are created."[232] Reconnaissance has become more narrowly focused, but highly targeted "surveillance" is not yet in play. Finally, the practitioner "exploits" the results of foraging by thoroughly examining what is found and extracting information as needed. This activity extrapolates from tacit sensemaker behaviors and information-based patterns to create hypotheses about what the information means. At this point, foraging evolves to sensemaking.

The appropriate amount of exploration depends on the context. However, there appears to be a limit after which more information does not increase accuracy although it does increase the sensemaker's overall confidence. One example of this phenomenon was discovered by Paul Slovic in an experiment with odds makers who, when predicting the winners of horse races, were not significantly more accurate if they used 40 variables or only 5 (out of sets of 88 possible variables).[233] What Slovic additionally observed, however, is that the odds makers' confidence did increase directly with the number of variables considered.[234] Slovic's findings about accuracy and confidence are reproduced in Figure 2.

The discussion of how much exploration is needed is germane because in the Pirolli-Card framework the sensemaker may believe she controls the amount of foraging. In a sense this is true. The sensemaker will stop foraging once she believes she has what she needs. But how much information is sufficient? Slovic's results and Heuer's subsequent discussion suggest that practical sufficiency is achieved at lower levels of exploration than expected.[235]

Further, contrary to the beliefs of the sensemaker, it is often information itself that controls the processes. Intelligence professionals are overwhelmed with more and more information that arrives faster and faster and may be valuable for shorter and shorter periods of time. This information flood challenges the sensemaker to efficiently find the information needed in order to make sense of the phenomena or issue under scrutiny in a timely

231 Pirolli and Card, "Sensemaking Process."

232 Pirolli and Card, "Sensemaking Process."

233 Paul Slovic, "Behavioral Problems of Adhering to a Decision Policy," Paper presented at the Institute for Quantitative Research in Finance, Napa, CA, May 1973. Cited hereafter as Slovic, "Behavioral Problems."

234 Slovic, "Behavioral Problems."

235 See Richards J. Heuer, Jr., *The Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999), 54. Cited hereafter as Heuer, *Psychology*.

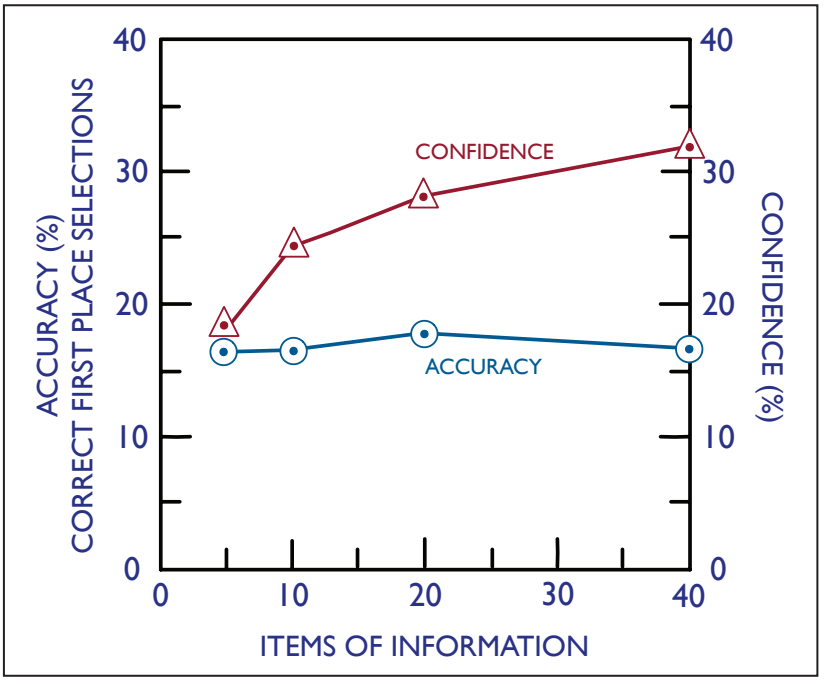


Figure 2. Changes in Predictive Accuracy and Confidence as Available Information Increases. The accuracy of odds-makers' predictions about horse races does not increase as they consider more items of information although their confidence in those predictions does.

Image Source: Richards J. Heuer, Jr., *The Psychology of Intelligence Analysis* (Washington, DC: Center for the Study of Intelligence, 1999), 54. The illustration reproduces one originally presented by Paul Slovic in 1973. See Slovic, "Behavioral Problems."

manner. Does one need to peruse all the information received? Would a different source be more productive by providing more focused information? These are examples of the difficult questions the sensemaker must consider. Compounding her deliberations further is the fact that she must answer this question in foresight; hindsight is too late.

Referring to the animal foraging analogy that underlies information foraging theory, one asks, is the nutrition gained of sufficiently low quality (even though there is lots of it) to justify seeking another source of unknown (but possibly higher) nutritional value? Failure to make the right decision may result in starvation. For the sensemaker this means she may never find what she needs. An implication is that her lack of information may contribute to an error leading to a catastrophic failure. To make such a decision wisely requires something she currently lacks: a practice of foraging. Such a

practice puts her, not the information, in control of foraging practice. It provides her with a systematic means of reducing her uncertainty.

Foraging practice begins with an understanding of what it is the sensemaker seeks to know, the foraging resources available, and the urgency of the issue. But how can an intelligence sensemaker know what to look for? To what degree does she need to explore, enrich, or exploit the information? Further, how does she know if she is getting what she needs?

A first step is to think critically about the issue itself and the resources needed. Using a metacognitive, process-focused critical-thinking model such as that adapted from Richard Paul, Linda Elder, and Gerald Nosich, the practitioner can dissect the issue and her thinking on the issue.[236] She makes assumptions explicit, explores relevant points of view, starts to consider the ramifications of the issue, and she asks important questions about what resources will best inform her about the issue; she considers the context in which she is working, and ponders the alternatives to her reasoning about where and how to forage. This critical thinking defines her foraging activities. She may engage in all three strategies at once or at different times as she engages in the analyses that produce her syntheses and the interpretations necessary to generate knowledge. A well-developed understanding of exploited information may direct her back to do additional exploring or enriching (or both).

In intelligence foraging as it traditionally has been practiced, there is a tendency to linger at a fruitful source rather than to explore elsewhere for the required information. This is a function of the confidence one gains in those systems that previously have supplied information, and the available tools for ferreting out the information. The danger, of course, is that the practitioner may limit the information she acquires and the relevant perspectives it informs. If, for example, the practitioner has a belief that two parties in whom she has an interest communicate via one means and she can acquire technical collection that captures the communications via those means, she may ignore the fact that they also use other methods to communicate. She may subsequently fail to task systems that collect those other communications in the belief that what she is getting suffices. Should the parties suspect that their communications are being targeted, they may engage in deceptive practices over that collected means and use the other non-collected methods for their real exchanges.

---

236 Moore, *Critical Thinking*, especially chapter 1. Also see: Richard W. Paul and Linda Elder. *Critical Thinking: Tools for Taking Charge of Your Professional and Personal Life* (Upper Saddle River, NJ: Prentice Hall, 2002); and Nosich, *Learning to Think Things Through.*

Foraging Challenges

Ongoing research at University College London offers a view of how younger sensemakers likely search for information. The researchers report that people foraging for information spend four to eight minutes viewing each resource.[237] Thus, a great many resources may be consulted but none of them very deeply. Within the context of intelligence, such foraging strategies may facilitate broad searches but leave open the question of whether deeper searches are also accomplished. As Nicholas Carr observes in the July/August 2008 *Atlantic*, Internet search strategies, as epitomized by the operation of search tools such as Google, will put in place a new behavior of foraging and consuming information. Carr notes:

> It is clear that users are not reading online in the traditional sense; indeed there are signs that new forms of "reading" are emerging as users "power browse" horizontally through titles, contents pages and abstracts going for quick wins. It almost seems that they go online to avoid reading in the traditional sense.[238]

From the perspective of actually making sense of issues, these strategies imply that the manner in which issues are understood is also likely to change. Are such new foraging practices suitable to meet the needs of intelligence consumers? Will they be better at satisfying those needs for knowledge than the paradigm previously practiced?

An additional challenge with information foraging is that if the practitioner misses the opportunity to acquire something, it may never again be obtainable. Like the elements of a fleeting interpersonal conversation, the original foraging behavior, if left un-captured, can never be recaptured. Indeed, there may be no indications that such a conversation even occurred.

A further consideration for the practitioner is the "self-marketing" of the information. Vivid stories market themselves much better than do flat ones. Exploited information that supports a favored hypothesis may be preferred over information that does not; an unfortunate reality is that little motivation remains for further exploration. The practitioner is human—she will not likely have a truly agnostic attitude about what she seeks and why.

Compounding this is the idea that sources and means for foraging are self-protective. For example, there is a presumption that sources will continue

---

237 Ian Rowlands and others. "The information Behaviour of the Researcher of the Future (Google Generation)," URL: <http://www.ucl.ac.uk/infostudies/research/ciber/downloads/ggexecutive.pdf>, accessed 27 May 2010.

238 Nicholas Carr, "Is Google Making Us Stupid?" *The Atlantic*, Online Edition (July/August 2008), URL: <http://www.theatlantic.com/magazine/archive/2008/07/is-google-making-us-stupid/6868>, accessed 27 May 2010. Cited hereafter as Carr, "Google."

to communicate via specific means. The methods that capture those communications and the people that support them tend to seek justification. Assets may be kept active after their usefulness expires. The practitioner returns to the same sources over and over because they have been useful in the past and such attention helps keep those sources actively collecting.

Critically assessing what she is doing is one way the sensemaking practitioner may be able to overcome these limiting tendencies. By constantly asking herself how she is thinking about the issue, what she seeks, other perspectives, her assumptions, as well as relevant concepts such as self-deception or adversarial deception, the practitioner may diminish the impact that her preferences play on her foraging decisions.

Another part of this critical assessment is the consideration of the costs of foraging. As Herbert Simon notes,

> What information consumes is rather obvious: it consumes the attention of its recipients. Hence a wealth of information creates a poverty of attention, and a need to allocate that attention efficiently among the overabundance of information sources that might consume it.[239]

Simon in fact anticipates the conclusions of Carr: The superabundance of information available on the Internet (and elsewhere) creates a "poverty of attention" to any one source. Rather, people skim across a great many sources.[240]

Questions the sensemaker must ask include whether or not she can afford to explore an issue's information field further. She needs to consider how certain she is that she has sufficient exploitable information to make sense of the issue. Further, if the issue is inadequately understood, opportunism may affect the foraging as a hunting analogy illustrates. A predator may go out seeking one type of prey and find none of it *but* there may be an abundance of some other kind of game. Within the context of intelligence such opportunism may or may not be appropriate (or even legal) when a technical system or an asset is tasked to provide information for intelligence. Lacking the desired information, a human source might opportunistically substitute what might be perceived as desired or desirable, even if it is not closely related to the issue at hand—or for that matter, even "true." It is used because it satisfices for the immediate term.

---

239 Herbert A. Simon, "Designing Organizations in an Information-Rich World," in Martin Greenberger, ed., *Computers, Communications, and the Public Interest* (Baltimore, MD: Johns Hopkins University Press, 1971), 40-41.

240 Carr, "Google."

Harvesting[241]

A special case of foraging involves "harvested" information. Technical agencies that field systems to gather information also can be characterized by a different model, that of harvesting. The systems employed simply harvest that which lies within their purview, then process it and store it in silos—data repositories from which sensemakers subsequently must forage.[242] Such systems are efficient at creating broad collections; they tend to be inefficient and unreliable when very narrowly focused. Thus, *directed* rather than broad collection of specific phenomena is needed.

Technical collection systems tend to provide—even in the negative—what sensemakers want to find. This can create a potentially dangerous confirmation of an idea that may be invalid. This tendency is exacerbated in the post-Cold War world. Although previously, certain intelligence targets did remain relatively unchanged over considerable periods of time, this is no longer the case.

The harvesting system automatically explores a subset of a larger reality based on a collective agreement among sensemakers that the subset is relevant. The sensemakers subsequently enrich their knowledge and in a best-case situation can exploit the information to provide themselves with the necessary information to make sense of the issue. A challenge is that it is impossible to collect everything. Yet, uncertainty about whether or not one *really* has collected what is necessary remains unresolved. While some technical systems are more usable for "random" exploration than others, most require a preexisting idea about what one seeks. Such preconceptions limit exploration.

Automated retrievals from information repositories typically provide sensemakers with what they believe to be the needed and relevant information—in short, their evidence. The evidence pertaining to specific issues arrives at the sensemaker's desk and reports are issued. At first, the evidence is carefully scrutinized and the system that provides it assessed. As the process repeats, however, as it certainly did in the Cold War era, complacency may set in. Critical assessment of *quality* and *quantity* may cease. And, one day, the evidence that a specific sensemaker requires no longer appears. The reporting on that specific issue withers. If sufficient evidence valuable to *other* sensemakers still is harvested, the value of the continued tasking of the system may

241 The author is indebted to Martin Krizan for raising this idea.

242 It should be noted that "reaping" and "threshing" both manipulate the collected information into usable formats. The processed information must be compatible with U.S. law and specific agency procedures for handling such information.

not be questioned. The failure is not noticed and may even be rationalized—perhaps as a failure to forage adequately—*if* it is noticed in the first place. Even when it is noticed, it may be impossible to determine *why* it occurred. Finally, no amount of foraging can discover valuable information if it has not been collected by some system—human or technical—in the first place.

Marshaling

What can be done to revolutionize the way information foraging is accomplished so as to overcome or at least mitigate these problems? Some answers lie in an understanding of marshaling. Part of the sensemaker's practice is to turn foraged and gleaned information into evidence. Doing so requires sifting and other organizing activities to determine which information is relevant to the issue. This is a broad activity, for if the issue has multiple explanations or future possibilities, then evidence will be information relevant to any, many, or even all of those explanations or possible outcomes. In order to make that determination, the sensemaker will need to have identified what those alternatives are and to have collected information (both disconfirming and confirming) about them.[243] This may require foraging from additional resources with all the attendant challenges discussed above. Conceivably this could overwhelm the sensemaker. However, questions such as "if this alternative were true, what would be the evidence for it?" can lead one to identify what she needs to know. Then asking whether or not she sees it, or where she might forage for it (and can do so), starts the process of marshaling. This activity represents a change from traditional practices because the intelligence professional goes beyond what she knows into what she knows she does not know.

Understanding

If we presume that foraging has yielded relevant and valuable information—evidence—on the issue under study, the next step is to determine what it means. This is the heart of sensemaking: evidence is dissected, reassembled

243 Disconfirming alternative explanations (or hypotheses) is one means of avoiding confirming a favored (and possibly wrong) possibility. This disconfirmatory approach is one of the strengths of Richards Heuer and Morgan Jones' independent work with hypothesis testing (Heuer calls it alternative competing hypotheses). How effectively this approach actually works is subject to debate. Another challenge is to define foraging strategies that yield disconfirming (i.e. negative evidence). An absence of evidence is insufficient. See Heuer, *Psychology*, Chapter 8, and Morgan Jones, *The Thinker's Toolkit* (New York, NY: Three Rivers Press, 1995), 178-216. For discussion about whether or not the method effectively disconfirms, see Brant A. Cheikes, Mark J. Brown, Paul E. Lehner, and Leonard Adelman, *Confirmation Bias in Complex Analyses*, Mitre Technical Report, MTR 04B0000017 (Bedford, MA: Mitre, 2004). Cited hereafter as Cheikes and others, *Confirmation Bias*.

with other evidence, and its meanings determined by analyzing, synthesizing, and then interpreting the evidence.

Analyzing

The intelligence issue or question itself requires analytic scrutiny. Different foraging disciplines represent different points of view. In other words, signals intelligence or SIGINT; human sources embodied in HUMINT; images and geospatial data (known as GEOINT), and others tell different stories about a phenomenon. Each story requires dissection. Similarly, within a foraged source, the different perspectives of the sensemaker require dissection. For example, is the sensemaker focusing on individual actors, the actions of a collection of actors, the beliefs that guide the activity, or the processes that determine the actions of the collective?[244]

The disaggregation of each of these perspectives and their associated stories provides a rich brew for sensemaking. For example, in the Cuban Missile Crisis of 1962, such a dissection reveals the intentions and underlying beliefs of the principal actors (Castro, Kennedy, and Khrushchev), as well as the roles and procedures of their larger collectives, in this case the Cuban and Soviet governments (specifically the Soviet Politburo and General Staff) as well as Kennedy's Executive Committee (EXCOM) and indeed the much larger American political collective. However, as rich as these stories become, they remain inadequate in assessing what is likely to happen. Dissecting the evidence is insufficient. Pulling the pieces together becomes the next step.

Synthesizing

Synthesizing is "the combination of ideas to form a theory or system."[245] Even as the intelligence professional analyzes the individual pieces of information, they are synthesized into a mental picture of the larger issue. Pieces of information are implicitly combined even when the sensemaker works within the yield of a particular foraging discipline or within a frame or reference. Such synthesis drives further foraging and analysis.

Synthesis needs to be explicit. In the example developed above, the intelligence professional is required to synthesize the differing trajectories

---

244 These four groups form the basis of a novel sensemaking approach developed by Monitor 360 for the National Security Agency and incorporated into a course on multi-frame sensemaking. As characterized in the course, the four groups or frames are the "empowered actor," "cooperation and conflict," "beliefs and affiliations," and "roles and procedures." The author is a champion of this approach, and worked with the senior course developer, Bruce Chew, in creating the course.

245 *New Oxford American Dictionary*, Apple Computer Edition, entry under "synthesis."

of the three principal actors, considering how their beliefs harden or soften their positions and how they are vulnerable to the actions, influences and processes of the groups. Doing so in a systematic fashion leads the intelligence professional to new insights about the situation: what is going on in Cuba and (from the U.S. perspective) what to do about it.

Interpreting

Issues can be dissected and reconstructed in a variety of ways, creating different meanings. Sense must be made of these different meanings. Interpreting, or "the action of explaining the meaning of something," is another component of sensemaking.[246] We may say that whereas analysis and synthesis establish the *what*, interpretation establishes the *so what*.

Depending on the frameworks involved, the interpretations of common information vary widely, as the above referenced experience of London subway bombing victim Rachel North illustrates. An evolving practice within intelligence of establishing competing teams of intelligence professionals to develop different aspects of an issue is an example whereby differing interpretations compete in an effort to establish "ground truth" about issues. A revolutionary approach to sensemaking now being undertaken by analysts from DIA, State, and CIA, is to engage in "adversarial briefing" of principals, where briefers adopt opposing perspectives for a thorough airing of the issue, complete with the participation of the principals themselves.

Communicating

New models of knowledge transfer recognize change in both message and medium. Social networking, peer-reviewed shared multimedia, and interactively blogged communications are examples of these new mediums. The message is short and subject to change by different contributors. Authority is based on consensus. The distinction—if it exists at all—between formal and informal communication is blurred. There are dangers here as authority and truth are no longer necessarily linked. One risk is that the "wisdom of a crowd" can in fact be the "madness of a mob"—a phenomenon occurring in both the public arena and within the IC's blogosphere. In both arenas the loudest voices strive to bludgeon into silence those who would disagree, all the while advancing their egocentric or sociocentric positions. Scientific knowledge and empirical facts matter little in such cases. The danger in both

246 *New Oxford American Dictionary*, Apple Computer Edition, entry under "interpretation."

arenas is, of course, that people make poor decisions based on information that later proves to be false.[247]

However, communications within the Intelligence Community remain firmly embedded in traditional formats of printing and briefing. It is true that blogging and informal communications are utilized, but these are used by intelligence practitioners to discuss the issues they make sense of *before* they craft their traditionally formatted assessments, briefings, and reports. The ultimate Intelligence Community report, the President's Daily Brief, remains primarily a hard copy document. While it has been updated incrementally over the years, the presentation remains similar to the summary that was nicknamed "Truman's Newspaper."

As has been noted, newer Intelligence Community directives provide for presenting alternative hypotheses as well as documenting confidence levels in sources and in intelligence assessments. Is this guidance sufficient and valid for sensemaking? In summarizing the "introspective works responding to…intelligence failures," Charles Weiss agrees that intelligence practitioners' failures include a lack of proper attention to hypotheses and data collection efforts that are contrary to what they regard as the most likely interpretation of available information."[248] One danger is that the very judgment about which the sensemaker is least confident might be the one that turns out to be correct. The fallacy of depending on the communication of confidence levels relates to the fact that each assessment or report only fills in some unknown portion of the gaps in the sensemaker's and policymaker's knowledge.

Presenting a novel hypothesis and interpreted argument about which one is uncertain, along with an assessment based on a more likely premise, also carries dangers. A policymaker might disregard the alternate possibility because of the declared lack of confidence (which might stem merely from a lack of evidence) and choose the evidentiarily better-supported hypothesis.[249] Here, a carefully considered, standardized metric of uncertainty could provide one means of assessing and communicating confidence independently

---

247 The "Swift Boat" controversy of 2004, the matter of autism-caused vaccines, and the uncivil discourse between the major political parties are several non-intelligence examples. These are different from debates, which advance knowledge through open discussion. These are about having one's way. Whoever can shout the longest and loudest wins. See also Peter Miller, *The Smart Swarm: How Understanding Flocks, Schools, and Colonies Can Make Us Better at Communicating, Decision Making, and Getting Things Done* (New York, NY: Penguin Books, 2010), chapter 5. Miller explores the transformation of the crowd to a mob, as well as the self-destructive behavior of the mob, through the example of locusts.

248 Charles Weiss, "Communicating Uncertainty in Intelligence and Other Professions," *International Journal of Intelligence and CounterIntelligence* vol. 21, no. 1 (Spring 2008), 57-58. Cited hereafter as Weiss, "Communicating Uncertainty."

249 Weiss, "Communicating Uncertainty," 62.

from the sensemaker. Weiss suggests that either Kent's scale[250] or its more recent instantiation by the Office of the Director of National Intelligence offers an appropriate means by which the uncertainty could be systematically captured.[251] The challenges inherent in such metrics are twofold. First, the evidentiary statistics necessary for their use are "typically unavailable to intelligence analysts—or it they are available, must be based on small samples of past events."[252] Additionally, scoring the conclusions from such small samples across production lines and even from day to day by a single intelligence professional can be observed to be inconsistent. Steve Rieber discusses calibrating sensemakers as a solution.[253] To date no such strategy has been implemented.

Peer-reviewed, discussed and argued findings published in blogs (as a formal means of communicating) would be a novel means of communicating results. If they are readily available to the policy community, they would enhance the capabilities of intelligence practitioners and policymakers alike to collaboratively make sense of the issues that policy faces. Intelligence could truly speak truth to power and policy could speak truth to intelligence. As an alternative communications medium where body language and other nonverbal cues can be read, the adversarial briefing initiative mentioned earlier offers an intermediate solution to the problem of communicating intelligence needs and perspectives.

At the same time, the blogosphere certainly provides an effective locus for discussion of developments surrounding ongoing issues. This is manifest in the IC's implementation of "A-Space" or Analysts' Space, a blogosphere where intelligence professionals can communicate among themselves regarding topical and methodological issues.[254] This new model for managing intelligence practitioners that respects their expertise and capabilities is an integral part of the ongoing revolution in communicating intelligence. A useful future step might be the inclusion of the consumer as part of the discussions; such a step would truly be revolutionary.

---

250 Sherman Kent's estimative probability scale appears in *Sherman Kent and the Board of National Estimates*, Collected Essays edited by Donald P Steury (Washington, DC: Center for the Study of Intelligence, 1994), 137. It is reproduced in modified form in Heuer, *Psychology*, 155.

251 Weiss, "Communicating Uncertainty," 61.

252 Weiss, "Communicating Uncertainty," 60-62.

253 Steven Rieber, "Intelligence Analysis and Judgmental Calibration," *International Journal of Intelligence and CounterIntellgience*, vol. 17, no. 1 (Spring 2004): 97-112.

254 Ben Bain, "A-Space Set to Launch this Month," *Federal Computer Week*, 3 September 2008, URL: <http://fcw.com/articles/2008/09/03/aspace-set-to-launch-this-month.aspx>, accessed 15 June 2010.

In the end, how these actors actually go about understanding the issues they consider is a complex process involving both the foraged and marshaled evidence as well as the beliefs and assumptions of the parties involved. Making sense of this requires both deliberative reasoning and intuitive approaches. Exploring how this works is the subject of the next chapter.

CHAPTER 5
A Practice of Understanding

David T. Moore and Robert R. Hoffman

We begin this chapter by considering intuition, trying carefully to define this nebulous term, and exploring the benefits and hazards of intuitive judgments. In order to accomplish this, an understanding of exactly what is meant by the similarly nebulous term 'judgment' is also needed. We develop our position from the work of Daniel Kahneman and Gary Klein as we explore skill-based and heuristic-based intuitive judgments and how they affect forecasting.[255]

Judgment in intelligence sensemaking, as in a number of other domains, likely improves as one progresses to higher levels of proficiency and expertise. However, prediction is both difficult and inherently unreliable because events of different kinds vary considerably in their inherent predictability. A common view is that prediction has these three features:

- It is the act of forecasting a specific future occurrence,
- It has some associated degree of probability and/or confidence, and
- It is linked logically to one or more specific courses of action that the predictor might take to achieve one or another specific goal.

We believe that another paradigm for shaping how we think about prediction is needed, along with fresh terminology. We present a view centered on the notion of "anticipation of ranges" and the concept of the "course of action envelope" as we begin to envision an alternative model of the phenomenon. We turn next to the implications of intuition and predictability for intelligence sensemaking. We conclude by looking ahead at some preliminary research into how the circumstances for sound reasoning may be improved, and we raise some questions about future directions for the Community.

Intuition

It is difficult to wrap appropriate words around the concepts that are at hand, thus care should be taken to make certain distinctions. Sometimes, judgments can be rapid, non-conscious, non-deliberative, and almost seem as if they are immediate perceptions and feelings rather than judgments. These

255 Kahneman and Klein, "Intuitive Expertise."

immediate attitudes can blend seamlessly into more deliberative or conscious reasoning, which in turn can, even if fleetingly, maintain the emotion and immediacy normally associated with intuition. Thereafter, we might say that purely deliberative and non-intuitional thinking might transpire. None of these distinctions is clear-cut in the social science approach to mental phenomena or in the annals of philosophy.

The process of intuitive thinking refers—according to psychologist David Myers—to the ability of individuals to fly "through life mostly on autopilot" even as they function effectively.[256] Neurologist Robert Burton observes this phenomenon in the actions of batters who can hit a ball (or miss it) in advance of their being able to consciously perceive it.[257] Burton also highlights a danger of such non-conscious thinking: People can misinterpret the input, leading us to think twice about relying on intuition for important decisions.[258] After all, as in the batter's case, it seems that intuition-based accuracy is limited to extremely rapid events.

At the same time, in fear and flight behavior, a certain level of inaccuracy can be tolerated. If early hominids misinterpreted, for example, the presence of certain shadows in the tall grass and reacted by running away, and the shadows were in fact benign, then the error had few consequences. Similarly, while one's "gut" may advise one not to get into a particular elevator late at night, people nonetheless tend to board the next one. Is there some stimulus of which one is not consciously aware—perhaps a shadow in the elevator—of someone who might be a mugger or worse? If one listens to one's "gut" and does not get on the elevator car, one will never know. Consequently, one will rationalize, "while I may have been wrong, at least I did not get mugged (or worse)."[259]

Intuitive, or, as it is sometimes called, *automatic* thinking forms the basis for much of our personal sensemaking.[260] It allows us to process

---

256 David G. Myers, *Intuition: its Powers and Perils* (New Haven, CT: Yale University Press, 2002), 16. Cited hereafter as Myers, *Intuition*.

257 Robert A. Burton, *On Being Certain: Believing You Are Right Even When You're Not* (New York, NY: St. Martin's Press, 2008), 75. Cited hereafter as Burton, *On Being Certain*.

258 When and how we intuit accurately (and inaccurately) is one of the themes of this chapter.

259 Only if one gets on the elevator, does not get mugged, travels safely to the desired floor, and then safely exits the elevator does one know that the instinct was incorrect. And even then, one merely has one anecdote's worth of experience contrary to that intuition. That nothing untoward occurred in this *specific instance* is no guarantee of the outcome in any future situations.

260 See Douglas J. Herrmann, and Roger Chaffin, "Memory before Ebbinghaus," in David S. Gorfein and Robert Hoffman, eds., *Memory and Learning: The Ebbinghaus Centennial Conference* (Hillsdale, NJ: Erlbaum, 1982), 35-56 and George A. Miller, "The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information," *Psychological Review*, vol. 63 (1956): 81-97. Cited hereafter as Miller, "Limits."

complex inputs that far exceed the "span of immediate apprehension" of approximately seven "chunks" or elements that individuals can consciously process in working (or short-term) memory.[261] Such thinking, for example, explains how people (mostly) drive successfully. Recent research revealing a correlation between cell phone use (especially texting) and accidents leads one to extrapolate that attention-requiring activities such as engaging in professional-level office conversation or dialing and conversing while mobile respectively impede otherwise effective automatic activities such as ten-finger typing or absent-mindedly but safely driving an automobile. In one study sponsored by the British Royal Automobile Club Foundation's Transport Research Laboratory, researchers found that texting while driving contributed to impaired driving more than either moderate alcohol or cannabis consumption.[262] From these and other similar studies it becomes clear that conscious reasoning can distract and thus decrease the effectiveness of "automatic thinking," leading to flawed and sometimes fatal decisions.

With other combinations of activities, people can simultaneously and very successfully perform more than one task. Many people are able, for instance, both to chop vegetables and converse casually. It seems that the mechanics of these two simultaneous activities are more automatic than deliberate. Further, we would expect that driving and conversing emotionally—arguing—would impair one's ability to negotiate traffic, for arguing requires deliberation, whereas the usual affective responses in conversation can be very rapid, or "pre-cognitive." In sum, humans are limited with respect to their mental resources for conscious and non-conscious thinking when engaged in complex tasks.[263] Psychological research has shown that with extensive practice and training one can learn to perform two tasks at once, even apparently incompatible tasks such as taking dictation while reading.[264] On the other hand, in most day-to-day "multitasking," performance generally suffers, even

---

261 Miller, "Limits."

262 Nick Reed and R. Robbins, "The Effect of Text Messaging on Driver Behaviour," *Published Project Report PPR 367*, RAC Foundation Transport Research Laboratory, September 2008. URL: <http://www.racfoundation.org/files/textingwhiledrivingreport.pdf>, accessed 9 December 2009. This is but one of a number of similar reports. For a summary of research in this domain see Transportation Research Board of the National Academies, *Selected References on Distracted Driving: 2005-2009*. URL: <http://pubsindex.trb.org/DOCs/Publications%20from%20TRIS%20on%20Distracted%20Driving.pdf>, accessed 9 December 2009.

263 Given the distracting effect of conscious thought on non-conscious activity in cases such as driving and cell phone use, an interesting experiment would be to examine the distraction posed by non-conscious activities on conscious reasoning.

264 See Elizabeth S. Spelke, William Hirst, and Ulric Neisser, "Skills of Divided Attention," *Cognition*, vol. 4 (1976), 215-230; and Christopher A. Monk, J. Gregory Trafton, J. G., and Deborah A. Boehm-Davis, "The Effect of Interruption Duration and Demand on Resuming Suspended Goals," *Journal of Experimental Psychology: Applied*, vol. 14 (December 2008): 299-313.

for individuals of the Web generation who are widely believed to be skilled at multitasking.[265]

There is another side of intuitive reasoning that sometimes works in opposition to one's survival. Intuitively reasoned responses to stress are often highly focused and narrow. Laurence Gonzales notes that in such reactions "the amygdala…in concert with numerous other structures in the brain and body, help to trigger a staggeringly complex sequence of events, all aimed at producing a behavior to promote survival."[266] But, in many cases, behavior is also locked down. Citing the cases of Navy and Marine Corps pilots who fly their aircraft into the "round down" or stern of aircraft carriers as well as his own experience of nearly crashing while landing a private plane, Gonzales observed that other vital input becomes "irrelevant noise, efficiently screened out by the brain."[267] However, unless such input is accounted for, accidents happen and people die. Non-intuitive input, then, needs to be considered; however, it may take too long to accomplish.

Intuitive or automatic thinking is a survival mechanism.[268] Gonzales notes that such mechanisms "work across a large number of trials to keep the species alive. The individual may live or die."[269] But over time—and in reference to humans—generally more live than die, leading to evolution and the genetic transmission of the "reflex." If a particular set of behaviors confers a survival value, that set can become more widespread in the population. Seen in this light, unease at entering an elevator at night could be a modern instance of sensing shadows in the tall grass.

On a shorter time horizon, people use experience-based intuitive patterns or mental models. These patterns or models direct how situations are perceived and how they are responded to. Mental models provide

---

265 For recent work in this area see Paul Raeburn, "Multitasking May Not Mean Higher Productivity," NPR News: *Science Friday*, 28 August 2009, URL: <http://www.npr.org/templates/story/story.php/storyId=112334449&ft=1&f=1007>, accessed 21 February 2010. Raeburn interviews sociologist Clifford Nass about his work on multitasking. For more on Nass' work see Eyal Ophir, Clifford Nass, and Anthony D. Wagner, "Cognitive Control in Media Multitaskers," *Proceedings of the National Academies of Science, Early Edition*, vol. 106, no. 37, 15583-15587, URL: <http://www.pnas.org/content/106/37/15583.full>, accessed 18 March 2010 ; and Lin Lin, "Breadth-Biased Versus Focused Cognitive Control in Media Multitasking Behaviors," *Proceedings of the National Academies of Science*, vol. 106, no. 37 (15 September 2009): 15521-15522, URL: <www.pnas.org!cgi!doi!10.1073!pnas.0908642106 PNAS>, accessed 18 March 2010.

266 Laurence Gonzales, *Deep Survival: Who Lives, Who Dies, and Why* (New York, NY: W.W. Norton, 2003), 35-36. Cited hereafter as Gonzales, *Deep Survival*.

267 Gonzales, *Deep Survival*, 39.

268 See William James, *Principles of Psychology*, two vols. (New York, NY: Henry Holt and Company, 1890).

269 Gonzales, *Deep Survival*, 39.

rapid shortcuts to determining the nature of situations and the appropriate responses.[270]

The challenge is that some intuitive mental models can ill-serve the individual. They can be incomplete or can contain incorrect concepts. As Gonzales notes, they can impede our "ability to use working memory properly, to process new information from the world, and to integrate it with long-term memory. And there's plenty of evidence that while they're not always lethal, such lapses are perfectly normal and happen all the time."[271]

In a recent article, Daniel Kahneman and Gary Klein engage in a surprising collaboration to clarify the roles of intuition in human decisionmaking, particularly in the realms of expert judgment.[272] Their collaboration is surprising because Kahneman and Klein come from different communities of practice. That Kahneman, as a recognized leader in the "judgment under uncertainty" decisionmaking community, and Klein, as a recognized leader in the naturalistic decisionmaking movement, find they agree on intuitive expertise opens new partnering opportunities for adherents of both paradigms to seek other common ground, enhancing our understanding of decisionmaking and judgment.

Their shared concern is with how "skilled intuitive judgment develops with experience" and the nature of "the activities in which experience is more likely to produce overconfidence than genuine skill."[273] The authors note that the "judgments and decisions we are most likely to call intuitive come to mind on their own without evoking cues and of course without an explicit evaluation of the validity of those cues."[274] Intuition and intelligence sensemaking are linked by the very concept of judgment as developed by Kahneman and Klein.

We turn next to an examination of types of judgment, distinguishing between those that are skill-based and those that rely on "heuristics," or learning through personal discovery whether rules of thumb are valid shortcuts to understanding an issue. We then link this dissection of judgment to the work of intelligence professionals.

---

270 Gary Klein and Robert R. Hoffman, "Macrocognition, Mental Models, and Cognitive Task Analysis Methodology," in Jan Maarten Schraagen, Laura Grace Militello, Tom Ormerod and Raanan Lipshitz, eds., *Naturalistic Decision Making and Macrocognition* (Aldershot, UK: Ashgate Publishing Limited, 2008), 57-80.

271 Gonzales, *Deep Survival*, 79.

272 Kahneman and Klein, "Intuitive Expertise."

273 Kahneman and Klein, "Intuitive Expertise," 515.

274 Kahneman and Klein, "Intuitive Expertise," 519.

Types of Judgment

First we must clarify the meaning of "judgment." A judgment can be an observer's belief, evaluation or conclusion *about* anything—one can form a judgment about anything of interest, including one's own reasoning.[275] Judgment also describes a *process*, surely more than one kind of mental process, by which one reaches a decision. Judgment can be expressed as affective evaluation (example: That is a good thing), objective evaluation (It looks like a cat, but it is just a stuffed cat), or categorical assignment (My judgment is that this is a case of highway robbery). Judgment as process can also be described as apodictic, modal, or oral, among others.[276]

Kahneman and Klein relate judgment to intuition with these diverse examples:

> The firefighter feels that the house is very dangerous, the nurse feels that an infant is ill, and the chess master immediately sees a promising move. Intuitive skills are not restricted to professionals: Anyone can recognize tension or fatigue in a familiar voice on the phone.[277]

A standard approach to understanding a phenomenon invokes categorization. For example, judgment can be seen as taking one of two forms: skill-based intuitive judgment, and heuristic-based intuitive judgment.

Skill-Based Intuitive Judgments

A simple example of skill-based intuitive judgment is the act of parallel parking by an experienced driver. The experienced driver has repeatedly parked in a similar manner over years of operating a vehicle and has become familiar with its dimensions; also, parking spaces are fairly uniform in size. These factors lead to a likely successful conclusion—dent-free parking.

Examples of skill-based intuitive judgment also seem to occur routinely in sports where repetition facilitates learning. A particular move becomes a habit, a reflex, or as we would say, automatic. The author (Moore) has repeatedly and deliberately capsized and righted his kayak in a similar manner over years of paddling on the Chesapeake Bay, nearby rivers, and elsewhere. He is intuitively familiar with his boat, how it behaves under various circumstances, and what it can be made to do (its "affordances"). He is also familiar with the supporting capacity of various paddles, and the motions

---

275 See James McCosh, LL.D., *Intuitions of the Mind: Inductively Investigated* (London: UK: Macmillan and Company, 1882).

276 See Franz Brentano, *Psychology from an Empirical Standpoint*, Antos C. Rancurello, trans. (New York, NY: Humanities Press, 1973). Originally published as *Psychologie vom empirischen Standpunkte*, by Dunker and Humblot, Leipzig, Germany, 1874.

277 Kahneman and Klein, "Intuitive Expertise," 519.

of his body and paddle. The upshot of such skill-based practice is that in an emergency, the author does not have to deliberate about what to do. Instead, he *knows* how to position himself and "roll up," righting the kayak. In actuality, intuition allows him to paddle in such a manner that post-capsize action is typically unnecessary. He knows the things he can do with his own body, his paddle, and the kayak to prevent capsize—his own "effectivities."[278]

Successful skill-based intuitive judgment presumes "high-validity environments and an opportunity to learn them." such as those found in parallel parking and kayak rolling.[279] This process only works when the environment surrounding the issue "provides adequately valid cues," and the sensemaker "has time to learn those cues."[280] Kahneman and Klein note that in intuition of this sort, "[no] magic is involved. A crucial conclusion emerges: Skilled intuitions will only develop in an environment of sufficient regularity, which provides valid cues to the situation."[281]

In terms of intelligence sensemaking, successful intuitive judgment arises from the tacit knowledge of experts who assess "normal" (in Kuhnian terms) situations, or as has been discussed above, the tame, familiar or regularly occurring kinds of problems (although they may be quite complex). Situations involving state-based actors or others for whom events tend to follow from earlier, observable indicators are an example of environments suitable for the operation of skill-based, expert intuitive judgment.

Heuristic-Based Intuitive Judgments

Heuristic-based intuition relies on "rules of thumb" in order to make sense of situations.[282] Rather than making judgments based on deliberation, the experienced sensemaker can at times recognize when a case fits a nominal type; that is, it is similar in many respects to a well-known instance of the situation. Based on recognition that a given case fits a type, the practitioner knows immediately what principles to apply or actions to take. Heuristic-based intuition, as Klein and Kahneman define it, is rapid and automatic,

---

278 Michael Young, Yi Guan, John Toman, Andy DePalma, and Elena Znamenskaia, "Agent as Detector: An Ecological Psychology Perspective on Learning by Perceiving-Acting Systems," in Barry J. Fishman & Samuel F. O'Connor-Divelbiss, eds., *Fourth International Conference of the Learning Sciences* (Mahwah, NJ: Erlbaum, 2000), 299.

279 Kahneman and Klein, "Intuitive Expertise," 519.

280 Kahneman and Klein, "Intuitive Expertise," 520.

281 Kahneman and Klein, "Intuitive Expertise," 520.

282 The term "rule of thumb" has unclear origins in antiquity, likely related to the idea of using the thumb as a measurement device. In computer science and cognitive science, heuristic rules are distinguished from algorithms. The latter are known to give precise answers in finite time. A heuristic is any short cut that is not guaranteed to give precise answers, but takes less time than required to use an algorithm.

almost like skill-based intuition. There is no pause to reason through a decision or judgment, but there is an act of recognition. The sensemaker recognizes that actions learned or developed in one context—rules of thumb—are appropriate in another situation. Where the environment is sufficiently unstable so as to preclude recognition and learning of appropriate cues (or the time to do so is too short), heuristics operate similarly to make sense of the situation and offer solutions. Often accompanying such judgment is an "unjustified sense of confidence," a concept Kahneman terms the "illusion of validity."[283] Under such circumstances, the success of intuitive judgment in such conditions may be limited.

However, it should be noted that the combination of skill-based and heuristic-based intuition confers a benefit to mindful experts: a sense of when a case seems typical at first glance, yet there is something not quite right about it. While the less experienced person may be lulled into believing the case fits a certain type, expert decision makers react differently. They note some worrisome clue that raises questions. "Maybe this is not a typical case," they venture. Eventually they may come to see that the case is in fact atypical. So informed, they make a different judgment, sometimes in disagreement with other experts. As we will now see, intuition certainly becomes a part of the intelligence process when practitioners make, or fail to make, useful and accurate predictions.

The Question of Predictability

Some in the IC argue that the pertinent aspects of all intelligence problems can be adduced, "if we only knew more" or "had the right algorithm or method." However, we mislead ourselves if we believe that any messy problem can be resolved with a probability-juggling program. The authors are reminded of the observation, "There are the hard sciences and then there are the difficult sciences." It is both impossible and inappropriate to attempt to remake social and cognitive sciences into emulations of calculational physical sciences. If the reduction were possible, someone would have achieved it, or would have at least made demonstrable progress toward its realization, in the 200-plus years during which psychology and the other "social sciences" have called themselves "sciences." If reduction was appropriate, and we could get "the right information to the right person at the right time," we would not need that right person—"truth" would be self-evident.

By contrast, sensemaking is all about creating and recognizing proximate knowledge and meaning through human cognition. A useful question is not "How can cognitive work be automated?" but "In what ways and to what

283 Kahneman and Klein, "Intuitive Expertise," 517.

extent might technology and software amplify and extend the human ability to engage in cognitive work?" In other words, the unexpected happens, even on a large scale, as is illustrated by the inaccurate predictions offered by a number of books published in the 1995-2001 period that addressed the issues of the looming 21st Century and missed climate change—and more importantly from the U.S. perspective—the likelihood of attacks such as those by Al Qaeda on the World Trade Center and the Pentagon on 11 September 2001.[284]

The IC's flagship, publicly available forecasting reports, the National Intelligence Council's (NIC) quinquennial "global trends" reports, also missed the opportunity to bring attention to a "global war on terror," although effects of climate change did receive consideration in the report published in 2000.[285] Inclusion of this latter driver is not surprising considering that the NIC's brief examination of climate change occurred at least a decade into the discussion and debate about "global warming," suggesting that the phenomenon was known even if the impact was not clearly predictable. One could argue that the likelihood of a war on terror was also knowable. At least one intelligence adviser, Richard Clarke, warned of what would come to be known as the 9/11 attacks during the spring and summer of 2001; that is, prior to the events of that tragic day.[286] The fact that some people did anticipate these trends and events relates to a conclusion of Kahneman and Klein, namely, that "widely shared patterns of association exist, which everyone can recognize although few can find them without prompting."[287]

Interestingly, *The Atlantic Monthly* did warn in a speculative piece published during the summer of 2005 of a looming economic crisis.[288] It blamed the crisis in part on people using home equity to buy stocks—at least getting "right" the fact that the then-future 2009-2010 crisis was (at least in part) about real estate.[289] The real culprit—as has become clear—was the

---

284 Peter Schwartz's *The Art of the Long View* (New York, NY: Doubleday, 1996) is an example. An irony here is that previously Schwartz headed the forecasting (scenario planning) unit at Royal Dutch Shell, which was (at least according to Schwartz) often correct in their predictions. Schwartz, conversation with the author, September 2006.

285 National Intelligence Council, *Global Trends 2015: A Dialogue About the Future with Nongovernmental Experts* (Washington, DC: Government Printing Office, 2000), URL: <http://www.dni.gov/nic/NIC_globaltrend2015.html>, accessed 15 February 2010. It should be noted that climate change was already a discussed topic at the time.

286 As also did others according to Berkowitz (referenced above). While a failure to alert and warn was part of the tragedy, so was a failure to *believe and act*.

287 Kahneman and Klein, "Intuitive Expertise," 520.

288 See James Fallows, "Countdown to a Meltdown," *The Atlantic Monthly*, July/August 2005, URL: <http://www.theatlantic.com/doc/200507/fallows>, accessed 15 February 2010.

289 As seen from hindsight. Mr. Fallows had no way of knowing in foresight which parts of his speculative piece would come "true."

behavior of banking institutions, not individual investors. In both cases greed was a motivating factor.[290] However, the same *Atlantic* piece also speculated on the impending death of Fidel Castro, expected in 2008.[291]

Some examples of mindful, heuristic-based decision making, especially pertinent because they involve the thinking habits of senior U.S. civilian and military officials as well as of their strategic advisors, are discussed in Neustadt and May's *Thinking in Time*.[292] The authors point out that a sensemaker's awareness of historical decision making in even loosely analogous situations helps to keep at bay the further unsettling idea that the present circumstances constitute a "crisis." Even in the absence of politically or militarily identical precedents as a guide, they note that George Marshall, Chief of Staff of the U.S. Army, read history and possessed "the kind of mental quality that readily connects discrete phenomena over time and repeatedly checks connections."[293] Decisions, as informed at times by the IC, might benefit from Neustadt and May's recommendation that heuristic-based decisions can grow from "imagining the future as it may be when it becomes the past."[294] This advice would seem to be useful in making decisions on a strategic basis rather than a more tactical, reactionary plane. From a national intelligence perspective, where proactive decisionmaking in the face of impending change in the national security environment ought to reign supreme, Neustadt and May's heuristic advice about "thinking in time" becomes apt: "You may even [achieve] headway toward identifying changes that might be *made* to take place."[295]

However, like all strategies for framing and re-framing, caution is needed, perhaps especially in considering Neustadt and May's specific method of heuristic reasoning. An awareness that some current occasion or event repeats one that occurred in the past, or that the patterns bear some similarities or symmetries, can serve as either a flashlight or a blindfold. The pattern suggests where to look in finding evidence, but it might also prevent one from looking for other possibilities and particularly for the unique elements of the situation at hand. The characterization by some of the 1991 Gulf War as "another Vietnam" cognitively blinded them to the specifics of the

---

290 But greed, although a constant or enabling condition, is not a good explanation of cause.

291 As of March 2011, Castro still lives.

292 Richard E. Neustadt and Ernest R. May, *Thinking in Time: The Uses of History for Decision Makers* (New York: The Free Press, 1986). See especially chapters 13 and 14. Cited hereafter as Neustadt and May, *Thinking*.

293 Neustadt and May, *Thinking*, 252.

294 Neustadt and May, *Thinking*, 253-254.

295 Neustadt and May, *Thinking*, 259.

case at hand. Similarly, those who considered the second Gulf War as one that completed the first apparently missed key unique elements of that situation. Even so, there are instances when such reasoning is possible and valuable, particularly when expertise can be acquired and is useful.[296]

The two types of intuition suggested here—skill-based and heuristic-based—arise from a number of cognitive processes, including "the operations of memory."[297] While Kahneman and Klein disagree on the frequency and utility of non-skill-based intuitive judgment, they do agree that intuitive judgment may be limited in situations when the decisionmaker is either unskilled or the environment fluctuates irregularly and therefore cannot be learned. "Anchoring," which is the biasing of a judgment because of the framing of the initial question, and "attribute substitution," arising from replacing a difficult question with an easier one, are two contributors to such flawed intuitive judgments.[298]

If venturing predictions is too uncertain for intelligence professionals, what can be done? We address this in our next section as we consider in more detail both why intuitive predictions fail, and when they may succeed. We also present an alternative paradigm for assessing the future.

Thinking About Anticipating

Jurisprudence, clinical psychology, and economic forecasting are all examples of domains where accurate prediction is difficult or impossible, and it is not terribly clear what it means for a person to be an expert in any of those fields. In the realm of jurisprudence, studies of the low rate of successful intuitive predictions about future recidivism among paroled offenders serves as one of many pieces of evidence showing that even highly experienced professionals in certain domains may be no better than laypersons at making intuitive judgments. As recounted by Myers, a 1998 Canadian Solicitor General research team found that the experts—in this case the clinicians—were one of the "*least* accurate predictors of future criminality."[299] Researchers at the University of Minnesota found such "expert" predictions were on average 10 percent less accurate than ones made with "mechanical" i.e. statistical, actuarial, or algorithmic techniques, although they did

296 We discuss this below in more detail along with a means of making use of the past to better understand the present and explore the future.

297 Kahneman and Klein, "Intuitive Expertise," 521.

298 Kahneman and Klein, "Intuitive Expertise," 520-21.

299 Myers, *Intuition*, 173; emphasis in original.

observe that in 63 of the 134 cases they studied, clinical predictions fared as well as mechanical ones.[300]

Admittedly one explanation (at least in the latter case) is that lack of timely feedback inhibits the acquisition of the skills needed for successful prediction. Psychologist James Shanteau observed that domains where the practitioner's task is to predict human activity have few "experts."[301] Indeed, the expertise may lie in tasks other than those that are assumed to be the principal task goals. Thus, for instance, we might think that to be an expert clinical psychologist, one would have to be able to correctly diagnose and then correctly predict the likelihood of recovery, and then correctly treat the client, but the true skill might lie in being a very good listener. Human activity often fails to provide the needed cues for timely feedback, and at a collective level is subject to too many unpredictable events and decisions at the same time as it is subject to known trends and forces. The viral spread of unsubstantiated ideas on the World Wide Web through such mechanisms as YouTube offers an example of how weak feedback at the collective level breeds low intrinsic predictability.

These domains contrast with those where it is relatively easy to identify experts on the basis of operational definitions that specify what it means for a person to be an expert, in terms of performance at principal task goals. Examples would be medicine, weather forecasting, piloting, musical performance, and industrial process control. These latter domains are known by convenience as "Type 1." They contrast with the formerly described domains, known as "Type 2."

How professionals fare in estimative judgments in these domains has been studied. The results of one study of members of the intelligence unit of the Canadian Privy Council Office, carried out by Defence Research and Development Canada, concluded that with ample time and resources the "quality of analytic judgments was 'good to excellent' across [a series of] various indices."[302] The researchers noted, "[experts] that perform well tend to work in areas that provide timely, unambiguous feedback on their performance"—in other words, in stable, Type 1 domains.

---

300 William M. Grove, David H. Zald, Boyd S. Lebow, Beth E. Snitz, and Chad Nelson, "Clinical Versus Mechanical Prediction: A Meta-Analysis," *Psychological Assessment*, vol. 12, no. 1 (2000), 25. Cited hereafter as Grove and others, "Meta-Analysis." As recounted by Myers (p. 173) 63 cases were also a draw; in only 8 cases did clinical methods fare better.

301 James Shanteau, "Competence in Experts: The Role of Task Characteristics," *Organizational Behavior and Human Decision Processes*, vol. 53 (1992): 252-266.

302 David R. Mandel, Alan Barnes, and John Hannigan, "A Calibration Study of an Intelligence Assessment Division," PowerPoint Presentation, Defense Research and Development Canada, Toronto, CA, n.d. Cited hereafter as Mandel, Barnes, and Hannigan, "Calibration Study."

For Type 2 domains, however, the evidence points the other way: we can expect intelligence professionals to be poorer at point prediction unless the predictions are very near term. This tendency is confirmed by the NIC long-range predictions contained in the *Global Trends* papers. In a related example, *The Economist* found greater accuracy in their control group than among the experts in a set of economic point predictions spanning 1984 to 1994.[303] About this experiment, the members of the U.S. Commission on National Security observed that of four groups of people—"finance ministers, chairmen of multinational corporations, Oxford University economics students, and, as a control group, four London garbage collectors"—"[every] group did poorly; the garbage collectors, as it happened, turned out to be the most accurate."[304] In commenting about its own study, *The Economist* concluded, "The contents of dustbins could well be a useful leading economic indicator."[305]

A Space-Time Envelope of Anticipation

What actually occurs when we think about an event or trend lying in the future? Hoffman suggests that causality arises from what he refers to as long-term forces and abstractions, rather than near-term events and decisions. We project past events, decisions, and perceived forces and abstractions forward in space and time toward the present effect or event as we begin trying to make sense of the future. Then we envision the reach and consequence of that effect or event further, into the future; we extrapolate future forces and abstractions from ongoing events and decisions. We therefore convert events of the present moment into a "specious present."

This all occurs in foresight. But we subsequently look at events in backward fashion. Someone got onto an airliner with a bomb in their underwear. What explains this? We can reason backward across actual time from effects and aftereffects (the attempt by the bomber to detonate his explosives and the successful preventative intervention) to causal explanations. And we

303 The United States Commission on National Security, *New World Coming: American Security in the 21st Century*, Study Addendum, Phase 1 (July 1998-August 1999), 1. Cited hereafter as Commission on National Security. Since the National Intelligence Council has an "Economics" portfolio, one safely can surmise that economics is an intelligence issue. Therefore the results from the experiment by *The Economist* study has relevance to the practice of intelligence.

304 Commission on National Security, 1. One might well wonder how a group of four intelligence professionals might have fared. Hoffman suspects that the researchers probably only looked at prediction hit-rate and did not drill down into the reasoning and knowledge content relied upon. It is there, he suspects that the expertise of the "experts" would have emerged. Still, because economics is a Type 2 domain, the results are not implausible.

305 *The Economist*, "Garbage In, Garbage Out," (U.S. Edition), 3 June 1970, 70.

always find those causal explanations; we're certain they're the right ones. For Type 1 domains we may be good at this. The very nature of Type 2 domains precludes any reasonable expectation of accuracy on our part about causal explanations. But, as Kahneman and others point out, people are nonetheless certain they are right: the "illusion of validity" prevails. Such cogitation in hindsight is a quite rational kind of sensemaking, as it is the reconsideration of a case after one has obtained more information about it. It works because we only consider what we knew afterward and what we could or should have known afterward. We do not consider the event from the perspective of what we knew *before* the event occurred, and this feeds into the blame game.

Such human thinking may be illustrated as a series of interlocking triangles set across a "space-time envelope of indeterminate causality" as shown in figure 3. "Effects" or events are predicated upon other events and decisions that are themselves influenced by forces and abstractions. They in turn give rise to new (or continuing) events and decisions that are in turn embodied in

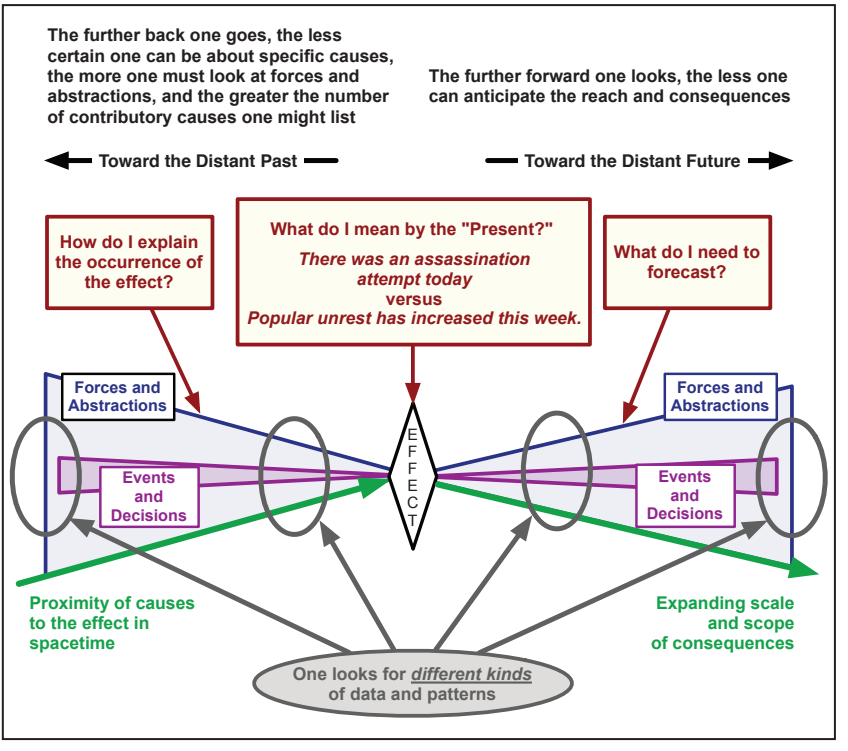


Figure 3. Space-Time Envelope of Indeterminate Causality.
Source: Robert Hoffman.

new (or continuing) forces and abstractions. These predicate and subsequent factors can be viewed from a variety of scales. Using a model of weather forecasting (from which this "envelope" was developed), we observe that at each scale, there are particular dynamics having particular space-time parameters. As one progresses from higher scales to lower, each scale provides the "boundary conditions" or forcing events for the scale below it. Each scale requires the examination of different kinds of data and emergent patterns as well as differing meanings. For example, at a microscale in weather forecasting, one might simply look up and observe what is going on locally over a period of a few minutes; at a continental or "synoptic" scale one makes sense of radar or satellite images showing events that transpire over a period of hours; at global scale observations consider the actions of the jet stream and the worldwide effects of phenomena such as *El Niño* over time spans of months. Dynamics are coupled to space-time, and because time is a factor, there is an explicit expression of increasing uncertainty the farther one is from the effect or event—either in the past or in the future. Placing an episode of intelligence sensemaking into this framework might help keep the thinking honest.

Let us consider that the point of view of the observer is one of an "unspecific present." This is not a single point in time but a range of time, a little in the future and a little in the past, depending on the context or events under analysis. Hoffman's model allows for the factors—at differing scales—to be mapped out conceptually as is shown in figure 4.

At the conclusion of making such a diagram, one has mapped out a path of reasoning—forward in foresight, backward in hindsight—identified the drivers, and placed them in one of three space-time envelopes: past, present, or future. The creation of diagrams of this sort has been useful in charting analyst reasoning and knowledge, making it explicit for discussion and also contributing to knowledge capture and preservation.[306] The diagram facilitates sensemaking by making explicit what one knows and when one knows it as well as how the various trifles of information are related and contribute to one another.

306 Robert R. Hoffman, "Use of Concept Mapping and the Critical Decision Method to Support Human-Centered Computing for the Intelligence Community." Report to the Palo Alto Research Center (PARC) on the Project, "Theory and Design of Adaptable Human Information Interaction Systems for Intelligence Work," Novel Intelligence From Massive Data (NIMD) R&D Program, Advanced Research and Development Activity (ARDA), Department of Defense, Washington, DC, November 2003; and Robert R. Hoffman, "Making Good Decisions about Decision-aiding?" panel on "Beyond Requirements: Decision Making Developing Software Tools for Intelligence Analysts" 49th Annual Meeting of the Human Factors and Ergonomics Society, Orlando, Florida, 2005.

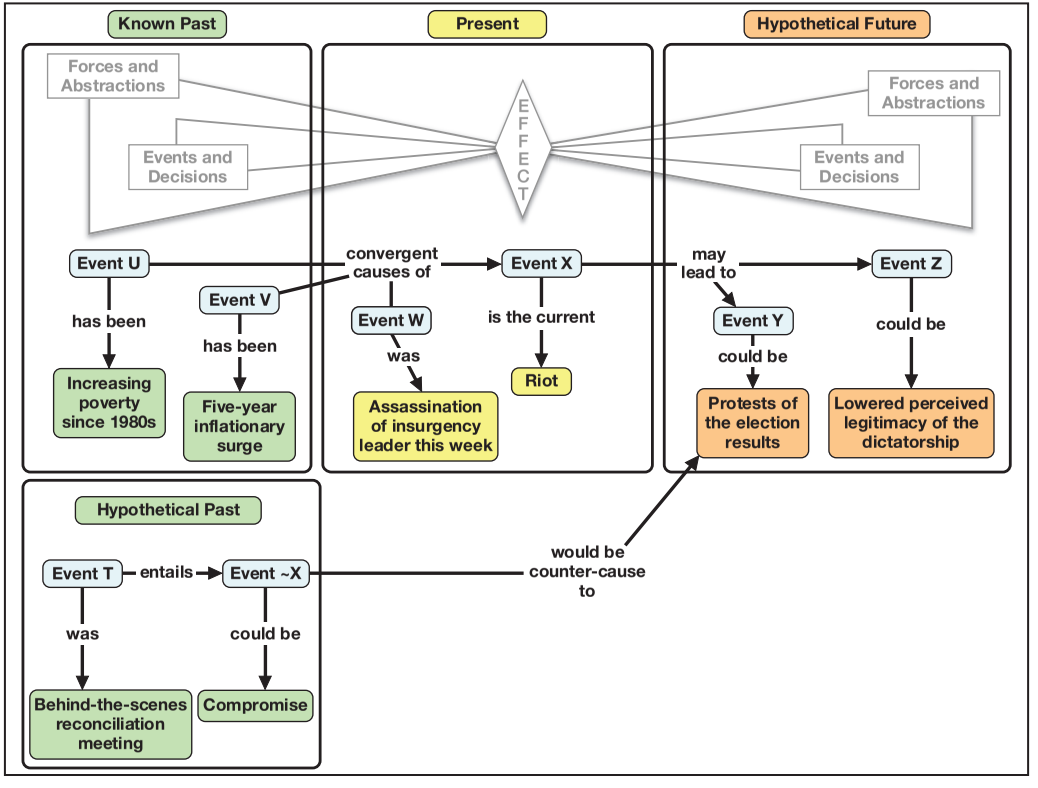


Figure 4. A Notional Example of Causality Across the Space-Time Envelope.
Source: Robert Hoffman.

Anticipating Deception: Applying the Space-Time Envelope

A recurring worry within alert intelligence services is whether they are being deceived by their adversaries. From Troy, in the second millennium BCE, through to mis-direction schemes in World War II, and on to the lead-up to the Iraq invasion of 2003, adversarial deception has played a strong or decisive role in final outcomes.[307]

World War II's Operation Mincemeat is of particular interest for the opportunity it affords for counterfactual examination, and thus for a sensemaker's anticipation of future strategic deception.[308] The premise of the Mincemeat deception was to employ a stratagem known as the "lost dispatch case," a sort of portable Trojan Horse, to mislead the Germans about where the Allies would invade as they moved from North Africa onto the European continent. To both sides, Sicily was the logical candidate for the initial landings. Thus, the English proposed floating a corpse ashore at Huelva, Spain, with a dispatch case containing letters and other references to invasion points through the Peloponnese, and Sardinia and Corfu; Sicily was to be a diversion. As both Montagu and Macintyre make clear, the Germans decided the recovered documents were authentic and redeployed troops to strengthen their positions in the incorrect locations. Subsequently the Allies faced considerably less resistance when they landed on Sicily.[309]

However, could the Germans have come to a different conclusion? Such counterfactual questions normally leave us with a less than satisfying answer. But in this case, in light of first-hand and well-founded knowledge of decisionmaking on both sides, we can marshal the authentic beliefs, events, and drivers that led to a decision to make a well-informed estimate of what could have evoked an opposing decision. As shown in figure 5, key evidence and beliefs, when laid out in the space-time envelope of anticipation, would facilitate the counterfactual process by indicating what underlies the German belief that the documents were authentic. Behind each "event" are in fact chains of evidence that could be explicitly included in a more detailed

---

307 For a very interesting take on the many layers of Iraqi deception see Kevin Woods, James Lacey and Williamson Murray, "Saddam's Delusions: The View From the Inside," *Foreign Affairs* (May/June 2006). It seems that Hussein was himself deceived even as he strove to convince his neighbors that he had weapons of mass destruction (WMD) and strove to convince the United States that he had gotten rid of his WMD—which apparently was the ground truth.

308 See Ewen Montagu, *The Man Who Never Was: World War II's Boldest Counterintelligence Operation* (Annapolis, MD: Naval Institute Press, 2001, reprinted from 1953 original). Cited hereafter as Montagu, *The Man Who Never Was*. The story, a first-hand account by Montagu as one of its planners, is also told in the 1956 movie of the same name. Also see Ben Macintyre, *Operation Mincemeat* (New York, NY: Harmony Books, 2010). Cited hereafter as Macintyre, *Operation Mincemeat*.

309 Macintyre, *Operation Mincemeat*, 284-285; Montagu, *The Man Who Never Was,* 139-146.

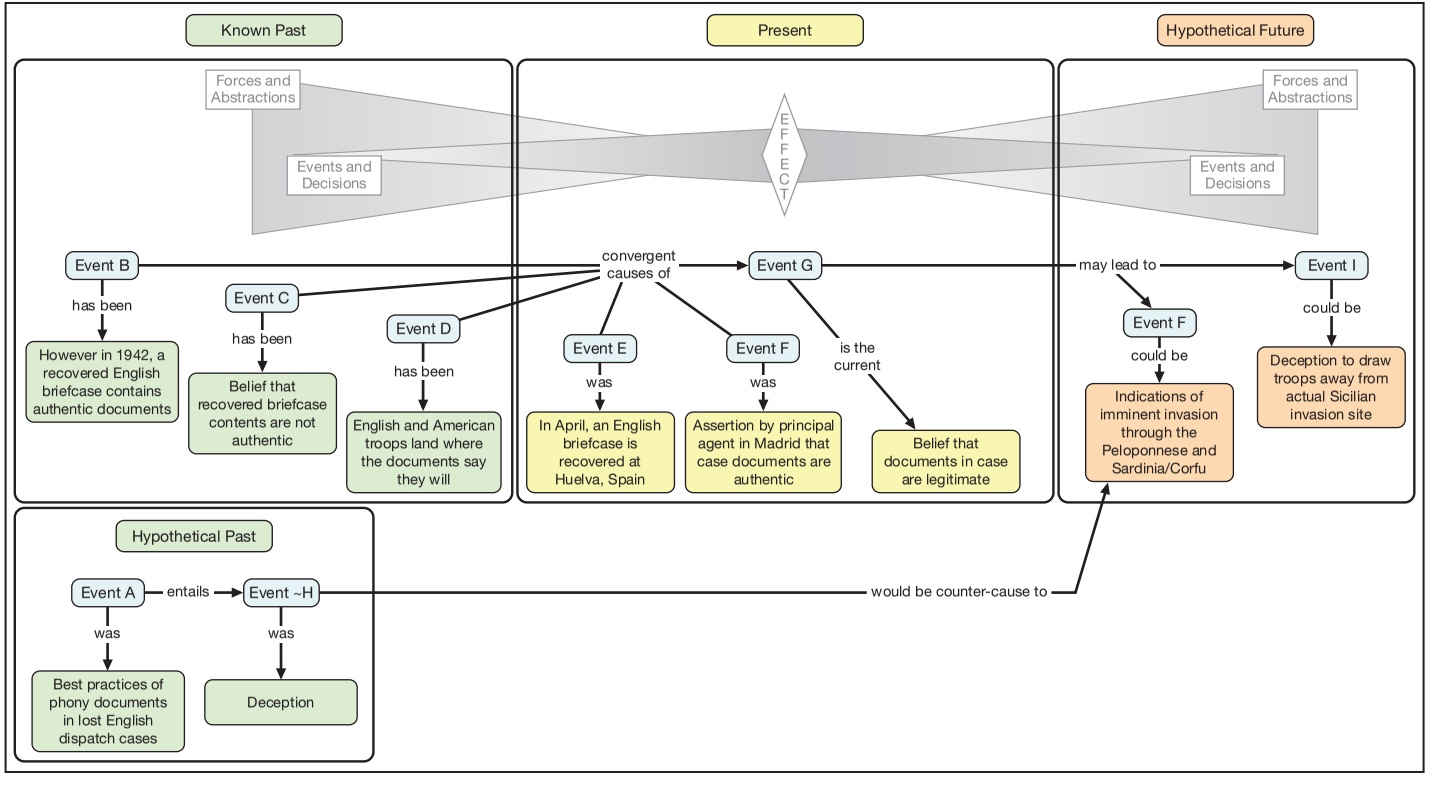


Figure 5. A Space-Time Envelope of Anticipation Regarding the Authenticity of the Documents Recovered at Huelva, Spain, 1943.
Source: Authors.

version of this sensemaking approach.[310] Had the Germans employed this cognitive tool, a different decision regarding the authenticity of the documents and therefore the location of the invasion *might* have been reached. The Allies might have been repulsed and the events of the remainder of the War would have been different.[311]

Implications of Visualizing Anticipation

Diagramming using Concept Maps (and related kinds of diagrams called causal maps and cognitive maps) has been used as a de-biasing technique for analysis under uncertainty. This use is well known in the field of business and strategic management:

> Causal maps allow the map maker to focus on action—for example, how the respondent explains the current situation in terms of previous events, and what changes he or she expects in the future. This kind of cognitive map is currently the most popular mapping method in organization theory and strategic management.[312]

And in the pages of *The Journal of Strategic Management*, Gerard Hodgkinson and his colleagues added:

> In addition to providing a useful means for gaining insights into the nature and significance of cognitive processes underpinning strategic decision making, this dynamic emphasis on antecedents, behaviors and consequences, renders causal cognitive mapping techniques particularly attractive as a potential means for overcoming the effects of framing (and possibly other cognitive biases) in situations involving relatively complex decision scenarios.[313]

Hodgkinson *et alia* investigated "the extent to which judgmental biases arising from the framing of risky decision problems [could] indeed be eliminated

---

310 This is known as "inference diagramming" and was developed for jurisprudence by jurist John Henry Wigmore (1863-1943). David Schum developed the paradigm for intelligence work, and Moore explored applications of it for intelligence work. See John Henry Wigmore, *The Science of Proof: As Given by Logic, Psychology and General Experience and Illustrated in Judicial Trials*, 3rd edition (Boston, MA: Little, Brown,1937); David A. Schum, *Evidence and Inference for the Intelligence Analyst*, Two Volumes, (Lanham, MD: University Press of America, 1987); and David T. Moore, *Creating Intelligence: Evidence and Inference in the Analysis Process*, MSSI Thesis chaired by Francis J. Hughes (Washington, DC: Joint Military Intelligence College, July 2002).

311 See for example, Peter G. Tsouras, *Third Reich Victorious: Ten Dynamic Scenarios in Which Hitler Wins the War* (London, UK: Lionel Leventhal Limited, 2002); and Peter G. Tsouras, *Disaster at D-Day: The Germans Defeat the Allies*, June 1944 (London, UK: Greenhill Books, 2000).

312 Anne Huff, ed., *Mapping Strategic Thought* (Chichester, UK: Wiley, 1990), 16.

313 Gerard P Hodgkinson and others, Nicola J. Bown, A. John Maule, Keith W. Glaister, and Alan D. Pearman, "Breaking The Frame: An Analysis Of Strategic Cognition And Decision Making Under Uncertainty," *Strategic Management Journal*, 20 (1999): 979. Cited hereafter as Hodgkinson and others, "Strategic Cognition."

through the use of this particular cognitive mapping technique" and found cognitive mapping to be "an effective means of limiting the damage accruing from this bias."[314]

Because Hoffman's approach is generalized from weather forecast modeling—which has become increasingly accurate at certain scales—it would be reasonable that against Type 1 domains this may be a useful approach. But, what of Type 2 domains? Given the appeal and excitement that come with attacking such mysteries, innovative experimentation remains the surest way to learn about how causality mapping might contribute to positive advances in intelligence sensemaking about Type 2 domains. Given the conclusions reached by Hodgkinson, it appears likely that intelligence professionals making sense of type 2 domains might mitigate framing effects through such diagramming.

The Roles of Intuitive Thinking in Intelligence Sensemaking

Given these considerations, what are (or should be) the roles of skills-based intuitive and heuristic-based intuitive thinking in intelligence sensemaking? Many, if not most, intelligence professionals have had a "feeling" about an issue and what is going to happen. Sometimes those intuitions are correct, particularly if the requirement entails real-time observation and situational awareness. When it comes to anticipatory sensemaking, however, the authors suspect that intelligence professionals may fare no better than does the average citizen in predictive situations.[315]

There are a number of reasons for this, not the least of which has to do with the availability of evidence, or relevant information. A somewhat persistent myth about intelligence is that its professionals have access to all the information they need and that they can get any and all other necessary information. This not only simply is not true but is likely highly undesirable. While it is true that intelligence professionals must make their assessments based on incomplete, often faulty, and sometimes deceptive information, at least they can do so. Forcing them to try to make sense of *all* the relevant information relating to an issue would likely burden them sufficiently so as to preclude anything but the most general findings being issued—if anything

314 Hodgkinson and others, "Strategic Cognition," 977, 979. Framing problems differently has been empirically shown to dramatically change the decisions people make. See Amos Tversky and Daniel Kahneman, "The Framing of Decisions and the Psychology of Choice," *Science*, vol. 211, no. 4481 (10 January 1981), 453-458.

315 A near synonym is "prediction." However, the term implies a future that can be anticipated along with the establishment of the likelihood (probability) that it can be determined. Rather than such probability juggling, what people really do is to anticipate ranges of situations. This is the meaning attributed to "anticipatory sensemaking."

can be issued at all. Finally, as was discussed above in relation to figure 1 (see Chapter 3), complexity, ambiguity, and uncertainty increase as one moves from Descriptive to Estimative (or Anticipatory) Intelligence.[316]

It is true that a so-called "smoking gun" may exist from time to time. For example, the images of the Soviet SS-4 MRBMs in Cuba collected on 15 October 1962 left little doubt as to what they were—but such occurrences are rare. Further, intelligence professionals compete against other foreign intelligence organizations whose professionals may be as skilled at obfuscating what their factions, groups, or nations are doing as we are at making sense of what they are doing. Sometimes that other side is, in fact, better. And, like a closely matched sports event, the difference between valid and true sensemaking versus invalid or untrue sensemaking—or even no sensemaking at all—might be the result of luck.

Whether or not intelligence professionals do indeed have any better predictive skills than non-professionals should be a testable question; however, it remains one of many questions about intelligence sensemaking that remain open because of gaps in the empirical foundation for a psychological theory of performance of intelligence sensemaking.[317]

Many intelligence professionals work in one or more Type 2 domains where it is far from easy to come up with good operational definitions to identify experts. For example, how does one determine that an intelligence professional is an expert? In Type 1 domains, as discussed above, this can be clear. Among the defining features are years and breadth of experience, but also measurable performance, and status within social networks (i.e., the expert is the "go-to" person for dealing with specialized problems).[318]

However, as Kahneman and Klein note, such is not the case when "experts" must work outside their favored domains or within ones that are unstable and do not provide the cues and feedback necessary for calibration.[319] Since such Type 2 domains are ones in which the primary task goals involve the understanding and prediction of the activities of individuals or groups, accuracy and precision are elusive. Consequently, as has been noted, Type 2 domains are also characterized by tasks involving a lack of timely feedback and a paucity of robust decision aids. Further, if the object of study

316 How much information is truly necessary is discussed in more detail below.

317 Robert R. Hoffman, "Biased about Biases: The Theory of the Handicapped Mind in *The Psychology of Intelligence Analysis*," Panel Presentation for "Designing Support for Intelligence Analysts," S. Potter, Chair, in *Proceedings of the 48th Annual Meeting of the Human Factors and Ergonomics Society* (Santa Monica, CA: Human Factors and Ergonomics Society, 2005), 409.

318 Robert R. Hoffman, "How Can Expertise be Defined?: Implications of Research from Cognitive Psychology," in Robin Williams, Wendy Faulkner and James Fleck, eds., *Exploring Expertise* (New York, NY: MacMillan, 1998), 85.

319 Kahneman and Klein, "Intuitive Expertise," 521.

does not know what she or they will do, how can someone else predict it reliably? Therefore, is it any surprise that in such domains, intuition is limited in its usefulness? What are intelligence professionals to do?

It should be reiterated that although over-estimative errors in intelligence sensemaking, as has been noted, are unacceptable, under-estimative errors are even less tolerated. It is better to have warned and been wrong than not to have warned and been wrong. False alarms are better than misses. A warning about an attempt by another individual to set off a bomb on a subway system—which subsequently does not occur—generates far less uproar (if any at all) than does a failure to warn of an individual who in fact plans to blow up an airliner, and through anticipatory sensemaking, being able to catch him preemptively. In the former case, the fact of the warning may even be viewed as the measure by which the attack was prevented. The would-be terrorist was scared off because his plans were publicized.

Unfortunately, this bias toward false alarms feeds into the blame game that demoralizes intelligence professionals. This creates a perception of an inevitability of failure perhaps captured by the water cooler joke, "How many analysts does it take to change a light bulb?" For which the answer is three: "One to not notice it is burned out, one to not change it, and one to take the blame."

Does More Information Improve Anticipation?

What about foraging for more information? Paul Slovic's 1973 research into the impact on the reliability of bookmakers as they brought more information into consideration noted that it did not increase their accuracy (figure 2, above).[320] Myers, in commenting on the Minnesota meta-study, notes further that providing clinicians with additional information from files or interviews actually reduced their accuracy.[321] The question becomes how much information is *enough*? A related question is, "how does one know that in advance?" It must be concluded that even with more information, Type 2 intuition remains of uncertain validity.

It is by no means obvious that simply throwing more information at a problem will make solving it any easier. For instance, to investigate the question of apparent under-utilization of information, Phelps and Shanteau (1978) used two methods to examine the strategies of livestock judges. In one situation, judges were presented with photos of female pigs (gilts) and asked

320 Slovic, "Behavioral Problems"; also Fischoff, "Condemned to Study the Past."

321 Myers, *Intuition*, 173-174. See W. M. Grove and others, "Clinical Versus Mechanical Prediction: A Meta-Analysis," *Psychological Assessment*, vol. 12 (2000): 19-30. Paul Slovic came to the same conclusions in 1973; see Slovic, "Behavioral Problems."

to rate each on breeding quality (their usual task). The results revealed the same sorts of limitations reported by other research, with each judge apparently relying on only a few of the 11 possible cues (e.g., weight, length, ham thickness, heaviness of bone structure, freeness of gait, etc.). In the second condition, judges were presented with verbal descriptions of the gilts (supposedly based on a telephone conversation) that listed the levels of the 11 attributes for each animal. In this case, analysis of the judgments of breeding quality revealed a subtle pattern: Judges used between nine and eleven cues, which tended to interact. Combined with results from a post-experimental interview, the judgments revealed an underlying strategy involving two waves of information integration: Measures are collapsed into intermediate judgments including size and meat quality; these judgments are then combined into an overall judgment.

The difference in results for the two tasks is striking. With the pictures of gilts, the relevant stimulus attributes were naturally correlated and perceptually chunked (e.g., tall gilts tend to be heavier and wider). Thus, even though a judge may have perceived all of the cues, only one significant cue might be needed explicitly to generate a given intermediate judgment. With the verbal descriptions, on the other hand, the cues were presented separately, the expert had to work through them explicitly, and the effects of cue intercorrelations revealed.

Benjamin Kleinmuntz obtained a similar result using the "Twenty Questions" game and a set of test cases to add structure to interviews with intern and resident neurologists.[322] Experience made a big difference in diagnostic accuracy, of course, but also in the number of questions asked about symptoms in each test case. In order to diagnose a case, the advanced experts asked fewer questions but they also spent less time pursuing incorrect hypotheses. Indeed, experts tended to ask about symptoms that yielded the greatest amount of diagnostic information relative to their hypothesis, reflecting "economy of effort."[323]

---

322 Benjamin Kleinmuntz, "The Processing of Clinical Information by Man and Machine," In Benjamin Kleinmuntz, ed., F*ormal Representations of Human Judgment* (New York, NY: Wiley, 1968), 149-186.

323 The field of expert reasoning has a particularly rich literature. See, for example Sylvia Scribner, "Studying Working Intelligence," in Barbara Rogoff and Jean Lave, *Everyday Cognition: Its Development in Social Context* (Cambridge, MA: Harvard University Press, 1984), 9-40; and Sylvia Scribner, "Thinking in Action: Some Characteristics of Practical Thought," in Ethel Tobach, Rachel Joffe Falmagne, Mary Brown Parlee, Laura M. W. Martin, and Aggie Scribner Kapelman, eds., *Mind and Social Practice: Selected Writings of Sylvia Scribner* (Cambridge, UK: Cambridge University Press, 1997), 319-337; K. Anders Ericsson, Neil Charness, Robert R. Hoffman, and Paul J. Feltovich, eds., *Cambridge Handbook of Expertise and Expert Performance* (Cambridge, UK: Cambridge University Press, 2006); and Robert R. Hoffman and Laura Grace Militello, *Perspectives on Cognitive Task Analysis: Historical Origins and Modern Communities of Practice* (Boca Raton, FL: CRC Press/Taylor and Francis, 2008).

Future Vision: Red Brains, Blue Brains?

Given the discussion to this point, it is not enough to continue to ask whether expertise hinders judgment, or whether more information improves prediction. One might ask more productively about how we might improve the circumstances for sound reasoning. A partial answer may lie in the work of a group of Southern California political scientists whose recent neurocognitive research addresses how people behave and make predictions. For example, Darren Schreiber *et alia* used functional MRIs (magnetic resonance imaging tests) to assess how people associated with the U.S. Republican and Democratic political parties deal with risk. The researchers discovered that members of the two groups used distinctly different portions of their brains when making "winning risky versus winning safe decisions."[324] The authors note that the different portions of the brain play different roles in human cognition and conclude that

> it appears in our experiment that Republican participants, when making a risky choice, are predominantly externally oriented, reacting to the fear-related processes with a tangible potential external consequence. In comparison, risky decisions made by Democratic participants appear to be associated with monitoring how the selection of a risky response might feel internally.[325]

While neurocognitive paradigms for intelligence sensemaking have not yet formally been identified or established, implications of this work—to the degree that intelligence professionals can speak to the concerns of decisionmakers who are, after all, particular political partisans—may be significant. The research to date shows that the cognitive mechanisms and especially the emotion-based attitudes of partisan sensemakers shape their reasoning as they assess uncertain and risky phenomena.

Additional research could explore biologically based differences that correlate with the strong intuitive tradition by which sensemakers (and others) analyze, synthesize, and interpret intelligence phenomena. For example, in what situations are the skills and services of externally oriented intelligence professionals required and in what situations are those of internally oriented professionals needed? Similarly, in communicating intelligence results to

---

324 Darren M. Schreiber and others, "Red Brain, Blue Brain: Evaluative Processes Differ in Democrats and Republicans," Paper delivered at the 2009 American Political Science Association Meeting, Toronto, CA, URL: <http://ssrn.com/abstract=1451867>, accessed 9 December 2009. Cited hereafter as Schreiber and others, "Red Brain, Blue Brain." While it is too soon to determine the impact of their (and similar) work, it may prove revolutionary to political affiliation studies.

325 Schreiber and others, "Red Brain, Blue Brain."

consumers, are briefers more effective if their neurocognitive "risk" strategies match those of their consumers?[326]

Looking Ahead

Intuitive reasoning is something that we do naturally, all the time. It cannot be prevented, is not easily neutralized, and it is sometimes useful and necessary in sensemaking. While it can be reliable when employed as the sole basis for actionably valid, predictive intelligence creation in Type 1 domains, it is highly fallible when used for intelligence creation in Type 2 domains.

What can be done to challenge and validate the surety one has about an intuitive intelligence judgment? Employing approaches to reasoning such as those found in critical thinking seminars and courses, especially as currently offered across the IC's educational institutions, and developing skills that aid mindfulness (as discussed in the Preface), offer possible means of accomplishing calibrated reasoning.[327] Diagramming such as was done in figure 4 may challenge and certainly will augment the reasoning. But what else can be done to increase certainty that derived conclusions are valid? This becomes the subject of the next chapter.

---

326 An important caveat is that just because one person exhibits a particular "style" of dealing with risk does not make them unsuited for other situations where a different approach may seem to be warranted. Such reasoning smacks of "biological determinism" and is no more appropriate in intelligence work than it was in the domains discussed in Richard Hernstein and Charles Murray's *The Bell Curve: Intelligence and Class Structure in American Life* (New York, NY: The Free Press, 1996). For a history and in-depth discussion of scientific determinism (sometimes also referred to as scientific racism) see Stephen J. Gould, *The Mismeasure of Man* (New York, W. W. Norton & Company, 1996).

327 That these approaches will be effective admittedly is a hypothesis in need of testing in real-life situations. In experiments with students, Jennifer Reed (among others) finds that critical thinking does improve the quality of judgment and decision-making. The handy difference between the world in which intelligence professionals find themselves and Reed's classroom setting is that while there are no answers in foresight in the former, truth can be known in advance in the latter. See Jennifer H. Reed, *Effect of a Model For Critical Thinking on Student Achievement In Primary Source Document Analysis And Interpretation, Argumentative Reasoning, Critical Thinking Dispositions, And History Content in a Community College History Course*, PhD Dissertation, College of Education, University of South Florida, December 1998, URL: <http://www.criticalthinking.org/resources/JReed-Dissertation.pdf>, accessed 2 February 2010.

CHAPTER 6
Considering Validation

How does one know if the knowledge that intelligence sensemakers create is itself valid? Does accuracy alone ensure validity? What was accurate when findings were communicated may not be accurate subsequently. This flux suggests a strong procedural basis for validation. For example, were steps followed to avoid perceptual errors and cognitive traps? Was the process documented? Were alternatives adequately explored? Given the inherent uncertainty in intelligence judgments, it remains possible that all the appropriate processes may be sufficiently applied and yet the judgment is wrong—cold comfort for relatives of the victims and the survivors if the result is a terrorist attack on a scale of those in September 2001. By exploring validation perspectives from cognate fields, we may advance our parochial understanding.

Analogies from Other Fields

Medicine

Medical practice is at times presented as having notable similarities to intelligence practice. For example, with respect to validation, an ultimate metric for failure in medicine is that the patient dies. But is medicine successful if the patient lives? At what quality of life and for how long are two additional questions. Perhaps death with a minimum of suffering is the most favorable medical outcome—is this a success? Depending on the specifics of the case, maybe it is. Is there a difference if the patient is very old or very young? The author's own experience with the death of his mother is that elderly, somewhat frail patients—in practice—do not seem to receive the same level of treatment as do younger but equally severely ill patients. In the former case the patient, the author's mother, died within about 72 hours without what appears to be undue suffering but also without significant treatment of the condition, only an easing of the symptoms. In the latter case, the child recovers. Are both treatment regimes successful? Does the inevitable or perhaps the perceived inevitability of death by the attending physician become a factor in determining the treatment?

In medicine, success is measured post-facto. Early organ transplants were successes if the patients lived only for a brief period afterward. Other

factors include quality of life, longevity, and costs. A recent T-cell-based, bioengineered trachea is considered a significant success not only because it succeeds but also because it dramatically improves the patient's quality of life:

> the successful outcome shows it is possible to produce a tissue-engineered airway with mechanical properties that permit normal breathing and which is free from the risks of rejection seen with conventional transplanted organs. The patient has not developed antibodies to her graft, despite not taking any immunosuppressive drugs. Lung function tests performed two months after the operation were all at the better end of the normal range for a young woman.[328]

If, a year later, however, the patient dies (from a related cause) was the expense worth it? Certainly, her family can be expected to indicate this is the case. But what of the cost to the larger society and perhaps other patients suffering from other ailments, who cannot get necessary resources because they are tied up in this specific treatment? Viewed in an intelligence context, if a terrorist attack is thwarted (characterized as a success) but a year later a larger and more devastating attack occurs, and it does so *because* the earlier attack was prevented, was the earlier disruption a success?

Jurisprudence

Jurisprudence is an adversarial system in which the ultimate confrontation is a trial wherein two advocates make inferences about evidence to argue opposite sides of a case before an impartial third entity or body (often of non-experts). This is the system at its best. In practice, the skill level of the advocates may vary. One may be more skilled or more proficient than the other. The impartial body (judge, jury) may be misled to a decision. Were this not the case then there would never (or very rarely) be cases where innocent people are convicted, imprisoned, and sometimes executed.[329]

While such failures appear to be rare, they may be examples of a limited consideration of evidence where only one side of an issue is examined. The fallacy is not new. Diagoras of Melos (5th Century BCE) was confronted with votive offerings carved by sailors in gratitude to the gods at their safe return from the sea. Diagoras unpopularly observed that only those who had

---

328 University of Bristol, "Adult Stem Cell Breakthrough: First Tissue-engineered Trachea Successfully Transplanted," *Science Daily*, 18 November 2008, URL: <http://www.sciencedaily.com/releases/2008/11/081119092939.htm>, accessed 21 November 2008.

329 For more on exonerations see Samuel R. Gross and others, "Exonerations in the United States, 1989 through 2003," *Journal of Criminal Law and Criminology* 95, no. 2 (2005): 523-560.

returned carved the votives; those who had not returned [the missing class of evidence] carved none.[330]

A success metric involving law would be one where either no challenge was made or it was repudiated and the convicted person was in fact guilty. But, what if the person is found innocent, or at least not guilty? They may be truly innocent. However, the prosecuting attorney may be incompetent, the evidence circumstantial or otherwise incomplete. In this case the actual innocence of the person may be independent of the findings of the court.

So, how does one measure success? There are at least five points of view involved in jurisprudence: That of each of the advocates, the judging entity (a jury or judge) the accused person, and the community or government. Each party, depending on the verdict, has a different metric for success. In certain types of cases such as those involving child molestation or alleged terrorism, the accused person tends to be deemed guilty by the community, prosecuting advocate, and government even if exonerated. In all cases where an opinion—particularly in the media—runs counter to the majority's views, the conclusion may be made that the court failed to render the "right" verdict as was also seen in the highly publicized cases of motorist Rodney King and the murder trial of O.J. Simpson.

Science

Science involves a number of metrics that include a sound method of documenting both process and results, as well as replication. Work is considered preliminary and non-definitive if it has not been replicated. As a typical example, in writing about the need for studies of the genetic bases of fidelity among humans, the editors of a collection of articles on genetics of behavior in *Science* refer to a comment by Australian psychologist, Simon Easteal, that despite the intellectual appeal of theories about genetic links to specific behaviors, "there are few replicated studies to give them heft."[331] In other words, the underlying theories may not be sound.

Science depends on refutation of alternative hypotheses, and replication studies attempt to refute that which has been shown. It is quite acceptable to be wrong so long as one admits it when the fact becomes apparent. Indeed, one model for science is that of competitive cooperation. Scientists attempt to tear down the new work of colleagues—without resorting to personal attacks. This dialectic approach may last generations or longer. In the process new knowledge is discovered and—if it cannot be refuted—validated.

---

330 Taleb, *The Black Swan*, 100.

331 Constance Holden, "Parsing the Genetics of Behavior," *Science*, vol. 322, no. 5903 (7 November 2008), 893.

Replication in Intelligence

The inability to replicate much of the process of sensemaking in intelligence limits the application of this indispensable practice of science. The pressures of real-time production inhibit the re-visitation of past judgments, although with at least one recent National Intelligence Estimate, the repetition of "alternative analysis" led to the questioning and revision of the original conclusions. Essentially, any meaningful replication of intelligence phenomena can only be accurately made in foresight, as in a National Intelligence Estimate. It is not replication if one group of practitioners performs sensemaking of an event before it happens and another group does so afterward.[332] Therefore, replication needs to occur *before* an event occurs.

When replication of methods against the same problem occurs it is typically in the intelligence school setting. It is the author's experience that such efforts yield a common set of explanations with some outliers.[333] For example, when intelligence students faced with a scenario involving three fictitious nations at odds with each other develop a common set of hypotheses regarding who will initiate a war and with whom, and are then given a finite set of evidence and a common method such as the Analysis of Competing Hypotheses, they come to similar conclusions as to which hypotheses are the least likely and therefore which eventualities can be expected.[334] Unfortunately there does not yet exist a similar body of results for real intelligence problems interpreted through the lenses of different intelligence disciplines and sources.

Yet, replication remains an important metric of the intelligence sensemaking process. As Caroline Park notes, "[the] basic reason research must be replicated is because the findings of a lone researcher might not be correct."[335] In the context of intelligence, un-reviewed and even reviewed conclusions of an intelligence professional may simply be incorrect. Admittedly a supervisory review process that grows more stringent as increasingly significant

---

332 The problem is that latter group has the benefit of being aware of what actually happened, a factor they are unable to ignore in their deliberations. Since the two groups therefore are working in different contexts, replication has not occurred.

333 The author observed this over a period of eight years of teaching new intelligence professionals at the National Security Agency in both a new employee orientation program and in the author's critical thinking and structured analysis course. At least 1,000 individuals have participated in the two courses the author offers. For more information on the course see Moore, *Critical Thinking*.

334 It is the outliers that are truly fascinating in this classroom experience. Unfortunately, given the context imposed by a classroom setting and operational constraints, it has so far not been possible to capture why some students offer the outlying positions.

335 Caroline L. Park. "What is the Value of Replicating other Studies?" *Research Evaluation* 13. No. 1 (December 2004), 198. Cited hereafter as Park, "Value."

implications emerge from the intelligence conclusions minimizes the likelihood of error. Still, errors do occur. One replicative method known within the IC, that of "Team A – Team B," appears not to be widely practiced although it has been used on specific issues.[336]

But what of the methods employed in the intelligence sensemaking process itself? Intelligence sensemaking can involve both quantitative and qualitative methods. As Park observes, quantitative research "can be replicated with great accuracy and precision."[337] Intelligence conclusions that result from counting observed phenomena such as aircraft located around an airfield can easily be repeated. But repeatedly and consistently measuring the intentions of the owners of those aircraft—the object of qualitative sensemaking—is more difficult although, as has been noted, not impossible.

Of note, however, is a danger of repetition confirming false results. Lynn Hasher, David Goldstein, and Thomas Toppino concluded that confidence in assertions increases through repetition of the assertions in situations when it is impossible to independently determine their truth or falsity.[338] Since intelligence evidence harbors a degree of uncertainty, repetition of evidence or even findings in proceedings designed to *confirm* their validity will only increase confidence that they are valid *irrespective of whether this is actually the case*. Ralph Hertwig, Gerd Gigerenzer, and Ulrich Hoffrage further show this "reiteration effect" is also part of evaluations made in hindsight.[339]

Validation in Foresight and Hindsight

People—and intelligence practitioners and their customers are merely people—evaluate judgments they have made in hindsight. They believe, according to Mark and Stephanie Pezzo, "that one could have more accurately predicted past events than is actually the case."[340] Thus, hindsight occurs at least in part because as people make sense of "surprising or negative" events,

---

336 Critical references to one effort commissioned by (then) DCI George Bush in 1976 regarding an NIE on Soviet Strategic Objectives are at URL: <http://intellit.muskingum.edu/analysis_folder/analysissov_folder/analysissovteams.html>, accessed 28 May 2010. In the referenced case CIA analysts conducted one analysis while a team of outside experts conducted an identical analysis.

337 Park, "Value," 190.

338 Lynn Hasher, David Goldstein, and Thomas Toppino, "Frequency and the Conference of Referential Validity," *Journal of Verbal Learning and Verbal Behavior*, vol. 16 (1977), 107. This work has been validated by Ralph Hertwig, Gerd Gigerenzer, and Ulrich Hoffrage, "The Reiteration Effect in Hindsight Bias," *Psychological Review*, vol. 104, no. 1 (1997): 194-202.

339 Hertwig, Gigerenzer, and Hoffrage, "The Reiteration Effect in Hindsight Bias," 194.

340 Mark V. Pezzo and Stephanie P. Pezzo, "Making Sense of Failure: A Motivated Model of Hindsight Bias," *Social Cognition*, vol. 25, no. 1 (2007), 147. Cited hereafter as Pezzo and Pezzo, "Making Sense of Failure."

"the reasons in favor of the outcome [are] strengthened, and reasons for alternative outcomes [are] weakened." Further, in hindsight all the relevant facts may be known whereas in foresight this is not the case. But evaluating "mistakes" in hindsight obscures an important point made clear by Taleb: Mistakes can only be determined as such by what was known at the time they were made and then only by the person making the mistake.[341] In other words, mistakes need to be evaluated from the points of view held in foresight. And seen from that perspective they may not be mistakes at all.

Applied to intelligence sensemaking, this means that many so-called intelligence errors and failures may, in fact, be well-reasoned and reasonable judgments based on what is known prior to the decision. Certainly, when viewed in hindsight they were wrong. But in foresight they were accurate and valid to the best of the sensemaker's abilities. How can this enduring problem be mitigated? One means involves making the process of sensemaking as deliberate and thorough as possible.[342] Doing so may reduce mistakes and failures as more alternative possibilities are considered and assessed. However, achieving this objective requires that the underlying practice be valid. Finally, it assumes that key evidence is knowable and known.

Validating the Practice of Intelligence Sensemaking

What else contributes to bringing about validated sensemaking? If a method does not do what it is commonly purported to do, is it invalid? This is one question that has been raised with regard to the Analysis of Competing Hypotheses, or as it is commonly known, ACH. Richards Heuer, Jr. initially developed the method for the detection and mitigation of attempts at adversarial denial and deception.[343] ACH forces consideration of alternative explanations for, or predictions about, phenomena.[344] It forces consideration of the entire set of evidence, not "cherry-picked" trifles that support a favored hypothesis. A common belief is that ACH mitigates what is sometimes known as the "Confirmation Bias," whereby people seek to prove a favored

341 Nassim Nicholas Taleb, *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets*, 2nd revised edition (New York, NY: Random House, Inc., 2004, 2008), 56.

342 One means of accomplishing this is discussed below in Chapter 8.

343 Heuer did not invent this method. The earliest use of multiple hypotheses in examining phenomena was by Thomas C. Chamberlin prior to 1890. See Thomas C. Chamberlin, "The Method of Multiple Working Hypotheses," *Science*, vol. 15 (old series), no. 366 (7 February 1890): 92-96. Another former CIA employee, Morgan Jones, offers a version of ACH he calls hypothesis testing. See Morgan D. Jones, *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*, revised edition (New York, NY: Crown Publishing, 1998). Jones' book also introduces the concept of and phrase "structured analysis."

344 Heuer, *Psychology*, Chapter 8.

hypothesis through (among other things) selective exposure and selective perception. Allegedly it does so by asking people to think in a disconfirmatory fashion. They are to use the available evidence to disprove as many of the existing hypotheses as possible. However, a study by MITRE failed to show that it does eliminate the confirmation bias.[345] Both the MITRE study and an earlier one by NDIC student Robert Folker do suggest that ACH is of value when used by novice intelligence professionals. However, Folker tentatively concluded that experts seem not to be aided by the method.[346] Is it still a valid method for intelligence sensemaking?

Perhaps it is. The method provokes detailed consideration of the issue and the associated evidence through the generation of alternative explanations or predictions and the marshaling of the evidence. It asks the sensemaker to establish the diagnosticity of each piece of evidence. In some versions of the method, evidence is weighted based on source and relevance. Some computer-assisted versions of ACH under review for application in the IC consider the likelihood that the sensemaker has omitted a relevant—and perhaps the correct—explanation. Therefore, it can prompt a broader yet more detailed *sensemaking* of the issue than might otherwise occur.

ACH further makes explicit the fact that evidence may be consistent with more than one hypothesis. Since the most likely hypothesis is deemed to be the one with the least evidence against it, honest consideration may reveal that an alternative explanation is as likely or even more likely than that which is favored. The *synthesis* of the evidence and the subsequent *interpretations* in light of the multiple hypotheses is also more thorough than when no such formalized method is employed.

Indeed, Robert Folker's "modest" experiment in applying qualitative structured methods—specifically ACH—to intelligence issues showed that "analysts who apply a structured method—hypothesis testing, in this case—to an intelligence problem, outperform those who rely on "analysis-as-art," or the intuitive approach."[347] Simply put, Folker experimentally showed that method improves the quality of practitioners' findings. Folker's study offers evidence that "intelligence value may be added to information by investing some pointed time and effort in analysis, rather than expecting such value to arise as a by-product of 'normal' office activity."[348]

---

345 Cheikes and others, *Confirmation Bias*, iii.

346 MSgt Robert D. Folker, Jr., USAF, *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods*, Occasional Paper Number Seven (Washington, DC: Joint Military Intelligence College, 2000). Cited hereafter as Folker, *Experiment*.

347 Folker, Experiment, 2.

348 Folker, Experiment, 2.

One variation on ACH implementation provides a structured means of developing issues. As applied by the faculty and students of the Institute for Intelligence Studies at Mercyhurst College, practitioners begin with a high-level question and use sequential iterations of ACH to eliminate alternative explanations.[349] The next phase takes the "non-losers" and develops them further. Another round is conducted and again the "non-losers" are selected and further developed. While this could generate a plethora of branching explanations, in reality it is the author's experience that it tends to disambiguate the issue fairly efficiently. At worst the structuring inherent in the method leaves the sensemaker with an in-depth understanding of the issue; at best, a couple of eventualities and their likely indicators are determined. Assets can then be tasked, foraging conducted, and more exact determinations made as the issue develops.

The question remains: Is the method valid? This question generates considerable discussion among practitioners. When used honestly, the method certainly prompts a more thorough assessment of the issue.[350] Evidence is considered singularly and severally. Alternative explanations for the phenomena are taken seriously. New possibilities are discovered. Even the skeptical MITRE team noted some validity in the method, whereby

> participant assessment of new evidence was significantly impacted by beliefs they held at the time evidence was received. Evidence confirming current beliefs was given more "weight" than disconfirming evidence. However, current beliefs did not influence the assessment of whether an evidence item was confirming or disconfirming.[351]

Appropriateness, flexibility, and ease of use are other criteria that need to be established with respect to the various sensemaking methods. Whether the method facilitates foraging, analysis, synthesis, interpretation or some combination of the foraging and understanding processes, some means is needed to operationalize validation procedures so that intelligence practitioners can increase their efficiency and accuracy.

Since Congress (in 2004) directed the Intelligence Community to employ "Alternative Analysis" in its intelligence deliberations, structured analytic methods now are taught to all new intelligence sensemakers.[352]

---

349 Kris Wheaton and others, *Structured Analysis of Competing Hypotheses* (Erie, PA: Mercyhurst College, 2005).

350 The issue of "honest use" is nontrivial. Less-than-scrupulous sensemakers are certainly free to cherry-pick favorite evidence and go through the motions of considering alternative hypotheses. Then, once they have eliminated competing alternatives, their favorite remains. The difficulty for them is what to do with the audit trail the method produces.

351 Cheikes and others, *Confirmation Bias*, iii.

352 U.S. Congress, IRTPA, 2004, 33. The phrase "Alternative Analysis" is interpreted as meaning structured analytic methods.

Many more experienced professionals also receive education and training in such methods.

Johnston observed that the IC has at its disposal "at least 160" [analytic methods]…but it lacks "a standardized analytic doctrine. That is, there is no body of research across the Intelligence Community asserting that method X is the most effective method for solving case one and that method Y is the most effective method for solving case two."[353] As referenced here, such a doctrine arises out of knowledge that the specific methods are valid, in other words it has been demonstrated *empirically* that they actually do what they claim to do. Such a doctrine proffers a menu of sensemaking options dependent on the goals of the sensemaker. The current model, where validity is presumed by intelligence professionals because they are taught the method(s) in the community's training schools, is insufficient because—at the most basic level such a metric is insufficient for determining validity. Further, there is little sense of what methods are appropriate in what situations. A claim of "we always do it that way," is known to be insufficient but remains part of the "corporate analytic tradecraft."

Heuer noted that "intelligence [error] and failures must be expected."[354] One implication of this assertion is that intelligence leadership cannot fall back on a "lack of skills" excuse when the next major intelligence failure occurs. However, without validating a canon of method and a taxonomy to characterize its use, intelligence professionals will remain hamstrung in their efforts to make fuller sense of threatening phenomena, increasing the likelihood of error and failure. It is reasonable to presume Congress will not let the Community commit failures similar to those of the past nine years without severe repercussions.[355]

Seeking Validation: Toward Multiple Methods

Within the canon of social science method lies an approach to sensemaking that may offer intelligence practitioners a means of disambiguating the wicked mysteries as well as the hard puzzles they face daily. Even in current practice, intelligence practitioners employ this approach when they do not rely on merely one method for sensemaking. Multi-method intelligence

353 Johnston, *Analytic Culture*, xviii.

354 Heuer, *Psychology*, 184.

355 As has been noted, such an *intelligence* failure occurred on 25 December 2009 in the skies over Detroit, Michigan (see URL: <http://intelligence.senate.gov/100518/1225report.pdf>). Two days after the release of the Senate report, 20 May 2010, partly as a result, Director of National Intelligence Dennis Blair left office at the request of the President. Even though the attempted attack was thwarted, it is reasonable to expect that intelligence professionals will be required to consider more possibilities and examine more information in the hopes they will notice its evidentiary value. They will need to be more imaginative.

sensemaking explores complex issues from multiple perspectives. Each method used—such as ACH—provides an incomplete understanding of the issue, leaving the intelligence professional the task of making sense of the differing sensemaking conclusions. While the results of different methods may converge, reinforcing a particular understanding of a phenomenon, they may also diverge and yield different interpretations. It is up to the intelligence professional to resolve and make sense of the differences.

For example, intelligence professionals who engage in a "multi-frame" sensemaking approach consider issues from multiple points of view created from the intersections of action- and process-focused vantage points and the perspectives of the individual and the collective. As developed by Monitor 360 for the National Security Agency's Institute for Analysis, it facilitates sensemakers' developing different answers to the intelligence question at hand.[356] They must combine the differing results, in other words, synthesize and interpret partial answers, in order to better understand the issue underlying the question and to determine a best (at the time) understanding of the issue.

The lexicon of multi-methodology provides a term for this combinatorial activity: triangulation, or pinpointing "the values of a phenomenon more accurately by sighting in on it from [the] different methodological viewpoints employed.[357] This is a process of measurement—which to be useful (accurate) "must give both consistent results and measure the phenomenon it purports to measure."[358] In other words, triangulation requires that the methods employed are repeatable and valid. Intelligence creation requires that those methods be applied with rigor.

Fortuitous circumstances allow the authors to present in the next chapter a multi-method case study of sensemaking in a Type 2 environment that illustrates the interplay of intuition, logic, analysis, synthesis and interpretation of an issue of interest to the National Intelligence Council.

---

356 While the approach is unclassified, it was first presented at an NSA (CLASSIFIED) conference on analysis. The author subsequently worked with a team from Monitor 360 to create a training course through which intelligence professionals could learn and apply this approach.

357 John Brewer and Albert Hunter, *Foundations of Multimethod Research: Synthesizing Styles* (Thousand Oaks, CA: Sage Publications, 2006), 5. Cited hereafter as Brewer and Hunter, *Multimethod Research*.

358 Brewer and Hunter, *Multimethod Research*, 5.

CHAPTER 7
Making Sense of Non-State Actors: A Multimethod Case Study of a Wicked Problem[359]

David T. Moore, with Elizabeth J. Moore, William N. Reynolds, and Marta S. Weber

> *A foolish consistency is the hobgoblin of little minds, adored by little statesmen and philosophers and divines. With consistency a great soul has simply nothing to do. He may as well concern himself with his shadow on the wall.*
>
> — Emerson, *Essay on Self-Reliance*

Introduction

In the pragmatic U.S. tradition invoked by Emerson, we question the utility of consistently following the Sherman Kent model where one or many solitary scholars try to work out the solution to problems. We also recognize that team-based intelligence production suffers from inherent drawbacks.[360] However revolutionary it may be, we find that a diversely practiced, multimethod approach that does incorporate a specific process, organizing principles, and an operational structure can fulfill the need for 21st century intelligence sensemaking. Such an approach reflects a Kendallian approach to intelligence sensemaking: It collaboratively paints a picture for a decision-maker rather than presenting a "scientific fact."

---

359 The authors would like to thank the following individuals for their assistance in the research that led to this chapter: David Colander, Richards J. Heuer, Jr., Robert K. Hitchcock, James Holden-Rhodes, Donald McGregor, Suzanne Sluizer, Joseph Tainter, Kristan J. Wheaton, and students in the 2007-2008 cohort of the Mercyhurst College Institute for Intelligence Studies. Thanks are also due to the participants of the Eurasia Group-sponsored conferences for their insights.

Work done by Least Squares Software was funded by IARPA under AFRL Contract Number FA8750-07-C-0312.

360 Johnston, *Analytic Culture*, 68-70. Johnston finds that "without specific processes, organizing principles, and operational structures, interdisciplinary teams will quickly revert to being simply a room full of experts who ultimately drift back to their previous work patterns."

The case study of sensemaking presented here is not merely a thought-experiment. It rests on a shortfall in understanding the security implications of non-state actors. In this instance, an original National Intelligence Council study prompted a further examination by an academic intelligence studies department and a government contractor. In all three studies partial sense of the issue was made. As we explore their independent work, we seek to apply intelligence rigor and discuss—admittedly in hindsight—how separate parts of the problem could benefit from a triangulation of concepts and approaches to provide a coherent, larger view of the security role of non-state actors.

Introducing the Wicked Problem of Non-State Actors

It is commonly thought that non-state actors are emerging as a dominant global force in the realm of national and international security, yet conclusive evidence confirming this belief is lacking. Part of the challenge is that non-state actors fit the profile of a wicked problem. While it is true they can be identified (the name accomplishes this — they are *non-state* versus *state* actors), there is no commonly accepted definition.[361] In other words, non-state actors are defined by what they are not, leaving room for disagreement as to what they are. Further, some non-state actors can be characterized as "good" and others as "bad." Differing points of view about whether a particular non-state actor is "good" or "bad" leads to varying characterizations of their activities. Attempting to "solve" a non-state actor problem leads to good or bad solutions that may provoke unanticipated (and undesired) consequences. For example, U.S. attempts to eliminate threats posed by Al Qaeda gave rise to a different and unexpected problem, that of a globally distributed network of Al Qaeda and Al Qaeda "wannabes." An argument could also be made that the apparently unique globalization of a terrorist organization was also unpredictable in foresight.[362]

---

361 National Intelligence Council, "Nonstate Actors: Impact on International Relations and Implications for the United States," Conference Report, August 2007, URL: <http://www.dni.gov/nic/confreports_nonstate_actors.html>, accessed 10 May 2010, The Conference Report suggested that "**Nonstate actors** are non-sovereign entities that exercise significant economic, political, or social power and influence at a national, and in some cases international, level. There is no consensus on the members of this category, and some definitions include trade unions, community organizations, religious institutions, ethnic groupings, and universities in addition to the players outlined above" (p. 2, emphasis in original)

362 In hindsight it seems obvious that, in an era when globalization is a driving force, a terrorist organization would naturally become a globalized phenomenon. However, we must adopt the point of view we enjoyed prior to 11 September 2001. At that time what occurred was largely unlooked for and unpredicted. Most of us simply could not conceive of such a group as being globalized or taking advantage of globalized resources. Therefore, in that context, it was unpredictable and we were surprised.

Issues involving non-state actors lack clear definitions and are resistant to traditional intelligence approaches due to their open-ended nature; potential solutions to problems are neither clearly right or wrong; and difficult-to-discern and complex inter-linkages exist, although drivers for issues involving non-state actors can be identified (see figure 6).

Once an insurgency or terrorist campaign (or any other non-state actor activity) begins, the issue shifts from being a merely wicked problem to a combination of wicked and tame problems. Some aspects of the issue remain wicked—ill-defined, no right or wrong solution, open-ended, and so on. However, other aspects of the issue are tame, although difficult to make sense of. For example, the tactics likely to be used in an insurgency are finite and understandable and making sense of them is a tame, bounded process. Yet countering them invokes a series of new wicked problems encapsulated in the larger issue and likely to lead to unanticipated consequences (many of them wicked problems in their own right)—as the United States discovered with its post-9/11 dealings with Al Qaeda.

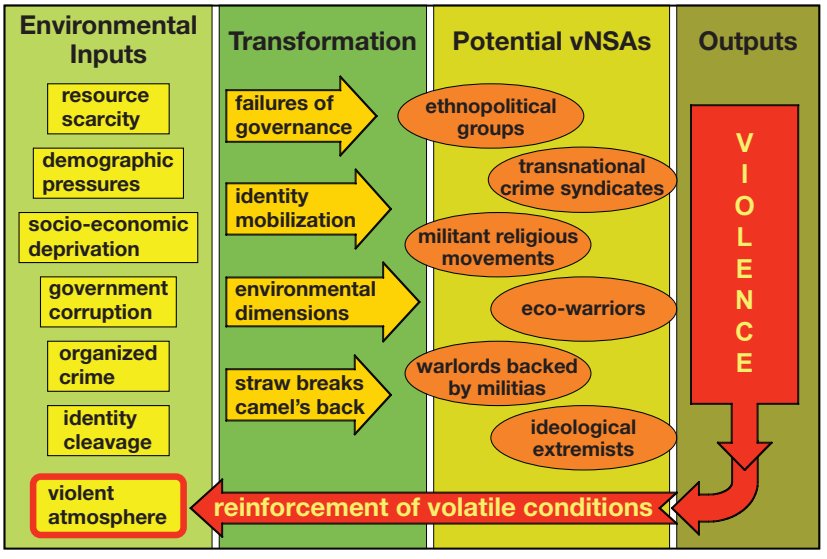


Figure 6. Drivers for the Rise and Growth of Violent Non-State Actors (vNSAs).
Sources: William Reynolds *et alia*, "Social Science Modeling Workshop: Understanding Iraqi Non-State Actors," Workshop Proceedings, Least Squares Software, Albuquerque, NM, 15 February 2008 (proprietary, used with permission). Image derived from Troy S. Thomas, Stephen D. Kiser, and William D. Casebeer, *Warlords Rising: Confronting Violent Non-State Actors* (Lanham, MD: Lexington Books, 2005).

Three Approaches to Making Sense of Non-State Actors

The starting point for this case study was a 2007 National Intelligence Council (NIC) Desktop Memorandum that analyzed key findings from a series of seminars co-hosted with the Eurasia Group, a global political risk research and consulting firm.[363] The Memorandum observes that non-state actors are of interest "because they have international clout, but are often overlooked in geopolitical analysis." The implicit but demanding questions of why and how much non-state actor "power" and "influence" have increased worldwide was not answered.[364] In light of this limitation, two follow-on projects were undertaken to complement the NIC study. First, the Mercyhurst College Institute for Intelligence Studies examined the impact of non-state actors in Africa. Then, a social science workshop convened by Least Squares Software of Albuquerque, New Mexico, under the auspices of IARPA, considered whether the influence and impact of non-state actors on international relations can actually be measured.

Key Findings of the NIC Study on Non-State Actors

A series of NIC-Eurasia Group seminars in 2006 and 2007 discussed in exploratory fashion how the proliferation of non-state actors since the end of the Cold War "is transforming international relations."[365] As a collaborative, prospective assessment, the study found that

> a globalization-fueled diffusion of finance and technology has enabled non-state actors to encroach upon functions traditionally performed by nation-states. This has facilitated their evolution into a

363 See the Eurasia Group web site, URL: <http://www.eurasiagroup.net/about-eurasia-group>, accessed 14 May 2010.

364 National Intelligence Council, "Nonstate Actors: Impact on International Relations and Implications for the United States," Conference Report, August 2007, URL: <http://www.dni.gov/nic/confreports_nonstate_actors.html>, accessed 27 April 2010, 2. Cited hereafter as NIC, "Nonstate Actors."

365 NIC, "Nonstate Actors," 1. The NIC study focused on so-called benign non-state actors—non-governmental organizations, multinational corporations, and super-empowered individuals—although it was impossible to have the discussions without frequent reference to terrorists, warlords, and other "malign" actors. The word "benign" is relative, but in this case refers to entities that at least give a nod to national and international institutions, laws, and norms. Nearly a decade earlier political scientists Philip Schrodt and Deborah Gerner derived similar conclusions about the post-Cold War explosion of *violent* non-state actors as agents of complex humanitarian crises. See Philip A. Schrodt and Deborah J. Gerner, "The Impact of Early Warning on Institutional Responses to Complex Humanitarian Crises," Paper presented at the Third Pan-European International Relations Conference and Joint Meeting with the International Studies Association, Vienna, Austria, 16-19 September 1998. Cited hereafter as Schrodt and Gerner, "CHC."

form unheard of even a few years ago. For example, "philanthrocapitalist" charities such as the Gates Foundation have greatly expanded notions of what a charitable NGO should look like.[366]

The discussions found that few non-state actors are completely independent of nation-states, and they do not have uniform freedom of movement. Further, non-state actors have the most latitude in either weak, or, at the other end of the spectrum, post-industrial states. The bulk of the world's population, however, lives in so-called "modernizing" states such as China, India, and Russia.[367] They remain entrenched in the class state system: firmly sovereign, centralized, and bureaucratic; using nationalism (including suppression of minorities) as an instrument of state power; and defining national security in terms of force. These nations have been highly effective in suppressing non-state actors or co-opting them through deployment of state-controlled substitutes including a subset of state-owned multinational corporations and enterprises (sometimes referred to as the mind-bending GONGO (government-operated non-governmental organization). The NIC-Eurasia Group discussions determined that the entity (aside from terrorists and criminals) that is most problematic for the United States is not technically non-state at all. It is instead the state-owned enterprise, often a front for advancing the interests of a modernizing-state government.

Finally, the NIC-Eurasia Group effort posited that the significance of "benign" non-state actors was that they propagated Western values in regions where these were absent. In this case, the problem was not that such actors were too powerful. Rather the opposite was the case: "in many parts of the world [benign non-state actors'] influence is limited—a factor that is contributing to the tilting of the global playing field away from the United States and its developed-world allies."[368]

Key Findings of the Mercyhurst Study on Non-State Actors

Students in the Mercyhurst College Institute of Intelligence Studies (MCIIS) focused on the roles non-state actors play and their expected impact in Sub-Saharan Africa over the next five years (*results*), and on building a multi-methodological paradigm for considering the issue (*process*).[369] Within this context, three additional questions were raised:

366 NIC, "Nonstate Actors," 1.

367 NIC, "Nonstate Actors," 1.

368 NIC, "Nonstate Actors," 1.

369 Mercyhurst College Institute for Intelligence Studies, "Terms of Reference: The Role of Non-State Actors in Sub Saharan Africa," Wikispaces.com, URL: < https://nonstateactorsafrica.wikispaces.com/Terms+of+Reference>, accessed 28 April 2010. Cited hereafter as MCIIS, "Terms of Reference."

- What is the likely importance of [Non-State Actors] vs. State Actors, Supra-State Actors and other relevant categories of actors in Sub-Saharan Africa?
- What are the roles of these actors in key countries, such as Niger?
- Are there geographic, cultural, economic or other patterns of activity along which the roles of these actors are either very different or strikingly similar?[370]

With respect to the first question, their research found that Africa can be organized into three geographical regions based on the roles that non-state actors play (figure 7): In Western Sub-Saharan Africa there are no clear trends in the roles played by non-state actors; in Central Sub-Saharan Africa, anti-government non-state actors are most active and likely to remain so over the next five years; and in Southern and Eastern Sub-Saharan Africa government

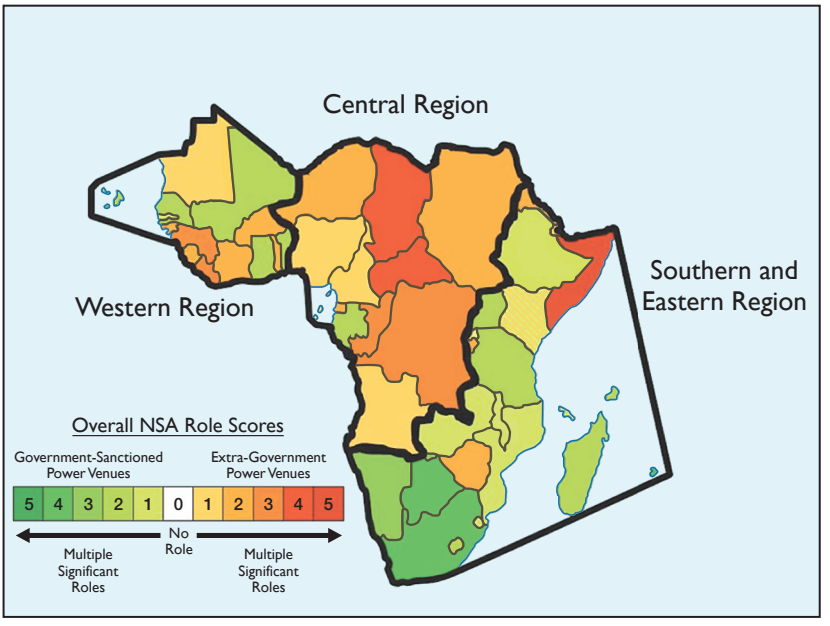


Figure 7. Composite Non-State Actor Role Scores for Africa.
Source: Mercyhurst College Institute for Intelligence Studies, URL: <https://nonstateactorsafrica.wikispaces.com/Are+there+geographic%2C+cultural%2C+economic+or+other+patterns+of+activity+along+which+the+roles+of+these+actors+are+either+very+different+or+strikingly+similar%3F>, accessed 2 March 2008.

370 MCIIS, "Terms of Reference."

sanctioned non-state actors are likely to wield the most influence.[371] Additionally, there appeared to be a strong correlation between the number of government-sanctioned multinational corporations and the number of NGOs. Finally, it seemed that terrorist organizations in Africa preferred operating in "countries with relatively more than less state control."[372]

The students developed a scoring system for both lawful and unlawful non-state actors, in terms of the socio-political environment, and applied this index to all 42 Sub-Saharan African countries (figure 7). The scoring characterized the roles of non-state actors vis-à-vis government and non-government interactions based on four drivers: An "ease of doing business" variable and a contrasting "corruption perception" variable; a democracy variable and a contrasting failed states variable.[373] Stable and failing states were revealed to have differing interactions with non-state actors. In the former, non-state actors were lawful actors who tended to have government-sanctioned role potentials, whereas in the latter they were typically unlawful actors engaged in anti-government roles. Botswana (a stable state) and the Central African Republic (a failed state) were representative of each (shown in figure 8). Of greater interest were the indicators for Kenya (figure 9), because they signaled or *anticipated* stability issues. The assessment was born out by the events that occurred during and after the early 2008 elections.[374]

Mapping significant multinational corporations, NGOs, and terrorist organizations to specific countries as representative of non-state actor activity revealed correlations between role potential spectra and geospatial data, whereby each generally supported the other.[375] Thus, geospatial sensemaking tended to confirm the conclusions derived from the non-state actor role spectra.

---

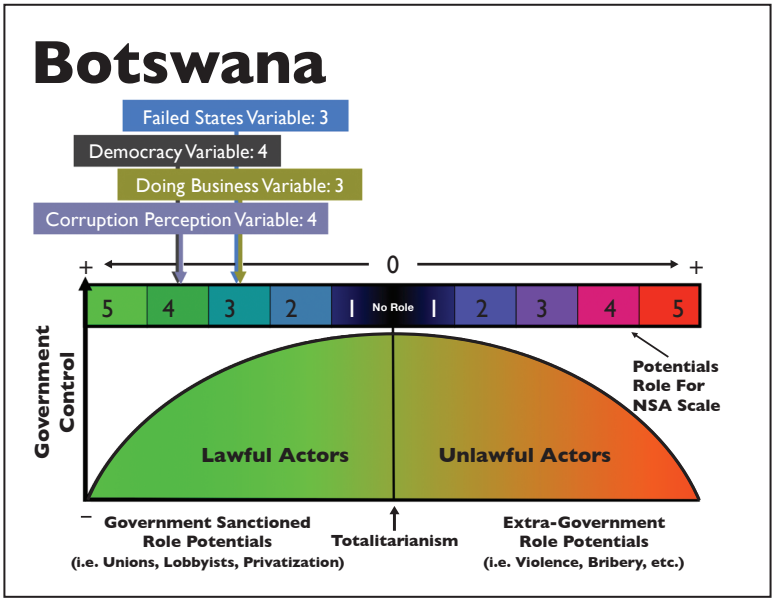
371 Mercyhurst College Institute for Intelligence Studies, URL: <http://nonstateactorsafrica.wikispaces.com/Key+Findings>, accessed 2 March 2008. Cited hereafter as MCIIS, "Patterns of Activity."

372 MCIIS, "Patterns of Activity."

373 MCIIS, "Process and Methodology." The roles of non-state actors were tracked on a scale anchored by scores from six sample totalitarian states: North Korea, Cuba, Iran, Syria, Myanmar, Laos, and Libya.

374 Kristan J. Wheaton, email to the author, 4 March 2008. Such foresightful activity by students is not unknown. Schrodt and Gerner report a similar result involving student predictions about the state of the Iraq-Kuwait crisis in December 1990. Kahneman and Klein's remark about some individuals being able to discern correctly patterns that others miss (Chapter 5) is probably relevant in explaining both phenomena. See also Schrodt and Gerner, "CHC", 5.

375 Mercyhurst College Institute for Intelligence Studies, "Non-State Actors in Sub-Saharan Africa 2007-2012 Outlook," URL: <https://nonstateactorsafrica.wikispaces.com/Key+Findings>, accessed 2 march 2008. Cited hereafter as MCIIS, "Outlook."



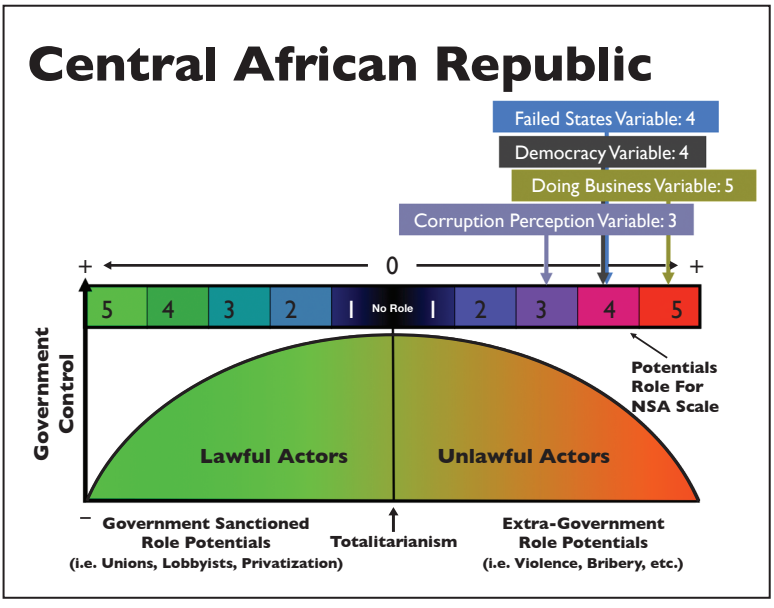


Figure 8. Non-State Actor Potential Spectra for Botswana and the Central African Republic.

Source: Mercyhurst College Institute for Intelligence Studies, "Role+Scores.ppt", URL: <https://nonstateactorsafrica.wikispaces.com/Model+for+SFAR>, accessed 2 March 2008. Cited hereafter as MCIIS, "Role Scores."

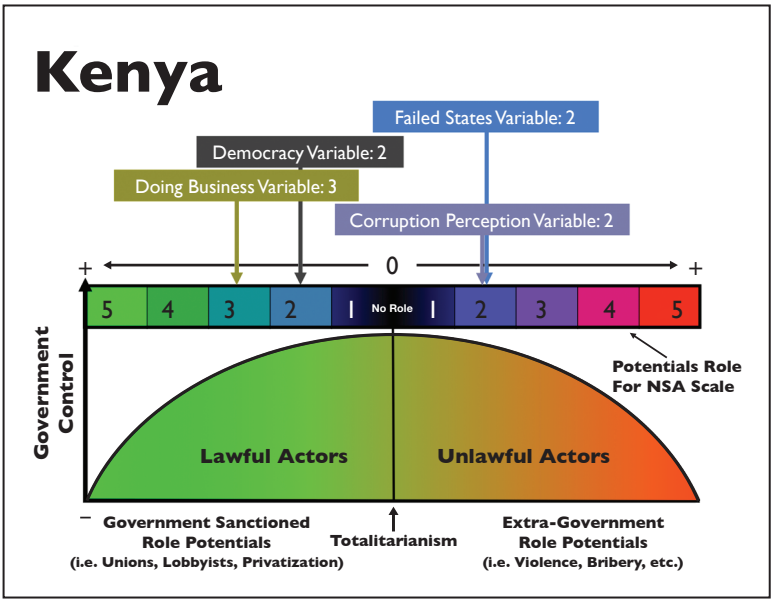


Figure 9. Kenyan Non-State Actor Potential Spectra.
Source: MCIIS, "Role Scores."

Key Findings of the Least Squares Study on Non-State Actors

The Least Squares study of non-state actors began with the hypothesis that "non-state actors emerge in vacuums and voids."[376] Their study focused on the issue of violent and non-violent non-state actors but also explored a set of contingent methodological approaches. The inquiry sought to contribute novel understanding of non-state actors by

> synthesizing available data and disparate taxonomies,…by generating and testing hypotheses concerning the key dynamics driving the transfer of power from states to [non-state actors] and favoring the emergence of novel [non-state actors] under globalization; and…by investigating the development of methodologies that might be most useful for future research.[377]

Two key findings revealed the critical role of environmental knowledge and of public expectations in motivating non-state actors, both as individuals and as members of the collective. Such findings were found to be

376 Marta S. Weber, William N. Reynolds, James Holden-Rhodes, and Elizabeth J. Moore, *Non-State Actors in the Post-Westphalian World Order: A Preliminary LSS Inquiry*, Final Report for Air Force Research Laboratory (AFRL) Contract FA8750-07-C-031, March 2007, 6. Cited hereafter as Weber and others, *Non-State Actors*.

377 Weber and others, Non-State Actors, 6.

significant to efforts aimed at mitigating the recruitment of specific Al Qaeda-associated individuals to assail the United States. Additionally, the team found that an approach based on critical thinking led to reasoning pathways that likely would not have been noticed or explored had a more intuitive and less rigorous approach been employed.[378]

Approaches and Methodologies

Thinking Critically about the Issue

In order to impose structured thinking on a highly unstructured problem, the NIC advisor to, and the members of LSS first inventoried their own understanding of the non-state actor issue using the "eight elements of reasoning" developed and espoused by the Foundation for Critical Thinking and used throughout much of the IC.[379] These elements include:

- Question at issue (What is the issue at hand?)
- Purpose of thinking (why examine the issue?)
- Points of view (What other perspectives need consideration?)
- Assumptions (What presuppositions are being taken for granted?)
- Implications and consequences (What might happen? What does happen?)
- Evidence (What relevant data, information, or experiences are needed for assessment?)
- Inferences and interpretations (What can be inferred from the evidence?)
- Concepts (What theories, definitions, axioms, laws, principles, or models underlie the issue?

A summary of several of the NIC and LSS perspectives on non-state actors based on this exercise are provided in table 4. Both groups agreed that a critical thinking approach was useful in developing a common understanding of the problem as it helped to ensure that the participants questioned their own thinking about non-state actors, rather than relying on previously held presumptions.

---

378 These points are derived from William Reynolds' observations of and discussions with fellow LSS Workshop participants.

379 Moore, *Critical Thinking*, 8-9; Richard Paul and Linda Elder, *The Miniature Guide to Critical Thinking: Concepts and Tools*, Sixth Edition (Dillon Beach, CA: Foundation for Critical Thinking, 2009), 3-6. Some practitioners in the U.S. Intelligence Community (among them one of the authors) in late 2008 expanded these eight elements of reasoning to ten based on the work of Gerald Nosich. Included were "alternatives," which makes explicit the fact that there are other ways to view an issue; and "context," which considers the fact that most issues or problems are themselves a piece of some larger issue or problem: There is a broader background for the issue that must be explored. See Nosich, *Learning to Think Things Through*, 96-98.

Table 4. Comparing NIC and LSS Critical Thinking Perspectives: Purpose, Points of View, and Assumptions	
Purpose	
NIC Perspective	***LSS Perspective***
To test whether the influence and impact of non-state actors on international relations can be measured; if so, whether they are serious competitors for power with nation-states; and the implications for US foreign policy.	ID role of non-state actors; Determine influence of non-state actors compared to state actors; Assess utility of sensemaking methodology/Multimethodology (MM) mechanisms of non-state actors role/influence; Develop/Define the concepts of non-state actors Influence/Impact; ID MM's useful for assessing impact/role of non-state actors; ID MM's/problem motifs of general interest to other research contracts;
Points of View	
NIC Perspective	***LSS Perspective***
Although non-state actors seem to be more powerful than ever before in history, few of them act in total independence from nation-states and their influence and impact are highly dependent upon which part of the world is under discussion. Another (and common) point of view is that powerful non-state actors are universal and a serious threat to nation-states.	"Victims"/Beneficiaries of non-state actor impact: Policy Makers Minimizing Risk Achieving Agenda Other non-state actors Analyst—understand/advise Methodologist/Researcher—Identify techniques for understanding Useful methods Understand/advise Sub interest structures within non-state actors and States

Table 4. Comparing NIC and LSS Critical Thinking Perspectives: Purpose, Points of View, and Assumptions (Continued)	
Assumptions	
NIC Perspective	***LSS Perspective***
Our point of view: implications for the US of the rise of powerful non-state actors depend upon which part of the world is under discussion. At times, our main concern may be that benign non-state actors are excluded from, or usurped by, certain states. The common point of view: all non-state actors in all parts of the world have serious implications for national governments (including that of the US).	Relation between nature of country and nature of economy—concept of *industrial* as an important discriminator; That we can induce truths from examples — commonalities -> analogy -> truth; Normative idea that pursuit of self interest a driver in observed outcomes: The frame of a value system—suicide bombing makes different sense in different frames; Idea of a pro/con/fix or ACH type approach to value outcomes in different frames; *International* means "between nations." Are we only concerned with "international" phenomena?

Source: Participant notes, edited by the authors.

Literature Consultation

Concurrent with their critical thinking, MCIIS, LSS, and others examined key academic and applied-academic works related to the assessment of non-state actors. Notable among them, work by Bas Arts and Piet Verschuren describes a qualitative method for assessing the influence of stakeholders in political decision-making.[380] The "triangulation" referred to in their title encompasses "(1) political players' own perception of their influence; (2) other players' perceptions of the influence brought to bear; and (3) a process analysis by the researcher."[381] Arts and Verschuren tested this method through an assessment of the influence of NGOs on the 1992 Climate Convention. Their

380 Bas Arts and Piet Verschuren, "Assessing Political Influence in Complex Decision-Making: An Instrument Based on Triangulation," *International Political Science Review*, vol. 20, no. 4 (1999): 411-424. Cited hereafter as Arts and Verschuren, "Assessing Political Influence."

381 Arts and Verschuren, "Assessing Political Influence," 411.

work remains significant because attempts to measure or associate numbers with non-state actor power or influence have been so rare.

Another contribution in the applied realm came from recent work by a new generation of military (and ex-military) authors who see the rise of non-state actors as a seminal event that will drive U.S. national security strategy. Among these sources is *Warlords Rising: Confronting Violent Non-State Actors*, whose authors anchor their work in open systems theory (the concept that actors and organizations are strongly influenced by their environment).[382] In particular, they ask what environments give rise to violent[383] non-state actors, what sustains them, and how changes to those environments might disrupt them.

Application: Indicators of Non-State Actor Power in Africa

The project afforded the Mercyhurst team an opportunity to develop a promising new method for intelligence sensemaking and to catalogue its advantages and disadvantages (table 5). The students were able to validate their findings employing three different methods as well as different evidence sets and also assess their methodological validity. This kind of meta-sensemaking could constitute a bridge between now-traditional IC efforts and a revolutionary approach to building a sensemaking argument in official circles.

Of note is a remark by project supervisor Professor Wheaton: "The big advantage [of the multimethodological approach] was the ability to see similar patterns crop up again and again by looking at the data in different ways. This increased their [the students'] confidence enormously."[384] Additionally, given the temporal context (short) and the scale of the project (large) a multimethodological approach was perhaps the only means of tackling the problem. Finally, as Wheaton also notes,

> we may well be wrong about Liberia or some other country in the current study but we are unlikely to be wrong about every country and highly unlikely to be wrong about every country in the same direction. Assuming the model is reasonably accurate and given

382 Troy S. Thomas, Stephen D. Kiser, and William D. Casebeer, *Warlords Rising: Confronting Violent Non-State Actors* (Lanham, MD: Lexington Books, 2005). Other key books in this genre are General Rupert Smith, *The Utility of Force: The Art of War in the Modern World* (New York, NY: Alfred A. Knopf, 2007) and John Robb, *Brave New War: The Next Stage of Terrorism and the End of Globalization* (New York, NY: John A. Wiley and Sons, 2007).

383 *Warlords Rising* is focused on violent non-state actors, but the present authors find that the question of environmental factors is readily applicable to benign non-state actors as well.

384 Kristan J. Wheaton, email to William N. Reynolds, 15 November 2007. Cited hereafter as Wheaton, email to Reynolds, 15 November 2007.

Table 5. Advantages and Disadvantages of Each Method	
Role Potential Spectrum Analysis	
Advantages	***Disadvantages***
Created a standardized foundation to measure environmental influences on the roles of non-state actors to produce comparable findings across Sub-Saharan Africa states. Created a prediction model for the roles of non-state actor in a country. The state centric environmental approach allowed the analysts to effectively consider key factors across the entire socio-political environment of individual Sub-Saharan African countries Able to represent both government sanctioned and extra government role potentials for non-state actors. Guided further efforts to efficiently identify and assess significant indicative characteristics of the socio-political environments in Sub-Saharan Africa.	The major indices in unaltered states are unsuited for measuring the role of non-state actors. The matrix required several weeks to finish, and took time away from starting and completing other types of analysis. Would be difficult for other analysts without statistical background to successfully complete.
Geospatial Analysis	
Advantages	***Disadvantages***
Created a visual representation allowing the team to identify patterns and correlations among different sets of data, particularly with the statistical matrix. Independent from other analyses. Information retrieved from uniform databases; not truly random, but relatively objective sample. Simple and easy to do with the information being imported from Excel Spreadsheets directly into Community Walk.	Much of the available information on NGOs, terrorist groups, and businesses was not in English, which made it difficult to collect a larger sampling of the information. The team limited the NGO map to development, women's rights, HIV/AIDS, human rights, and environmental issues. This was not an exhaustive list of all the different NGOs operating within the region.

Table 5. Advantages and Disadvantages of Each Method (Continued)	
Analysis of Competing Hypotheses	
Advantages	***Disadvantages***
Able to detect an increase or decrease in the roles of non-state actors. Uniform sources throughout. Easy for team to complete (received in-class instruction on this type of analysis).	Dependent upon completion of the matrix analysis. Evidence selected tends to be subjective. Susceptible to confirmation bias and the anchoring effect.

Source: Mercyhurst College Institute for Intelligence Studies, "Teams' Non-State Actors Process and Methodology Report," Wikispaces.com, URL: <https://nonstateactorsafrica.wikispaces.com/Process+and+Methodology>, accessed 2 March 2008. Cited hereafter as MCIIS, "Process and Methodology."

> the sample size, then, we can have more rather than less confidence about the broader conclusions and are likely right about the overall picture.[385]

Such a conclusion is significant for the larger IC. Through this still-experimental application of methods and models we may be able to develop a means of increasing the accuracy of intelligence sensemaking when time is short and the scope is large.

Application: A Multi-Disciplinary Workshop on Non-State Actors

In February 2008, LSS brought together a methodologist, an economist, a political scientist, two psychologists, an anthropologist, and a computer scientist to test the *Warlords Rising*, open-systems approach against a real-life problem: the roles of three sets of non-state actors (representing the three major ethnic groups) in Iraq: Shi'a militia, Sunni sheiks, and Al Qaeda in Iraq (AQI). Participants used three frameworks to consider the environment within which the three groups exist and operate.

- ***Points of segmentation*** are the boundaries or borders between and among groups of people, where the degree of disagreement on

385 Wheaton, email to Reynolds, 15 November 2007.

issues is indicated numerically.[386] Points of segmentation can track inherent characteristics such as gender or ascribed cultural differentiators such as Sunni or Shiite. The set of points distinguishes one individual or group from another and identifies possible points of cooperation and conflict that can be exploited. Specific values for points of segmentation are derived from an expert assessment of the strength of the actors' expressed attitudes, reinforced by observable behavior. They distinguish one individual or group from another, and identify the points most suitable for exploitation by the protagonist. Numbers were elicited from experts, calibrated against one another for consistency, and used to quantify expert consensus. Computer modeling by Least Squares addressed five pertinent actors: two state-associated, the Iraqi government and the U.S.-led coalition forces; and three non-state-associated actors, the Shi'a militia, the Sunni sheiks, and AQI. The modeling was conducted along five points of segmentation: Arab versus non-Arab; Islamicist versus non-Islamicist; rural versus urban; Sunni versus Shi'a; and strength of tribal allegiance. These issues form a 5-dimensional space — the cells in figure 10 depict the distance between players in this issue space.[387] One especially revealing point of segmentation centers around the question of expected attitudes and behavior in Anbar Province found AQI and Coalition forces on one side, with Shi'a militia, Sunni sheiks, and the Iraqi government on the other side.

As noted by one of the workshop participants, there are three significant implications to segmentation for policy and decisionmakers: First, projects proceed most smoothly *within* a segment. Second, segments that are neglected or discriminated against will push back. Finally, brokers mediating inter-segmental projects need to be viewed as impartial.

---

386 Points of Segmentation is an anthropological term referring to the natural pattern of social divisions within kinship-based societies, in which kinship units form as internally cooperative units. Conflict occurs between segments composed of distinct kinship lines. Segmentation is also used to describe the anthropological analysis of societies into kinship-based units. See Rudolph J. Rummel, *Understanding Conflict and War: War, Power, Peace* (Beverly Hills, CA: Sage Publications, 1991); Benoit Rihoux, "Constructing Political Science Methodology: From Segmented Polarization to Enlightened Pluralism," Joint Chair, Standing Group on Political Methodology. IPSA Conference, Montreal, Canada, 2008; George De Vos and Lola Romanucci-Ross, eds., *Ethnic Identity: Cultural Continuities and Change* (Palo Alto, CA: Mayfield, 1982); and William S. McCallister, "COIN and Irregular Warfare in a Tribal Society," *Small Wars Journal, Blog and Pamphlet, 4 February 2008*, URL: <http://www.smallwarsjournal.com/documents/coinandiwinatribalsociety.pdf>, accessed 31 May 2010.

387 The technique can be further refined by weighting the different issue axes using expert knowledge. We have omitted this part for brevity.

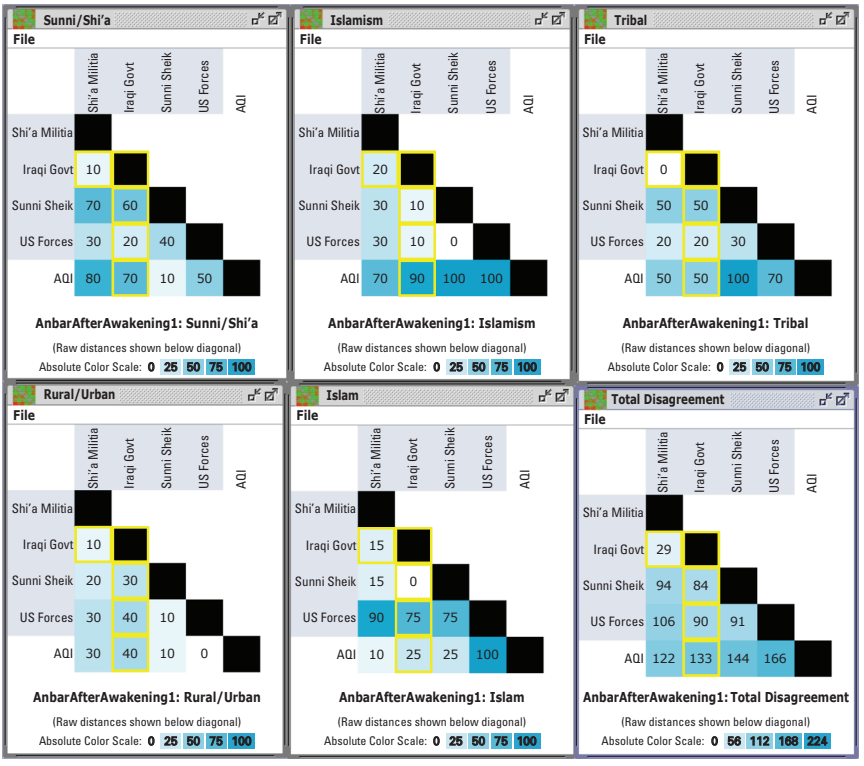


Figure 10. Iraqi Points of Segmentation.

Source: William Reynolds *et alia*, "Social Science Modeling Workshop: Understanding Iraqi Non-State Actors," Workshop Proceedings, Least Squares Software, Albuquerque, NM, 15 February 2008.

- ***Prospect theory***, originally developed by Kahneman and Tversky, posits that "people tend to be risk-preferring when facing long shot risks involving significant gains, such as betting on race horses, and are risk averse when facing significant losses: [in other words, when] buying a home or car insurance" respectively."[388] Workshop participants concluded that in Iraq, expectations contribute to environments where individuals (and communities) are likely to support or to become non-state actors. Assessment of findings from

388 "Why do People 'Play the Longshot' and Buy Insurance? It's in Our Genes," *Genomics and Genetics Weekly*, 29 January 2010, 184. For a technical description of prospect theory see Daniel Kahneman and Amos Tversky, "Prospect Theory: An Analysis of Decision Under Risk," *Econometrica*, vol. 47, no. 2 (March 1979): 263-291; and Amos Tversky and Daniel Kahneman, "Advances In Prospect Theory: Cumulative Representation of Uncertainty," *Journal of Risk and Uncertainty*, vol. 5 (1992): 297-323.

the application of prospect theory to the Iraqi environment are ongoing, and will be published in forthcoming studies.

- ***Institutional interactions*** is the name associated with a systematic model that allowed workshop participants to explore the complex roles non-state actors play as they influence (and are influenced by) overlapping institutional capabilities and needs.[389] The participants concluded that even a simple model of institutional networks has enormous complexity—or high entropy—making it a good candidate for a subsequent in-depth modeling project. Due to imposed time constraints, development and application of the modeling was not completed.
- ***Morphological Analysis*** was identified as an additional approach through the institutional interactions method. Morphological analysis considers an entire space of possible implications opening the way for follow-on disambiguation (perhaps using additional multimethodological approaches) in order to abductively and soundly derive the kind of judgments that become useful knowledge.[390]

The workshop participants were unable to formally triangulate the results from the three approaches, also because of insufficient time. Their discussions and modeling, however, supported the *Warlords Rising* thesis: that environment is a critical factor in understanding the emergence and roles of non-state actors. Additionally, the modeling appeared to provide a promise of metrics that, with further development, can be applied against the non-state actor problem.

Critical Assessment: Lessons Learned from the Study of Non-State Actors

No matter what the methodological approach, project participants emphasized that close attention to environmental factors remains a key to understanding non-state actors. Nonetheless, even those approaches that emphasized environmental factors fell prey to certain inadequacies.

---

389 The application of this model is exemplified in Robert Gibbons and Andrew Rutten, "Institutional Interactions: An Equilibrium Approach to the State and Civil Society," *IQ* online journal, The Institute for Quantitative Social Science at Harvard University. URL: <http://www.iq.harvard.edu/files/iqss/old/PPE/gibbons+rutten.pdf>, accessed 14 May 2010.

390 Morphological Analysis is an approach for considering all the factors and their interrelationships in non-quantifiable, multidimensional problems. Developed by Swiss astrophysicist Fritz Zwicky, morphological analysis begins with the premise that "within the final and true world image everything is related to everything, and nothing can be discarded *a priori* as being unimportant." [Fritz Zwicky, *Discovery, Invention, Research—Through the Morphological Approach* (Toronto, CA: The Macmillan Company, 1969), 44.] It is particularly well suited (and often used) to make sense of non-quantifiable wicked problems.

Both the Mercyhurst and the LSS teams adopted multimethodologically rich approaches to making sense of non-state actors; both quantitative and qualitative methods were employed. While novel insights were generated as has been noted, no means emerged to quantify a specific increase or decrease in non-state actor roles worldwide. Although the multiple methods framed the issues in both complementary and contradictory ways, none, singly or in combination, answered the question of "how much non-state actor 'power' and 'influence' have increased worldwide."[391]

That the members of each study group were working independently supports the contention that the groups were not somehow engaged in a confirmation exercise of each other's work; the conclusions were independently derived. What cannot be determined, however, is the extent—if any—to which specific methods employed in the specific efforts may have impacted conclusions derived from subsequently employed methods (especially in the cases of the MCIIS and LSS teams).

Serendipitous conclusions such as the possible indicator of state instability as illustrated in the case of Kenya by the Mercyhurst team, and the interesting points of segmentation found by the LSS team, suggest further avenues of intelligence research and modeling. The division of Africa reflecting three zones of non-state actor influence was also interesting. But these conclusions, while novel, did not satisfy the initial requirement, a quantification of phenomena associated with change in the power positions of various non-state actors. While all three teams clearly engaged in critical thinking about the issue, as viewed in hindsight, different purposes (specifically as expressed by the NIC/LSS team) led to conclusions different from those of the original, albeit implied, question. That these purposes were different could have been seen as an indicator that the teams were working on different problems within the issue of non-state actors. Coming to a consensus of what the actual tasking was could be expected to have narrowed the divergent results and provided a more specific answer about how the roles of non-state actors have changed.

Changes in the Roles of Non-State Actors: An Alternative View

A systematic review of what was done and not done in the three non-state actor studies provides insights into how critical thinking can combine with multimethodological, mindful sensemaking, to provide a paradigm for 21st Century intelligence creation and its active communication to

391 NIC, "Nonstate Actors," 6.

policymakers in a fashion that transcends the Sherman Kent tradition. This review is facilitated by employing the ten elements of reasoning noted above.

- **Question:** the beginning question of the NIC-Eurasia Group seminars was, "If non-state actors are emerging as a dominant global force, where is the evidence?" In other words, while there appears to be a consensus that they are a dominant global force, where is the formal evidence? For example, given the premise that we are experiencing an emerging phenomenon, is there evidence that non-State actors wield more power in 2010 (or in 2007 when the original study was made) than they did a decade earlier? A key question, and really the central question, to be answered is first, how does one measure the relative power of non-state actors? A follow-on question to this becomes, "Is such power therefore sufficient to render them dominant global forces?"
- **Purpose:** Determine whether or not there is evidence that non-state actors are emerging as a dominant global force. This problem is one of basic research to determine if the evidence in fact exists. However, the underlying issue of how we might measure relative power must first be conceptualized and addressed.
- **Points of View:** As we consider the original and complementary studies, there are two predominant points of view at issue: first, that of the NIC and its customers—who may believe that non-state actors are an emerging global force and want to quantify this shift in influence and power. The other, unavoidable point of view is that of non-state actors—some of whom would believe they are an emerging force and some who would not believe they are. For example, Al Qaeda, as a non-state actor, might want to believe (and might be justified in believing) that they are a significant global force. On the other hand, a super-empowered individual might believe she or he is not a significant global force (and yet, might be one).

  Each group that considered the issue also reflected different points of view. The NIC-Eurasia Group study focused on three broad categories of "benign" non-state actors: non-governmental organizations, multinational corporations, and super-empowered individuals. Mercyhurst focused on all categories of non-state actors and the LSS workshop focused primarily on violent non-state actors in Iraq. Among other things, this differentiation of what constitutes a non-state actor also reflects different interpretations of the key question. Each group brought its own perspectives about its larger focus as well. For example, both the Mercyhurst and LSS approaches to the

issue reflected a strong reliance on structured methods as the means of making sense of issues. The Eurasia group imparted a more intuitive approach by subject matter experts. A more explicit accounting of the points of view embodied at each stage of an ongoing study would help both intelligence producers and their policymaking counterparts maintain a focus on their respective stakeholders' concerns and opportunities.

- **Assumptions:** The use of the term "non-state actor" as an apparent all-encompassing term in the initial problem question and statement presumes an initial understanding and consensus about what is or is not a non-state actor. This is actually inaccurate as the differing foci of the three groups make clear. However, the differences in this case become evident in hindsight although measures could be taken in foresight to at least check the understanding of different groups engaged in collaborative assessments.

  Greater precision of the term non-state actors is needed. Differentiating between benign and non-benign non-state actors is a first step. Subsequent refinements of "benign non-state actors" into non-governmental organizations, multinational corporations, and super-empowered individuals is also useful. A similar set of distinctions within the set of violent non-state actors is also necessary. Then, a crosscheck among the teams must be accomplished so that consensus on the meaning and use of these terms is achieved.

  Another assumption involves what is meant by the term "dominant global force." Again, both greater precision and clarity is needed in coping with this assumption. One key question is, "Exactly what does dominant global force mean?" One answer to this could be that everywhere on the planet non-state actors are *the* force affecting politics and life. Such a simplified and simplistic view is likely inaccurate, and a range of political process models—among them those of the "rational actor," of "bureaucratic politics," and of "organizational process," need to be parsed.

- **Implications and Consequences:** The consideration of implications and consequences means to anticipate and explore the events that follow a decision, and to put in play especially the interpretive aspect of sensemaking. In the context of non-state actors, it means to explore what happens if non-state actors are (or are not) emerging as dominant global forces and we are right or wrong about their power. Regardless of whether non-state actors are a dominant global force, if their influence is underestimated then surprises can

be expected: Some non-state actor is likely to act in a fashion that is completely unexpected and with unanticipated results. On the other hand, overestimating the influence of non-state actors might create self-fulfilling prophecies. If, though, the influence of non-state actors is accurately measured it may be possible to mitigate that influence (where the non-state actors are acting on interests at odds with those of the United States). Alternately, where non-state actors are acting in consonance with the interests of the United States or are able to exploit opportunities put in place to get them to be helpful, the United States fulfills its goals.

Finally, the sensemakers' interpretation of likely actions or events allows the implications and consequences of those actions to be considered, even if absolute prediction is elusive. Here, in the context of collaborative sensemaking through the communication of intelligence to a policymaker, we understand the admonition of Sherman's Kent's contemporary critic, Willmoore Kendall, that intelligence most critically "concerns the communication to the politically responsible laymen of the knowledge which…determines the 'pictures' they have in their heads of the world to which their decisions relate."[392] This vision suggests communication of intelligence as an "insider" rather than offering "intelligence input" at arms length in the Kent paradigm.[393] Kendall faults Kent's equation of wartime and peacetime intelligence, insisting that peacetime intelligence represents a more strategic calling that requires intelligence to consider the course of events as something one must influence, by making what he distinguishes as "contingent predictions."[394] An issue in the case at hand is whether interactions of the United States with non-state actors represent those of war or peacetime intelligence frameworks. Additionally, given the wicked nature of the issue, Kendall's more tailored, "insider" paradigm may prove better in assisting the policy customer in grasping the issue and its contingent predictions.

---

392 Kendall, "The Function of Intelligence," 550. One might guess that Kendall had in mind the clear depiction of what we now typically call "scenarios."

393 Richard K. Betts, in *Enemies of Intelligence* (chapter 2), argues for a modulated "politicization" of intelligence. He identifies Secretary of Defense and former Director of Central Intelligence Robert Gates as an effective leading exponent of the "insider" approach. Ultimately, Betts declares, "Taxpayers hire intelligence analysts not to produce truth for its own sake but to produce useful truth," 78.

394 Kendall, "The Function of Intelligence," 549.

- **Evidence:** What evidence is needed to determine that non-state actors are, and as importantly, are *not* an emerging dominant global force? As we have seen, each group gathered and sifted considerable information on non-state actors, some of it highly relevant to the central question and some not. To the best knowledge of the authors, each of the three groups chose and evaluated evidence only with inductive logic. They did not take advantage of a means, available in particular to a community with robust intelligence capabilities, to deductively eliminate one of the two possibilities.

  A seminal essay by an Israeli intelligence practitioner, Isaac Ben-Israel, explains how a technique, viewed in retrospect, would have led the Israelis to dismiss deceptive indicators of Arab preparations and to expect the coordinated attack in October 1973.[395] His finding rests on the idea that intelligence foraging and marshaling capabilities can be used efficiently to focus on a greatly reduced information stream if the reports that support both options (in this case Arab war preparations or exercise) are simply set aside. Reports that are incompatible with either war preparations, on the one hand, or with activity being only an exercise on the other, are few enough to explore with special intelligence means.[396] A focus on detecting evidence of deception in either of those sets would at least bring efficiency to the sensemaking process. In the case of the emerging roles of non-state actors, examining evidence that neither is happening and why would yield alternative views and might also force a disconfirmatory framework allowing better disambiguation of all the hypotheses. The application of this method to intelligence issues is likely not as difficult or inconvenient as practitioners may guess.[397]

---

395 Isaac Ben-Israel, "Philosophy and Methodology of Intelligence: The Logic of Estimate Process," *Intelligence and National Security*, vol. 4, no. 4 (October 1989): 660-718. Cited hereafter as Ben-Israel, "Philosophy and Methodology of Intelligence."

396 Ben-Israel, "Philosophy and Methodology of Intelligence," 709.

397 The challenge of "one-off" prediction is especially inviting to proponents of applying deductive logic to the collection and analysis of evidence. Practitioners who consciously employ this technique can demonstrate to later investigators or inquisitors the logical as well as intuitive steps they took with respect to evidence, such as often occurs in intelligence. In other domains (such as weather forecasting) predictions are constantly updated as inputs to atmospheric models change and as new inputs are revealed. Further, if only an inductive approach to evidence collection and processing is used, when intelligence predictions change, intelligence customers and overseers are often quick, in their own inductive and intuitive way, to criticize either the original or revised results (depending on which set of results they agree with). Thus, a 21st Century approach to forecasting must adopt a constantly updated, deductive paradigm if it is going to be accurate against constantly shifting adversaries and issues.

- **Inferences and Conclusions:** With three different and independent efforts, the challenge lies in ensuring a useful triangulation of the results of those potentially disparate efforts. The Mercyhurst approach (internally triangulated) found that non-state actors, both legal and extralegal, are least effective in authoritarian states. Using Iraq as a case study, the Least Squares workshop demonstrated that within the context of either failed or failing states, expectations and perceptions of the public, or the political environment, are key drivers in anticipating the likelihood of actions by (violent) non-state actors. Strident or acrimonious expression of dissent that arises when domestic and international political/economic issues reinforce each other within the United States and Europe suggest a possible correlation in post-industrial states. This leads to a general conclusion that when expectations are at odds with situational reality, non-state actor activity increases.

  Together, these findings may assist in anticipating the likelihood of future actions by non-state actors. As Schrodt and Gerner note, "political predictions tend to be short-term rather than long-term."[398] Yet, as they also note, effective warning (of a complex humanitarian crisis, for example) requires a fairly long lead-time:

  > Warnings of less than three months provide insufficient lead time for most non-military organizations to react; in other words, the responses to a warning of less than three months will look pretty much the same as a response to a situation that develops without warning.[399]

- **Concepts:** Not only the assumptions, but other concepts as well were in play at multiple levels in the non-state actor case studies. The very notions of "non-state actor" and the ideas of democracy, authoritarianism, and anarchy needed clarification, ideally through well-grounded, empirical as well as theoretical research, to ensure common understanding.
- **Alternatives:** If non-state actors are not emerging as a dominant global force, then what can we say about their global role? Is their influence staying the same? Is it diminishing? Given a credible means of measuring change in the influence and power of non-state actors, the next step in this study of non-state actors would be to examine hypotheses generated from these alternative questions.

398 Schrodt and Gerner, "CHC," 4.
399 Schrodt and Gerner, "CHC," 4.

Such follow-on studies also examine and attempt to make sense of instances where non-state actor influence has waned. As was noted by the Eurasia group, in some situations, pro-Western non-state actors actually shift influence away from themselves and the United States and its allies.

- **Context:** As has been repeatedly noted, non-state actors present both a challenge to U.S. interests and an opportunity for advancing those interests. The U.S. would like to mitigate the challenges and take advantage of the opportunities. How to make that happen in domains and regions of little existing U.S. influence or of waning U.S. and Western influence becomes a key concern as the United States strives to carry out a meaningful global role. Future attempts to make sense of the role of non-state actors may benefit from tapping into the larger context of recent policy-relevant literature on the problem of fragile states in applied academic journals.[400]

Moving Beyond a Proto-Revolution

Microcognition and Macrocognition in the Study of Non-State Actors

There emerge two very general domains of which intelligence professionals must make sense: that of the relatively static, state-based system and that of the much more dynamic non-state actor. Of course, these do not exist in isolation from one another. There are boundaries, interstices, and points of segmentation; there is considerable overlap when one usurps or adopts the actions of the other. Further, the separate domains of domestic and foreign areas of interest and action, embraced by the Kent model of intelligence creation and communication, have been superseded by an indivisible, worldwide web of personal and organizational relationships. Broadly speaking, the "classic" model of intelligence sensemaking largely sufficed and perhaps continues to suffice when issues remain clearly tied to the political entities associated with the Westphalian system of state-based power. However when dealing with non-state actors, a new, revolutionary paradigm becomes essential for making sense of issues as well as their interactions with the states of the other paradigm. In the former, a traditional, intuitive and expert-supported approach was largely adequate. In the case of the latter, as is glimpsed in this case study, a more rigorous approach is required.

400 For example, see Kenneth Menkhaus, "State Fragility as a Wicked Problem," *Prism*, vol. 1, no. 2 (March 2010): 85-100. URL: <http//:www.ndu.edu/press/lib/images/prism1-2/6_Prism_85-100_Menkhaus.pdf>, accessed 14 May 2010.

Such an approach is "macrocognitive" in the terminology developed by those who study naturalistic decisionmaking.[401] In national intelligence terms, practitioners and their customers work in a macrocognitive environment as they manage the uncertainty they face in dealing with wicked problems.[402] Macrocognition, then, includes a focus on process as well as results—what we have labeled mindful, self-reflective sensemaking.

Klein *et alia* observe that intelligence professionals and decisionmakers traditionally are "microcognitively" focused. That is, like those who follow in the Sherman Kent tradition, they are concerned with solving puzzles, searching, and "estimating probabilities or uncertainty values" for different phenomena of interest.[403] As has been discussed, such an approach still may be suitable for solving tame problems or those of the Type 1 domain. Thus, microcognition describes the reductionist foci of the current intelligence "analysis" paradigm. However, this is not sensemaking, which requires another approach.

The transition or shift to macrocognition requires a focus on "planning and problem detection, using leverage points to construct options and attention management."[404] Elements of the foregoing case study exemplify this strategy. Both the Mercyhurst Role Spectrum Analysis and the Least Squares Points of Segmentation identified potential leverage points that revealed truths about non-state actors, leading to more robust problem detection. A next step would have been to take the triangulated results from all the deployed sensemaking methods and use the results to construct options for dealing with nonstate actors in multiple environments. Such a macrocognitive approach would allow more persistent attention to the *anticipation* of the broad course of events (in this case involving non-state actors), in contrast to a microcognitive focus on *predicting* more isolated and specific future incidents.

Next Steps in Revolutionary Sensemaking about Non-State Actors

The foregoing elaboration of non-coordinated sensemaking activities, even with its limitations, moved beyond the traditional model of intelligence creation. It specifically identified the multiple approaches taken by

401 Gary Klein and others, "Macrocognition," *IEEE Intelligent Systems*, vol. 18, no. 3 (May/June 2003), 81. Cited hereafter as Klein and others, "Macrocognition."

402 Pietro C. Cacciabue and Erik Hollnagel, "Simulation of Cognition: Applications," in Jean-Michel Hoc, Pietro C. Cacciabue, and Erik Hollnagel, eds., *Expertise and Technology: Cognition and Human-Computer Cooperation* (Hillsdale, NJ: Lawrence Erlbaum Associates, 1995), 55-73.

403 Klein and others, "Macrocognition," 82.

404 Klein and others, "Macrocognition," 82.

independent teams who used alternative schema and methods that, perhaps unsurprisingly, resulted in a broader understanding of the problem. Much of the multimethod work was based on differing perceptions of the task at hand. Triangulation was largely informal both within and between the groups. Thus, the work met the criteria for a *transitional* intelligence sensemaking project. The participants in all three efforts engaged in critical thinking to one degree or another. All were also mindful of the wicked issue of non-state actors and its significance.

To move farther toward a revolutionary paradigm for intelligence, these approaches need to be formalized beyond the transitional phase provided here into a new paradigm of sensemaking. This does not mean that the structured methods of "science" are to be imposed blindly on an issue.[405] Rather than leading to a scientific approach, this could lead to scientism, wherein meaning accrues only to measurable phenomena for which our understanding rests on hypothesis testing and refutation.[406] Instead, the adoption of the new paradigm for sensemaking depends on bringing into play a cooperative spirit of science and scientific inquiry to the process of intelligence creation and communication. Mindful, critical thinking-based, multimethodological approaches to analysis, synthesis and interpretation are one means of doing this. Additionally, a means needs to be found to ensure that this approach to sensemaking remains rigorous. This becomes the subject of the next chapter.

405 Here, one is reminded of a quote attributed to Secretary of Defense Robert McNamara: "We need to stop making what is measurable important and start making what is important measurable."

406 Friedrich August Hayak, a Nobel Prize-winning economist, developed the distinction between science and scientism. See Friedrich August Hayak, *The Counter-Revolution of Science: Studies on the Abuse of Reason*, 2nd Edition (Indianapolis, Indiana: Liberty Fund, Inc., 1979), 19-25.

CHAPTER 8
Establishing Metrics of Rigor

Defining Intelligence Rigor

> I know the distinction between inductive and deductive reasoning. An intelligence officer is inherently inductive. We begin with the particular and we draw generalized conclusions. Policymakers are generally deductive. They start with the vision or general principle and then apply it to specific situations. That creates a fascinating dynamic, when the intelligence guy, who I call the fact guy, has to have a conversation with the policymaker, who I tend to call the vision guy. You get into the same room, but you clearly come into the room from different doors. The task of the intelligence officer is to be true to his base, which is true to the facts, and yet at the same time be relevant to the policymaker and his vision. That's a fairly narrow sweet spot, but the task of the intelligence officer is to operate in that spot.
>
> — GEN Michael V. Hayden (Ret.),
> former Director of the Central Intelligence
> Agency and the National Security Agency[407]

Michael Hayden's view that the intelligence officer needs to operate in the "sweet spot" linking intelligence and policymaker cognitive worlds coincides with the aim of the sensemaking paradigm. To bring these two worlds together, intelligence professionals can take advantage of the opportunity to meld their fact-based inductive tendencies with the visionary, deductive model of policymakers through the application of collective rigor to well-conceived questions. This approach allows intelligence professionals to embrace a triangulation on wicked problems from their professional perspective, and to improve their chance to communicate with policymakers whose circumscribed comfort zone may accept or even welcome wicked problems as opportunities to apply their vision to bring about politically rewarding solutions.

---

407 From a 9 August 2010 interview on national security and U.S. strategy, aired by C-SPAN radio, URL: <http://www.cspan.org/Watch/Media/2010/08/09/Terr/A/36779/Gen+Michael+Hayden+Ret+The+Chertoff+Group+Principal.aspx>, accessed 11 August 2010.

At present most tradecraft for sensemaking triangulation remains intuitive, operating in the realm of tacit knowledge. Thus, part of a revolution in intelligence requires that more formal and explicit means of triangulation be developed. It may be that some existing analytic tradecraft, when conscientiously applied, will improve synthesis and interpretation. Another option is to explore and experiment with new tools for conceptualizing rigor in information analysis, synthesis and interpretation.

Rigor in sensemaking can refer to inflexible adherence to a process or, alternatively, to flexibility and adaptation "to highly dynamic environments."[408] As proponents of the latter approach, Daniel Zelik, Emily Patterson, and David Woods recently reframed the idea of rigor into a more manageable concept of "sufficiency."[409] In the applied world of sensemakers, then, an apt question is: "Were sufficient considerations made or precautions taken in the process of making sense of the issue?" Zelik *et alia* observe that this requires a "deliberate process of collecting data, reflecting upon it, and aggregating those findings into knowledge, understanding, and the potential for action."[410] In order to achieve answers to this question Zelik *et alia* developed an eight-element taxonomy of sufficiency and a trinomial measurement of rigor: Each element was calibrated in terms of high, medium or low rigor. In their examination of information products, an overall score could be computed that, in intelligence terms, would communicate to both the practitioner's management and to consumers the rigor of the crafted intelligence product. Their model of the metric is shown in figure 11 and its attributes are reproduced in table 6.

---

408 Daniel J. Zelik, Emily S. Patterson, and David D. Woods, "Understanding Rigor in Information Analysis," in Kathleen Mosier and Ute Fischer, eds., *Proceedings of the Eighth International NDM Conference*, Eighth International Naturalistic Decision-Making Conference, Pacific Grove, CA, June 2007, 1. Cited hereafter as Zelik, and others, "Rigor."

409 Zelik and others, "Rigor," 1. Note that "sufficiency" differs from "satisficing," by definition a low-rigor process where only enough sensemaking is conducted to get to an initial answer. Indeed, satisficing may be considered the epitome of low rigor.

410 Daniel J. Zelik, Emily S. Patterson, and David D. Woods, "Measuring Attributes of Rigor in Information Analysis," in Emily S. Patterson, and Janet E. Miller, *Macrocognition Metrics and Scenarios: Design and Evaluation for Real World Teams* (Aldershot, UK: Ashgate, 2010), 65. Cited hereafter as Zelik and others, "Measuring Rigor."

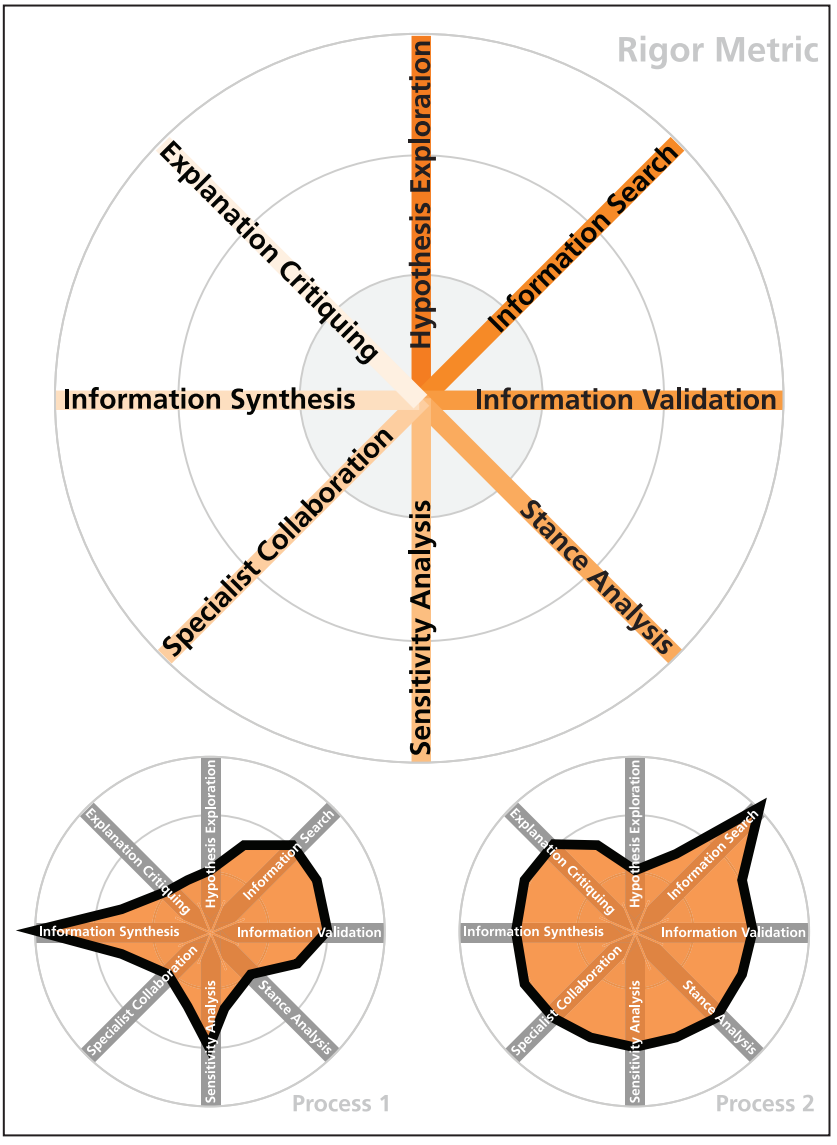


Figure 11. A Metric for Rigor.

Source: Daniel J. Zelik, Emily S. Patterson, David D. Woods, "Modeling Rigor in Information Analysis: A Metric for Rigor," Cognitive Systems Engineering Laboratory, The Ohio State University. Used with permission.

Table 6. Attributes of the Rigor Metric
Hypothesis Exploration describes the extent to which multiple hypotheses were considered in explaining data. In a low-rigor process there is minimal weighing of alternatives. A high-rigor process, in contrast, involves broadening of the hypothesis set beyond an initial framing and incorporating multiple perspectives to identify the best, most probable explanations.
Information Search relates to the depth and breadth of the search process used in collecting data. A low rigor analysis process does not go beyond routine and readily available data sources, whereas a high rigor process attempts to exhaustively explore all data potentially available in the relevant sample space.
Information Validation details the levels at which information sources are corroborated and cross-validated. In a low-rigor process little effort is made to use converging evidence to verify source accuracy, while a high-rigor process includes a systematic approach for verifying information and, when possible, ensures the use of sources closest to the areas of interest.
Stance Analysis is the evaluation of data with the goal of identifying the stance or perspective of the source and placing it into a broader context of understanding. At the low-rigor level an analyst may notice a clear bias in a source, while a high-rigor process involves research into source backgrounds with the intent of gaining a more subtle understanding of how their perspective might influence their stance toward analysis-relevant issues.
Sensitivity Analysis considers the extent to which the analyst considers and understands the assumptions and limitations of their analysis. In a low-rigor process, explanations seem appropriate and valid on a surface level. In a high-rigor process the analyst employs a strategy to consider the strength of explanations if individual supporting sources were to prove invalid.
Specialist Collaboration describes the degree to which an analyst incorporates the perspectives of domain experts into their assessments. In a low-rigor process little effort is made to seek out such expertise, while in a high-rigor process the analyst has talked to, or may be, a leading expert in the key content areas of the analysis.
Information Synthesis refers to how far beyond simply collecting and listing data an analyst went in their process. In the low rigor process an analyst simply compiles the relevant information in a unified form, whereas a high-rigor process has extracted and integrated information with a thorough consideration of diverse interpretations of relevant data.

Table 6. Attributes of the Rigor Metric (Continued)
Explanation Critique is a different form of collaboration that captures how many different perspectives were incorporated in examining the primary hypotheses. In a low-rigor process, there is little use of other analysts to give input on explanation quality. In a high-rigor process peers and experts have examined the chain of reasoning and explicitly identified which inferences are stronger and which are weaker.

Source: Zelik *et alia*, "Rigor," 4.

The tradecraft underlying these attributes assesses the domains of intelligence foraging and intelligence sensemaking (analyzing, synthesizing, and interpreting) as described here. The study by Zelik *et alia* reveals that what might at first glance be considered the application of a low level of rigor really is merely a function of a varying distribution of rigor applied among the attributes. In their study some notable differences appeared in the absolute scores on the rigor scale as different products were scrutinized. However, the more interesting cases involved notable swings in specific attribute scores. Thus, in a test scenario assessing the work of two practitioners (see figure 11), one with a predetermined "high rigor" score and the other with a predetermined "low rigor," the fact that the high-rigor practitioner (Process 2) had a high score for *information search* and a medium score for *information synthesis* whereas the low-rigor practitioner (Process 1) had a medium score for *information search* and a medium score for *information synthesis* is noteworthy.

This distinction suggests a profound insight, namely that information search is perceived as more highly valued than *information synthesis*. In the case above, a definitive judgment about this insight cannot be made, as the other attributes of the two assessments were not identical. Still, it seems clear that at least the participants in the study were still wrestling with a consideration formally discussed by Richards Heuer, Jr. (and many others before and since—including Moore and Hoffman above): How much information is necessary for effective sensemaking?[411] The observations may also reflect the "data-centric" culture of the participants. Finally, it offers a means to counter a tendency or preference among "Google Generation" foragers, as described in Chapter 4, for broad but shallow searches. A next step in examining the metric is to apply it to an assemblage of intelligence assessments. An illustration of how this might work using the case study of the previous chapter appears below.

411 Heuer, *Psychology*, Chapter 5. See also, Slovic, "Behavioral Problems."

Assessing Sensemaking Rigor in Studies of Non-State Actors

Table 7. Comparative Scores of the Three Efforts Examining the Roles of Non-State Actors			
Criteria	**NIC-Eurasia Group**	**Mercyhurst**	**LSS**
Hypothesis Exploration describes the extent to which multiple hypotheses were created and considered in explaining data.	*Low*	*High*	*High*
Information Search relates to the depth and breadth of the processes used in foraging and harvesting data.	*Medium*	*High*	*High*
Information Validation expresses the level to which information sources are corroborated and cross-validated.	*Medium*	*Medium*	*Medium*
Stance Analysis is the evaluation of data with the goal of identifying the stance or perspective of the sources and their placement into a broader context of understanding.	*Medium*	*Medium*	*High*
Sensitivity Analysis considers the extent to which the analyst considers and understands the assumptions and limitations of their analysis.	*Medium*	*High*	*High*
Specialist Collaboration describes the degree to which an analyst incorporates the perspectives of domain experts into their assessments.	*High*	*Low*	*High*

Table 7. Comparative Scores of the Three Efforts Examining the Roles of Non-State Actors (Continued)			
Criteria	**NIC-Eurasia Group**	**Mercyhurst**	**LSS**
Information Synthesis refers to how far beyond simply collecting and assembling data an analyst progressed.	*High*	*High*	*High*
Explanation Critique is a measure of collaboration that captures how many different perspectives were incorporated in examining the primary hypotheses.	*Medium*	*Medium*	*High*
Team Scores (Each low = 1; medium = 2; high = 3)	**17**	**19**	**23**

Sources: Zelik *et alia*, "Rigor," 4; Author.

The case study in the previous chapter affords an opportunity to demonstrate how this rigor metric functions when applied against the work of real intelligence professionals—or in this case, teams of intelligence professionals. In this example the informed judgment of the author leads to three individual rigor metric diagrams as well as a composite; finally, a table summarizes the results.[412] Applying a scoring metric of 1 point for a Low Score, 2 points for a Medium Score, and 3 points for a High Score yields a range of 8 to 24 possible points. For the reviewers, when no evidence pointed clearly to a low or high score, a default position of medium was presumed.

412 The author is indebted to Russell Swenson who reviewed the assessments (and agreed with the scoring of the author). Numerical scores were assigned at his suggestion. It should be observed that this assessment is not intended to be authoritative. Rather it is provided as an example of how rigor can be assessed.

Rigor and the NIC-Eurasia Group Effort

The NIC-Eurasia Group effort (summarized in figure 12 and column one of table 7) garnered the fewest points of the three groups. **Hypothesis Exploration — Low:** The NIC-Eurasia Group memorandum noted that non-state actors are of interest "because they have international clout, but are often overlooked in geopolitical analysis." The implicit but demanding questions of why and how much non-state actor "power" and "influence" have increased worldwide were not answered, nor was a time frame established. This failure to broaden the hypotheses beyond the initial framing of the issue led to a lack of incorporation of multiple perspectives to identify at least "best," and perhaps most probable answers to these questions. **Information Search — Medium:** Based on the memorandum there was no evidence of a "high rigor" or exhaustive information search. **Information**

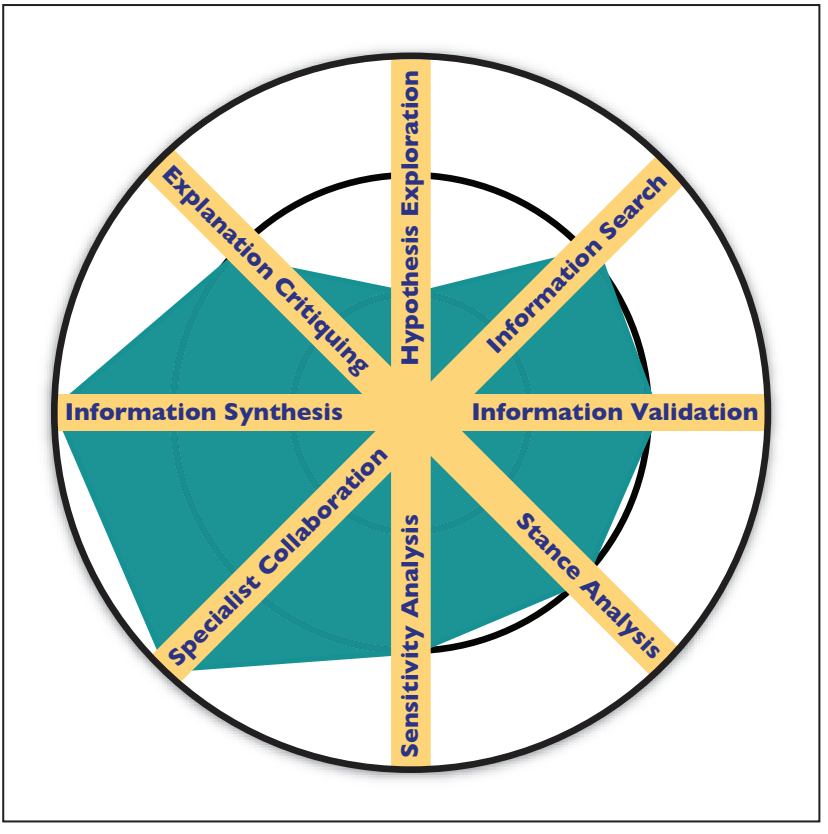


Figure 12. The Rigor of the NIC-Eurasia Group Study of Non-State Actors.
Source: Author, based on Zelik *et alia*, "Rigor."

Validation — Medium: Convergence of evidence was apparent in the NIC-Eurasia Group desktop memorandum. **Stance Analysis — Medium:** This was found to be a process-related metric and the desktop memorandum did not adequately reveal the process undertaken. However, some evidence exists that consideration of the source backgrounds took place. **Sensitivity Analysis — Medium:** While the NIC-Eurasia Group's explanations went beyond the "surface level," no obvious evidence was presented of an explicit strategy to consider the strength and sensitivity of explanations about non-state actors. **Specialist Collaboration — High:** Such a score was expected. Eurasia Group is an organization of experts; this is one of its values to the Community (and others). Leading experts provided their informed opinions about the roles of non-state actors. **Information Synthesis — High:** The NIC-Eurasia Group desktop memorandum presented integrated information with a thorough consideration of the underlying evidence such as the conclusion that "state-owned enterprises" posing as NGOs often are a front for advancing the interests of a modernizing state-government. **Explanation Critique — Medium:** A discussion process presumes the examination and critique of each participant's chains of reasoning. Since discussions were a part of the sensemaking process undertaken by the NIC-Eurasia Group participants, this form of collaboration was present. However, the degree to which this occurred could not be determined from the desktop memorandum, resulting in a score of medium.

Rigor and the Mercyhurst Effort

The work of the Mercyhurst College students earned a score midway between the other two groups. Their **Hypothesis Exploration** was judged to be **High**. Their considerations of the issue clearly went beyond their initial framing of the issue. Similarly, their **Information Search** also scored **High**. A broad range of evidence was employed in making sense of non-state actors in Africa.[413] On the other hand, while the information convergence necessary for the "non-state actor potential spectra" was indicative of high rigor, an informal non-systematic approach resulted in **Information Validation** being assigned a **Medium** score. **Stance Analysis** also was scored as **Medium**. As was the case with the NIC-Eurasia Group effort, this process-related metric could not be further evaluated. With regard to **Sensitivity Analysis**, the Mercyhurst effort was scored as **High:** The participants focused on the non-state actors themselves as well as the means by which they could be assessed. Such a focus leads naturally to a consideration of the

413 This was not unexpected. A finely honed skill of participants in the Mercyhurst College Institute for Intelligence Studies program is that of effective, broad and deep search.

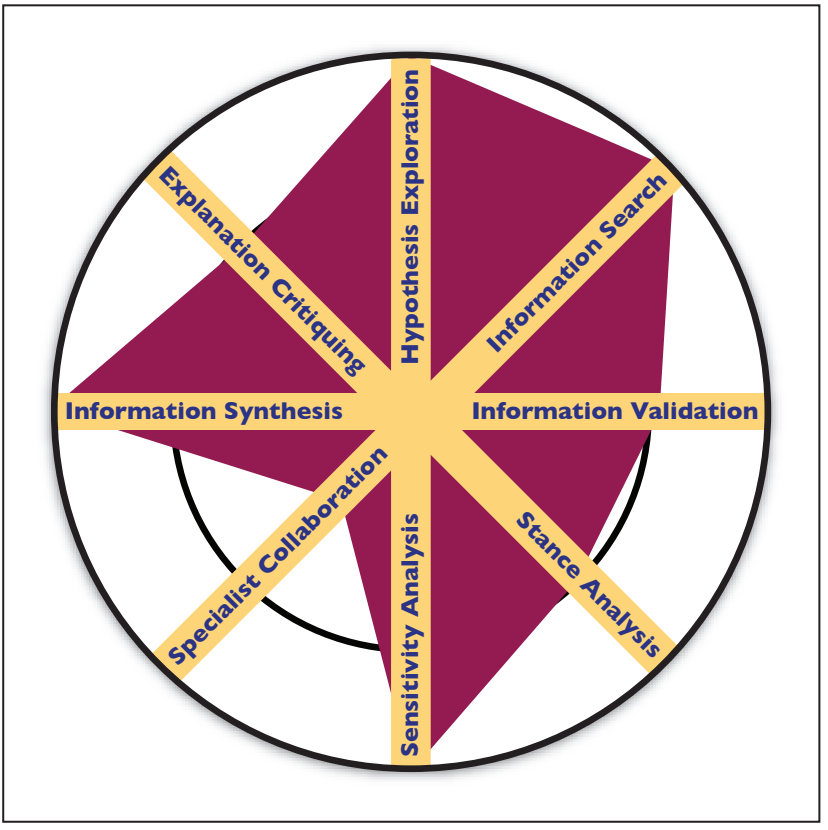


Figure 13. The Rigor of the Mercyhurst College Students' Study of Non-State Actors.
Source: Author, based on Zelik *et alia*, "Rigor."

strengths and weaknesses of explanations. The Mercyhurst students relied on published data. No evidence of consultation with external experts was evident. While this was to be expected given the demographics of a student team, it nevertheless led to a score of **Low** for the **Specialist Collaboration** metric. By contrast, **Information Synthesis** received a **High** score. The consideration of diverse interpretations of the data led the Mercyhurst students to anticipate that Kenya had stability issues well in advance of the breakout of politically related violence. This was unexpected and possibly unanticipated elsewhere. Finally, the **Explanation Critique** metric was scored a **Medium**. The review by the mentoring faculty member and fellow students provided a level of critique that, while valuable, did not meet the standard set by a full peer and expert review of inferences and conclusions, which is necessary for a high score in this category.

Rigor and the LSS Effort

The LSS social science study of non-state actors scored the highest of all three groups, earning a high in each metric save one, **Information Validation**, where they scored a **Medium**. In this case, while converging information was employed to cross-validate source accuracy for the evidence closest to the areas of interest, a systematic approach for doing this was not evident, resulting in the lower score.[414] Overall the LSS effort went well beyond the initial framing of the issue, resulting in a **High** score for **Hypothesis Exploration**. Similarly, their **Information Search** considered every source they could access within their available resources. It was clearly evident that

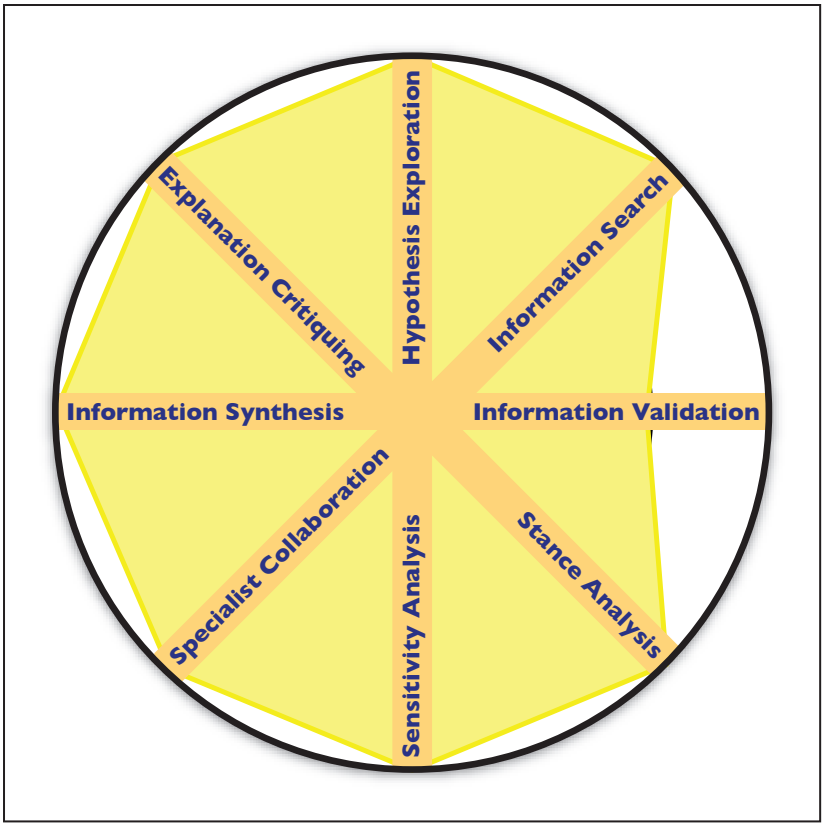


Figure 14. The Rigor of the Least Squares Social Science Study of Non-State Actors.

Source: Author, based on Zelik *et alia*, "Rigor."

414 This determination may be overly stringent, as the LSS Stance Analysis (a related metric) was rated as high.

this group conducted rigorous research into source background, facilitating an understanding of how their respective points of view might influence their stances on the issues of violent non-state actors. The use of a formal model of critical thinking added considerable rigor to both **Hypothesis Exploration** and **Sensitivity Analysis**. Furthermore, their conversations specifically focused on the strength of explanations. The use of multiple points of segmentation also captured the diverse alternatives of this complex (or "wicked") issue. Since the entire team was made up of specialists, their score in **Specialist Collaboration** should come as no surprise. Similarly, the involvement of diverse social scientists as well as the involvement of external peers foreordained that the **Explanation Critique** would be rigorous. All the individuals brought differing perspectives as they identified the strengths and weaknesses of each other's inferences and conclusions. Finally, an explicit multi-methodological approach forced consideration of diverse interpretations of the evidence—a highly rigorous example of **Information Synthesis**.

Observations and Discussion

It is no accident that the traditional means by which assessments of such issues are created, as evidenced by the NIC-Eurasia Group effort, resulted in a relatively weak score, whereas the highly rigorous, critical-thinking based, multimethodological effort by a collaborative team of diverse experts led to a relatively high score (a comparison highlighted by figure 15). It should also be noted that absent the LSS effort, a composite effort by the NIC-Eurasia Group and Mercyhurst teams would have come close to the score attained by the LSS group (21 versus 23 points). Here again, the utility of this metric becomes evident. Teams that complement each others' strengths and mitigate each others' shortcomings can be assigned the same general problem, with the expectation of a more rigorous composite effort and more suitable result. As has been illustrated here, the results of individual efforts and combined efforts can be assessed for their rigor as a guide to the purposeful improvement of sensemaking. Specific feedback can be provided so that efforts can be adjusted.

Another advantage of graphic analysis using Zelik *et alia's* metric is that more information can be clearly conveyed. For example, in examining the composite efforts of all three groups of participants in the non-state actor study, it is evident that Information Validation could have been improved through the use of a more rigorous systematic approach, ensuring that the sources were deemed valid and "closest to the areas of interest."[415] In 2005,

415 Zelik and others, "Rigor," 4.

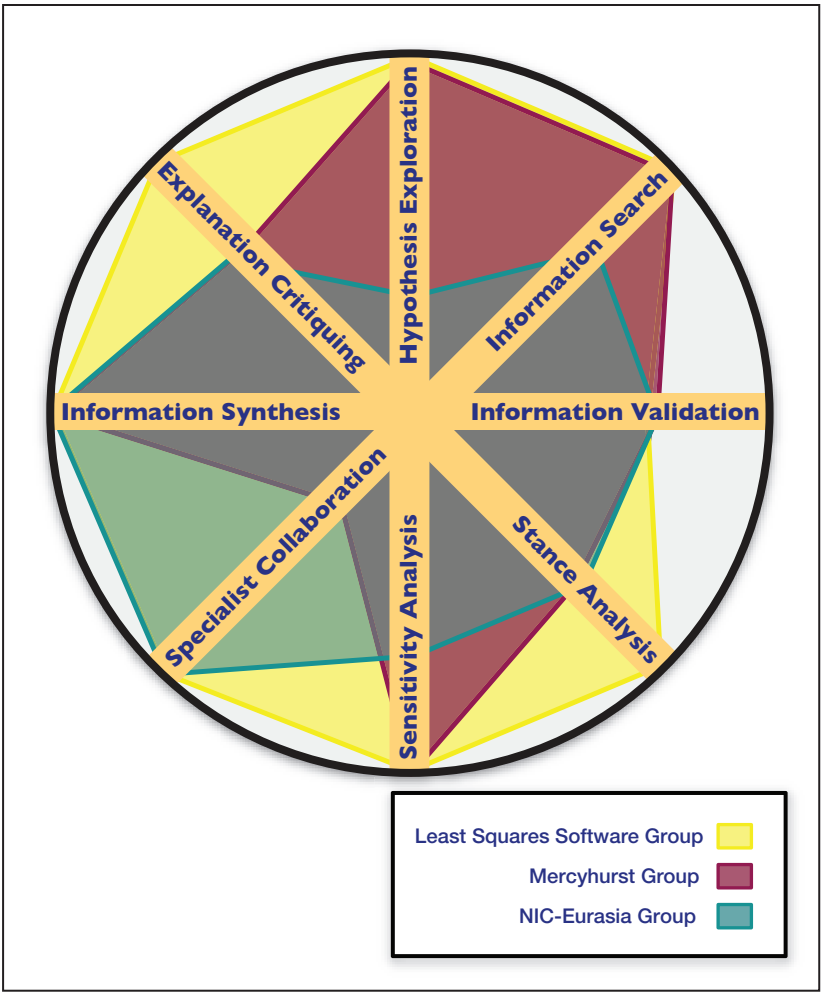


Figure 15. The Composite Rigor of the Three Studies of Non-State Actors.
Source: Author, based on Zelik *et alia*, "Rigor."

an official report on the IC's performance specifically called for improvement in this area.[416]

Despite this call for improvement, there appear to be several reasons why information is often not fully validated in intelligence work. First,

416 The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction (WMD) *Report to the President of the United States* (Washington, DC: Government Printing Office, 31 March 2005), 15, and 371-372. The report recommends that asset validation procedures (a part of information validation) be systematized and standardized.

validation is difficult and the intelligence professional may decide the result is not worth the effort, or that initial conditions *suggest* validity. "Information hubris"—arising when similar information has without negative consequence been presumed or found to be valid, may compound this effort. Wishful thinking and belief in the infallibility of the source are other factors that may contribute to this pathology. Finally, information uncertainty may allow it to resist validation. Unfortunately any or all of these can lead to intelligence errors and failures, suggesting that information validation, despite its inclusion in the rigor metric itself, may require a transcendent application of rigor.

In applying the metric it becomes apparent that some disambiguation is necessary between several of the individual considerations. The differences between high rigor assessments involving Stance Analysis and Sensitivity Analysis at first glance appear to be unusually subtle, suggesting a need for an explanatory critique as part of the standard process assessment. Additionally, because several of the specific metrics are process-related, assessors need to be present to observe the process or otherwise have access to appropriate and sometimes-scarce process-associated materials. Alternately, a formal means for capturing applied (and omitted) sensemaking processes needs to be developed.

In developing the rigor metric, Zelik *et alia* note that it is "grounded largely in the domain of intelligence analysis."[417] Looking at the metric from a generalizing point of view, Zelik *et alia* are interested in whether it can be broadened to other disciplines such "as information search by students working on educational projects, medical diagnosis using automated algorithms for x-ray interpretation, and accident investigation analyses."[418] For those of us within the domain of intelligence, however, that this model "emerged from studies of how experts 'critique' analysis (rather than how experts 'perform' analysis." is a strength.[419] The rigor metric has been *empirically*, if tentatively, shown (according to Daniel Zelik) to "reveal [some of the] "critical attributes to consider in judging analytical rigor" in intelligence sensemaking.[420] In so doing, Zelik and his colleagues also validated the usefulness of the model within the intelligence domain.

---

417 Zelik and others, "Measuring Rigor," 77.

418 Zelik and others, "Measuring Rigor," 77-78. Some of these domains contain applicability to intelligence. Given a tendency for shallow searches by younger people, then a metric for rigor that offers guidance may facilitate the "deep diving" necessary for adequate information foraging.

419 Daniel J. Zelik, email to the author, 15 October 2010. Cited hereafter as Zelik, email, 15 October 2010.

420 Zelik, email, 15 October 2010.

While the rigor metric requires further development, it offers an effective means of assessing the processes underlying intelligence assessments. The rigor metric provides a means of assessing the processes of intelligence sensemaking, allowing managers of intelligence professionals to ascertain whether or not more work is required before the results of the sensemaking are communicated. Additionally, it offers a practical technique to facilitate communication between practitioner and consumer; that is, to promote *sensemaking*. A danger inherent in any process of making sense of an issue exists when the "process is prematurely concluded and is subsequently of inadequate depth relative to the demands of [the] situation."[421] Finally, the metric suggests other sensemaking considerations that, if used, may help reduce inadequacies in the consideration of intelligence issues. This may lead further to an honest reduction in sensemakers' and their customers' uncertainty about issues being examined. In sum, the metric for rigor developed by Zelik and his colleagues is itself an objectification of what they find rigor to be and warrants further study.[422] Zelik, *et alia* note that the metric "represents a current iteration of an ongoing direction of exploration."[423] Such studies, rigorously making sense of rigor, would be yet another example of the model for intelligence sensemaking that has been championed in this book. As Zelik *et alia* conclude, "the concept of analytical rigor in information analysis warrants continued exploration and diverse application as a macrocognitive measure of analytical sensemaking activity."[424] But what does it mean if such a model is adopted, or not adopted? The final chapter examines the implications of either outcome.

421 Zelik and others, "Measuring Rigor," 65.
422 Zelik and others, "Rigor," 5.
423 Zelik and others, "Measuring Rigor," 78.
424 Zelik and others, "Measuring Rigor," 78.

CHAPTER 9
In Search of Foresight: Implications, Limitations, and Conclusions

Considering Foresight

We turn in conclusion to a discussion of the purpose of mindful, critical sensemaking for intelligence. The discussion may be best framed by pertinent questions: To what end is intelligence intended? In other words, intelligence professionals and their overseers critically ask "knowledge of what?" and, secondly, "knowledge for whom?" One answer to these questions is embodied in the concept of foresight: Intelligence knowledge advises policymakers and decisionmakers about what phenomena are likely precursors of events of interest before they occur. Such foresight—in light of the discussions in this book—does not entail specific predictions. Rather, it allows us to anticipate a range of alternative event sequences.

Foresight informs policy and decisionmakers about what could happen so that those individuals can improve the quality of their decisions. Done mindfully, its vision shifts and evolves apace with the phenomena about which it makes sense. Done wisely in such a manner as presented here, it augments the vision of leaders, enabling mobilization and discouraging two traits that often handicap visionaries: recklessness and intolerance. Done rigorously, it cannot be accused of failing to be imaginative. This prospective approach contrasts with the current practice and paradigm for intelligence production.

Reprising Anthony Olcott's observations reminds us again that Sherman Kent's vision of national intelligence—his "intellectual genetics"—has predominated in U.S. national intelligence since the late 1940s.[425] That it did so was because it "served the United States extremely well for a long time. However, as happens when environments undergo dramatic change, successful adaptations for one environment can prove to be much less efficacious—perhaps even fatal—in a new environment."[426] In the Kent tradition, as has been noted (and is summarized in figure 16), intelligence knowledge of "analyzed" issues becomes and tends to remain disaggregated into constituent parts—oriented, as Treverton notes, toward solving isolated "puzzles" rather

425 Olcott, "Revisiting the Legacy," 21.
426 Olcott, "Revisiting the Legacy," 21.

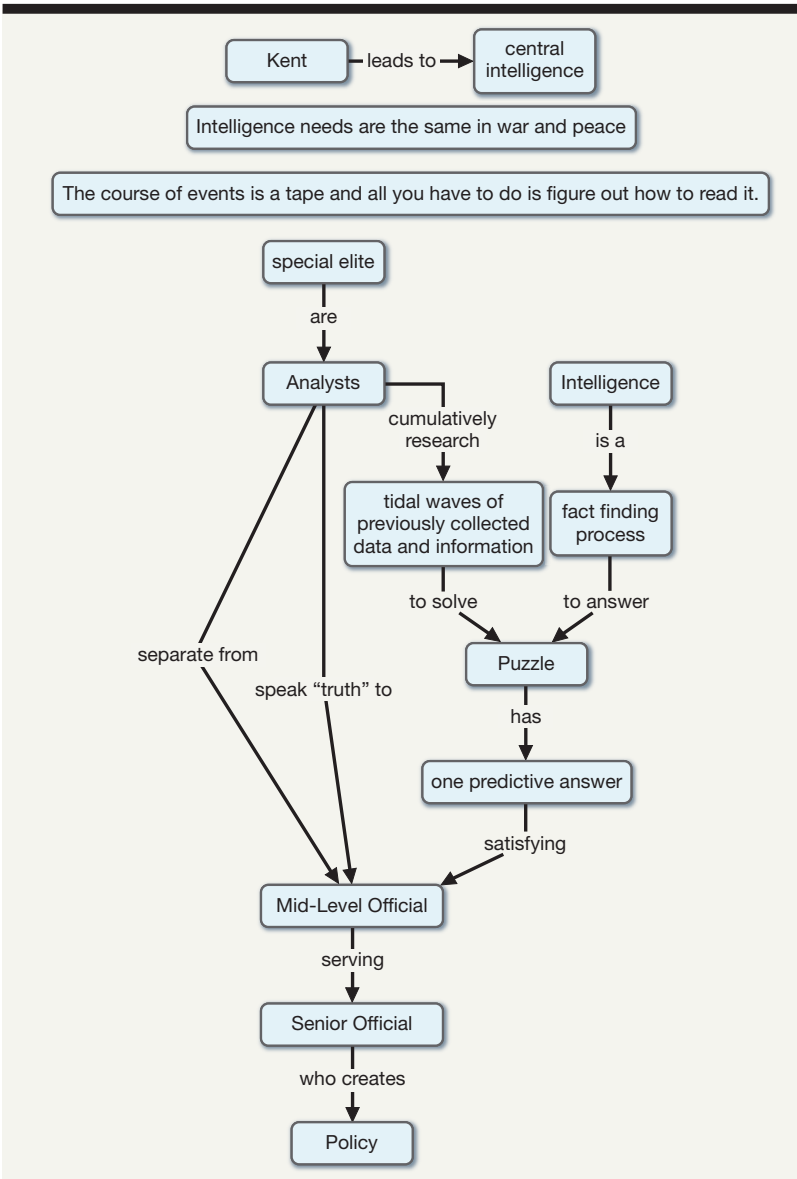
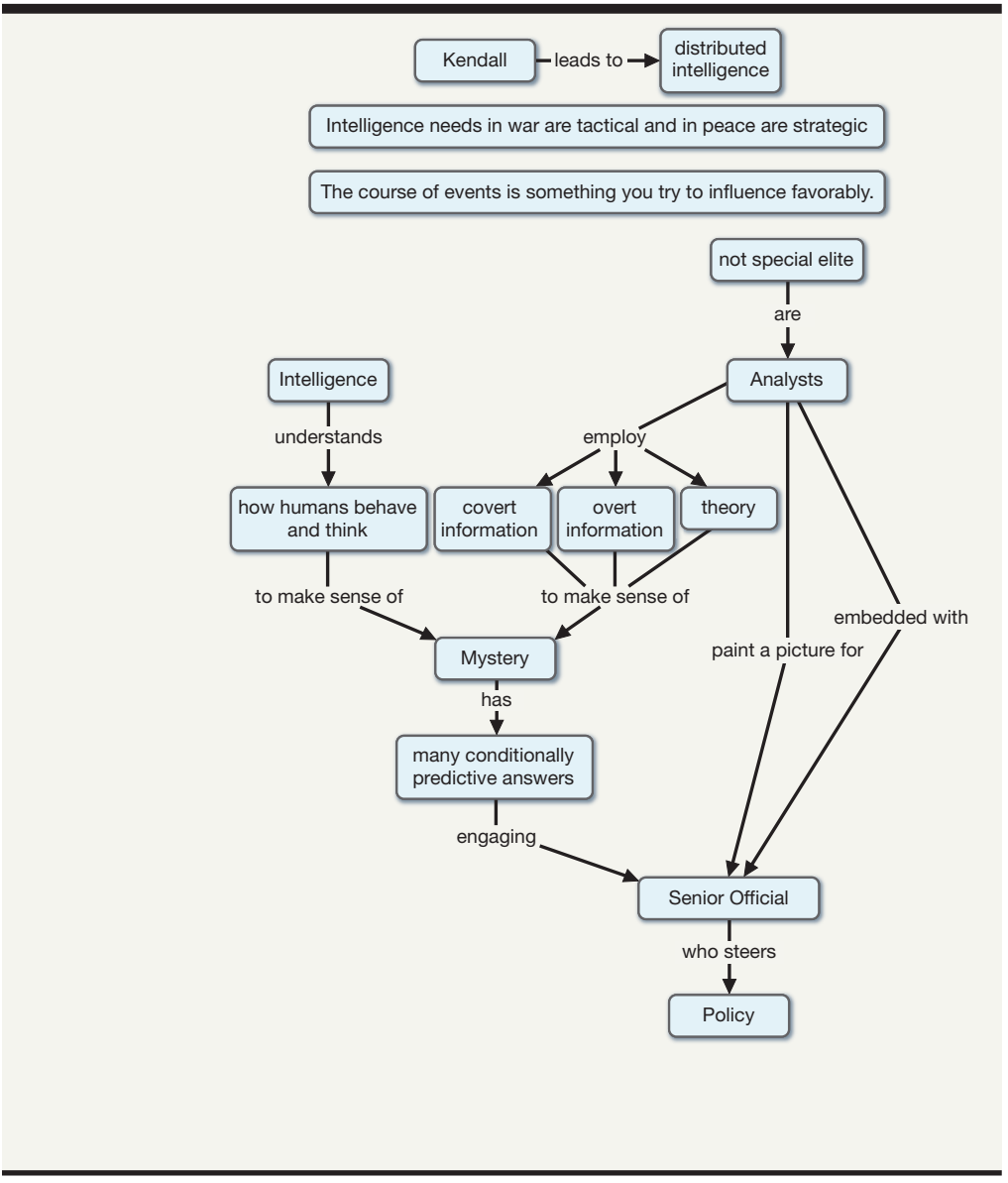


Figure 16. Conceptual Comparison of Kent and Kendall. These diagrams track the potent nodes that signal the differences in the visions of Sherman Kent and Willmoore Kendall. The diagram to the right also traces a revolutionary, Kendallian pathway toward the creation and communication of strategic intelligence.

Sources: Author; based on Jack Davis, "Analysis and Policy: The Kent-Kendall Debate of 1949," *Studies in Intelligence*, vol. 36, no. 2 (1992); Kendall, "Function of Intelligence;" Kent, *Strategic Intelligence*; Olcott, "Revisiting the Legacy;" and Treverton, "Estimating."


Kendall
leads to
distributed intelligence
Intelligence needs in war are tactical and in peace are strategic
The course of events is something you try to influence favorably.
not special elite
are
Analysts
Intelligence
understands
employ
how humans behave and think
covert information
overt information
theory
to make sense of
to make sense of
Mystery
has
many conditionally predictive answers
engaging
embedded with
paint a picture for
Senior Official
who steers
Policy

than the more holistic "mysteries" of the intelligence world. On the other hand, we have discussed how Kendall's competing idea, that intelligence knowledge should "paint a picture" (by way of a macrocognitive, holistic approach) for the policy maker as a fellow "insider," is consistent with a model of intelligence where the predominant method and motive of intelligence sensemaking is through aggregation and the articulation of a fact-based "vision" recognizable by national-level policymakers (figure 16). Even in an operational military scenario, where isolated, specific facts are essential to successful employment of mission knowledge, a larger intelligence sense of who the ultimate commanders are and why they are doing what they're doing, remains the essence of useful, foresightful strategic knowledge—also known as national intelligence.

Implications

Creating intelligence as presented here is a mindful process of sensemaking, encompassing the activities of planning, foraging, marshaling, understanding, and communicating. It is critical of itself and the means that are employed in bringing it about. It lies within the largely overlooked Kendallian vision of what national intelligence ought to accomplish. This approach allows a focus on better and worse solutions, and anticipation of likely futures, instead of a more narrow focus on right and wrong answers in an intellectual environment trained on predictive and specific warning. It can make sense of wicked problems.

By contrast, intelligence as it is currently practiced is still somewhat akin to the practice of medicine in the 14th Century. In Medieval medicine, herbs and poultices were applied without (from a modern perspective) an understanding of why they might work. If the patient survived, then the method worked. If not, then from the medieval perspective, God willed it otherwise. Intelligence practitioners find themselves in a similar situation. They often do not know why they do what they do, only that the last time, it "worked"—or that it is an "accepted practice." They do not acknowledge that they have "forgotten" all the times it did not work. Yet, intelligence practitioners who would wear the "professional" label need to know what they are doing and why.[427]

One means set forth for "improving intelligence" is to capture the processes by which sense is made of an issue. It is certainly true that imposing audit trails is a critical step because they encourage process improvement

427 It is pertinent to note that suggesting, "God willed it otherwise," is unacceptable for justifying either an intelligence error or an intelligence failure.

in the light of serious errors, and stimulate repetitive analysis, synthesis, and interpretation for validation in the full course of sensemaking. However, auditing trails remain inadequate when the Community cannot understand from an epistemological point of view what does and does not work and in what situations.

The major intelligence failures of the first years of the present decade, as well as repeated failures over at least six decades, demonstrate what happens when there is a formal failure to synthesize and interpret beyond what is popularly believed or even to recognize that a situation exists that requires new synthesis and interpretation. A popular hypothesis is that tradecraft can minimize the likelihood of such failures of imagination. Yet this hypothesis remains untested except in some anecdotal cases which, given the Type 2, wicked nature of the intelligence issues now often faced by the Community, is inadequate. Indeed, as Grove *et alia* discovered in their psychological meta-study (discussed above), technological approaches (a structuring of sorts) provided accurate solutions less that half the time.[428] Thus, a Community effort to research, test, and evaluate tradecraft remains a need if for no other reason than so the IC can understand what approaches to foresightful sensemaking are likely to be useful and in what circumstances. The above-mentioned failures (and others) show that the typical "analytic" paradigm that remains in place leads to failures of imagination in policy circles as well as in intelligence cloisters.[429] The most recent failures point out that the Community still does not understand how desperately it needs to make sense.

Limitations

It should be noted that a tradecraft of mindful understanding does not guarantee accurate findings. Any of the components of sensemaking can be done poorly yet "correct" answers can be reached. Disaggregating phenomena can be done well yet yield faulty results. Synthesis and interpretation of analyzed phenomena can still lead to faulty conclusions. However, analysis, synthesis and interpretation within the framework of appropriately applied, multimethod tradecraft does guarantee more rigorous sensemaking. As illustrated in the case study presented above (chapter 7), greater rigor can reveal the hidden discrepancies in an intelligence problem. In the example contained in chapter 5, it can be seen that increased rigor may reveal whether the discrepancies comprise self-generated erroneous conclusions or whether one has been manipulated by a deceptive adversary. A rigorous

428 Grove and others, "Meta-Analysis," 25.

429 *The 9/11 Report*, 339. The four failures are discussed in depth in subsequent sections of the commission's report.

multimethodological approach will increase the reliability and validity of the findings. Taken together, the entire process certainly will increase the intelligence practitioner's understanding of the issue, allowing more informed communication of associated knowledge to a decisionmaker. This may lead to increased "accuracy." At best, errors will occur with less frequency, or at least they are more likely to be caught.

Conclusions

As has been noted repeatedly in this book, many 21st-Century intelligence issues are wicked problems: They are ill-defined and poorly understood issues with multiple goals that must be made sense of within severe time constraints; the stakes and risks are high and there exists no tolerance for failure. As a means of increasing situational awareness, merely creating mindfulness about such complex issues falls short. On the other hand, a mindful *sensemaking* approach to situational awareness accomplishes more by enabling the intense, holistic scrutiny of a complex developing scenario, as suggested in the case study in chapter 7. This macrocognitive approach ensures that the knowledge created also evolves.

Schwartz and Randall believe that to be successful against strategic surprise—a goal the IC seeks—organizations must be both imaginative and systematic.[430] This is so, because "[one] cannot foresee strategic surprise without being imaginative, but the results will not be believable without being systematic."[431] If intelligence is to rise above the noise and get the attention of policy and then be acted upon it must be both. A critical, mindful process of sensemaking offers a means for this to occur. As we have seen, it covers the issue broadly, takes into account its complexity, is systematic and rigorous. It offers the best means currently understood for making sense of what is known and knowable.

There is and will always be information of which intelligence professionals are unaware. There is certainly information that does not exist because its precursors have not yet occurred. There also is information that exists but is unavailable to the intelligence sensemaker and their associated decisionmakers. Any of this information can change the conclusions reached in making sense of it. In short, intelligence professionals currently make judgments and will continue to make judgments that, while they appear valid at the time, differ from what ultimately occurs, either because of omission or commission. For evidence of this one need not look further than at the differing

430 Schwartz and Randall, "Ahead of the Curve," 96-100.

431 Schwartz and Randall, "Ahead of the Curve," 97.

judgments contained in the U.S. National Intelligence Council's series of global trends summaries published every five years since 1995.[432] These documents, which look outward 15 years, perhaps are better seen as expressing the issues and concerns of the times in which they are written, suggesting the validity of Taleb's point that to predict the future one must already be in the future.[433]

The spread and use of the sensemaking paradigm, wherein intelligence professionals move from a reductionist, analytic view to formally include the other elements of sensemaking—synthesis and interpretation—increases the value of intelligence findings. Engaging in macrocognitive sensemaking, with its multiple foci of (re)planning for problem detection, use of leverage points in constructing options, and management of both attention and uncertainty, further creates an approach that will improve communication with consumers of intelligence.[434] As Zukav's epigraph at the beginning of this book reminds us, "[nonsense] is nonsense only when we have not yet found that point of view from which it makes sense."[435] Such an inclusive process provides that point—or rather *points*—of view; nonsense is transformed into vital, strategic, and foresightful knowledge facilitating better decisions by leaders.

Some elements of the IC have begun to establish "tradecraft" cells or similar centers focusing on the practice and process of intelligence. Typically, however, they have not transcended the "analysis" paradigm and remain mired in the uncertainty reduction that is characteristic of the practice of the past sixty-plus years. At best, they are not yet able to transform a professional workforce. Pierre Baumard in 1994 anticipated the persistence of this state of affairs: "[Individuals] act on incomplete and variously reliable information. Caught by approaching dead-lines, surrounded by urgency, individuals seek the simplest means to reduce complexity according to the criteria on which they will be *locally* judged."[436] Although some might gain hope from the renewed interest in tradecraft, the fact that the same errors are being repeated by a new generation of intelligence professionals certainly should lead one to doubt that an underlying and necessary paradigm shift has occurred. That is, the change is not occurring because before the "opponents" die off they are

---

432 The most recent version of the NIC forecasts is *Global Trends 2025: A Transformed World*, URL: <http://www.odni.gov/>, accessed 12 December 2008.

433 Taleb, *The Black Swan*, 173.

434 Klein and others, "Macrocognition," 82-83.

435 Gary Zukav, *The Dancing Wu Li Masters: An Overview of the New Physics* (New York, NY: Harper Collins, 2001), 117.

436 Baumard, "From Noticing to Making Sense, 31-32. Emphasis in original.

acculturating a new, younger generation.[437] If the community is to change it cannot wait for another generation (or longer), especially if that new generation is hired and acculturated into the inadequate paradigm of the preceding or present generations.[438]

Achieving this paradigm shift therefore requires revolutionary action by a revolutionary workforce. Aggressive, mindful sensemaking is one pathway to this new paradigm, and may require a different mix of skills and abilities than is currently present. It certainly requires greater, authentic diversity. Considering the present community, one is reminded of Kent's quip, "When an intelligence staff has been screened through [too fine a mesh], its members will be as alike as tiles on a bathroom floor—and about as capable of meaningful and original thought."[439] In contrast, making sense of the 21st Century's intelligence challenges requires as much rigorous, "meaningful and original thought" as we can muster. Sensemaking, as it has been developed here, offers us a means of creating that desperately needed thought.

For the Community to remain unchanged is unacceptable: the implications of being wrong are too dire. Developing a validated practice of mindful sensemaking for intelligence, while not a panacea, is a necessary first step in making sense of the nonsense. The results from IARPA's ongoing exploration of sensemaking, if successful, also can be expected to shed light on how this can practically and functionally be accomplished. Both represent a step toward a true professional practice of intelligence that can meaningfully make sense of the national security challenges of the 21st Century.

---

437 Planck observed, "A new scientific truth does not triumph by convincing its opponents and making them see the light, but rather because its opponents eventually die, and a new generation grows up familiar with it." Max Planck, *Scientific Autobiography and Other Papers*, F. Glynor, trans. (New York, NY: Philosophical Library, 1949), 33-34. Cited in Charles Weiss, "Communicating Uncertainty in Intelligence and Other Professions," *International Journal of Intelligence and CounterIntelligence*, vol. 21, no. 1 (Spring 2008), 78-79.

438 While beyond the scope of this book, organizing to bring about a "revolution in intelligence affairs" is another important aspect of focusing intelligence for the century in which it finds itself. William Nolte, writing in *Studies in Intelligence*, explores the environment for reorganization. Yet, Nolte also presages the argument of this volume in noting that "we need to focus less on structure and more on behavior." See William Nolte, "Keeping Pace with the Revolution in Military Affairs," *Studies in Intelligence*, vol. 48, no. 1 (Winter 2004), 1-10.

439 Kent's comment appears in a footnote on page 74 of his *Strategic Intelligence for American World Policy* (1951 and 1966 printings). It is reproduced in Jack Davis' Occasional Paper for the Kent Center at the CIA. Although Kent was reacting to the stringent security policies of the McCarthy era, his remark also applies to all workforce acquisition practices that promote anything but the widest of diversity. See Jack Davis, "Sherman Kent and the Profession of Intelligence Analysis," *The Sherman Kent Center for Intelligence Analysis*, Occasional Papers, vol. 1, no. 5 (November 2002), URL: <https://www.cia.gov/library/kent-center-occasional-papers/vol1no5.htm>, accessed 10 June 2010.

REFERENCES

Anonymous. *For Want of a Nail Rhyme*. URL: <http://www.rhymes.org.uk/for_want_of_a_nail.htm>. Accessed 10 September 2007.

Argyris, Chris. *Reasons and Rationalizations: The Limits of Organizational Learning*. Oxford, UK: Oxford University Press, 2006.

Bain, Ben. "A-Space Set to Launch this Month." F*ederal Computer Week*, 3 September 2008. URL: <http://fcw.com/articles/2008/09/03/aspace-set-to-launch-this-month.aspx>. Accessed 15 June 2010.

Baron, Joan Boykoff and Robert J. Sternberg, eds. *Teaching Thinking Skills: Theory and Practice*. New York, NY: Freeman, 1987.

Baumard, Philippe. "From Noticing to Making Sense: Using Intelligence to Develop Strategy." *International Journal of Intelligence and CounterIntelligence* 7, no 1 (Spring, 1994): 29-73.

Berkowitz, Bruce. "U.S. Intelligence Estimates of Soviet Collapse: Reality and Perception." In Francis Fukuyama, ed. *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics*. Washington, DC: Brookings Institution Press, 2007: 29-41.

Ben-Israel, Isaac. "Philosophy and Methodology of Intelligence: The Logic of the Estimate Process." *Intelligence and National Security* 4, no. 4 (October 1989): 660-718.

Betts, Richard K. *Enemies of Intelligence: Knowledge and Power in American National Security*. New York: Columbia University Press, 2007.

Bialki, Carl. "Swine Flu Count Plagued by Flawed Data." *Wall Street Journal*. Online edition, 23 January 2010. URL: <http://online.wsj.com/article/SB10001424052748704509704575019313343580460.html>. Accessed 2 February 2010.

Blight, James G. and David A. Welch, Eds. *Intelligence and the Cuban Missile Crisis*. London, UK: Frank Cass, 1998.

Bouquet Cyril and Ben Bryant. "The Crisis Is Here To Stay. Do You Have The Key To Coping?" *Forbes*. Online edition, 21 April 2009. Online Edition. URL: <http://www.forbes.com/2009/04/21/stress-coping-mindfulness-leadership-managing-fixation.html>. Accessed 13 January 2010.

REFERENCES (Continued)

Brei, William S., CAPT, USAF. *Getting Intelligence Right: The Power of Logical Procedure*, Occasional Paper Number Two. Washington, DC: Joint Military Intelligence College, 1996.

Brentano, Franz. *Psychology from an Empirical Standpoint*. Antos C. Rancurello, trans. New York, NY: Humanities Press, 1973.

Brentano, Franz. *Psychologie vom empirischen Standpunkte*. Leipzig, DE: Dunker and Humblot, 1874.

Brewer, John and Albert Hunter. *Foundations of Multimethod Research: Synthesizing Styles*. Thousand Oaks, CA: Sage Publications, 2006.

Bryant Ben and Jeanny Wildi. "Mindfulness." *Perspectives for Managers* 162 (September 2008). URL: <http://www.imd.ch/research/publications/upload/ PFM162_LR_Bryant_Wildi.pdf>. Accessed 14 January 2010.

Burton, Robert A. *On Being Certain: Believing You Are Right Even When You're Not*. New York, NY: St. Martin's Press, 2008.

Cacciabue, Pietro C. and Erik Hollnagel, "Simulation of Cognition: Applications," Expertise and Technology: Cognition and Human-Computer Cooperation. In Jean-Michel Hoc, Pietro C. Cacciabue, and Erik Hollnagel, eds. *Expertise and Technology: Cognition and Human-Computer Cooperation*. Hillsdale, NJ: Lawrence Erlbaum Associates, 1995: 55-73.

Campbell, Kenneth J. "Major General Charles A. Willoughby: A Mixed Performance," unpublished paper, URL: <http://intellit.muskingum.edu/wwii_folder/wwiifepac_folder/wwiifepacwilloughby.html>. Accessed 5 January 2010.

Campbell, Kim, ed. *Addressing the Causes of Terrorism: The Club de Madrid Series on Democracy*, Volume 1. Madrid, SP: Club de Madrid, 2005.

Cantor, Norman F. *In the Wake of the Plague: The Black Death & the World it Made*. New York, NY: The Free Press, 2001.

Central Intelligence Agency. "Iraq's WMD Programs: Culling Hard Facts from Soft Myths." Press Release, 28 November 2003. URL: <https://www.cia.gov/news-information/press-releases-statements/press-release-archive-2003/pr11282003.html>. Accessed 9 December 2009.

REFERENCES (Continued)

Chamberlin, Thomas C. "The Method of Multiple Working Hypotheses." *Science* 15 (old series), no. 366 (7 February 1890): 92-96.

Charnov, Eric L. "Optimal Foraging: The Marginal Value Theorem." *Theoretical Population Biology* 9, no. 2 (April 1976): 129-136.

Cheikes, Brant A., Mark J. Brown, Paul E. Lehner, and Leonard Adelman. *Confirmation Bias in Complex Analyses*. Mitre Technical Report, MTR 04B0000017. Bedford, MA: Mitre, 2004.

Christensen, Clayton. *The Innovator's Dilemma*. Cambridge, MA: Harvard University Press, 1997.

Christensen, Karen. "Thought Leader Interview, Chris Argyris." *Rotman: The Magazine of the Rotman School of Management*. University of Toronto, Winter 2008: 10-13.

Cilliers, Paul. "Knowing Complex Systems." In Kurt A. Richardson, ed., *Managing Organizational Complexity: Philosophy, Theory, and Application*. Greenwich, CT: Information Age Publishing, 2005, 7-19.

Clapper, James. "Remarks and Q & A by Director of National Intelligence Mr. James Clapper." Bipartisan Policy Center (BPC) — The State of Domestic Intelligence Reform. 6 October 2010. URL: <http://www.dni.gov/speeches/20101006_speech_clapper.pdf>. Accessed 29 October 2010.

Clayton, James, D. Y*ears of MacArthur, 1945-1964*. Boston: Houghton Mifflin, 1985.

Cloud, John. "Losing Focus? Studies Say Meditation May Help." *Time*. Online edition, 6 August 2010. URL: <http://www.time.com/time/health/article/0,8599,2008914,00.html>. Accessed, 11 August 2010.

Cohen, Robert S., Paul K. Feyerabend, and Marx W. Wartofsky. *Essays in Memory of Imre Lakatos: Boston Studies in the Philosophy of Science*, Volume XXXIX. Dordrecht, HL: D. Reidel Publishing Company, 1976.

Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction. Report to the President of the United States. Washington, DC: Government Printing Office, 31 March 2005.

REFERENCES (Continued)

Cooper, Jeffrey. *Curing Analytic Pathologies: Pathways to Improved Intelligence Analysis*. Washington, DC: Central Intelligence Agency, Center for the Study of Intelligence, 2005.

Crenshaw, Martha. "Political Explanations." In Kim Campbell, ed. *Addressing the Causes of Terrorism: The Club de Madrid Series on Democracy*, Volume 1. Madrid, SP: Club de Madrid, 2005: 13-18.

Davis, Jack. "Sherman Kent and the Profession of Intelligence Analysis." *The Sherman Kent Center for Intelligence Analysis*. Occasional Papers 1, no. 5 (November 2002). URL: <https://www.cia.gov/library/kent-center-occasional-papers/vol1no5.htm>. Accessed 10 June 2010.

Davis, Jack. "Introduction — Improving Intelligence Analysis at CIA: Dick Heuer's Contribution to Intelligence Analysis." In Richards J. Heuer, Jr. *Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence, 1999.

Davis, Jack. "Analysis and Policy: The Kent-Kendall Debate of 1949." *Studies in Intelligence* 36, no. 5 (1992): 91-103.

Dervin, Brenda. "Sense-Making Methodology Site." URL: <http://communication.sbs.ohio-state.edu/sense-making>. Accessed 12 September 2007.

Dervin, Brenda, Lois Foreman-Wernet, and Eric Lauterbach. *Sense-Making Methodology Reader: Selected Writings of Brenda Dervin*. Cresskill, NJ: Hampton Press, Inc., 2003.

De Vos George and Lola Romanucci-Ross, eds. *Ethnic Identity: Cultural Continuities and Change*. Palo Alto, CA: Mayfield, 1982.

Economist. "Garbage In, Garbage Out." 3 June 1970: 70.

Economist. "Which MBA? 2009 Full-time MBA Ranking." URL: <http://www.economist.com/business-education/whichmba/>. Accessed 15 January 2010.

Eggen, Dan and Walter Pincus. "Ex-Aide Recounts Terror Warnings: Clarke Says Bush Didn't Consider Al Qaeda Threat a Priority Before 9/11." *The Washington Post*, 25 March 2004, A01.

REFERENCES (Continued)

Ekman, Paul. *Telling Lies: Clues to Deceit in the Marketplace, Politics, and Marriage*. New York, NY: W.W. Norton, 2009.

Emerson, Ralph Waldo. *The Essay on Self-Reliance*. East Aurora, NY: The Roycrafters, 1908.

Ennis, Robert. "A Taxonomy of Critical Thinking Skills and Dispositions." In Joan Boyloff Baron and Robert J. Sternberg, Eds. *Teaching Thinking Skills: Theory and Practice*. New York, NY: Freeman, 1987, 9-26.

Ericsson, K. Anders, Neil Charness, Robert R. Hoffman, and Paul J. Feltovich, eds. *Cambridge Handbook of Expertise and Expert Performance*. Cambridge, UK: Cambridge University Press, 2006.

Faculty of the School for Advanced Military Studies. *The Art of Design*, Volume 2. Fort Leavenworth, KS, 2010. URL: <http://www.cgsc.edu/events/sams/ArtofDesign_v2.pdf>. Accessed 20 May 2010.

Fagan, Garrett G. *Archaeological Fantasies: How Pseudoarchaeology Misrepresents the Past and Misleads the Public*. London, UK: Routledge, 2006.

Fallows, James. "Countdown to a Meltdown." *The Atlantic Monthly*, July/August 2005. URL: <http://www.theatlantic.com/doc/200507/fallows>. Accessed 15 February 2010.

Feltovich, Paul J., Robert R. Hoffman, Axel Roesler, David Woods. "Keeping It Too Simple: How the Reductive Tendency Affects Cognitive Engineering." *IEEE Intelligent Systems* 19, no. 3 (May/June 2004): 90-94.

Financial Times. "Executive Education — Open — 2009." URL: <http://rankings.ft.com/businessschoolrankings/executive-education---open>. Accessed 15 January 2010.

Fischoff, Baruch. "For Those Condemned to Study the Past: Heuristics and Biases in Hindsight." In Daniel Kahneman, Paul Slovic, and Amos Tversky. *Judgment Under Uncertainty: Heuristics and Biases*. Cambridge, UK: Cambridge University Press, 1982, 335-351.

Fishbein, Warren and Gregory Treverton. "Making Sense of Transnational Threats." *Sherman Kent Center Occasional Papers* 3, no. 1 (October 2004).

REFERENCES (Continued)

Fishman Barry J. and Samuel F. O'Connor-Divelbiss, eds. Fourth International Conference of the Learning Sciences. Mahwah, NJ: Erlbaum, 2000.

Folker, Robert D., Jr., MSgt, USAF. *Intelligence Analysis in Theater Joint Intelligence Centers: An Experiment in Applying Structured Methods*, Occasional Paper Number Seven. Washington, DC: Joint Military Intelligence College, 2000.

Ford, Harold P. "The CIA and Double Demonology: Calling the Sino-Soviet Split." *Studies in Intelligence* 42, no. 5 (Winter 1988-1989): 57-71.

Ford, Harold P. *CIA and Vietnam Policymakers: Three Episodes 1962-1968*. Washington, DC: Center for the Study of Intelligence, 1998.

Foreman-Wernet, Lois. "Rethinking Communication: Introducing the Sense-Making Methodology." In Brenda Dervin, Lois Foreman-Wernet, and Eric Lauterbach. *Sense-Making Methodology Reader: Selected Writings of Brenda Dervin*. Cresskill, NJ: Hampton Press, Inc., 2003, 1-10.

Fukuyama, Francis. "The Challenges of Uncertainty: An Introduction." In Francis Fukuyama, ed. *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics*. Washington, DC: Brookings Institution Press, 2007, 1-6.

Fukuyama, Francis, ed. *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics*. Washington, DC: Brookings Institution Press, 2007.

Garthoff, Raymond L. "US Intelligence in the Cuban Missile Crisis." In James G. Blight and David A. Welch, Eds. I*ntelligence and the Cuban Missile Crisis*. London, UK: Frank Cass, 1998, 18-63.

Genomics and Genetics Weekly. "Why do People 'Play the Longshot' and Buy Insurance? It's in Our Genes." 29 January 2010: 184.

George, Roger Z. and James B. Bruce. *Analyzing Intelligence: Origins, Obstacles, and Innovations*. Washington, DC: Georgetown University Press, 2008.

REFERENCES (Continued)

Gibbons Robert and Andrew Rutten. "Institutional Interactions: An Equilibrium Approach to the State and Civil Society." *IQ* online journal. The Institute for Quantitative Social Science at Harvard University. URL: <http://www.iq.harvard.edu/files/iqss/old/PPE/gibbons+rutten.pdf>. Accessed 14 May 2010.

Gigerenzer, Gerd. *Simple Heuristics That Make Us Smart*. Oxford, UK: Oxford University Press, 1999.

Gilovich, Thomas, Dale Griffin, Daniel Kahneman. *Heuristics and Biases*. Cambridge, UK: Cambridge University Press, 2002.

Goldenberg, Jacob, David Mazursky, and Sorin Solomon. "Essays on Science and Society: Creative Sparks." *Science* 285, no. 5433 (3 September 1999): 1495-1496.

Gonzales, Laurence. *Deep Survival: Who Lives, Who Dies, and Why*. New York, NY: W.W. Norton, 2003.

Gorfein David S. and Robert Hoffman, eds. *Memory and Learning: The Ebbinghaus Centennial Conference*. Hillsdale, NJ: Erlbaum, 1982.

Gould, Stephen J. *The Mismeasure of Man*. New York, W. W. Norton & Company, 1996.

Greenberger, Martin, ed. *Computers, Communications, and the Public Interest*. Baltimore, MD: Johns Hopkins University Press, 1971.

Gross, Samuel R., Kristen Jacoby, Daniel J. Matheson, Nicholas Montgomery, and Sujata Patil. "Exonerations in the United States (1989 through 2003)." *Journal of Criminal Law and Criminology* 95, no. 2 (2005): 523-560.

Grove, William M. "Clinical Versus Statistical Prediction: The Contribution of Paul E. Meehl." *Journal of Clinical Psychology* 61, no. 10 (2005): 1233-1243.

Grove, William M., David H. Zald, Boyd S. Lebow, Beth E. Snitz, and Chad Nelson. "Clinical Versus Mechanical Prediction: A Meta-Analysis," *Psychological Assessment* 12, no. 1 (2000): 19-30.

Haines Gerald K. and Robert E. Leggett, eds. *Watching The Bear: Essays on CIA's Analysis of the Soviet Union*. Washington, DC: Center for the Study of Intelligence, 2003.

REFERENCES (Continued)

Hampson, Fen Osler. "The Divided Decision-Maker: American Domestic Politics and the Cuban Crises." *International Security* 9, no. 3 (Winter 1984-1985): 130-165.

Hansen, James H. "Soviet Deception in the Cuban Missile Crisis." *Studies in Intelligence* 46, no. 1 (2002): 49-58.

Hasher, Lynn, David Goldstein, and Thomas Toppino. "Frequency and the Conference of Referential Validity." *Journal of Verbal Learning and Verbal Behavior* 16 (1977): 107-112.

Hayak, Friedrich August. *The Counter-Revolution of Science: Studies on the Abuse of Reason*, 2nd Edition. Indianapolis, Indiana: Liberty Fund, Inc., 1979.

Hayden, GEN Michael V. (Ret.). Interview on national security and U.S. strategy. C-SPAN Radio. 9 August 2010. URL: <http://www.cspan.org/Watch/Media/2010/08/09/Terr/A/36779/Gen+Michael+Hayden+Ret+The+Chertoff+Group+Principal.aspx>. Accessed 11 August 2010.

Herlihy, David. *The Black Death and the Transformation of the West*. Samuel K. Cohn, Jr., ed. Cambridge, MA: Harvard University Press, 1995.

Herrmann Douglas J. and Roger Chaffin, R. "Memory before Ebbinghaus." In David S. Gorfein and Robert Hoffman, eds. *Memory and Learning: The Ebbinghaus Centennial Conference*. Hillsdale, NJ: Erlbaum, 1982.

Hernstein, Richard J. and Charles Murray. *The Bell Curve: Intelligence and Class Structure in American Life*. New York, NY: The Free Press, 1996.

Hertwig, Ralph, Gerd Gigerenzer, and Ulrich Hoffrage. "The Reiteration Effect in Hindsight Bias." *Psychological Review* 104, no. 1 (1997): 194-202.

Heuer, Richards J., Jr. *Psychology of Intelligence Analysis*. Washington, DC: Center for the Study of Intelligence, 1999.

Heuer, Richards J., Jr. and Randolph H. Pherson. *Structured Analytic Techniques for Intelligence*. Washington, DC: CQ Press, 2010.

REFERENCES (Continued)

Hilton, Denis. "Causality vs. Explanation: Objective Relations vs. Subjective Interests." *Interdisciplines*. Institute of Cognitive Sciences. University of Geneva. URL: <http://www.interdisciplines.org/causality/papers/14>, accessed 1 November 2010.

Hoc, Jean-Michel, Pietro C. Cacciabue, and Erik Hollnagel, eds. *Expertise and Technology: Cognition and Human-Computer Cooperation*. Hillsdale, NJ: Lawrence Erlbaum Associates, 1995.

Hoffman, Robert. R. "How Can Expertise Be Defined? Implications of Research from Cognitive Psychology." In Robin Williams, Wendy Faulkner and James Fleck, eds. *Exploring Expertise*. New York, NY: MacMillan, 1998, 81-100.

Hoffman, Robert. R. "Biased about Biases: The Theory of the Handicapped Mind in *The Psychology of Intelligence Analysis.*" Panel Presentation for "Designing Support for Intelligence Analysts," S. Potter, Chair. In *Proceedings of the 48th Annual Meeting of the Human Factors and Ergonomics Society*. Santa Monica, CA: Human Factors and Ergonomics Society, 2005, 406-410.

Hoffman, Robert. Conversation with the author, 4 October 2007.

Hoffman Robert R. and Laura Grace Militello. *Perspectives on Cognitive Task Analysis: Historical Origins and Modern Communities of Practice*. Boca Raton, FL: CRC Press/Taylor and Francis, 2008.

Holden, Constance. "Parsing the Genetics of Behavior." *Science* 322, no. 5903 (7 November 2008): 892-895.

Horn, Robert. Conversation with the author, 6 October 2010

IARPA. *Integrated Cognitive-Neuroscience Architectures for Understanding Sensemaking*. Broad Area Announcement IARPA-BAA-10-04, 1 April 2010. URL: <http://www.iarpa.gov/solicitations_icarus.html>. Accessed 1 June 2010.

James, William. *Principles of Psychology,* two volumes. New York, NY: Henry Holt and Company, 1890.

Jervis, Robert. "Why Intelligence and Policymakers Clash." *Political Science Quarterly* 125, no. 2 (Summer 2010): 185-204.

REFERENCES (Continued)

Johnston, Rob. *Analytic Culture in the U.S. Intelligence Community: An Ethnographic Study*. Washington, DC: Center for the Study of Intelligence, 2005.

Jones, Morgan, D. *The Thinker's Toolkit: 14 Powerful Techniques for Problem Solving*, Revised and Updated. New York, NY: Crown Publishing: 1998.

Kahneman Daniel, and Gary Klein. "Conditions for Intuitive Expertise: A Failure to Disagree." *American Psychologist* 64, no. 6 (September 2009): 515-526.

Kahneman, Daniel and Amos Tversky. "Prospect Theory: An Analysis of Decision Under Risk" *Econometrica* 47, no. 2 (March 1979): 263-291.

Kahneman, Daniel, Paul Slovic, and Amos Tversky. *Judgment Under Uncertainty: Heuristics and Biases*. Cambridge, UK: Cambridge University Press, 1982.

Kaiser Family Foundation. "WHO Rejects Accusations It Mishandled H1N1, Updates Worldwide Stats." Kaiser Family Foundation. URL: <http://globalhealth.kff.org/Daily-Reports/2010/January/25/GH-012510-Swine-Flu.aspx?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+kff%2Fkdghpr+%28Kaiser+Daily+Global+Health+Policy+Report%29>. Accessed 2 February 2010.

Kendall, Willmoore. "The Function of Intelligence." *World Politics* 1, no. 4 (July 1949): 542-552.

Kent, Sherman. "A Crucial Estimate Relived." *Studies in Intelligence* 8, no. 2 (Spring 1964): 1-18 (originally classified SECRET). Declassified and reprinted in vol. 36, no. 5 (1992): 111-119.

Kent, Sherman. *Strategic Intelligence for American World Policy*. Princeton, NJ: Princeton University Press, 1949.

Kerbel, Josh and Anthony Olcott. "Synthesizing with Clients, Not Analyzing for Customers." *Studies in Intelligence* 54, no. 4 (December 2010): 1-13.

Kilbourne, Edwin D. "Influenza Pandemics of the 20th Century." *Emerging Infectious Diseases* 12, no. 1 (January 2006): 9-14. URL: <www.cdc.gov/eid>. Accessed 30 March 2010.

REFERENCES (Continued)

Klein, Gary and Robert R. Hoffman, "Macrocognition, Mental Models, and Cognitive Task Analysis Methodology." In Jan Maarten Schraagen, Laura Grace Militello, Tom Ormerod, and Raanan Lipshitz, eds. *Naturalistic Decision Making and Macrocognition*. Aldershot, UK: Ashgate Publishing Limited, 2008, 57-80.

Klein, Gary. "Flexecution as a Paradigm for Replanning, Part 1." *IEEE Intelligent Systems* 22, no. 5 (September/October 2007): 79-88.

Klein, Gary. "Flexecution as a Paradigm for Replanning, Part 2." *IEEE Intelligent Systems* 22, no. 6 (November/December 2007): 108-112.

Klein, Gary, Brian Moon, and Robert R. Hoffman. "Making Sense of Sensemaking 2: Alternative Perspectives." *IEEE Intelligent Systems* 21, no. 4 (July/August 2006): 70-73.

Klein, Gary, Brian Moon, and Robert R. Hoffman. "Making Sense of Sensemaking 1: A Macrocognitive Model." *IEEE Intelligent Systems* 21, no. 5 (September 2006): 88-92.

Klein, Gary, Karol G. Ross, Brian M. Moon, Devorah E. Klein, Robert R. Hoffman, and Erik Hollnagel. "Macrocognition." *IEEE Intelligent Systems* 18, no. 3 (May/June 2003): 81-85.

Kleinmuntz, Benjamin. "The Processing of Clinical Information by Man and Machine." In Benjamin Kleinmuntz, ed. *Formal Representations of Human Judgment*. New York, NY: Wiley, 1968, 149-186.

Knowles, David. *Great Historical Enterprises and Problems in Monastic History*. London, UK: Thomas Nelson and Sons, 1962.

Kosso, Peter. "Introduction: The Epistemology of Archaeology." In Garrett G. Fagan, *Archaeological Fantasies: How Pseudoarchaeology Misrepresents the Past and Misleads the Public*. London, UK: Routledge, 2006, 3-22.

Krizan, Lisa A. *Intelligence Essentials for Everyone*. Occasional Paper Number Six. Washington, DC: Joint Military Intelligence College, 1999.

Kuhn, Thomas S. *The Structure of Scientific Revolutions*. Chicago, IL: University of Chicago Press, 1962.

REFERENCES (Continued)

Kuhn, Thomas S. *The Road Since Structure: Philosophical Essays, 1970-1993, with an Autobiographical Interview*. James Conant and John Haugeland, eds. Chicago, IL: University of Chicago Press, 2000.

Langer, Ellen J. *Mindfulness*. Cambridge, MA: Da Capo Press, 1989.

Leedom, Dennis K. *Final Report Sensemaking Symposium*. Command and Control Research Program Office of the Assistant Secretary of Defense for Command, Control, Communications and Intelligence, 23-25 October 2001.

Lester, Gregory W. "Why Bad Beliefs Don't Die." *Skeptical Inquirer* 24, no. 6 (November/December 2000). URL: <http://www.csicop.org/si/archive/category/volume_24.6>. Accessed 22 September 2009.

Lin, Lin. "Breadth-Biased Versus Focused Cognitive Control in Media Multitasking Behaviors." *Proceedings of the National Academies of Science* 106, no. 37 (15 September 2009): 15521-15522. URL: <www.pnas.org!cgi!doi!10.1073!pnas.0908642106 PNAS>. Accessed 18 March 2010.

MacEachin, Douglas. *Predicting the Soviet Invasion of Afghanistan: The Intelligence Community's Record*. Washington, DC: Center for the Study of Intelligence, 2002.

Macintyre, Ben. *Operation Mincemeat*. New York, NY: Harmony Books, 2010.

MacLean, Katherine A., Emilio Ferrer, Stephen R. Aichele, David A. Bridwell, Anthony P. Zanesco, Tonya L. Jacobs, Brandon G. King, Erika L. Rosenberg, Baljinder K. Sahdra, Phillip R. Shaver, B. Alan Wallace, George R. Mangun, and Clifford D. Saron. "Intensive Meditation Training Improves Perceptual Discrimination and Sustained Attention." *Psychological Science* 21, no. 6 (2010): 829-830.

Mandel, David R., Alan Barnes, and John Hannigan. "A Calibration Study of an Intelligence Assessment Division." PowerPoint Presentation. Defense Research and Development Canada, Toronto, CA, not dated.

Manjoo, Farhad. *True Enough: Learning to Live in a Post-Fact Society*. Hoboken, NJ: John Wiley & Sons, 2008.

REFERENCES (Continued)

McCosh, James. LL.D. *Intuitions of the Mind: Inductively Investigated*. London: UK: Macmillan and Company, 1882.

McCallister, William S. "COIN and Irregular Warfare in a Tribal Society." *Small Wars Journal*, blog and pamphlet, 4 February 2008. URL: <http://www.smallwarsjournal.com/documents/coinandiwinatribalsociety.pdf>. Accessed 31 May 2010.

Menkhaus, Kenneth. "State Fragility as a Wicked Problem," *Prism* 1, no. 2 (March 2010): 85-100. URL: <http//:www.ndu.edu/press/lib/images/prism1-2/6_Prism_85-100_Menkhaus.pdf>. Accessed 14 May 2010.

Meszerics, Tamas and Levente Littvay, "Pseudo-Wisdom and Intelligence Failures," *International Journal of Intelligence and Counterintelligence* 23, no. 1 (December 2009): 133-147.

Mercyhurst College Institute for Intelligence Studies. "Non-State Actors in Sub-Saharan Africa 2007-2012 Outlook." URL: <https://nonstateactorsafrica.wikispaces.com>. Accessed 28 April 2010.

Miller, George A. "The Magical Number Seven, Plus or Minus Two: Some Limits on Our Capacity for Processing Information." *The Psychological Review* 63 (1956): 81-97.

Miller, Linda K. and Mary McAuliffe. "The Cuban Missile Crisis," *Magazine of History* 8 (Winter 1994). URL: <http://www.oah.org/pubs/magazine/coldwar/miller.html>. Accessed 5 January 2010.

Miller, Peter. *The Smart Swarm: How Understanding Flocks, Schools, and Colonies Can Make Us Better at Communicating, Decision Making, and Getting Things Done*. New York, NY: Penguin Books, 2010.

Monk Christopher A., J. Gregory Trafton, and Deborah A. Boehm-Davis. "The Effect of Interruption Duration and Demand on Resuming Suspended Goals." *Journal of Experimental Psychology: Applied* 14 (December 2008): 299-313.

Montagu, Ewen. *The Man Who Never Was: World War II's Boldest Counterintelligence Operation*. Annapolis, MD: Naval Institute Press, 2001.

Moore, David T. *Creating Intelligence: Evidence and Inference in the Analysis Process*. MSSI Thesis chaired by Francis J. Hughes. Washington, DC: Joint Military Intelligence College, July 2002.

REFERENCES (Continued)

Moore, David T. *Critical Thinking and Intelligence Analysis*, Occasional Paper Number Fourteen, Revised. Washington, DC: National Defense Intelligence College, 2009.

Moore, David T., and Lisa Krizan. "Core Competencies for Intelligence Analysis at the National Security Agency." In Russell G. Swenson, ed., *Bringing Intelligence About: Practitioners Reflect on Best Practices*. Washington, DC: Joint Intelligence Military College, 2003, 95-132.

Moore, David T., Lisa Krizan, and Elizabeth J. Moore. "Evaluating Intelligence: A Competency-Based Approach." *International Journal of Intelligence and CounterIntelligence* 18, no. 2 (Summer 2005): 204-220.

Moore, David T. and William N. Reynolds, "So Many Ways To Lie: The Complexity of Denial and Deception." *Defense Intelligence Journal* 15, no. 2 (Fall 2006): 95-116.

Morens, David M. and Jeffery K. Taubenberger. "Influenza and the Origins of The Phillips Collection, Washington, DC." *Emerging Infectious Diseases* 12, No. 1 (January 2006): 78-80. URL: <www.cdc.gov/eid>, accessed 30 March 2010.

Mosier, Kathleen and Ute Fischer, eds. *Proceedings of the Eighth International NDM Conference*. Eighth International Naturalistic Decision-Making Conference, Pacific Grove, CA, June 2007.

Myers, David G. *Intuition: Its Powers and Perils*. New Haven, CT: Yale University Press, 2002.

Mylroie, Laurie. "Who is Ramzi Yousef? And Why It Matters." *The National Interest*, 22 December 1995. URL: <http://www.fas.org/irp/world/iraq/956-tni.htm>. Accessed 12 October 2010.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*. Washington, DC: Government Printing Office, 2004.

National Intelligence Council. *Global Trends 2015: A Dialogue About the Future with Nongovernmental Experts*. Washington, DC: Government Printing Office, 2000. URL: <http://www.dni.gov/nic/NIC_globaltrend2015.html>. Accessed 15 February 2010.

REFERENCES (Continued)

National Intelligence Council. "Nonstate Actors: Impact on International Relations and Implications for the United States." Conference Report, August 2007. URL: <http://www.dni.gov/nic/confreports_nonstate_actors.html>. Accessed 27 April 2010.

National Intelligence Council. *Global Trends 2025: A Transformed World*. Washington, DC: Government Printing Office. URL: <http://www.odni.gov/>. Accessed 12 December 2008.

Neustadt, Richard E. and Ernest R. May. *Thinking in Time: The Uses of History for Decisionmakers*. New York, NY: The Free Press, 1986.

New Oxford American Dictionary, Apple Computer Edition, 2005. Various entries.

Nolte, William. "Keeping Pace with the Revolution in Military Affairs." *Studies in Intelligence*, 48, no. 1 (Winter 2004): 1-10.

Nosich, Gerald R. *Learning to Think Things Through: A Guide to Critical Thinking Across the Curriculum*, 3rd edition. Upper Saddle River, NJ: Prentice Hall, 2008.

Obama, Barack. "Remarks by the President on Security Reviews," 5 January 2010. URL: <http://www.whitehouse.gov/the-press-office/remarks-president-security-reviews>. Accessed 7 January 2010.

Oberdorfer, Don. "Missed Signals in the Middle East, *The Washington Post Magazine*, 17 March 1991: 19-41.

Office of the Director of National Intelligence. *Intelligence Community Directive Number 203: Analytic Standards* (21 June 2007). URL: <http://www.fas.org/irp/dni/icd/icd-203.pdf>. Accessed 16 October 2010.

Olcott, Anthony. "Revisiting the Legacy: Sherman Kent, Willmoore Kendall, and George Pettee — Strategic Intelligence in the Digital Age." *Studies in Intelligence* 51, no. 2 (June 2009): 21-32.

Ophir, Eyal, Clifford Nass, and Anthony D. Wagner. "Cognitive Control in Media Multitaskers." *Proceedings of the National Academies of Science, Early Edition* 106, no. 37: 15583-15587. URL: < http://www.pnas.org/content/106/37/15583.full>. Accessed 18 March 2010.

REFERENCES (Continued)

Pappas, Aris A., and James M. Simon, Jr. "The Intelligence Community: 2001-2015: Daunting Challenges, Hard Decisions," *Studies in Intelligence* 46, no. 1 (2002). URL: <http://www.cia.gov/csi/studies/vol46no1/article05.html>. Accessed 10 January 2006.

Park, Caroline L. "What Is the Value of Replicating other Studies?" *Research Evaluation* 13. no. 1 (December 2004): 189-195.

Patterson Emily S. and Janet E. Miller. *Macrocognition Metrics and Scenarios: Design and Evaluation for Real World Teams*. Aldershot, UK: Ashgate, 2010.

Paul, Richard W. and Linda Elder. *Critical Thinking: Tools for Taking Charge of Your Professional and Personal Life*. Upper Saddle River, NJ: Prentice Hall, 2002.

Paul, Richard and Linda Elder. *The Miniature Guide to Critical Thinking: Concepts and Tools*, Sixth edition. Dillon Beach, CA: Foundation for Critical Thinking, 2009.

Peirce, Charles Sanders. "Lowell Lectures (1903)." In Charles Hartshorne and Paul Weiss, eds. *Collected Papers of Charles Sanders Peirce, Volume 1*. Cambridge, MA: Harvard University Press, 1931.

Peirce, Charles Sanders. "A Letter to Lady Welby (1904)." In Arthur W. Burks, ed. *Collected Papers of Charles Sanders Peirce, Volume 8*. Cambridge, MA: Harvard University Press, 1958.

Pezzo, Mark V. and Stephanie P. Pezzo, "Making Sense of Failure: A Motivated Model of Hindsight Bias," *Social Cognition* 25, no. 1 (2007): 147-164.

Phelps, R. H. and James Shanteau, "Livestock Judges: How Much Information Can an Expert Use?" *Organizational Behavior and Human Performance* 21 (1978): 213-222

Pirolli, Peter. *Information Foraging Theory: Adaptive Interaction with Information*. Oxford, UK: Oxford University Press, 2007.

Pirolli, Peter, and Stuart Card. "The Sensemaking Process and Leverage Points for Analyst Technology as Identified Through Cognitive Task Analysis." Paper presented a the 2005 International Conference on Intelligence Analysis, Vienna, Virginia, 2-6 May 2005, URL: <https://analysis.mitre.org/proceedings_agenda.htm#papers>. Accessed 11 March 2009.

REFERENCES (Continued)

Pirolli, Peter and Stuart Card, "Information Foraging," *Psychological Review* 106, no. 4 (October 1999): 643-675.

Pitt, Will. "Interview: 27-Year CIA Veteran." *Truthout*, 26 June 2003. URL: <http://www.truthout.org/docs_03/ 062603B.shtml>. Accessed 12 March 2007.

Planck, Max. *Scientific Autobiography and other Papers*, F. Glynor, trans. New York, NY: Philosophical Library, 1949.

Raeburn, Paul. "Multitasking May Not Mean Higher Productivity." NPR News: *Science Friday*, 28 August 2009. URL: <http://www.npr.org/templates/story/story.php?storyId=112334449&ft=1&f=1007>, accessed 21 February 2010.

Rand, Ayn. *Introduction to Objectivist Epistemology*. New York, NY: Mentor, 1979.

Reed, Jennifer H. "Effect of a Model For Critical Thinking on Student Achievement In Primary Source Document Analysis And Interpretation, Argumentative Reasoning, Critical Thinking Dispositions, and History Content in a Community College History Course." PhD Dissertation. College of Education, University of South Florida, December 1998. URL: <http://www.criticalthinking.org/resources/JReed-Dissertation.pdf>. Last accessed 2 February 2010.

Reed, Nick, and R. Robbins. "The Effect of Text Messaging on Driver Behaviour." *Published Project Report PPR 367*. RAC Foundation Transport Research Laboratory, September 2008. URL: <http://www.racfoundation.org/files/textingwhiledrivingreport.pdf>. Accessed 9 December 2009.

Reynolds, William N. and others. "Social Science Modeling Workshop: Understanding Iraqi Non-State Actors." *Workshop Proceedings*. Least Squares Software, Albuquerque, NM, 15 February 2008.

Richardson, Kurt A., ed. *Managing Organizational Complexity: Philosophy, Theory, and Application*. Greenwich, CT: Information Age Publishing, 2005: 7-19.

REFERENCES (Continued)

Ricks, Thomas E. "A Marine's Afghan AAR (XIV): Get Rid of the iPods on Patrol," Web Log, *Foreign Policy*. Weblog Entry, 20 January 2010. URL: <http://ricks.foreignpolicy.com/posts/2010/01/20/a_marine_s_afghan_aar_xiv_get_rid_of_ the_ipods_on_patrol>. Accessed 26 January 2009.

Rieber, Steven. "Intelligence Analysis and Judgmental Calibration." *International Journal of Intelligence and CounterIntellgience* 17, no. 1 (Spring 2004): 97-112.

Rieber, Steven, and Neal Thomason. "Towards Improving Intelligence Analysis: Creation of a National Institute for Analytic Methods." *Studies in Intelligence*. Online edition 49, no. 4 (Fall 2005). URL: <https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/csi-studies/studies/vol49no4/Analytic_Methods_7.htm#_ftn10>. Accessed 7 January 2009.

Rihoux, Benoit. "Constructing Political Science Methodology: From Segmented Polarization to Enlightened Pluralism." Joint Chair, Standing Group on Political Methodology. *IPSA Conference*. Montreal, Canada, 2008.

Rittel, Horst W. J. and Melvin M. Webber. "Dilemmas in a General Theory of Planning." *Policy Sciences* 4 (1973): 155-169.

Robb, John. *Brave New War: The Next Stage of Terrorism and the End of Globalization*. New York, NY: John A. Wiley and Sons, 2007.

Rochman, Bonnie. "Samurai Mind Training for Modern American Warriors." *Time*. Online edition, 6 September 2009. URL: <http://www.time.com/time/nation/article/0,8599,1920753,00.html>. Accessed 4 August 2010.

Rogoff, Barbara and Jean Lave. *Everyday Cognition: Its Development in Social Context*. Cambridge, MA: Harvard University Press, 1984.

Ronson, Jon. "What Part of 'Bomb' Don't You Understand?" *This American Life*, Episode 338, 3 August 2008. URL: <http://www.thislife.org/Radio_Episode.aspx?episode=338>. Accessed 4 August 2008.

Rosenhead, Jonathan, ed. *Rational Analysis for a Problematic World: Problem Structuring Methods for Complexity, Uncertainty and Conflict*, 2nd edition. Hoboken, NJ: John Wiley & Sons, 2001.

REFERENCES (Continued)

Rosenhead, Jonathan. "Complexity Theory and Management Practice." URL: <http://www.human-nature.com/science-as-culture/rosenhead.html. Accessed 23 December 2008.

Rummel, Rudolph. J. *Understanding Conflict and War: War, Power, Peace*. Beverly Hills, CA: Sage Publications, 1991.

Russell, Dennis M., Mark J. Stefik, Peter Pirolli, and Stuart Card. "The Cost Structure of Sensemaking." Paper presented a the INTERCHI '93 Conference on Human Factors in Computing Systems, Amsterdam, NL, 24-25 April 1993. URL: <http://www2.parc.com/istl/groups/uir/publications/items/UIR-1993-10-Russell.pdf>. Accessed 18 August 2010.

Schacter, Daniel L., Donna Rose Addis and Randy L, Buckner. "Remembering the Past to Imagine the Future: The Prospective Brain," *Nature Review Neuroscience* 8 (September 2007): 657-661.

Schraagen, Jan, Maarten, Laura Grace Militello, Tom Ormerod, and Raanan Lipshitz, eds. *Naturalistic Decision Making and Macrocognition*. Aldershot, UK: Ashgate Publishing Limited, 2008.

Schreiber Darren M., Alan N. Simmons,, Christopher T. Dawes, Taru Flagan, James H. Fowler, and Martin P. Paulus. "Red Brain, Blue Brain: Evaluative Processes Differ in Democrats and Republicans." Paper delivered at the 2009 American Political Science Association Meeting, Toronto, CA, 3-6 September 2009. URL: <http ://ssrn.com/abstract=1451867>. Accessed 9 December 2009.

Schrodt Philip A. and Deborah J. Gerner. "The Impact of Early Warning on Institutional Responses to Complex Humanitarian Crises." Paper presented at the Third Pan-European International Relations Conference and Joint Meeting with the International Studies Association. Vienna, Austria, 16-19 September 1998.

Schum, David A. *Evidence and Inference for the Intelligence Analyst*, two volumes. Lanham, MD: University Press of America, 1987.

Schwartz, Peter. *The Art of the Long View*. New York, NY: Doubleday, 1996.

Schwartz, Peter, and Doug Randall. "Ahead of the Curve: Anticipating Strategic Surprise." In Francis Fukuyama, ed. *Blindside: How to Anticipate Forcing Events and Wild Cards in Global Politics*. Washington, DC: Brookings Institution Press, 2007: 93-108.

REFERENCES (Continued)

Scribner, Sylvia. "Studying Working Intelligence. Everyday Cognition: Its Development in Social Context." In Barbara Rogoff and Jean Lave. *Everyday Cognition: Its Development in Social Context.* Cambridge, MA: Harvard University Press, 1984, 9-40.

Scribner, Sylvia. "Thinking in Action: Some Characteristics of Practical Thought." In Ethel Tobach, Rachel Joffe Falmagne, Mary Brown Parlee, Laura M. W. Martin, and Aggie Scribner Kapelman, eds. *Mind and Social Practice: Selected Writings of Sylvia Scribner*. Cambridge, UK: Cambridge University Press, 319-337.

Sethi, Deepak. "Mindful Leadership." *Leader to Leader* 51 (Winter 2009): 7-11.

Shanteau, James. "Competence in Experts: The Role of Task Characteristics." *Organizational Behavior and Human Decision Processes* 53 (1992): 252-266.

Shryock, Richard. "For An Eclectic Sovietology." *Studies in Intelligence* 8, no. 1 (Winter 1964): 57-64.

Simon, Herbert A. "Designing Organizations in an Information-Rich World." In Martin Greenberger, ed. *Computers, Communications, and the Public Interest*. Baltimore, MD: Johns Hopkins University Press, 1971, 40-41.

Slovic, Paul. "Behavioral Problems of Adhering to a Decision Policy." Paper presented at the Institute for Quantitative Research in Finance, Napa, CA, May 1973.

Smith, Rupert. *The Utility of Force: The Art of War in the Modern World*. New York, NY: Alfred A. Knopf, 2007.

Snowden, David, PhD. Conversation with the author, 22 January 2008.

Spelke, Elizabeth S., William Hirst, and Ulric Neisser. "Skills of Divided Attention." *Cognition* 4 (1976): 215-230.

Stanger-Hall, Kathrin. "Accommodation or Prediction?" Letter in response to Peter Lipton, "Testing Hypotheses: Prediction and Prejudice." *Science* 308 (3 June 2005): 1409.

Stefik, Mark. "The New Sensemakers: The Next Thing Beyond Search Is Sensemaking." *Innovation Pipeline* (15 October 2004). URL: <http://www.parc.com/research/publications/files/5367.pdf>. Accessed 11 March 2009.

REFERENCES (Continued)

Stephens, David W., and John R. Krebs. *Foraging Theory*. Princeton, NJ: Princeton University Press, 1986.

Steury, Donald P., Ed. *Sherman Kent and the Board of National Estimates*, Collected Essays. Washington, DC: Center for the Study of Intelligence, 1994.

Swenson, Russell G., ed. *Bringing Intelligence About: Practitioners Reflect on Best Practices*. Washington, DC: Joint Military Intelligence College, 2003.

Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable*. New York, NY: Random House, 2007.

Taleb, Nassim Nicholas. *Fooled by Randomness: The Hidden Role of Chance in Life and in the Markets*, 2nd revised edition. New York, NY: Random House, Inc., 2008.

Tavris, Carol and Elliot Aronson. *Mistakes Were Made (But Not by Me): Why We Justify Foolish Beliefs, Bad Decisions, and Hurtful Acts*. Orlando, FL: Harcourt, 2007.

Thomas, Troy S., Stephen D. Kiser, and William D. Casebeer. *Warlords Rising: Confronting Violent Non-State Actors*. Lanham, MD: Lexington Books, 2005.

Tobach, Ethel, Rachel Joffe Falmagne, Mary Brown Parlee, Laura M. W. Martin, and Aggie Scribner Kapelman, eds. *Mind and Social Practice: Selected Writings of Sylvia Scribner*. Cambridge, UK: Cambridge University Press, 1997.

Transportation Research Board of the National Academies. "Selected References on Distracted Driving: 2005-2009." URL: <http://pubsindex.trb.org/DOCs/Publications from TRIS on Distracted Driving.pdf>. Accessed 9 December 2009.

Treverton, Gregory F. *Intelligence for an Age of Terror*. Cambridge, UK: Cambridge University Press, 2009.

Treverton, Gregory F. *Reshaping National Intelligence for an Age of Information*. UK: Cambridge University Press, 2001.

Treverton, Gregory F. "Estimating Beyond the Cold War." *Defense Intelligence Journal* 3, no. 2 (Fall 1994): 5-20.

REFERENCES (Continued)

Treverton, Gregory F. and C. Bryan Gabbard. *Assessing the Tradecraft of Intelligence Analysis*. TR-293. Santa Monica, CA: RAND Corporation, 2008.

Tsouras, Peter G. *Disaster at D-Day: The Germans Defeat the Allies, June 1944*. London, UK: Greenhill Books, 2000.

Tsouras, Peter G. *Third Reich Victorious: Ten Dynamic Scenarios in Which Hitler Wins the War*. London, UK: Lionel Leventhal Limited, 2002.

Tversky, Amos and Daniel Kahneman. "Availability: A Heuristic for Judging Frequency and Probability." *Cognitive Psychology* 5 (1973): 207-232.

Tversky, Amos and Daniel Kahneman. "Advances In Prospect Theory: Cumulative Representation Of Uncertainty." *Journal of Risk and Uncertainty* 5 (1992): 297-323.

United States Commission on National Security. *New World Coming: American Security in the 21st Century*. Study Addendum, Phase 1 (July 1998-August 1999).

United States Office of Personnel Management. Workforce Compensation and Performance Service. *Introduction to the Position Classification Standards*, TS-107 August 1991. URL: <http://www.opm.gov/fedclass/gshbkocc.pdf>. Accessed 11 December 2009.

United States Office of Personnel Management. *Position Classification Standard for Intelligence Series*, GS-0132 TS-28 June 1960, TS-27 April 1960. URL: <http://www.opm.gov/fedclass/html/gsseries.asp>. Accessed 11 December 2009.

United States Senate. *Report on the U.S. Intelligence Community's Prewar Intelligence Assessments on Iraq*. Select Senate Committee on Intelligence. 108th Congress. 7 July 2004.

University of Bristol, "Adult Stem Cell Breakthrough: First Tissue-engineered Trachea Successfully Transplanted." *Science Daily*, 18 November 2008. URL: <http://www.sciencedaily.com/releases/2008/11/081119092939.htm>. Accessed 21 November 2008.

REFERENCES (Continued)

Van Gelder, Tim. "Mindfulness Versus Metacognition, and Critical Thinking." *Bringing Visual Clarity to Complex Issues*. Weblog Entry, 27 May 2009. URL: <http://timvangelder.com/2009/05/27/mindfulness-versus-metacognition-and-critical-thinking/>. Accessed 13 January 2010.

von Clausewitz, Carl. *On War*. COL James J. Graham, trans. London, UK: Keegan Paul, Trench, Truebner & Co., Ltd.,1908.

Weber, Marta S. Conversation with the author, 2 August 2009.

Weber, Marta S., William N. Reynolds, James Holden-Rhodes, and Elizabeth J. Moore. *Non-State Actors in the Post-Westphalian World Order: A Preliminary LSS Inquiry*. Final Report for Air Force Research Laboratory (AFRL) Contract FA8750-07-C-0312. March 2007.

Weick Karl E. and Kathleen M. Sutcliffe. *Managing the Unexpected: Assuring High Performance in an Age of Complexity*. San Francisco, CA: Jossey-Bass, 2001.

Weick, Karl E. *Sensemaking in Organizations*. Thousand Oaks, CA: Sage Publications, Inc., 1995.

Weiss, Charles. "Communicating Uncertainty in Intelligence and Other Professions." *International Journal of Intelligence and CounterIntelligence* 21, no. 1 (Spring 2008): 57-85.

Westrum, Ronald. "Social intelligence about hidden events." *Knowledge: Creation, Diffusion, Utilization* 3, no. 3 (1982): 381-400.

Wheaton, Kristan J. Email to William N. Reynolds, 15 November 2007.

Wheaton, Kristan J. Email to David T. Moore, 4 March 2008.

Wheaton, Kristan J. and others. *Structured Analysis of Competing Hypotheses*. Erie, PA: Mercyhurst College, 2005.

Wigmore, John Henry. *The Science of Proof: As Given by Logic, Psychology and General Experience and Illustrated in Judicial Trials*, 3rd edition. Boston, MA: Little, Brown, 1937.

Wikipedia, entry under "Analysis." URL: <http://en.wikipedia.org/wiki/Analysis>. Accessed 26 September 2007.

REFERENCES (Continued)

Wikipedia. Entry under "Normal Science." URL: <http://en.wikipedia.org/wiki/Normal_science>. Accessed 26 September 2007.

Williams, Robin, Wendy Faulkner and James Fleck, eds. *Exploring Expertise*. New York, NY: MacMillan, 1998.

Winograd, Eugene and Ulric Neisser, Eds. *Affect and Accuracy in Recall: Studies of "Flashbulb" Memories*. Emory Symposia in Cognition. Cambridge, UK: Cambridge University Press, 1992.

Wohlstetter, Roberta. *Pearl Harbor: Warning and Decision*. Stanford, CA: Stanford University Press, 1962.

Woods, Kevin, James Lacey, and Williamson Murray. "Saddam's Delusions: The View From the Inside." *Foreign Affairs* (May/June 2006).

Young, Michael, Yi Guan, John Toman, Andy DePalma, Elena Znamenskaia. "Agent as Detector: An Ecological Psychology Perspective on Learning by Perceiving-Acting Systems." In Barry J. Fishman and Samuel F. O'Connor-Divelbiss, eds. *Fourth International Conference of the Learning Sciences*. Mahwah, NJ: Erlbaum, 2000, 299-301.

Zelik, Daniel J., Emily S. Patterson, and David D. Woods. "Understanding Rigor in Information Analysis." In Kathleen Mosier and Ute Fischer, eds. *Proceedings of the Eighth International NDM Conference*. Eighth International Naturalistic Decision-Making Conference, Pacific Grove, CA, June 2007, 1-8.

Zelik, Daniel J., Emily S. Patterson, and David D. Woods. "Measuring Attributes of Rigor in Information Analysis." In Emily S. Patterson and Janet E. Miller, and David D. Woods. *Macrocognition Metrics and Scenarios: Design and Evaluation for Real World Teams*. Aldershot, UK: Ashgate, 2010: 65-83.

Zelik, Daniel J. Email to the author, 15 October 2010.

Zukav, Gary. *The Dancing Wu Li Masters: An Overview of the New Physics*. New York, NY: Harper Collins, 2001.

Zwicky, Fritz. *Discovery, Invention, Research — Through the Morphological Approach*. Toronto, CA: The Macmillan Company, 1969.

ABOUT THE AUTHOR

David T. Moore is a senior intelligence professional and educator. He teaches critical thinking and structured techniques for intelligence sensemaking and his research focuses on developing multidisciplinary approaches to facilitate intelligence sensemaking. His most recent posting was to the School of Leadership and Professional Development at the National Geospatial-Intelligence Agency. Formerly he served as a technical director at the National Security Agency where he advocated and mentored best practices in intelligence sensemaking. He is an adjunct faculty member of the National Cryptologic School; has taught at Trinity University, Washington, DC; and lectures at the National Defense Intelligence College and the National Defense University. He received a Master of Science of Strategic Intelligence from the National Defense Intelligence College in 2002.

Mr. Moore's publications include:

- "Species of Competencies for Intelligence Analysis," *Defense Intelligence Journal* 11, no. 2 (Summer 2002): 97-119.
- "Species of Competencies for Intelligence Analysis," *American Intelligence Journal* 23 (2005): 29-43 (an expanded version of the original article).
- *Critical Thinking and Intelligence Analysis*, Occasional Paper Number Fourteen; Authorized, Revised Edition (Washington, DC: National Defense Intelligence College, 2006, 2009).
- With coauthor Lisa Krizan:
    - "Intelligence Analysis, Does NSA Have What It Takes?" *Cryptologic Quarterly* 20, nos. 1/2 (Summer/Fall 2001): 1-32.
    - "Core Competencies for Intelligence Analysis at the National Security Agency," in *Bringing Intelligence About: Practitioners Reflect on Best Practices*, Russell Swenson, ed. (2004): 95-131.
- With coauthors Lisa Krizan and Elizabeth J. Moore:
    - "Evaluating Intelligence: A Competency-Based Approach," *International Journal of Intelligence and CounterIntelligence* 18, no. 2 (Summer 2005): 204-220.

- With coauthor William N. Reynolds:
    - "So Many Ways To Lie: The Complexity of Denial and Deception," *Defense Intelligence Journal* 15, no. 2 (Fall 2006): 95-116.
    - "Advancing the Practice: Multi-methodological Analysis for Intelligence", forthcoming.

The author can be contacted via email at *david.t.moore@ugov.gov*.

ABOUT THE CONTRIBUTORS

Robert R. Hoffman, PhD. A world leader in the field of cognitive systems engineering and Human-Centered Computing, he is a Fellow of the Association for Psychological Science and a Fulbright Scholar. Following post-doctoral work at the Center for Research on Human Learning at the University of Minnesota, Dr. Hoffman joined the faculty of the Institute for Advanced Psychological Studies at Adelphi University. Dr. Hoffman has been recognized internationally for his research on cognitive task analysis and the design of macrocognitive work systems.

Elizabeth J. Moore is a senior intelligence professional. She holds a BA in Russian Studies from Randolph-Macon Woman's College, and an MA in International Politics from American University. Ms. Moore began her government career as a Russian linguist in 1982, and has served in a number of language and analysis positions at the Defense, State, and Treasury Departments; at the National Intelligence Council; as a Director of National Intelligence Fellow attached to the National Security Council; and overseas.

William N. Reynolds, PhD. The founder, President and Chief Science Officer of Least Squares Software, he has been a principal researcher and innovator in the field of complexity for more than twenty years. Over the past eight years, he has focused on the role of complex systems in intelligence analysis, especially complexity-based analytic methodologies. In this capacity, Dr. Reynolds has formulated numerous intelligence analysis case studies assessing the impact of technology on efficiency and effectiveness in analytic practice.

Marta S. Weber, PhD. A psychologist who has applied thirty years of clinical and forensic training and experience to the intelligence domain, Dr. Weber pioneered in the development of sophisticated remote profiling and behavioral forecasting techniques. She is an internationally recognized expert in that highly specialized field. She founded and heads Applied Behavioral Sciences, LLC, a boutique consultancy specializing in primary human-source, human-subject research, analysis, strategic consultation and training.

INDEX

A

Adversarial deception 19, 60, 85, 100
    Operation Mincemeat 85
Analysis
    definition xxxv, 16, 34
    function of ii, 16, 55, 150
    imprecision and inaccuracy of concept 43, 48
Analysis of competing hypotheses xi, 98, 102, 119
    definition 62
    Folker's experiment 101
    Mercyhurst structured version 102
    MITRE critique 101
    value and limitations xi, 118-119
Analytic pathologies 25, 26
Anchoring 24, 119
    definition 79
Automatic thinking 70-72
    definition 70
    risks 71

C

Cognitive dissonance 11
    strategies for coping with 11
Communication
    dangers in xxiv, xxxvi, 64, 65
    IC models of xiv, 5, 123, 129, 154
    new models of 64
    uncertainty in xx, 8, 58, 65-66, 129
    use of blogs in 66
Complexity xxx, 19, 33-36, 39, 47, 89, 122, 154-155
    confounds Kent paradigm 34-35
Complexity theory 19, 33-34, 39
    analysis inadequate 47, 52, 63, 147, 153, 156
    definition 34-35
Concept map 83, 86-87
    use of 84, 87
    value of 87

INDEX (Continued)

Critical thinking xx, xxi, xxiv, xxvi-xxix, xxxi, xxxiii, xxxv, 2, 8, 49, 51, 58, 60, 93, 98,114-116, 123, 130, 131, 144
and role in intelligence planning 8, 51
assists mindfulness xxvi-xxix, 8, 93
defines foraging activities 58, 60

D

Decision making
Examples 11, 48, 65, 116
Diagoras of Melos 96

E

Evidence
changes theories 22, 39, 42, 44, 63
definition 8, 37
epistemological justification of 7, 37-39, 42-43, 48
function of 44, 96, 139
marshaling multiple contexts for 7, 37, 62, 101, 127
relation to truth 37-38, 85, 99, 126
requires agnosticism 42
source of xxviii, 22, 63, 65, 98, 101, 136, 141, 143-144

F

Failure of imagination xix, 12, 15-16, 44, 153
Foraging
and critical thinking xxi, 8, 51, 58, 60
and enriching 55-56, 58
and exploiting 55
and exploring 55-56, 58
and intelligence 7-9, 51, 54-59, 60-63, 90, 102, 127, 137, 146, 152
and planning 8, 51, 54
costs of 60
definition 58
emerging strategies for 59
self-marketing information for 59
self-protective assets in 59-60
sufficiency in 56

INDEX (Continued)

H

Harvesting 61, 138
Heuristic-based judgment 42, 69, 73-76, 79
Hypotheses
    use of alternative 37, 41, 43, 62, 65, 97-98, 100-102, 127-128, 136

I

IARPA xxxiii-xxxiv, 4, 9, 54, 105, 108, 156
Illusions of validity 76, 82
Information
    how much is enough 56, 89-90, 137
    definition 8
Intelligence
    20th century paradigm 45
    adequacy of sensemaking paradigm 18, 46, 130, 153, 156
    and highly dynamic adversaries 16, 18, 25, 127
    and meliorists 2, 3
    and multiframe analysis 63, 103-104
    as activity 35, 50
    as knowledge 35, 50
    as organization 35, 50
    attribute substitution 79
    Cold War paradigm for ix, xi, 1, 4, 45, 47
    core competencies in 8, 49-50
    definition xxxv
    expertise in xvii, xxviii, 26, 49, 66, 69, 73, 76, 79, 81, 89, 92, 129
    flaws in Kent paradigm for xxi, 7, 10, 46, 126, 129, 149
    flaws of "standard model" for 16
    foresight in xvii, xxiii, 16, 30, 33, 35, 57, 81, 83, 98, 100, 125, 149
    hindsight in 99-100
    inadequacy of disaggregative paradigm for xxxv
    Kendall's paradigm for xiii, xxi, 16, 44, 105, 126, 151-152
    Kent's purpose of 44, 149
    lack of evidence in 65, 97, 106
    multiple method triangulation in 104, 106, 116, 127, 130, 133-134
    no standardized doctrine for 103
    old paradigm for xi, 1, 5, 46
    "over" versus "under" estimation in 48
    probing 53, 78, 127

INDEX (Continued)

purpose of 44, 149
replication of results in 97-98
signal and noise in xxiii, 16
skeptics of 2-3
source of xxiii, xxviii, 15, 22, 55, 57-59, 60, 63, 65, 98, 101, 119, 141, 146
standard model for 16, 34, 103
validity of methods in 4, 28, 90, 99, 102-103, 117
Intelligence error
and intelligence failure xxiii, xxv, 12-15, 22, 25, 42, 46-48, 57, 77, 90, 95, 99-100, 103, 146, 152, 153
and paradigm failure xix, 1, 7, 46-47, 153
and poor or missing data 12, 46
caused by selective exposure 11-12, 20, 42, 101
caused by selective perception 11-12, 15, 20, 42, 101
definition 12, 46
Intelligence failure
and inadequate or erroneous hypotheses x, 12, 43, 46, 62, 65, 100
as recurring theme 13
and relation to policy failure 2, 12-15, 26, 44, 46, 48, 65, 153
and relaxation xxv
caused by selective exposure 11-12, 42
caused by selective perception 11-12, 15, 42
definition 12, 16, 46, 48
example of 11-12, 15, 21, 48, 96
explanations of 13
fixation and xxv
Intelligence sensemaking
components 18, 153
definition xxxv, 8-9
planning 5, 8, 53-54, 152, 155
Interpretation
definition 144
Intuition
and expert judgment 69, 73-76, 79
and limits of prediction 70, 76, 79, 90
as automatic thinking 70, 74-75
cognitive processes 73, 75-76, 79
definition 69-70, 79
mental models of 70, 73-74

INDEX (Continued)

J

Judgment
and intuition 69, 73-76, 79
definition 69, 75
heuristic-based 42, 69, 73-76, 79
skill-based 69, 74-76, 79-80
skill-based example of 75, 80, 92
skill-based success in 75-76, 79-80

K

Kendall
and purpose of intelligence 44
Kent
and purpose of intelligence 44, 149
analytic framework of 7, 16, 46, 105
Cold War legacy of 6, 14
intelligence method of 6, 105, 123, 130

L

London subway bombing 64

M

Macrocognition 147, 152, 154-155
anticipation versus prediction 130
definition 129, 155
Marshaling 15, 37, 50-51, 101, 127, 152
definition 62
Mental model 16
definition 72-73
Metacognition and mindfulness xxvi
inverse relationship of xxvi
Microcognition 129-130
definition 130
Mindfulness
acquisition of xxv-xxvii, xxx, 129
and critical thinking xxvi-xxvii, xxix, xxxi, 8, 93, 123, 130-131
and here and now awareness xxviii
and intuitive judgment xxvii, 76, 93, 129

INDEX (Continued)

and meditation xxvi, xxx-xxxi
and sensemaking xxxi, 6, 8, 13, 76, 93, 123, 129-130, 152-154, 156
characteristics of xxv-xxviii, xxx-xxxi, 8
definition xxv-xxviii
example of xxv-xxviii, xxx
IC development of xxxi, 93
means of enhancing xxxi
responsibility of individual for xxvi, xxxi
Mindlessless
and relaxation xxv
definition xxiii
example of xxiii
fixation on xxv
source of xxx
unacceptability of xxv, xxx

N

National Public Radio 11, 72
National Intelligence Council 6, 77, 81, 104, 106, 108, 155
Non-state actor xxi, 47, 49, 105-109, 111, 113-126, 128-130, 138-141, 143-144
Africa examples 108-112, 117-118, 123, 141
and importance of environmental considerations 22, 107, 111, 113, 117-118, 121, 127
definition 106
Iraq examples 107, 111, 119-120, 121, 124, 127
Normal intelligence 11, 37, 44-45, 47-49, 75
and incremental increase of knowledge xxv, 45
definition 45, 75
no revision of paradigm for 22, 45
purpose of 11, 44

P

Pandemic xxxv, 28-33
characterized as wicked problem 28-32
Paradigm shift xxi, 4, 47, 130, 149, 155-156
definition 48-49
reasons for 5, 47, 127

INDEX (Continued)

Planning
as emergent process xxx, 8, 52-53, 152, 155
as flexecution 52-54
as flexible execution 52-53
definition 5, 51
for tame problems 51-52
Points of segmentation 119-121, 123, 129, 130, 144
definition 119-120
Iraq example 121
Policy failure
and Admiral H. Kimmel 13
example of 2, 12, 15, 48, 65
recurrence of 13-14, 48
Prediction
compulsive preoccupation with 44
critique of 44
more interesting than explanation 43
reasons for error in 57, 100
Prospect theory 121
definition 121

R

Rachel North 11, 64
Rigor
and explanation critique 135-145
and hypothesis exploration 131, 135-145
definition xviii, 133
in sensemaking xix, xxi, 8, 104, 106, 124, 131, 134, 137-138, 146-147, 153-154, 156
in information search 134-146
in information synthesis 134-146
in information validation 136-146
metric for determining 133-147
sensitivity analysis and 136-146
specialist collaboration and 136-145
Rigor Metric
assessment of sensemaking 137, 146-147

INDEX (Continued)

S

Scientism 26, 131
Selective exposure 11-12, 20, 42, 101
Selective perception 11-12, 15, 20, 42, 101
Sensemaking
    as macrocognitive activity 129-130, 147, 152, 154-155
    cognition in x, 49-50, 87-88, 99, 129
    components of 153
    definition xxxv, 8-9
    goals of 38, 53, 154
    IARPA's definition of 9, 105, 156
    intuitive trianglation in 127, 134
    role of 5, 63
    use of evidence in 5, 8, 12, 62, 88, 98, 100-102, 125-127, 141
Skill-based judgment
    intelligence success from 74-76
Space-time envelope of indeterminate causality 81-86
    definition 81-83
Sustained-attention failure xxx
Synthesis xxxv, 63-64, 101-102, 104, 131, 134, 136, 139-145, 153, 155
    definition 63

T

Tame problem 17-18, 21, 27-30, 36, 40-41, 51-52, 75, 107, 130
    9/11 attacks as example of 107
    definition 17, 52
Type 1 domain 80, 82, 88-89, 93, 130
    intelligence example of 89
Type 2 domain 80-81, 89
    intelligence example of 89

V

Validation of intelligence 99, 102-103, 136-146, 153
    definition 95
    insufficiency of current paradigm for 103
    insufficiency of hindsight for xvii, 99
    multiple method approach to 103-104, 144
    replication and 98

INDEX (Continued)

W

Wicked problem 17-25, 27-36, 40-41, 51-54, 105-107, 122, 129-130, 133, 144, 152-154
characteristics of 18-19
complexity of 33-36, 154
definition 18-19, 28
goal of sensemaking for 51-53, 154
pandemic as intelligence example of 28-33

COLOPHON

A colophon records the details of the layout and design of a publication. It acknowledges the craftsmanship and artistic sense required for an attractive graphic representation of ideas. Whereas the acknowledgements record the textual assistance an author receives, a colophon records the equally important technical assistance received.

The text of this book was set in Minion Pro, an Adobe Originals typeface designed by Robert Slimbach. It was inspired by classical old-style typefaces of the late Renaissance, a period of elegant, beautiful, and highly readable type designs. Minion Pro exhibits the aesthetic and functional qualities that make text type highly readable, yet is also suitable for display settings. Tables are presented in Neue Helvetica. Helvetica was developed in 1957 by Max Miedinger with Eduard Hoffmann at the Haas'sche Schriftgiesserei (Haas type foundry) of Münchenstein, Switzerland. Haas set out to design a new sans-serif typeface that would compete well in the Swiss market, and be suitable for a wide variety of signage. After further development, the typeface's name was changed by Haas' German parent company to Helvetica (derived from *Confoederatio Helvetica*, the Latin name for Switzerland), to make it more marketable internationally. This Neue Helvetica features a more structurally unified set of heights and widths.

This publication was written on an iMac and a Macbook Pro using Microsoft Word. Typesetting was done using Adobe Systems InDesign. Illustrations were prepared in Omni Systems Omni Graffle and Adobe Photoshop.

Type fonts, as well as iMac, Macbook Pro, Acrobat, InDesign, Omni Graffle, and Photoshop are registered trademarks of their respective companies.

Desktop composition by Joseph Gallagher.

The cover was designed by Bridgette White.

Published by the National Defense Intelligence College Press, March 2011. Printed at the Defense Intelligence Agency, Washington, DC.

This Page Is Intentionally Left Blank

The Applied Critical Thinking Handbook

(Formerly the Red Team Handbook)

A product of the TRADOC G2
Operational Environment Enterprise

7.0

JAN 2015

DISTRIBUTION RESTRICTION

This handbook is approved for public release.
Distribution is unlimited.

Points of Contact

UFMCS http://usacac.army.mil/cac2/UFMCS/index.asp
University of Foreign Military and Cultural Studies
TRISA (TRADOC G2 Intelligence Support Activity)
803 Harrison Drive, Building 467, Room 315
Ft Leavenworth, KS 66027-2308
FAX 913-684-3887
DSN 552

Director 913-684-3860

Operations 913-684-3857

Security 913-684-4336

Technology 913-684-4339

Curriculum 913-684-4321

Instructors 913-684-3892/3959

SMEs 913-684-4323/4338

Librarians 913-785-3001/3081

Enrollment

1. Go to https://www.atrrs.army.mil/atrrscc/search.aspx
2. Select a *Fiscal Year*, i.e., 2015.
3. Select the *School Code*: 159 (UFMCS).
4. Click *Search the ATRRS course catalog* button (near the bottom).
5. Select a *UFMCS* course from the table.

Table of Contents

CHAPTER I: Introduction....1
Why Red Teaming?....1
What is Red Teaming?....2
How is Red Teaming Conducted?....4
How is a UFMCS Education Unique?....5
Why this Red Teaming Handbook?....7
Summary....8
Endnotes....8
CHAPTER II: Self-Awareness....9
What is Self-Awareness?....9
Who Am I?....10
Journaling Daily....15
Interpersonal Communication....16
Personality Temperaments....18
Summary....21
Endnotes....21
CHAPTER III: Fostering Cultural Empathy....22
Cultural Awareness....23
Ethnocentrism....24
Some Cultural Frameworks....27
Functional Systems Approach....32
Cultural Relevance....37
Summary....38
Endnotes....41
CHAPTER IV: Critical Thinking....43
Introduction....43
What Do Critical Thinkers Do?....43
Why is Critical Thinking Necessary?....47
Summary....55
Endnotes....56

CHAPTER V: Groupthink Mitigation & Decision Support 57
Groupthink.....57
Groupthink Mitigation 59
Military Decision Making Process.....62
Mitigating Groupthink during the MDMP.....62
Red Teaming During Planning 64
Red Teaming During Problem Framing.....65
Red Teaming During Operational Design.....71
Summary.....73
Endnotes 73
CHAPTER VI: Red Teaming TTP.....74
1-2-4-Whole Group 74
1 on 1, 2 on 2, Exchange Emissaries.....76
4 Ways of Seeing.....77
5 Whys.....78
5 Will Get You 25.....79
6 Empathetic Questions.....80
6 Words 80
Alternative Futures Analysis.....81
Analysis of Competing Hypotheses (ACH) 84
Argument Deconstruction 87
BATNA.....89
Brainstorming.....90
Challenges to Effective Planning 93
Circle of Voices.....104
Circular Response 105
Cognitive Biases 106
Common Logic Fallacies.....108
Critical MDMP Questions 110
Critical Review Steps.....112
Critical Thinking Traits 113

Critical Variables (CVs) 116
Cultural Perception Framework 123
Deception Detection 142
Determining the Suitability of an Analogy 144
Devil's Advocacy 146
Divergence - Convergence 148
Dot Voting 149
Fishbowl 150
Frame Audit 151
High-Impact/ Low-Probability Analysis 153
Indicators or Signposts of Change 155
Key Assumption Check 157
Liberating Structures 159
Mitigating Groupthink 160
My 15% 162
Onion Model 163
Outside-In Thinking 165
Premortem Analysis 167
Problem Restatement 170
Quality of Information Check 172
Red Team Analysis 174
Red Teaming – Assessment Questions 177
Red Teaming – Assumption Questions 178
Red Teaming – Key Questions 180
Red Teaming – MDMP Actions 181
Shifting the Burden 186
Stakeholder Mapping 188
Strategies for Structured Analysis 193
String of Pearls 195
S-W-O-T Analysis 206
Team A / Team B Analysis 207

Telling Stories 209
TRIZ 210
Troika Consulting (Ad Agency) 211
Validating Assumptions 212
What if? Analysis 224
Why Assess? 226
Endnotes 229
Bibliography 233
Abbreviations 238
Index 240
My Notes 241

CHAPTER I: Introduction

"We need to help our commanders and staffs escape the gravitational pull of Western military thought."

-- CSA Peter Schoomaker[1]

Why Red Teaming?

The premise of the program at the University of Foreign Military and Cultural Studies (UFMCS) is that people and organizations court failure in predictable ways, that they do so by degrees, almost imperceptibly, and that they do so according to their mindsets, biases, and experience, which are formed in large part by their own culture and context. The sources of these failures are simple, observable, and lamentably, often repeated. They are also preventable, and that is the point of 'red teaming'.

Our methods and education involve more than Socratic discussion and brainstorming. We believe that good decision processes are essential to good outcomes. To that end, our curriculum is rich in divergent processes, red teaming tools, and liberating structures, all aimed at decision support.

We educate people to develop a disposition of curiosity, and help them become aware of biases and behavior that prevent them from real positive change in the ways they seek solutions and engage others.

We borrow techniques, methods, frameworks, concepts, and best practices from several sources and disciplines to create an education, and practical applications, that we find to be the best safeguard against individual and organizational tendencies toward biases, errors in cognition, and groupthink.

Red teaming is diagnostic, preventative, and corrective; yet it is neither predictive or a solution. Our goal is to be better prepared and less surprised in dealing with complexity.

What is Red Teaming?

Red teaming is a function that provides commanders an independent capability to fully explore alternatives in plans, operations, concepts, organizations and capabilities in the context of the operational environment (OE) and from the perspectives of partners, adversaries and others.

A Red Team performs three general types of tasks:

- Support to operations, planning, and decision support
- Critical review and analysis of already-existing plans
- Intelligence support (Threat Emulation)

(UFMCS provides education for the first two tasks; TRADOC's Intelligence School and Center provides education on the third.)

In order for a Red Team to effectively contribute to decision making all of the following elements are required:

- The ability to think critically about the problem. While this may seem obvious, the reality is that critical thinking is a skill set that requires training, education and tools. The Army assimilates people from different backgrounds across the nation. One of the drawbacks of that assimilation is our military tendency to reflect the same biases and perspectives. We pride ourselves in common values—which while ingrained in the Army culture are not universal outside of that culture.
- Thinking critically and challenging the group is an unnatural act for military staffs. Doing so effectively requires tools and methods that enable leaders to see different perspectives.
- Red Teams require top cover to be allowed to challenge the conventional wisdom and the organization's leaders. No matter the quality of the Red Team or the methods they employ, dictatorial or toxic leaders are incompatible with successful red teaming.

- Red teaming is not easy, and not everyone can do it. Red Teamers must be effective written and oral communicators. They must have credibility in the area in which they are providing red teaming insights. They must be able to constructively challenge the plan. This means focusing on what is truly important, able to explain why it is being challenged and offering some alternative ways to think about the problem. Constituting a Red Team with those the organization 'can afford to give up' is a sure recipe for failure.
- There is no given template for a red teaming approach to a problem, no "one size fits all." Red teaming activity must be tailored to specific requirements. Time available is a critical factor, as is expertise with the issue at hand, the makeup of the team, engaged leaders and their predisposition to provide too much input, etc.

A Red Team works best behind the scenes, assisting the commander and staff in a non-critical, helpful manner, without taking credit. (It is hard enough to accept someone criticizing your thinking—it is much tougher if they are obnoxious and loud about it.)

While there is no formula for red teaming, there are some common activities that most Red Teams do most of the time. These include challenging facts and explicit assumptions, looking for implicit (unstated) assumptions, identifying cultural assumptions and developing targeted cultural questions for subject matter experts (SMEs), challenging the problem frame (and proposing alternative frames), identifying cognitive biases and symptoms of underlying groupthink, etc. All of these activities lead to the development of alternative perspectives.

How is Red Teaming Conducted?

Not everyone should practice medicine. Scalpels, drugs, and the procedures in which they are used are not to be trusted to those with a passing familiarity of their application. Everyone should have a basic knowledge of how to maintain their health and wellness (basic elements of diet, exercise, sleep). Red teaming is like medicine. Medicine is diagnostic, preventative, and corrective. It works best when applied in small applications over time. And so it is with red teaming. Everyone needs medicine at one time or another. Not everyone needs the same dose. You want a well-trained Red Team for the same reasons you want a well-trained physician. As with your relation with your physician, monitoring and periodic checkups are preferable to intervention. What does your unit need… intervention, prevention, triage, a second opinion, or a dose of common sense? The applications for red teaming are dependent on the needs of the unit. The following are some important questions to consider when practicing red teaming. Some have definite answers; some answers are dependent on context and the needs of the unit:

- What does a Red Team look like? (Ad hoc, standing team, an individual, or an on-call team)?
- What does it do? (Challenges assumptions, tests hypotheses, explores alternatives, and heightens awareness).
- Who are the best people to do it? (Rank and education are not exclusive discriminators. You want reflective, critical thinking persons with a curious disposition.)
- When is it done? (Continuous, on call, in planning, or when things are going poorly)?
- To whom does the Red Team belong? (Optimally, to the commander, though they may work directly for the Chief of Staff.)
- Where in planning does red teaming belong? (Everywhere.)

How is a UFMCS Education Unique?

Our approach has proven effective in units and organizations from brigades to the Joint Staff. UFMCS' curriculum is designed to improve critical thinking, and proceeds from a premise that before you point out to someone the errors of their thinking, you had better understand your own.

Most of us are disinclined to naturally challenge prevailing thoughts. We challenge students to examine things they hold sacrosanct. We expose them to the ethnocentrism of their own thinking, their overreliance on method, their tendency to default to Western/Aristotelian logic, their lack of appreciation for the frames that subconsciously capture their thinking, their failure to avoid common cognitive biases, and their predisposition to seek consensus while exhibiting classic symptoms of groupthink.

UFMCS' curriculum revolves around some fundamental questions:

- What does it mean to be "self-aware?"
- When I perceive and interpret information, what are those interpretations based upon?
- What do I value and believe? Why? How do these values and beliefs motivate my behavior? How do others' values and beliefs motivate their behaviors *differently*?
- How can cultural anthropology help me think about another culture without resorting to mirror imaging?
- How do I improve my ability to think critically?

UFMCS' curriculum is organized around the following major areas, designed to improve a soldier's ability to think and understand in new and continually evolving environments:

Self-Awareness: Understanding how our values and beliefs affect how we think and decide … and how that differs for others. Major sub-elements:

- Personal reflection, Jungian typology, Personality Dimensions, Thomas-Kilmann conflict mode instruments, etc.
- Watershed event story telling
- Daily Journaling

Groupthink Mitigation & Decision Support: The challenges inherent in hierarchical environments and elite teams—groups which might value maintaining social relationships more than making a tough decision.

- Use of fungible, small group techniques to mitigate groupthink: use of anonymous feedback, liberating structures, etc.
- How to connect critical thinking to operational design, problem framing, assumption validation, assessment tools, and MDMP.

Critical Thinking: Support for planning and decision making - deconstructing arguments, examining analogies, challenging assumptions, and exploring alternatives.

- The role of intuition—System 1 versus System 2 thinking.
- Numerous tools to examine a plan through different lenses—*Premortem Analysis*, *Stakeholder Mapping*.
- Thinking meta-cognitively, and enabling graduates to understand how humans think, and how culture shapes thoughts.

Fostering Cultural Empathy: Developing better questions about culture, in order to facilitate strategic and operational decision making which is informed by cultural empathy.

- Culture examined from the perspective of a cultural anthropologist, versus “dos and don’ts.”

- Conscious examination of the roles of ethnocentrism, versus cultural relativism.
- Culturally-centric case studies.
- Tools to help understand foreign cultural contexts, and to foster empathy.

Our intent is to inculcate behaviors designed to make critical thinking a discipline. The outcome of this process is a student with a bundle of cognitive capabilities—at the heart of which is a better ability to apply one's normal thought processes and their common sense, to the circumstances of a given situation.

Why this Red Teaming Handbook?

The purpose of this Red Teaming Handbook is to provide an aide memoir for UFMCS graduates, and an introduction to the concepts for those unfamiliar with red teaming. This handbook is not a checklist of actions or tasks, but rather serves as a compendium of key ideas and information taught in the UFMCS curriculum to help facilitate practical red teaming. The contents of this handbook are neither doctrine nor the "school solution."

This handbook represents the essence of what students study at UFMCS. It provides an overview in the four major educational areas of the red teaming program as described earlier in this introduction. Each chapter points the user to tools and methods in Chapter VI for use when confronting challenges associated with: Self Awareness and Reflection, Groupthink Mitigation and Decision Making, Critical Thinking, or Fostering Cultural Empathy.

This handbook is a living, UNCLASSIFIED document. We welcome your comments, suggestions, and input. Time and personal preference of different facilitators may result in some of these ideas or tools being new to you despite having attended the program. As you go through this handbook, if you see things you were not exposed to in class, please engage our faculty.

Summary

People and organizations court failure in predictable ways, by degrees, almost imperceptibly, and according to their own culture and context. As a countermeasure, we can fully explore alternatives in that context and from differing perspectives. We call this function *red teaming*.

Red teaming requires challenging the facts, problem frame, and assumptions. This function also seeks to qualify the assumptions, develop targeted cultural questions, and propose alternative perspectives, as well as identify any cognitive biases, groupthink mitigations, etc.

To that end, organizations can utilize individuals taught to execute red teaming, or charter an empowered *Red Team* (standing, ad hoc, or on-call). Either way, red teaming has worked best behind the scene.

UFMCS offers a unique red teaming education. The curricula is designed to challenge one's view of the surrounding world and self. The school creates an experience built upon: self-awareness, cultural awareness, critical thinking, groupthink mitigation, decision support, and practical experiences with red teaming tools.

Endnotes

[1] Conversation CSA Schoomaker, Greg Fontenot and Steve Rotkoff, Spring 2006.

CHAPTER II: Self-Awareness

Everything that irritates us about others can lead us to an understanding of ourselves. **-- *Carl Jung***[1]

Most of the shadows of life are caused by standing in our own sunshine. **-- *Ralph Waldo Emerson***[2]

The unexamined life isn't worth living. **-- *Socrates***[3]

What is Self-Awareness?

Everyday life is a flurry of activity that demands our attention. From training and deployment schedules, to children and home life responsibilities, we are always on the go. As a result, we have little time for self-awareness and personal development. The process of improving self-awareness via introspection happens when we take a dedicated look inward and examine our own thoughts, feelings, and motives. But, who has the time to do that?

Self-awareness is the capacity for introspection and the ability to recognize oneself as an individual separate from the environment and other individuals.

Why is Self-Awareness Important?

The self-aware person is more enabled as a critical thinker, more aware of personal biases and recognizes his or her own cultural framework. It is with this understanding of self that an expanded world view opens—one that is more empathetic to the differences of other cultures and ways of thinking and thus primed to engage as a Red Teamer.

UFMCS focuses on four areas to develop Self-awareness:

1. Study of Temperament, Personality Dimensions® Instrument and Model, Introversion and Extraversion
2. Study of Interpersonal Communications
3. Introspection Exercise—Who Am I?
4. Daily Journaling Exercise

People are complex and diverse. A self-aware person has dedicated introspective time to acknowledge personality traits, personal values, habits, psychological needs and emotions that drive behaviors.

Personality - An understanding of your personality can help create awareness of strengths and weaknesses, talents, motives, stressors and motivators for decision making and interpersonal communications.

Values - It's important that we each know and focus on our personal values. In doing so, we are more likely to accomplish what we consider most important.

Habits - Our habits are the behaviors that we repeat routinely and often automatically.

Needs - Our needs cause motivation; and when needs aren't satisfied, they can cause frustration, conflict and stress.

Emotions - recognizing your own feelings, what causes them, and how they impact your thoughts and actions is emotional self-awareness.

Who Am I?

The *Who Am I* exercise requires reflection and introspection of your personal family narratives and dynamics, regional culture, religion, educational experiences, and critical watershed moments that shape your worldviews and values—that all put together construct an idea of who you are as an individual. In its whole, the exercise enhances the individual's self-awareness while at the same time creates cohesion and relationship bonding within the participating group.

There are two critical elements to the exercise: private preparation through solo reflection and introspection, and group sharing and storytelling.

1. Individuals first must do the hard work of reflection, of recalling the seminal life events that were critical in shaping their personalities and deeper values. One might

think of these events as crucibles, both difficult and triumphant, that forged the individual's character. In essence, this private preparation is intended to encourage introspection. Such deep reflection takes time, and must be built into the structure of the entire exercise.

What exactly participants choose to share with their classmates in the verbal portion is a different question. It is important during preparation that participants be completely honest with themselves as to how they developed into the person they are today. This preparation can take an hour or longer, and is ideally conducted at least one day prior to the group sharing.

2. In the second step, the group sits together in a private setting, and one by one the individuals hold the floor, sharing aloud their story. Participants should take as long as they want, uninterrupted while providing their story. This enables a degree of rambling which intentionally creates an environment where many people end up sharing more than they originally planned. This open time frame can be very liberating, as for many this is the first opportunity they have ever had to share aloud with others why they are who they are.
3. As such, any interruptions in the form of questions or time limits tend to kill the magic of the moment. To mitigate the abuse of this open ended opportunity to talk, facilitators are encouraged to get their story down under 15 minutes, as this then sets an example that most others will naturally follow. The story should be conducted entirely as narrative—no power point slides or film clips etc.—nothing to distract from the story each person is telling the group, and nothing to hide behind. This activity should be like telling stories around the campfire—but the story we tell is about ourselves.
4. There is no question and answer period following the story so as to avoid any semblance of an 'interrogation', and also to keep the playing field even, (i.e., if the

facilitator were to ask one participant three questions and another only one, it might leave the impression that the first participant‘s story was more interesting, etc.)

5. Every member of the group who is not sharing is asked to practice ‘full-body’ listening by giving their complete and unfettered attention to the person speaking. Receiving this attention while sharing is extremely powerful and the facilitator can both model this and suggest that participants give the kind of attention you yourself would want to receive.
6. Every participant must provide a narrative, but the order of presentation is purely voluntary, an important factor in creating safety. While every participant must share something, precisely how much to reveal about themselves is an individual decision. In this way, the exercise entails individually manageable personal risk.
7. No more than three personal narratives are conducted in a row. If someone goes exceedingly long this may be shortened to two or even simply one. In order for the group to exercise ‘full-body’ listening and remain engaged, the entire group ‘who am I’ must be spaced out over time. Done right, the story is often draining both for the listeners and the presenters. Each hour of stories should be broken up with an hour or more of some other less emotionally investing activity.
8. It is highly recommended that the facilitator models their own story before the participants commence their solo reflection. What the facilitator shares will set the tone for what the participants share. Facilitators are urged to go out on a limb and reveal meaningful events in their life that genuinely shaped them as people. By taking action and modeling this openness first, the facilitator encourages participants to risk being personally vulnerable themselves.
9. From past experience, several participants have initially told the group that they had felt they did not know

everyone well enough to completely share who they are and everything they had learned about themselves in preparing for the exercise. In most cases, they came forward later and decided to redo their story on their own initiative—sharing things they had learned through introspection but needed time to process. This methodology allows people to operate within their comfort zone while simultaneously establishing a group norm that encourages them to both reflect and share.

10. By now, it should be clear that this exercise is definitely NOT a normal biographical recitation. Positions held, size and composition of family, etc. are not important unless they are linked to some watershed event. In an Army context, when someone commanded a company or held some other position of importance is not relevant UNLESS some critical event happened while in that position that has stayed with, and continues to shape their daily outlook. Similarly, while the birth of a child is without question a significant event in anyone's life, it may or may not necessarily change your worldview about things like the nature of personal responsibility, values, etc. Hence participants are ideally sharing events that were personally transformational on a fundamental level.
11. Finally, and most importantly, this all requires a degree of confidentiality among the group. While not confession or protected speech, it is critical that if someone chooses to share personal vulnerabilities (e.g., current struggles at home or difficult events from the past) that this content does not become fodder for gossip. To gain buy-in on this, the facilitator should openly propose confidentiality as a group norm, and foster a brief discussion about what this means. A good rule of thumb is —what happens in 'Who Am I', stays in 'Who Am I'.

Outcomes of Introspection

'Who Am I' is a deceptively simple exercise that works on many personal and emotional levels simultaneously. Several outcomes are enumerated below:

1. Using introspection to better understand how one engages the world, allows participants to view themselves in profound ways at depths rarely encouraged in the Army. Results may be scary for those unlocking doors in their head that may have long been closed, but it universally produces a better self-understanding.
2. When participants share their story, and listen as others share their own, it invariably dawns on them that they are not alone in coping with problems in life such as grief, prejudice, disappointment, relationship issues, etc. This leaves participants feeling significantly more connected with the group and less alone in the world.
3. Practicing active listening is not something we routinely do or reward in leader development. In fact, in some cases people are penalized for not contributing in volume to class discussions. This creates an environment where we reward the loudest who frequently crowd out and undermine efforts at collaboration. This exercise reinforces active listening and more importantly it reinforces listening for a deeper understanding of what they mean. This understanding promotes a connection on an emotional level. This is an exceedingly important skill for leaders to develop. Organizations where leaders and those led are emotionally connected have higher morale, are more committed to the mission, can better discern intent in the absence of explicit orders, and are more adaptable in extreme circumstances.
4. This exercise creates an environment where alternative perspectives can be valued. When a participant hears another tell a personal story about encountering direct prejudice and how that shaped them, they are less likely to think of that participant as simply 'hypersensitive.'

They understand *where* that person is coming from and *why* they see the world as they do—elements foundational to actual communication and education.

5. Finally, this is a tremendous team building vehicle. Upon completion, each member of the group knows all other members in a deeper way, faster than such knowledge normally develops. Often group members express that they now know other participants better than long time neighbors or even some members of their own family.

Journaling Daily

UFMCS requires students to journal daily, reflect on events and information. This layer of personal consciousness is seldom explored in the normal course of a day; paramount to critical thinking habits. Through introspective time with personal thoughts and feelings, this writing process induces the reflection on, and synthesis of, concepts as well as the subsequent application to one's own life experiences.

Journals are not intended to be simple regurgitations of the day's events. Entries should reflect a deeper and more considered review of the day's topics as well as down other paths those considerations lead. The act of journaling often leads the person writing the journal to examine their beliefs, attitudes, and values beyond what was discussed in class.

While students are required to turn in their journals, it is important to remember that the act of keeping a journal is designed to provide a vehicle for reflection for the individual writing them. Entries are not be looked on as graded writing. Bottom-line, they are designed for the writer not the reader.

Prompting questions:

- What have I learned about myself?
- What have I learned about my emotional responses?
- What learning topics or tasks did I respond to most easily/ with most difficulty?
- What do I feel proudest about/ most dissatisfied about regarding my personal growth?

Interpersonal Communication

Interpersonal communication is the face to face exchange between two or more persons that conveys ideas, emotions, and information; what is said and what is received verbally and nonverbally via body language and facial expressions. Personal objectives are one of the many driving forces underlying interpersonal communication.

- Interpersonal communication involves the use of semiotics which includes verbal and non-verbal representations of ideas, emotions, or events.
- Interpersonal communication occurs between people who are themselves developing and changing.
- Ethics, the use of moral principles to guide action, are part of interpersonal communication.
- Interpersonal communication can be strategic.
- Consider how one's communication affects others.
- To achieve their goals, communicators must be competent, meaning both appropriate and effective.

The many benefits of effective interpersonal communication include personal and professional success, more satisfying relationships, and goal achievement.

Strategic Questioning: seeking information to facilitate choices or open a space for new ways of thinking about a problem. It is open and closed questions, not a statement in the form of a question.

When to do it:

- Your professional role demands it
- As part of Critical Thinking
- You are confused about the purpose of the interaction
- You are problem-solving

How to do it:

- Use active listening
- Weigh they are saying against your goals
- Ask clarifying questions and offer paraphrases
- Stay open to new discoveries

Strategic Listening": listening to shape the outcome and help you accomplish your ends; measured later, by whether you gain information or improve the relationship. It considers when to use open and closed questioning, not stating the form of a question.

When to do it:

- Your professional role demands it
- As part of Critical Thinking
- You are confused about the purpose of the interaction
- You are problem-solving

How to do it:

- Use active listening
- Weigh they are saying against your goals
- Ask clarifying questions and offer paraphrases
- Stay open to new discoveries

Active Listening**":** listening to foster social relationships. This is measured at the time by how well you show your interest. It shows respect and involvement. Its absence can show lack of interest and dismissal.

When to do it:

- When the relationship matters
- As part of strategic listening

How to do it:

- Keep your eyes on the other's face
- Show emotional reaction but don't interrupt
- Echo parts of what they are saying

Empathic Listening": listening in support of emotions, demonstrating care and involvement. In the moment it helps the person feel understood and supported. Its absence can show impatience, disinterest, or dismissal.

When to do it:

- When you can be sincere
- When you truly understand or want to understand how your counterpart feels

- When you want to defuse strong emotions

How to do it:

- Show emotional reaction but don't interrupt; murmur
- Use indirect questions to echo parts of what they say
- Keep your eyes on the other's face
- Comment on their emotions

Personality Temperaments

Interpersonal Conflict

An awareness of others' temperaments can be quite helpful when conflict arises. Acknowledging the similarities and differences between the four temperaments allows for bridging strategies to be developed. In other words, courses of action that take into account each temperament's needs, motivators, and skills to form a more mutually beneficial outcome to manage the conflict.

Learning the four temperaments and examining your own personal patterns (dominant to least used) helps to frame your own personal needs, values, inter-personal stressors, and biases. An understanding your own and observing the patterns of others you work and live with allows you to:

- Influence and persuade others in a positive manner.
- Acknowledge your talents and those of others.
- Improve interpersonal communication.
- Identify potential problems early.
- Support and encourage others.
- Narrow gaps and differences.
- Improve team performance.
- Negotiate more effectively.
- Organize efficient teams.
- Increase productivity.
- Elevate morale.

Temperament

Temperament is defined as a pattern of observable personality traits, such as habits of communication, patterns of action, and sets of characteristic attitudes, values, and talents. It also encompasses personal needs, the kinds of contributions that individuals make in the workplace, and the roles they play in society. In essence, the study of temperament describes the 'why' of our behaviors, motivators and sources of stress.

Historically, theorists have identified four unique patterns of individual tendencies, values, and needs. These patterns were not arbitrary collections of characteristics, but sprang from an interaction between basic dimensions of human behavior: our communication and our action, our words and our deeds, or, simply, *what we say* and *what we do*.

Personality Dimensions® is a human relations and communications model rooted in Jungian typology and temperament theory that creates a common language for understanding self and others. The model examines four temperaments with innate psychological needs, values, talents, and behaviors.

Personality Dimensions®	**Core Needs**	**Values**
Inquiring Green	knowledge, competence, mastery, & self-control	scientific inquiry, concepts, theories, & logical consistency
Authentic Blue	finding significance, meaning, & unique identity	harmony, cooperation, ethics, & authentic relationships
Organized Gold	membership, belonging, responsibility and duty	stability, security, procedures, and group preservation
Resourceful Orange	freedom to act in the moment; make an impact, & expediency	variety, adventure, excitement, and performance with skill

Introversion and extraversion were first popularized by Carl Jung. This concept frames a continuum of traits with discernible differences or identifiers for preferences on the extraversion ↔ introversion continuum. Regardless of where one may naturally fall on the continuum, most will develop skills to effectively augment behaviors along the entire continuum to fulfill core needs and motivations.

Those who prefer ***introversion*** will often:

- Do their best thinking, learning, and decision making through quiet reflection and individual contemplation.
- Seek stimulation from within and direct their energies inward in reflection.
- Prefer to inwardly think things through before sharing any of their thoughts.

Those who prefer ***extraversion*** will often:

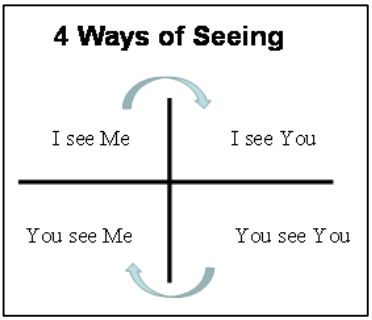
- Discuss thoughts out loud as a method to process information and make decisions.
- Seek stimulation from external sources and direct their energies outward.
- Prefer brainstorming out loud to get their creative juices flowing.

Linda Berens, *Understanding Yourself and Others*, also addresses the *core self*, the predisposition with which we are born. The *developed self*; the skills and behaviors we learn as we grow and mature; and the *contextual self*, how we prefer to react to a given situation. Berens claims that, given our "core self" and our "developed self", we are able to behave and react in a variety of ways in different situations or contexts. She states that we have the choice of: giving in to our core self, or following our developed self, or selecting an appropriate contextual response.

Summary

Self-Awareness and time introspecting is a fundamental element of the red teaming education. Self-awareness includes acknowledging that each of us come with differing values, behaviors, beliefs, personal stories, motivations and goals. Self-awareness enables the Red Teamer to improve their own: interpersonal communication, critical thinking, empathy for others, and cohesion within the group.

An understanding of individual temperament patterns and *introversion ↔ extraversion* confirms how we see ourselves (what we say and what we do) may be quite different from how others perceive what we say and what we do, and vice versa.



Endnotes

[1] C.G. Jung, *Memories, Dreams, Reflections,* (New York: Pantheon Books, 1963), 247.

[2] "Wisdom Quotes." Ralph Waldo Emerson Quote: "Most of the Shadows Of..." January 1, 2014. Accessed November 24, 2014. http://www.wisdomquotes.com/quote/ralph-waldo-emerson-162.html.

[3] While this saying is attributed to Socrates, it was captured in Plato's *Apology*. Benjamin Jowett, *Six Great Dialogues,* (Mineola, N.Y.: Dover Publications, 2007), 18.

CHAPTER III: Fostering Cultural Empathy

"I don't think we should study things in isolation. I don't think a geographer is going to master anything, or an anthropologist is going to master anything, or a historian is going to master anything. I think it's a broad-based knowledge in all these areas, the ability to dissect a culture or an environment very carefully and know what questions to ask, although you might not be an expert in that culture, and to be able to pull it all together. Again, an intelligence analysis that isn't an order-of-battle, militarily oriented one, but one that pulls these factors together that you need to understand…"I mean, as simple as flora and fauna all the way up to basic geographic differences, environmental differences – cultural, religious and everything else. That becomes your life as a planner, or as the director of operations, and as the key decision maker."

-- General Anthony Zinni, 1998[1]

This chapter is about developing better questions concerning culture, in order to facilitate planning, policy making, and strategic and operational decision making which is informed by cultural empathy and enhanced by red teaming tools and a functional systems approach. Red teaming methods and tools prevent us from accepting easy answers to hard questions about culture and its complexity. The functional systems approach enhances our ability to translate the abstractions and nuances of culture into doctrinal, operational terms. To that end, we emphasize the following in our approach to the red teaming method of cultural examination:

- Conscious examination of the roles of ethnocentrism vice cultural relativism
- Culturally centric case studies
- Tools to foster empathy

"Cultural analysis is intrinsically incomplete. And, worse than that, the more deeply it goes the less complete it is. It is a strange science whose most telling assertions are its most tremulously based, in which to get somewhere with the matter

> *at hand is to intensify the suspicion, both your own and that of others, that you are not quite getting it right. But that, along with plaguing subtle people with obtuse questions, is what being an ethnographer is like."*
>
> ***-- Anthropologist Clifford Geertz, 1973***[2]

Cultural Awareness

In the above passage from *The Interpretation of Cultures,* Clifford Geertz was describing what it is like to be an ethnographer, but he may just as well have been describing a Red Team tasked with cultural analysis. A curious, skeptical disposition, rather than one of certainty befits the Red Teamer. For the Red Teamer, awareness means the discovery that there is no "normal" position in cultural matters.[3]

For the Red Teamer, culture may be best approached with techniques borrowed from the perspective of a cultural anthropologist instead of a prescriptive framework or list of 'dos and don'ts'; in other words, there is value in passively regarding what *is*. However, "Anthropology, or at least interpretive anthropology, is a science whose progress is marked less by a perfection of consensus than by a refinement of debate. What gets better is the precision with which we vex each other."[4] This will not do. What is needed is a systemic approach to culture the outcome of which is designed to enhance military planning.

To observe dispassionately is the role of the ethnographer, but not necessarily the role of the military commander or Red Teamer. Their role is to decide what to "do," based on their observation and analysis.

Cultural awareness is not the same thing as cultural sensitivity. The idea is not to escape or discard our own deeply held values, beliefs, and ideals, or to practice cultural relativism, but to better understand the distinctions and similarities between our own and those held by others (both adversaries and allies) for the purpose of avoiding missteps in planning and policy formulation. Our methods and

outcomes as military planners differ from those of the ethnographer or anthropologist in that our task is not only to observe, but also to plan and act upon our analysis.

With that in mind, keep this caution in mind as you read this chapter and as you begin on any cultural examination: when we analyze another culture we must do so with full consciousness that our vantage point lies outside of it. Moreover, the things we see are the things we most often attempt to manipulate. These things are the superficial edifices of culture. Real wisdom here is to allow for the deep, unalterable foundations of culture, not to reconstruct it in the manner we desire.[5]

Ethnocentrism

One aim of the red teaming cultural methodology is the reduction of blind ethnocentrism. Ethnocentrism, the belief that *one's own culture is inherently superior to other cultures* is a natural tendency of most individuals[6] (Haight, 1990). This is a problem in planning when the planner is so bound by their own culture as to be "blind to the ability to see the world through the eyes of another national or ethnic group."[7] Negative or distorted stereotypes too, are a challenge to complete cultural understanding as well. Stereotypes by themselves are not negative. At issue here is whether they are accurate or distorted. Distorted stereotypes are polarized, simplistic, and self-serving. Race and ethnicity are common characteristics that are historically susceptible to distorted stereotypes.

> *"Stereotyping is a process by which individuals are viewed as members of groups and the information that we have stored in our minds about the group is ascribed to the individual"*
>
> ***-- Behavioral Scientist Taylor H. Cox, 1994***[8]

Often we tend toward oversimplification of cultural complexity in matters of planning. Our natural inclination is to construct simplified models of a complex reality in order to explain things. We develop simplified explanations based upon selected cultural aspects of the OE that facilitate our

planning and desired end states. The tendency is to regard culture as a block, a category with geographic or ethnic boundaries, and not as the people, the individuals that make up what is the human domain. For example, a simple answer to the question “Where is Mexico?” might be one that explains geographical boundaries, as on a political map. A more insightful answer is “It’s where Mexicans are,” or where Mexican food is, where “Mexican” Spanish language is spoken, or wherever Cinco de Mayo is celebrated, by whomever and for whatever reason. Cultures have social and psychological as well as geographical contexts. Culture’s complexity is illustrated by the hundreds or perhaps even thousands of culturally learned identities, affiliations, and roles we each assume at one time or another. “Complexity involves the identification of multiple perspectives within and between individuals.”[9] Multiple and alternative perspectives, better questions, and thinking more “complexly” is the aim of the red teaming approach to culture.

To that end, we adopt the position that the study of culture is “not an experimental science in search of law but an interpretive one in search of meaning.”[10] There are several challenges to forming an interpretive approach to culture, but that is our aim. We seek an explanation that accounts for the occurrence of certain phenomena in culture, in a place, at a certain time, for a certain group, for the purpose of planning, policy formulation, and decision support.

Challenges to interpreting culture

- To choose apperceptive (conscious perception with full awareness) frameworks that are sufficiently rigorous without being reductive.
- What cultural skills should a Red Teamer have?
- How are these skills best introduced in our practice?
- The most important aspects of multicultural awareness may be learned but cannot be taught.[11]

- Good training can create favorable conditions for multicultural awareness to occur and provide the necessary knowledge and skills
- What is "good" training for Red Teams?

> *"It is difficult to know the cultures of others until and unless you have an awareness of your own culturally learned assumptions as they control your life"*
>
> ***-- Psychologists Mary Connerley and Paul Pedersen, 2005***[12]

When seeking to interpret, understand, or analyze a culture, nothing is more essential than to realize the extent to which the interpretation is uniquely our own, with all the inherent and inescapable biases and ethnocentricity that comes with it. While we cannot completely escape our culturally learned ethnocentricity, there are tools, methods, and frameworks we employ to give us greater awareness of it and how it shapes our thinking and decision making.

There are hundreds of definitions of culture. Some are broad, general, and inclusive, while others are specific to the interest of the practitioner (ethnographer, social scientist, psychologist, warfighter, etc.).

Some definitions:

- "Whatever it is one has to know or believe in order to operate in a manner acceptable to its members."[13]
- "The webs of significance designed by men for themselves."[14]
- "The collective programming of the mind that distinguishes the members of one group or category of people from another."[15]
- Operational Culture: Those aspects of culture that influence the outcome of a military operation; conversely, the military actions that influence the culture of an area of operations (AO)."[16]
- "A theory on the way in which a group of people in fact behave."[17]

The key point to remember is *it is all theory until you get there*.

Culture…

- Is learned.
- Is shared.
- Changes over time.
- Is not always rational to outsiders.

There are several frameworks that attempt to capture aspects of culture for the purpose of studying them. These are broad frameworks that lay out major categories of cultural differences.

Differences of the various approaches relate directly to the purpose of the research. Cultural frameworks do not explain everything, but they still explain something, and our attention should be focused on isolating what that something is with regard to military planning.

There is no ideal framework or best way to classify a culture. Moreover, frameworks should not supplant a straightforward explanation. The Red Teamer should understand that classifications and categories often only serve to provide a simplified basis for analysis. Opting for one categorization or framework over another not only determines the kind of questions we may ask, but may obscure other important questions that should be asked. For this reason, the Red Teamer should employ several frameworks or cultural "lenses" (like *4-Ways of Seeing*, p. 76) when conducting cultural analysis.

The Red Teamer views frameworks (including PMESII-PT as diagnostic tools, not by themselves explanations for the way things are.

Some Cultural Frameworks

While PMESII (Political, Military, Economic, Social, Information, Infrastructure) is the most frequently used method of organizing militarily-relevant knowledge about a place it is not the only valid framework nor is it complete in

and of itself. Graduates are encouraged to ask themselves the question 'What is missing in an exclusively PMESII analysis…does it cover the WILL of the people in question, does it address how they view TIME either historically or day to day etc. Frameworks of all kinds are diagnostic tools not explanations for the way things really are in the society.

<table>
<tr><td colspan="2">Kluckholn's Six Age-Old Dimensions of Culture:
• The nature of people, good or bad?
• The relationship between people and nature, Harmony or subjugation?
• The relationship of people, individualism or Group?
• The primary mode of activity, Being or Acting?
• Conception of space, private or public?
• Time orientation, past, present or future?</td></tr>
<tr><td colspan="2">Nesbitt on Cognitive Differences:
• Patterns of attention and perception
• Assumptions about the composition of the world
• Beliefs on controllability of the environment
• Assumptions about stability and change
• Preferred patterns of explanation of events
• Habits of organizing the world
• Use of formal logic rules
• Application of dialectical approaches</td></tr>
<tr><td colspan="2">Hall on Communication Patterns:
• Context, what must be explicitly stated?
• Space, how much personal space is necessary?
• Time, monochromic (events occur one at a time) or polychromic (simultaneity)</td></tr>
<tr><td>Ofstede's Country Profiles:
• Power distance
• Uncertainty avoidance
• Individualism
• Masculinity/femininity
• Time Horizon</td><td>Five Operational Cultural Dimensions:
1. The Physical Environment
2. The Economy
3. The Social Structure
4. The Political Structure
5. Beliefs & Systems
From Operational Culture for the Warfighter</td></tr>
</table>

In the end, the framework(s) we choose is/are based on what we want to know and what we plan to do. We want to gather not only analysis and facts but explanations that lead to empathy / understanding that contribute to a methodological approach to operational Design, joint and service military decision making processes.

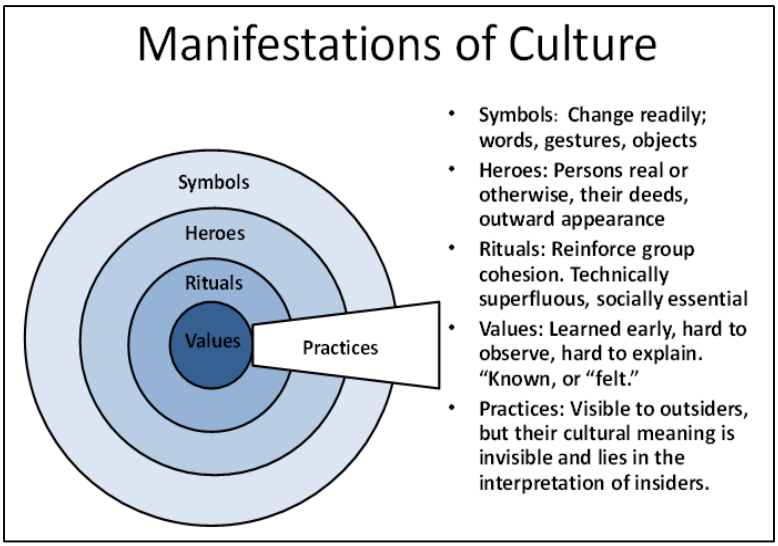
Every Red Teamer should possess a general OE knowledge of:

- Dimensions of Culture
- Aspects of National Culture
- Distinct motivational values born of cultural upbringing and context

Red-teaming instruction at UFMCS focuses on culture at the general level of knowledge. Emphasis is placed on culture because culture was identified as a gap in the understanding of the OE during OIF and OEF, and because culture is historically difficult to understand as its substance and significance is often abstract and not immediately observable.

The UFMCS Culture curriculum includes lessons focused principally on four subjects that are uniformly acknowledged in anthropological studies as foundational to any cultural study: social structure, politics (power and authority), economics, and religion (belief systems). The assumption is that to understand any one part of a culture or society we must look at all the rest of the socio-cultural context. The purpose of separating a society or culture into elemental parts or basic principles is not to isolate these elements, but to determine the nature of the whole.

General knowledge focuses learning about a complex OE on what is important for military planning and decision making. General knowledge is not concrete but an abstraction from experience; generalizations abstracted from multiple specific cases. Generalization simplifies a complex reality; complexity that otherwise overwhelms our ability to understand. An example of a model or framework that serves to simplify and illustrate an otherwise complex cultural reality is Hofstede's "Onion" model of Cultural Manifestations.



This simple, general model (p. 161), when populated, presents the Red Teamer with a cultural "… set of patterns, of and for behavior, prevalent among a group of human beings at a specified time period and which … presents … observable and sharp discontinuities."[18] Models like this one allow the Red Teamer to analyze what is the same, and what is different, the "sharp discontinuities" of the cultural context. It provides general categories and asset of patterns with which to begin a cultural examination of the OE that may be useful in the development of the Environmental frame of the Design process.

Without general categories we easily get lost in the complexity of specific details. At the population level, the human domain is extremely complex and is continuously changing which makes analysis to identify what can be influenced to achieve the desired outcome intractable. There are too many interconnected variables—at some level most all variables are connected—and causal relationships are constantly changing. This fact alone is enough to make planners take an essentialist view of culture, "It's always been that way with these people."

> *"To explain different patterns of culture we have to begin by assuming that human life is not merely random or capricious. Without this assumption, the temptation to give up when confronted with a stubbornly inscrutable custom or institution becomes irresistible" -- **Anthropologist Marvin Harris, 1989**[19]*

Organization of cultural information is more than simple aggregation or populating a rigid systems model with general information. Important nuances of culture may be missed in a simple aggregation and cannot be examined by looking only at institutional design. This is where red teaming tools may be useful in determining which information, general and specific, is contextually important in the design or planning process, and help us to avoid the temptation to "give up," or generalize in a stereotypical fashion.

The complexity of the human domain may be simplified by organizing specific information into general categories important for military operations. These general categories are based on what is important to know. At the highest level of organization for military operations, these general categories are the military operational variables, PMESII-PT. These categories simplify reality and provide a framework to focus collection of Regional Expertise and Culture (REC) - specific information relevant for military analysis.

Systems Thinking: According to CJCSI 3126.01A, *Language, Regional Expertise, and Culture (LREC) Capability Identification, Planning, and Sourcing*, systems thinking is: "Understanding how ...variables in the regional system interact with one another and change over time."[20] At the population level, it is an understanding of the interaction of variables across a population. Given complexity, as mentioned above, "systems thinking" is enabled by the simplification of reality into relevant general categories of variables. The task for the Red Teamer is to render reality as simple as possible, but no simpler, for the purpose of military planning. For this reason, a functional approach to cultural analysis of the OE is suggested as one approach the Red Team may take for the purpose of connecting cultural

analysis to planning and operations. The following Functional Systems Approach to cultural analysis for planning is adapted from the USAFAS Regional Expertise and Culture Instructor Course (Pilot) developed by Dr. Daryl Liskey.

Functional Systems Approach

A *System* is an analytical approach to understand regular interacting relationships (links) and the associated entities (nodes) in an OE (see JP 2 01.3).[21] It is an analytic device for separating from its context a set of phenomenon we want to study. Anthropologist Ronald Cohen describes it this way:

> The system as a whole does something. It can be characterized as having an activity or activities, and its various parts contribute to the fulfillment of these ends. Indeed systems designers are quite clear on this point when they design systems, *since they start with functions* (emphasis added) and then work back to create a set of interrelationships that will, in fact, describe the carrying out of these ends.[22]

How variables are related to produce a specific outcome is the definition of a *function*. The functional system consists of the regular patterns of interacting variables that cause the output. A functional systems approach is useful because it provides a systemic approach to analyzing interactions on what is important to know.

Keep in mind that the functional systems approach is not theory, nor is it doctrine. It is a method that links all aspects of cultural research together (Red Teaming, Design, LREC, PMESII, etc.). It is but one of many methods that may be used to enhance apperception (conscious perception with full awareness). Its intended use is as a bridging device between red teaming analysis and doctrine. The goal of this approach is an accurate description of a culture, leading to an explanation, and ultimately better informed planning and decision making.

The PMESII systems (which the Army identifies as the Operational Variables) purport to identify the *most important outputs or effects* relevant for military operations in a typical country at the campaign level of planning.

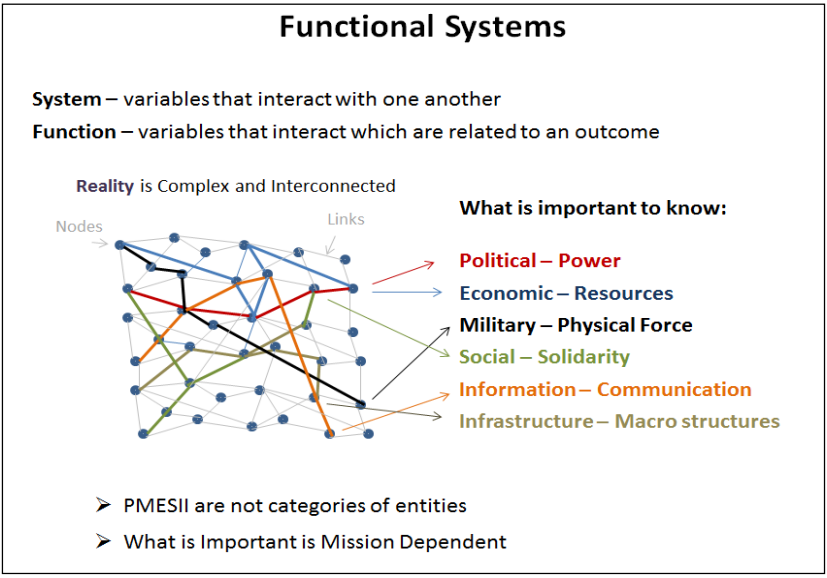
In functional terms, the Operational Variables are:

Political – power: how binding decisions are made

Military – physical force: how physical force is exercised

Economic – resources: how goods and services are produced, distributed, and consumed

Social – solidarity: how people interact in their everyday lives



Infrastructure – physical macro systems: how critical resources and activities move across man-made physical systems

Information – communications: how information is produced, distributed, and consumed

A functional understanding differs from but is consistent with the description of the operational variables in ADRP 5 and other Army and Joint Publications like JP 2-01.3.

At UFMCS, we include **Religion**, or belief systems, as a function.

In general, the PMES variables are important functions of any population, which is well established in the academic literature. A PMESII systems approach can be useful across the levels of war: a village, for example, may be usefully analyzed in terms of a PMESII framework for missions that cross the full range of military operations.

Caveats: In general, a PMESII Operational Variables approach is consistent with a functional systems approach given two ***caveats***:

- ***PMESII are not meant to be stand-alone descriptive bins for categorizing entities (e.g., persons or institutions)***. In other words, it is unnecessary to think of any element of the system as a compartmentalized function which must be sharply separated from its context. A single entity or institution may be important across the PMESII operational variables. For example, a sheik may be an important variable in an analysis of power, force, resources, and solidarity of a tribe. If the sheik is categorized as a social variable but not a political variable, then the analysis of power misses an important variable. In more complex societies, institutions may be structured to perform a single specialized function; for example, a business enterprise is organized to perform an economic function or a government to perform a political function. However, a political analysis of American politics can include military, economic, and social institutions as important variables. If economic institutions are walled off from Political, then the analysis will be partial or biased and unlikely to accurately estimate the effect.

- ***Mission Dependent***: What functions are important in a particular military mission may differ depending on the mission. As noted in JP 2 01.3, *Joint Intelligence Preparation of the OE*, for more-focused military operations, a full analysis of the PMESII variables is not needed. As, in governance operations, analysis of the political system can be the most useful (keeping in mind that PMESII are not descriptive categories) while for military force-on-force operations the analysis of the Military system is likely the most useful.

By now we have established that there are several frameworks, procedures, and models by which to examine culture. Whatever design we decide upon is dependent on the answer to four critical questions (adapted from Keesing, 1970):

1. What will be the shape and design of the cultural description?
2. What is the relation of such a cultural description to the overall goals of the military plan or decision?
3. How is the adequacy of the description to be evaluated?
4. What evidence is there that the descriptions we have sketched will be productive?

The purpose of these questions is to explain culture to what end? What is the connection? And the answers to these questions are critically important in determining the validity of whatever cultural framework, process or model we choose. The answer must be better understanding to inform the planning process.

The human domain is infinitely complex. It pushes back, evolves, and changes rapidly and unpredictably. We currently lack sufficient analytical power to reliably understand functions in the human domain in the same way we can in the biological or engineering domains. Institutions can be *engineered* to perform a function, but the OE outside

institutions, is more complex. Rather, red teaming tools and a functional approach to the human domain generate research questions that focus the purpose for an analysis and what casual relationships are important. Given a certain question, we structure research areas by identifying what is necessary to answer the question based on our general knowledge. To the extent that general knowledge is true, the categories and relationships will be true. It provides our "best initial guess" which is preferable to the alternatives. The Cultural Perceptions Framework (p. 122), Critical Variables (p. 115), and "Onion" model (p. 161) are useful red teaming tools in generating questions and categories that support the functional systems approach and in generating broader understanding (empathy) and alternative perspectives for cultural analysis.

Advantages of a Functional Approach: There are three important advantages of a functional approach.

- ***Focuses Analysis on Outcomes and Effects***: Observing entities alone can tell us little about what is important for outcomes like power (control). A local government official or *sheik* may not be an important variable. In a village, the priest or large land owner may exercise more power. Or, power, more likely, is distributed throughout a functional political system. By understanding the functional system, entities or relationships can be identified that are important for causing an outcome. Systemic functional analysis increases the likelihood of developing course of action (COA) that will achieve a desired effect.
- ***Identifies what is important across specific areas***: A functional approach also enables a REC-general understanding applicable across any area. Understanding key specific functional relationships like decision making, execution, and enforcement enables identification of the specific institutions across specific regions or systems. The specific institutional form can vary greatly: the ultimate decision-making function can

be exercised by Congress in the United States, the Central Committee in the People's Republic of China, or the religious leader in Iran. It may also be shared among different institutions to varying degrees. Understanding of functions provides general knowledge of what is important across specific areas where institutional form can vary widely.

- ***Synchronizes knowledge and analysis across echelons*:** Specific forms of institutions also vary across echelons within an AO. For example, political parties may have a national level organization, linked to regional political groups, which in turn are linked to local informal power holders in a village. A functional analysis enables an understanding of vertical as well as horizontal system relationships related to outcomes despite specific differences in form. This enables an analysis of how one level affects the other as well as enabling the aggregation of information and analysis across echelons.

Cultural Relevance

A few rules of thumb apply to recognize when culture may be more important:

Greater Cultural Differences: Culture is more important when cultures differ from our own. In countries like Afghanistan, these differences can be marked and more important than institutional considerations. In more Westernized cultures, culture differences may be few and institutional differences will matter more.

Unstable Countries: Where institutions are weak or are collapsing, cultural ties are relatively more important and can become a critical source of conflict as well as resilience.

Marked Differences within a Country: The cultures within a country can vary markedly. The culture in rural areas is less Westernized compared to major urban areas and the culture can vary from area to area within a country. Differences in culture can produce strong cultural dynamics

within a country even in highly institutionalized Western countries and these dynamics can be critical for Western countries.

Additionally, culture can be a more critical consideration in population Inform and Influence operations and, at the individual and organizational levels, operating with JIIM partners.

Summary

Anthropology is about observation, collection, and cross-cultural comparisons. Military planning is oriented toward action, and exhibits a bias toward a particular type of action (security, stability, decisive action, etc.) The processes of military planning can have a dramatic effect on the goals of those actions. Red teaming is about apperception, theory construction and testing. These fields frequently overlap, but tend to use different methodologies and techniques. Red teaming methods and tools aim at improving cultural understanding with the goal of enhancing the chances of successful outcomes in military planning. In the case of cultural empathy it is about explanations of the relationships of cultural functions. Red teaming represents a methodology, and the approach affects the method. The order of application reflects a strategy. The aim of the strategy is the support of operational planning in the form of Design and MDMP. The following are some thoughts for the Red Team to keep in mind when conducting cultural analysis:

- The study of culture is not performed in isolation. It is only meaningful when regarded as part of a larger body of thought (e.g., strategy, design, campaign planning).
- Cultural analysis is part of the larger intellectual process of war fighting and peace keeping.
- The tendency to depend on one authority, one theory, or one approach to cultural apperception is extremely dangerous in military planning.

- Red teaming cultural methodology is not a new way of knowing—it is a systematized approach—a synthesis of several works.
- A functional systems approach is useful because it provides a systemic way of analyzing what is important to know about the OE.
- Red teaming methodology does not produce solutions, but insights that inform planning—a logic of inquiry.
- The aim is to avoid spurious correlations and conclusions.
- The goal is to make sense of—or meaning of—what goes on in a particular cultural milieu; for that time, and in that context, for the purpose of planning and policy making.
- The red teaming cultural methodology aims to inventory and understand a people and their motivations at a level of general knowledge for the purpose of resolving or avoiding violence and conflict.
- The goal of general knowledge is not prediction per se, but understanding in order to control and influence the outcomes we desire in military operations.

And finally, some observations on "why we study culture"[23] from Dr. Geoff Demarest:

1. To find people and things. Cultural knowledge helps locate individuals, their wealth and their supporters. 'Locate' means establish their precise whereabouts -- where they will sleep tonight, where their mother is buried, the number of their bank account and the bank routing number, where their motorcycle is sitting, their email address, where and when they play golf…and where they feel safe. For the competitor in a violent struggle this is the first and most compelling reason for cultural knowledge. It is what Sam Spade, the private investigator, knows. The rest is useful, too, but if he knows where you are while you don't know where he is,

you are the prey. To control anonymity, you must know the culture.

2. To communicate good. Cultural knowledge can improve communications with others so as to endear and not offend, to facilitate collaboration and compromise, and to settle disputes peacefully when preferable. This involves language beyond the verbal, and into customs, prejudices, habits, mores, expectations, fears, historical grievances, community pride and the like. All knowledge is grist to the mill. It will be especially productive to identify aspects of the culture related to honor and dishonor.
3. To identify objects of desire, sources and holders of power, grievances, agents (especially 'exclusive' agents), resolution mechanisms, debts, tax relationships, jurisdictions and expectations. In short, to comprehend the territorial geography of conflict and conflict resolution.
4. To set reasonable objectives. Knowing how or if to change the social compact, how long it might reasonably take you to implement such a change, and how long the changes might last. This may include determining the interrelationship between peoples' behaviors and their surrounding environment in order to derive durable improvements in human flourishing and harmony. When good intentions are not built on sufficient knowledge, the reward may be a set of nasty unintended consequences. In a domestic legal setting we demand due diligence of doctors and lawyers -- that they avoid negligent practice. Strategic due diligence presupposes the programmed and resourced study of foreign cultures in order to avoid strategic negligence.
5. To put things in the right places. Whether you want to optimally place a fish pond, police station, camera, or a shooter, it is local cultural knowledge (and usually the kind that cannot be gained via remote sensing) that will guide best.

6. To correctly time actions and activities. Knowing when to act and not act is a much easier standard if we are steeped in local cultural knowledge.
7. To get the joke or make the joke. Jokes work the same mental pathways as military deceptions. For practical purposes, military deceptions are jokes. Irregular armed conflicts are generally clothed in law, economics, propaganda and other aspects of quotidian, civilian life. Not being able to get civilian jokes means being vulnerable to the dangerous military or criminal ones. Just as the insurgent can move from military uniform to civilian attire, so can military thought hide in civilian guise.

Endnotes

[1] Anthony Zinni , "Non-Traditional Military Missions: Their Nature, and the Need for Cultural Awareness & Flexible Thinking" in *Capital "W" War: A Case for Strategic Principles of War : (because Wars Are Conflicts of Societies, Not Tactical Exercises Writ Large)*, by Joe Strange (Quantico, VA: Marine Corps University, 1998), 282.

[2] Clifford Geertz, *The Interpretation of Cultures: Selected Essays (* New York: Basic Books, 1973), 29.

[3] Geert Hofstede, Foreward to *Leadership in a Diverse and Multicultural Environment: Developing Awareness, Knowledge, and Skills* by Mary Connerley and Paul Pederson, (Thousand Oaks, Calif.: Sage Publications, 2005), ix-x.

[4] Geertz, *The Interpretation of Cultures*, 29.

[5] Ibid, page #?.

[6] Haight, G. "Managing Diversity." *Across the Board* 27, no. 3 (1990): 22.

[7] Ken Booth, *Strategy and Ethnocentrism, (*New York: Holmes & Meier, 1979),15.

[8] Taylor Cox, *Cultural Diversity in Organizations: Theory, Research, and Practice, (*San Francisco, Calif.: Berrett-Koehler, 1993), 88.

[9] Mary L. Connerley and Paul Pedersen, *Leadership in a Diverse and Multicultural Environment: Developing Awareness, Knowledge, and Skills, (*Thousand Oaks, Calif.: Sage Publications, 2005), 29.

[10] Geertz, *The Interpretation of Cultures,* 5.

[11] Connerley and Pedersen, *Leadership in a Diverse and Multicultural Environment*, xii.

[12] Ibid, xi.

[13] Ward Hunt Goodenough, *Culture, Language, and Society,* 2d ed., (Menlo Park, Calif.: Benjamin/Cummings Pub., 1981), 109.

[14] Geertz, *Interpretation of Cultures,* 5.

[15] Geert H. Hofstede and Gert Jan Hofstede, *Cultures and Organizations: Software of the Mind: Intercultural Cooperation and Its Importance for Survival,* Rev. and Expanded 3rd ed., (New York: McGraw-Hill, 2010), 6.

[16] Barak A. Salmoni and Paula Eber, *Operational Culture for the Warfighter: Principles and Applications,* (Quantico, Va.: Marine Corps University ; Washington, DC :, 2011) 15.

[17] Florence Rockwood Kluckhohn and Fred L. Strodtbeck, *Variations in Value Orientations, (*Evanston, Ill.: Row, Peterson, 1961) 7.

[18] Claude Levi-Strauss, The Elementary Structures of Kinship. (Boston: Beacon Press, 1967), 10.

[19] Marvin Harris, *Cows, Pigs, Wars & Witches: The Riddles of Culture*, (New York: Random House, 1989), 4.

[20] CJCSI 3126.01A. *Language, Regional Expertise, and Culture (LREC) Capability Identification, Planning and Sourcing*, H-1.

[21] JP 2-01.3, *Joint Intelligence Preparation of the Operational Environment*, (21 May 2014).

[22] Ronald Cohen, "The Political System," in A Handbook of Method in Cultural Anthropology, eds. Raoul Naroll and Ronald Cohen, pp. 484-499. New York & London: Columbia Press, 1970.

[23] Demarest, Geoffrey. Winning Irregular War. Leavenworth, Kansas: Foreign Military Studies Office, 2014, pp. 153-154.

CHAPTER IV: Critical Thinking

> *In all affairs it's a healthy thing now and then to hang a question mark on the things you have long taken for granted.*
>
> *Many people would sooner die than think. In fact, they do.*
>
> ***-- Bertrand Russell***[1]

Introduction

Critical thinking is a term that many institutions hold in high regard, that most people have heard about, and that almost nobody practices on a thorough and systematic basis. This section of the Red Team Handbook is designed to acquaint you with many of the fine points associated with critical thinking by doing two things: exploring what critical thinking is, and addressing why critical thinking is necessary.

Critical thinking is hard, deliberative work and it takes an open, inquisitive mind. It is not easy, but it doesn't take a genius either. You can choose to believe whatever you hear and see. But to be a critical thinker, you must learn to ask yourself whether you *must* believe what you hear and see. *Ultimately, critical thinking is about what to believe.*

What Do Critical Thinkers Do?

What exactly is critical thinking? A common approach to answer that question is to consider how the term is defined. Let's look at a few definitions of critical thinking. Drs. Richard Paul and Linda Elder, authors of many critical thinking books and documents, define critical thinking as

> "A process by which the thinker improves the quality of his or her thinking by skillfully taking charge of the structures inherent in thinking and imposing intellectual standards upon them… [It requires] a commitment to overcome our native egocentrism and sociocentrism."[2]

Robert Ennis, also recognized as an expert in critical thinking, defines it differently: "Critical thinking is a process,

the goal of which is to make reasonable decisions about what to believe and what to do."[3]

Are either of those definitions sufficient to explain what critical thinking *is* in full, or what critical thinkers do? Certainly not. Neither enumerate *what* critical thinking is, nor point us in the right direction in terms of *how* to think critically. The challenge of defining critical thinking is that it seems to defy definition—at least a definition that stands alone, fully explaining what it is and how to do it. In fact, several authors who have written about critical thinking do so without attempting to define the term. Among them are Stephen Gerras ("Thinking Critical About Critical Thinking"), Stephen Brookfield (*Developing Critical Thinkers*), Tim Hurson (*Think Better*), and Peter Facione (*Critical Thinking: What It Is and Why It Counts*).

Although the definitions leave us with questions concerning what critical thinking is and how to do it, they do provide insight. By closely reviewing several definitions, we can ferret out ideas that help us better understand the nature of the critical thinking.

Look at the definition by Drs. Paul and Elder above. Several tangible ideas emerge: critical thinking is a *process*, and it deals with the *quality of thinking* by *imposing intellectual standards*. In fact, in other writing these two authors assert that critical thinking *considers points of view*, *the quality of information*, *interpretation and inference*, *assumptions*, and *implications* and *consequences*, and that critical thinkers *think open-mindedly,* and *gather, assess* and *interpret relevant information*.[4]

Additional verbiage from other critical thinking experts, with their key ideas italicized, are as follows:

- Stephen Brookfield (*Developing Critical Thinkers*): Critical thinking consists of *challenging assumptions* and *exploring alternatives*.[5]

- M. Neil Browne and Stuart M. Keeley (*Asking The Right Questions*): "Critical thinking consists of an *awareness* of a set of interrelated critical questions, plus the ability and willingness to ask and answer them at appropriate times" (Italics added.)[6]
- Gary Jason (*Critical Thinking*): "Broadly defined, critical thinking means *developing an ever better worldview* and using it well in all aspects of your life… the essence of critical thinking is *questioning* and *arguing logically*. … the heart of critical thinking is the ability to … infer or reason well… questioning and arguing logically" (Italics added).[7]
- Sylvan Barnet and Hugo Bedau (*Critical Thinking, Reading, and Writing*): "[Critical thinking includes] *searching for hidden assumptions*, noticing various facets, unraveling different strands, and evaluating what is most significant … [critical thinking] implies conscious, deliberate inquiry, and especially it implies *adopting a skeptical state of mind*." "Critical thinkers are…sufficiently *open-minded*… [and] adopt a *skeptical* attitude." "Critical thinking means questioning not only the assumptions of others, but also *questioning your own assumptions*" (Italics added.)[8]

Make a short list of all of the italicized words in the definitions shown thus far. Collectively, these words help illuminate what critical thinking *is*, and what critical thinkers *do*. Here is an initial list of the ideas expressed in italics:

- Critical thinking is:
  - *awareness.*
  - a *process.*
  - *quality of thinking.*
  - *imposing intellectual standards.*
  - *challenging assumptions* and *exploring alternatives.*
  - *searching for hidden assumptions.*

  - *questioning* and *arguing logically.*
  - *developing an ever better worldview.*
- Critical thinkers:
  - *are open-minded.*
  - *adopt a skeptical state of mind.*
  - *gather, assess*, and *interpret relevant information.*
  - *question [their] own assumptions.*
  - *consider points of view*, *the quality of information*, *interpretation and inference*, *assumptions*, and *implications* and *consequences.*

Let's elaborate on a few of the ideas expressed above. First, critical thinking is *awareness*: critical thinkers are aware of their surroundings, what they do know and (more importantly) what they do not know, and how their thinking can often fool them. Because of this, critical thinkers are self-reflective and defer judgment: they do not jump to conclusions, but rather take time to ask questions, ensure they've considered various perspectives, ask themselves what's missing that needs to be considered, and reflect upon how their values and beliefs may be conspiring to fool them.

Critical thinking is also a *process*. Good critical thinkers consider various frameworks when thinking about problems, because frameworks force us to consider alternative perspectives that we wouldn't naturally consider. The latter portion of the Red Team Handbook is filled with frameworks with which we can think critically about various challenges.

Critical thinking includes knowing that for many issues, assumptions prevail. Often these assumptions are hidden, or *implicit*: we make them without realizing that we are doing so. *All* assumptions need to be challenged. When the assumptions are challenged and found to be faulty, we may have better insight into the nature of the problem.

Exploring alternatives is equally important. Otherwise, we take for granted that the first thing that comes to our mind is the way it really is—we fall prey to default-mode thinking, allowing ourselves to be comfortable with the first conclusion we settle upon.

Considering the collective list of extracted ideas from critical thinking experts is a first step toward more fully appreciating what critical thinking is, and how to do it. To add to the list above, think of someone you admire as a critical thinker. What is it that s/he does that you admire? How is it that this person "thinks critically?" What habits of thought does this person exhibit? There is no perfect, all-inclusive list of critical thinking traits. But by constructing such a list, we can better understand the aspects of critical thinking that definitions alone won't provide.

In summary, critical thinking definitions—however eloquently stated—often do not provide complete, self-contained understanding because there is much more to critical thinking than any one definition can provide. Rather than focus on definitions of critical thinking, we invite you to review the list of *Critical Thinking Traits* (p. 112). Review each item on this list. If you aren't doing all of the things noted on the list, perhaps your critical thinking has room for improvement. Make sure to explore those ideas that you don't understand.

This completes the discussion of what critical thinking is, and what critical thinkers do. But is critical thinking a necessity?

Why is Critical Thinking Necessary?

We maintain that critical thinking is indeed vitally necessary. Why? For a number of reasons—among them the fact that we spend most of our waking day on "cognitive autopilot," not consciously thinking about the choices that we make; that each of us perceives and interprets the same information in several different ways; and that there are ingenious attempts on the part of the few to fool the many. This section will briefly examine these reasons.

Most human beings are on "cognitive autopilot" most of the time. Think about it: since you woke up this morning, how much of your daily routine has been just that—a routine? Unless you're a child, and haven't yet learned all of the things necessary to survive and thrive in the modern world, we don't usually give a second thought to many of the things we do during the day. This includes dangerous activities—driving a car on a busy highway; playing ice hockey; working in a noisy, dangerous automotive plant; or crossing a busy street while listening to music on an iPod.

According to Daniel Kahneman, most impressions and thoughts arise in your conscious experience without your knowing how they got there. The mental work that produces impressions, intuitions, and many decisions *goes on in silence in our mind*. As we navigate our lives, we normally allow ourselves to be guided by impressions and feelings, and the confidence we have in our intuitive beliefs and preferences is usually justified.

But not always.[9]

According to Richards Heuer (*The Psychology of Intelligence Analysis*) and Morgan D. Jones (*The Thinker's Toolkit*), we do not approach analysis with empty minds. Our minds are full of biases and assumptions. Unless we are forced to stop and think through a particular challenge, we are able to blot out much of the complexity surrounding us and rely on routines of habit. Usually, this works fine until we treat a truly unique situation as yet another *routine* situation, at which point we are taken by complete surprise. Hopefully we survive and learn. Sometimes we're profoundly embarrassed.

Critical thinking helps us break the bond of unreflective dependence upon our intuition. It is a counter-weight to "cognitive autopilot." Why? For several reasons, among them our reliance upon mental models, patterns and intuition; the effects of "frames"; and our values, beliefs and worldviews.

When we perceive and interpret information, we usually use mental models, patterns, and anomalies: our intuition. Mental models—also referred to as "mindsets"—are tools that we unknowingly create to replicate how we believe the world actually works. They act as *implicit* assumptions—unstated, hidden assumptions we don't consciously make, but which nonetheless exist. We use these mental models to simplify our daily lives. Mental models allow us to cope with reality by providing a ready-made default mechanism: "when I see the following, here's how I interpret it and here's how I act." Most of these mental models, like our values and beliefs, reside in our subconscious, which means that we are not normally cognizant when we are using them. Mental models do make our lives easier; they simplify the environment by bringing to each new experience a pre-established frame of reference. The absence of mental models would require us to figure out every situation as it presents itself, and we would soon be overwhelmed.

When our mental models of the world do not match the reality that we face, we often ignore that reality. Unfortunately, we often try to project our own mental models onto situations, whether or not they actually fit. We tend to perceive what we expect to perceive in the world around us, valuing information that is consistent with our views, and rejecting or overlooking information that is inconsistent with our views. And we perceive in a way that is least likely to disturb what we expect to see—least likely to disturb the mindsets buried in our subconscious.[10]

Related to mental models are sets of patterns that we establish throughout our experiences in life. The longer we live, the more experiences we gather and the more we are able to operate autonomously through the use of these patterns. Sometimes when a particular pattern that we expect doesn't present itself—when we spot an anomaly—we are able to act upon that information too. Many times, however, spotting anomalies is difficult, especially if we are not looking for them in advance.

When we view the world around us in terms of patterns, however, we get into trouble when those patterns don't actually exist. This is a description of a "cognitive bias" called the Narrative Fallacy.

We can also fall into a trap of allowing our minds to jump to conclusions—having been deceived by the faulty use of mental models or patterns—and form a conclusion to a particular problem without first considering alternatives, simply because that's what our mental models or overreliance on patterns tells us is the truth. This is an example of what we call Confirmation Bias, which is another of the *Cognitive Biases* (p. 105). In order to preclude Confirmation Bias, we should not seek to confirm anything. Rather, we should seek to *disconfirm*, or disprove an idea, especially if that idea comes in the form of an assumption. An ideal tool that uses the principle of disconfirming evidence is the *Analysis of Competing Hypotheses* (p. 83).

A concept closely related to mental models is frames, which according to Edward Russo and Paul Schoemaker are "mental structures that simplify and guide our understanding of a complex reality."[11] Frames are hard to recognize, and distort what we see. Most of us don't realize that we have various frames and mental models. We often use frames to consider problems or situations, but fail to realize that we should use several frames instead of just one. Rather, we normally use the first frame that occurs to us. Challenging our frames is a necessity, but we can't challenge our frames if we don't realize that they exist. A useful tool in working with frames is the *Frame Audit,* p. 150).

Our values, beliefs and worldview act as filters to skew our perception and interpretation of information, and they motivate our subsequent behavior. Most of our values and beliefs reside in our subconscious; we know we have them, and when forced to think about them we can generally describe what they are. Values and beliefs are both forms of assumptions about how the world works, and our worldview

could be considered as a compilation of these beliefs and values.

Since each of us (even within the same culture) are apt to have subtle differences in our values, beliefs and worldview, it should be easy to understand that each of us is apt to perceive and interpret information differently from each another. Of course, when we work with people from other cultures, the differences are apt to be much more significant. Critical thinking helps us to think about each others' perspectives.

One way to think critically about issues in which our values, beliefs and worldview may have affected us is to adopt the role of a Devil's Advocate. *Devil's Advocacy* (p. 145) is a process which forces us to think through an issue from a completely different perspective, one which we wouldn't normally consider. *Each of us perceive and interpret information differently—for several reasons.* Among these reasons are the physical limitations of our perceptive processes; our inability to reason properly; our inability to differentiate between causation and correlation; and our difficulty in "thinking complexly" about complex problems.

We are limited in terms of what we can physically perceive. Hence, each of us is apt to see different elements of the same information. When we observe something, we often miss many things. According to Dr. Marcus Raichle, a neurologist at Washington University, each of us has ten *billion* bits of information hitting the backs of our retinas every second—of this, only six *million* bits make it to our optic nerve, and 100,000 bits make it to our visual cortex. Yet only *100* bits of information make it to our conscious brain each second. That is a significant physical filtering of information—from 10^{10} power to 10^{2} power. Even if Dr. Raichle's numbers are a bit off, the effect should be readily apparent. We simply do not have the capability to register and think about everything we can perceive. When several of us look at the same thing, we often notice different aspects of it. Why? Our mental models, the patterns we've

experienced, our frames, our values and beliefs, and our worldview. This is why diversity among groups is important: each of us is apt to be able to think about key aspects and perspectives that others in our group are not, and vice versa.

Our vision is a *construction*. The process of observing includes recreating in our minds—constructing—what we believe we are observing. When we observe, our brains take in information, and relate that information to the surrounding context. Given all of the information that is physically filtered out, we are inclined to fill in the gaps by making assumptions in a way that makes sense to us: we assign meaning to what we perceive, because we are generally uncomfortable with a completely abstract picture devoid of meaning. The more abstract a perception, the more our brains will add meaning to it. (If you don't believe that, assemble a group of people and view the most abstract art you can find. Many will perceive and interpret the art piece in demonstrably different ways, in part because of the physical limitations described above, and in part due to the mental models, patterns, frames, and beliefs and worldview described above.) The completed "picture" that we see is not necessarily the reality in front of us; rather, it is the constructed version of that reality that reflects assumption-based conclusions to which our brains have already jumped. Again—this is why diversity of experience is crucial to groups conducting critical thinking.

Often our reasoning is faulty. We reason in one of a couple of ways—deductively or inductively. Deductive reasoning relies upon drawing a conclusion from two or more premises. So long as the premises are facts—the truth—then our conclusion is certain to be true. Deductive reasoning tends to be faulty, however, when one or more of our premises are not in fact true, but rather are unrealized assumptions that we have overlooked. In order to ensure that we deduce properly, it pays to think critically and ask whether each and every premise upon which we base our conclusion is factual information, and not a *presumed* fact—an assumption.

Inductive reasoning is different. When using inductive reasoning, we infer a conclusion that, at best, is probable (vice certain). The probability of the conclusion's truth varies directly with the degree of likelihood that its premises are true. Inductive reasoning occurs in a number of different ways: reasoning from a sample to a larger population; reasoning from a population to a sample; accepting a conclusion based on what people report observing; inferring "why" something happened; and reasoning from one sample to another, or analogizing (*Determining the Suitability of an Analogy*, p. 143). In all cases, the first requirement of a critical thinker is to realize that he is resorting to inductive reasoning, and as such acknowledge that his inferences and conclusions are at best probabilities. Following that, a critical thinker must ascertain the degree of probability to his conclusion in order to avoid surprise.

In thinking critically about either deductive or inductive reasoning, a valuable tool to consider using is the *5 Why's* (p. 77), which helps us by revealing unsound logic in our thinking.

We fail to differentiate between causation and correlation. Distinguishing between cause and correlation is an important function of critical thinking. Most of us are unaware that the two concepts exist, and tend to fall into a trap of connecting two events in a linear cause-and-effect relationship. We often fail to understand that linear chains of cause-and-effect are rarely the reality. Instead, what we perceive as a cause-and-effect relationship is in fact a correlative one. For example, during an insurgency we might infer that heaps of trash in the city are causing increased levels of violence among the insurgents. Based upon that linear cause-and-effect analysis, removing the trash should eliminate the insurgent violence. Closer examination, however, might dispel that hypothesis. Although both appear to happen with some relatively predictable levels, there is most likely a correlation between the two—that removal of the trash might

help reduce the level of insurgent activity, but not completely eliminate it.

A critical thinker asks himself, therefore, the following question: is there a cause-and-effect relationship at work here, or are the two actions I observe in some correlative relationship? If so, what is the nature of that correlative relationship? Once a critical thinker develops that hypothesis, s/he should test and amend it as necessary, based upon feedback. (Note: an even more troubling question a critical thinker should ask is whether s/he is inferring (or imagining) a relationship that doesn't exist at all. This question is related to the Narrative Fallacy, one of the *Cognitive Biases* (p. 105), as well as to a famous Logic Fallacy entitled *The False Cause* (p. 108).

We fail to appreciate the complexity in systems, and instead resort to "linear" cause-and-effect thinking. Life around us is incredibly complex, yet we tend to think in linear cause-and-effect relationships, according to Dietrich Doerner (*The Logic of Failure*) and Peter Senge (*The Fifth Discipline*). Most of us attempt to act upon a simple, single variable which creates unintended, cascading effects. Instead, we should consciously account for the interrelated variables in a particular scenario by creating and testing a hypothesis of what we believe the complex system consists of. We then should assess the feedback of our actions, amending our initial hypothesis until we have confidently figured out the system with which we're working. Several tools help when working with complexity: *Premortem Analysis* (p. 165), *Shifting the Burden* (p. 184), and *S-W-O-T Analysis* (p. 204).

Finally, we need to think critically because a lot of people are constantly trying to trick us. Beyond all of the reasons cited above for why critical thinking is necessary, there is also the fact that many people are simply trying to fool us. Unfortunately, for the most part they succeed—because most of us don't think critically enough, or recognize many of the tricks that these folks use. Examples of these rhetorical tricks such as Appeal to the Masses, Appeal to Fear, Ad

Hominum, False Dichotomy, and the Slippery Slope, are all *Common Logic Fallacies* (p. 107). Critical thinkers are knowledgeable of these common logic fallacies and use logic to deconstruct arguments based upon them.

For all of the reasons cited above, critical thinking is a necessity. One of the most robust tools for thinking critically about written and oral argumentation is the *Argument Deconstruction* (p. 86).

Summary

That is critical thinking. As you can see, it is pretty involved—deliberative, hard work. To do it properly, you have to know a great deal—about how we perceive and interpret information differently from others, how our thinking can be affected by a number of things like mental models and values and beliefs, and how others are constantly trying to fool us. But with some diligence and hard work, critical thinking can become a valuable habit. We need to practice it thoroughly and systematically at all times.

Remember: critical thinking is about what to believe. We *can* believe most anything.

But *must* we?

The ideal critical thinker is habitually inquisitive, well-informed, trustful of reason, open-minded, flexible, fair-minded in evaluation, honest in facing personal biases, prudent in making judgments, willing to reconsider, clear about issues, orderly in complex matters, diligent in seeking relevant information, reasonable in the selection of criteria, focused in inquiry, and persistent in seeking results which are as precise as the subject and circumstances of inquiry permit.[12]

Endnotes

[1] "Quotations by Author." Bertrand Russell Quotes. January 1, 2013. Accessed November 24, 2014. http://www.quotationspage.com/quotes/Bertrand_Russell/.

[2] Richard Paul and Linda Elder, *The Miniature Guide to Critical Thinking: Concepts and Tools,* 6th ed., (Dillon Beach, Calif.: Foundation for Critical Thinking, 2009), 1.

[3] Robert Hugh Ennis, *Critical Thinking,* (Upper Saddle River, NJ: Prentice Hall, 1996), xvii.

[4] Paul and Elder, *The Miniature Guide to Critical Thinking*, 5.

[5] Brookfield, Stephen. *Developing Critical Thinkers: Challenging Adults to Explore Alternative Ways of Thinking and Acting*. San Francisco, Calif.: Jossey-Bass, 1987.

[6] M. Neil Browne, M. Neil and Stuart M. Keeley, *Asking the Right Questions: A Guide to Critical Thinking,* 8th ed., (Upper Saddle River, N.J.: Pearson Prentice Hall, 2007), 3.

[7] Gary James Jason, *Critical Thinking: Developing an Effective Worldview,* (Belmont, CA: Wadsworth Thomson Learning, 2001), 2.

[8] Sylvan Barnet and Hugo Bedau, *Critical Thinking, Reading, and Writing: A Brief Guide to Argument,* 7th ed., (Boston, MA: Bedford/St. Martins, 2011), 3-5.

[9] Daniel Kahneman, T*hinking, Fast and Slow,* (New York: Farrar, Straus and Giroux, 2011), 4.

[10] The section above refers to ideas found in Richards Heuer's book, *The Psychology of Intelligence Analysis,* and Morgan D. Jones' book, *The Thinker's Toolkit.*

[11] J. Edward Russo and Paul J. H. Schoemaker, *Winning Decisions: Getting It Right the First Time*, (New York: Currency, 2002), 21.

[12] Peter A. Facione, *Critical Thinking: What It Is and Why It Counts: A Resource paper* (Millbrae, CA: California Academic Press, 1998), 3.

CHAPTER V: Groupthink Mitigation & Decision Support

The penultimate purpose of red teaming and applying critical thinking techniques is to support the organization in reaching good decisions while avoiding the lure of groupthink. This sounds very simple but as Clausewitz reminded us, "Everything in war is very simple, but the simplest thing is difficult."[1] This section covers identifying groupthink and recommendations for groupthink mitigation, how red teaming fits into the Army Design Model, and the Red Team's role in the MDMP process.

Groupthink

Groupthink is one of a number of terms that we use without truly realizing what it is, why it occurs, and how we can mitigate it. Group norms—and the social pressures to conform to them—are in tension with the need for a staff to consider alternatives during decision-making.[2]

Irving Janis has defined groupthink as: "a mode of thinking that people engage in when they are deeply involved in a cohesive in-group, when the members' strivings for unanimity override their motivation to realistically appraise alternative courses of action." And, "Groupthink refers to a deterioration of mental efficiency, reality testing, and moral judgment that results from in-group pressures."

Janis outlined seven defects in decision-making attributed to groupthink. We list them below for reference. During the conduct of the military decision making process watch for the indicators of these defects and apply red teaming methods and techniques to overcome them.

- Discussion limited to merely two or a few alternative courses of action (often only two)
- No survey of objectives to be fulfilled and the values implicated by the choice

- Failure to reexamine the selected COA from the standpoint of non-obvious risk and drawbacks not considered during the original evaluation
- Neglect COAs initially evaluated as unsatisfactory
- Little or no attempt to gain information from experts on other COAs
- Interest only in information that supports the group decision
- Failure to work out contingency plans to cope with foreseeable setbacks

The Army stresses teamwork, shared understanding and *esprit de corps*. These are admirable traits in the profession of arms. Janis points out however, "The more amiability and esprit de corps among the members of a policy making in-group, the greater is the danger that independent critical thinking will be replaced by groupthink, which is likely to result in irrational and dehumanizing actions directed against out-groups." Officers educated in red teaming, whether or not they are acting as a Red Team or simply a member of a plans team, must ensure groupthink does not take hold.

Symptoms of groupthink are:

- Overestimations of the groups power/invulnerability, and morality
- Closed mindedness and the tendency to rationalize away contrary information
- Pressures toward uniformity of thought within the group
- Self-censorship by individuals in the group, inclination to keep quiet
- The emergence of self-appointed mind-guards to protect group from adverse information
- Stereotyped views of enemy leadership and culture

The consequences of groupthink as stated by Janis are; "whenever a policy making group displays most of the symptoms of groupthink, we can expect to find that the group also displays symptoms of defective decision-making." How can a team avoid the consequences of groupthink?

Groupthink Mitigation

To mitigate groupthink in an organization certain techniques have been developed to try to overcome the symptoms identified by Janis. These techniques are targeted at the organizations as a whole, and situations where groups within that organization are in the decision making process. Janis discusses a number of themes at the organizational level that help mitigate groupthink:

- Senior leaders set the tone for the organization by encouraging decision making groups to air objections and doubts during the decision making process, and discourage members from soft-pedaling disagreements.
- Leaders in the organization should not prejudice the decision-making group with his/her favored course of action. The leader should allow the group to explore impartially a wide range of courses of action without the group feeling the pressure to conform to the leader's views.
- The senior leaders should setup multiple groups to examine the same problem. This allows for differing views and solutions for the leader to consider (see *Team A / Team B*, p. 205)
- Senior leaders should bring in outside expertise to challenge the views being developed by the decision-making group.
- The leaders should assign individuals (if not individuals from the Red Team) to act as "devil's advocate" for solutions and COAs the group is developing.

During the actual decision-making process the following actions can be initiated to mitigate groupthink tendencies in a decision-making group:

- One of the keys to mitigating groupthink is to have all members of the group express their opinion absent pressure from the leader or group to conform. Weighted anonymous feedback techniques give the individual the ability to express his or her opinion in an anonymous fashion without being crushed by group pressure. The leader of the group can have the individuals in the group pre-commit their ideas by writing down their initial answers to the problem being discussed before the meeting occurs. This helps establish the individuals' ideas prior to the group's deliberation, and mitigate the pull towards conformity. Another technique, *5 Will Get You 25* (p. 78), will give each individual a voice in the finding the best COA without the group being dominated by the senior leader or one individual.
- To better facilitate discussion within a group there are a number of techniques which help all members of a group communicate better without being dominated by the senior leader or one dominating individual. Techniques like *1-2-4-Whole Group* (p. 73), *5 Whys* (p. 77), *Circle of Voices* (p. 103), and *Troika Consulting* (p. 209) provide forums for everyone in the group to participate in the discussion concerning the problem.
- To better understand a problem the group faces, the group can use a number of techniques. Techniques like *Shifting the Burden* (p. 184), *Stakeholder Mapping* (p. 186), and *TRIZ* (p. 208) help the group elucidate the problem in a more coherent fashion and provide each individual an opportunity to participate in the discussion and become more aware of the nuances of the problem.
- To help generate a wider range of options/COAs for a problem, the group needs to go through a divergence-convergence thought process. Divergence thinking allows

the group to explore multiple solutions to problems without constraints. A divergence technique like *Brainstorming* (p. 89) allows each group member to offer ideas for a solution to a problem without the idea being judged or "shot down" by the senior or dominating individual in the group. Once the group has identified a number of solutions/COAs, they can begin the convergence process of whittling down and refining viable options by using techniques like *6 Words* (p. 79), *Dot Voting* (p. 148), *My 15%* (p. 160), *Troika Consulting (Ad Agency)* (p. 209). All of these techniques help the group collectively come up with the best COA without being dominated by one individual.

The Operational Environment Laboratory (OEL) at Fort Leavenworth invited a Red Team in for a three-day leader program. The OE lab was being restructured and wanted to use red teaming techniques as a means of identifying and addressing organizational priorities. Much as described above, the Red Team facilitators used weighted anonymous feedback and other tools to identify the single most critical problem the leadership had to address in the near term. The OEL leaders then broke into small groups to work through some solutions. Towards the end of the second day the group appeared to have developed a plan to address its single biggest problem. The OEL Director and all of his lieutenants seemed in agreement.

The Red Team facilitator asked everyone to take out a piece of paper and anonymously provide feedback on the action plan to address the problem. Feedback was a simple: Yes, I think we are on the right track; No, this will not work and the reason why is as follows; or this issue does not affect my section I choose to abstain on judging the merits of the solution.

The facilitator asked the director of the lab to predict, based on the discussion, how many would vote in which manner. The director predicted three of his subordinates would choose to abstain and the remaining six would all vote that the plan was a good one. What actually happened is three did in fact abstain; the remaining six, when allowed anonymity, all said the plan was not executable. In one form or another their major objection to the plan was it lacked any forcing function which would require them to participate in providing the data required to implement the plan. They knew how busy they were and they knew without some hammer they would simply not comply with the very solution they designed. The remaining day of the engagement was spent designing the forcing function that would enable the policy.

Military Decision Making Process

"The *military decision making process* (MDMP) is an iterative planning methodology to understand the situation and mission, develop a course of action, and produce an operation plan or order. The MDMP combines the conceptual and detailed aspects of planning and integrates the activities of the commander, staff, subordinate headquarters, and other partners throughout the planning process. The MDMP helps leaders apply thoroughness, clarity, sound judgment, logic, and professional knowledge to understand situations, develop options to solve problems, and reach decisions. The MDMP results in an improved understanding of the situation and a plan or order that guides the force through preparation and execution."[3]

Army Doctrine Publication [ADP] 5-0, *The Operations Process*, and Army Doctrine Reference Publication [ADRP] 5-0, *The Operations Process*, 26 September 2011, serve as the primary references for the Army's planning and operations system. Red Team members must understand this planning process in order to know *how and when to influence the planning process*. Red Teams supports the wide range of operations across the spectrum of conflict and during all phases of an operation – from shaping to post-conflict stability and support operations.

Chapter VI provides Critical MDMP Questions on p. 109.

Mitigating Groupthink during the MDMP

There is a tendency for organizations, during the Design and the MDMP, to follow formalized procedures which can limit individual participation and lead to groupthink. With the groupthink mitigation recommendations in the paragraphs above, a Red Team can help the organization integrate the full potential of the staff and assist the organization in avoiding groupthink. The following are areas where integration of the mitigating techniques can be integrated in the Design and MDMP processes.

- The Design process, in itself, was developed as a collaborative activity; however personalities can force it down the groupthink path. Within an Operational Planning Team (OPT) the Red Team member can help the team leader overcome groupthink by using groupthink mitigating techniques such as *Team A / Team B Analysis* (p. 205), to help the group look at the problem from multiple perspectives. This will help the OPT Leader maximize all individuals in the group and allow more divergent viewpoints to emerge. Techniques such as *4 Ways of Seeing* (p. 76), *Alternative Future Analysis* (p. 80), *Shifting the Burden* (p. 184), *Stakeholder Mapping* (p. 186), and *TRIZ* (p. 208) can help the group elucidate the problem within steps 1-5 of the Design process, and bring greater participation by all members of the planning team. In smaller organizations, where there are no formalized/separate planning teams (Brigade Combat Teams, Battalions), the XO or Deputy Commander can use the techniques outlined above to avoid the closed-mindedness, self-censorship, and pressure to conform within normally extremely cohesive groups during the design process. Further, individuals in smaller organizations could have a tendency to view problems in a more limited fashion, given the possible commonality of the staff's background. The groupthink mitigating techniques will help the XO/Deputy Commander facilitate the staff in looking at the problem in a broader framework during the design process.
- The MDMP process is one of the most formalized and systematic processes that the U.S. Military uses on a habitual basis. Units have a tendency to conduct the MDMP in a systematic, and in some cases, a lock step approach to produce a decision or an order for execution. This formalized approach to decision-making lends itself to many aspects of groupthink, to include limited COAs, using information that only supports the group's COAs and decisions, lack of outside input from SMEs, self-censorship, mind guards, and ethnocentrism towards the

enemy. The groupthink mitigating techniques helps organizations make the MDMP more dynamic by using the full potential of the personnel in the OPT or staff. During steps 1 and 2 of the MDMP the leader of the OPT or staff can use similar mitigating techniques (*4 Ways Of Seeing* p. 76, *Shifting the Burden* p. 184, *Stakeholder Mapping* p. 186) as in the design process to frame and explore all aspects of the problem more fully. During the COA development the OPT/staff can use the divergence-convergence thought process to develop a broader range of COAs. *Brainstorming* (p. 89) is particularly helpful for expanding the group capability to develop multiple COAs. During the COA war-gaming and COA decision mitigating techniques such as *5 Will Get You 25* (p. 78) and *Dot Voting* (p. 148), can help the OPT/staff narrow and refine the COA options. Once the COA is decided upon by the commander, the OPT/staff can continue to improve and refine the selected COA by using *Troika Consulting (Ad Agency)* (p. 209), again giving the group a collective stake in developing the best possible COA for the organization. All the groupthink mitigating techniques outlined above will help organization execute more comprehensive decision-making, while providing for the fuller use of the greater potential of the OPT/staff as a whole.

Red Teaming During Planning

The commander/chief of staff's guidance, available time, and size of the team will influence the tasks to be completed.

- Red Teams should participate at each phase in the planning process—often without overt intervention and largely remaining in the background.
- Red Teams should avoid briefing in staffing meeting or open forums.
- The Red Team's communication skill and finesse will determine their effectiveness in the planning process.

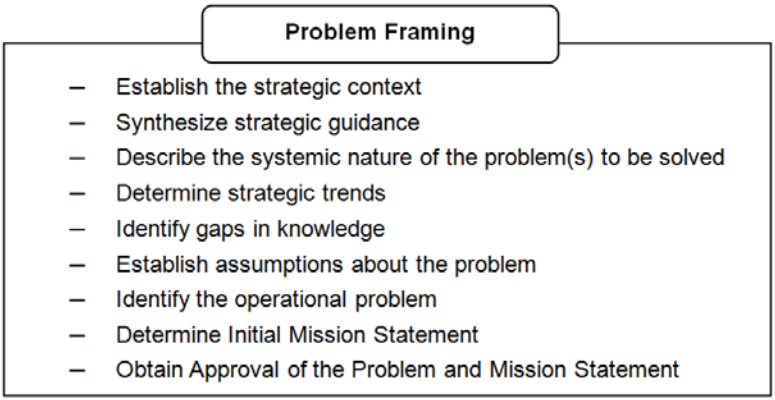
- Identify unseen opportunities, alternatives, gaps and vulnerabilities, and threats to the friendly courses of actions that may generate development of additional branches and sequels not previously considered—determines the Red Team's "value added."
- Timely and tailored Red Team input to the staff and the commander avoids having them move backward in the planning sequence. Early engagement is paramount.
- The echelon, size and expertise of the team, time, and the information available influences the scope of the effort and ability of the Red Team to support the planning process.
- Discuss and consider Red Team inputs at the lowest appropriate level in order to resolve, discount, or incorporate them into the plan.
- Items discounted by the staff but determined as critical to the success of the mission by the Red Team Leader should be elevated–first with the individual staff member, followed by the primary staff member, the Chief of Staff, and ultimately to the Commander (if required).

Red Teaming During Problem Framing

This section contains key ideas and questions to assist Red Teams during problem framing. Below are concepts and several key questions for the Red Team in the design process.[4] Problem framing establishes an initial hypothesis about the character of the friendly, adversarial, and wider environmental factors which define the situation. Problem framing also explores cultural narratives, institutional histories, propensities, and strategic trends in order to postulate a general structure of the factors and their relationships. This hypothesis will be incomplete at first, but will provide a basis from which the commander can visualize the design of his campaign and begin operations to uncover the true nature of the problems. The hypothesis thus defines

the art of the possible, warns what may be unachievable, and anticipates how the situation might evolve.

The art of framing the problem is the art of seeing the essential and relevant among the trivial and irrelevant; penetrating the logic of the broad received mission and its messy contextual situation; and reshaping it into a well-enough structured working hypotheses. It requires commanders to inquire into the nature or character of the factors—friendly, opposing, and the larger environmental—which define the situation into which his command will operate. The figure below refers to the strategic level but the steps are equally applicable to the operational and tactical levels of war.



1. Establish the strategic context. Context establishes the reasons why the problem came to exist, its history, and

how it may develop. Consider and define both the domestic and international context:

- political and/or diplomatic long- and short-term causes of conflict
- domestic influences, including public will, competing demands for resources, and political, economic, legal, and moral constraints
- international interests (reinforcing or conflicting with U.S. interests, including positions of parties neutral to the conflict), international law, positions of inter-governmental organizations, and other competing or distracting international aspects of the situation.

When considering the strategic context, the commander should consider the following questions:

(a) What is the history of the problem? What is its genesis?

(b) Who are the parties interested in the problem

(c) What are the implications of likely outcomes?

(d) What caused the problem to come to the fore?

(e) Why is this emerging problem important to the nation's strategic leaders? Determine how they "see" the problem. For example:

- Are national interests and ideals at stake?
- What are the economic considerations of action?
- Are there treaty obligations that require or block the ability to act?

2. Synthesize strategic guidance: must identify logical boundaries for the problem by establishing its essential relationship to the nation's strategic aims.

- Do the currently tasked strategic aims/objectives vary with previously established policy and objectives? If so, why?

- What policy objectives or statements serve as potential limitations to meeting current strategic guidance?
- Determining the desired strategic ends. What strategic aims define the strategic conditions that constitute success?
- Determining the expected outcomes in terms of time and resources.

3. Describe the systemic nature of the problem. Key components include:
   - Defining the factors, constituents, and relationships, bearing on the problem.
   - Consider the relationships from the points of view of the constituents:
   - Friendly forces, organizations, and entities.
   - Adversaries and those opposed.
   - Neutrals: both with and without interests relative to the problem at hand.
   - Unknowns: those with clear interests and influence but whose intentions are unknown. Consider using *4 Ways Of Seeing* (p. 76) and the *Cultural Perception Framework* (p. 122).
   - Defining the interests and strategies of each constituent, as they understand them, and how they relate—positively and/or negatively—to one another, as well as to those of the U.S. Government.
   - Defining/synthesizing the problem in terms of its constituents' systemic components:
     - How are the constituent parts of the problem related and influenced in terms of capabilities, interests, and intent, from the perspective of culture, politics, social infrastructure, economy, military power, and information?

- What are the power groups and functional components of these systems?
- How do these systems relate to one another? Are there relationships to the constituent's strategic outlook?
- How do these systems sustain themselves?
- Describing the tensions in these relationships and identify opportunities for exploitation, positively or negatively, during the conduct of the campaign.

4. Determine strategic trending. This activity involves describing how the strategic situation might evolve over time. What are the possible "futures" that could unfold based on current understanding? Consider using *Alternative Future Analysis* (p. 80).
5. Identify gaps in knowledge.
6. Establish assumptions about the problem.
7. Identify the operational problem. Based on the tasks above, the commander must identify the critical factors of the problem in order to satisfy strategic aims or objectives. Binding the problem this way requires the commander to distill the essential components from the broad set of factors bearing on the problem to focus the command's efforts to achieve the best effect.
8. Determine initial mission statement.
   - Express the mission in terms of who, what, when, where, and why (purpose).
   - Frame the mission with a clear, concise statement of the essential task(s) and the purpose(s).
9. Obtain approval of the problem and mission statements. The final task in framing the problem requires the commander to obtain approval of the problem statement, the rationale for the development of the problem

statement, and the initial mission statement from his superior.

Conduct mission analysis after you frame the problem and the commander obtained approval of the mission statement. Unlike the traditional mission analysis described in the military decision making process—this mission analysis is just that—an analysis of the mission. This process does not result in a restated mission as the mission has been approved as a result of framing the problem.

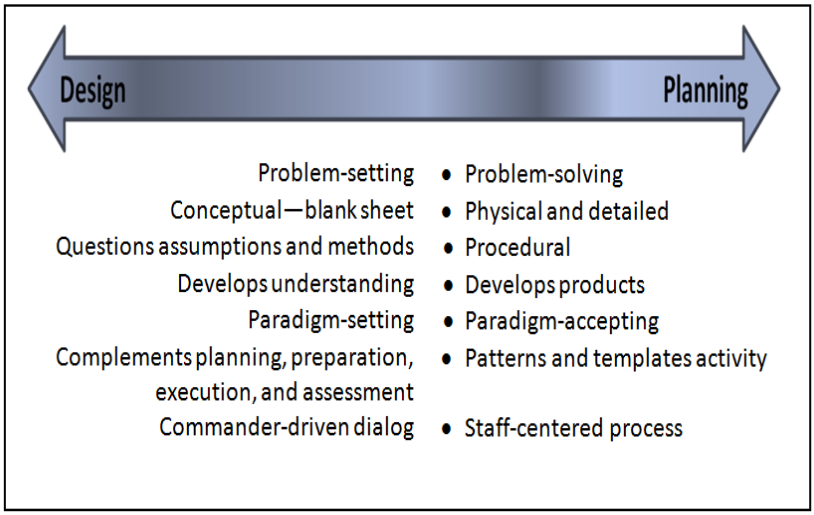
Red Teaming During Operational Design

Design is embedded in Joint and Army doctrine. Army Doctrine Reference Publication, ADRP, 5-0, *The Army in Unified land Operations*, states:

> "The Army design methodology is a methodology for applying critical and creative thinking to understand, visualize, and describe problems and approaches to solving them. The Army design methodology is particularly useful as an aid to conceptual thinking about unfamiliar problems."[5]

When contemplating unfamiliar problems, design aids the commander's visualization of the problem, the initial understanding of the OE, and provides the foundation for the commander's initial intent statement or planning directive.

A key element of design is the collaboration among commanders and their design teams to determine and frame the problem and visualize potential solutions (as illustrated below). A Red Team or the use of red teaming techniques reinforces the effort to frame the correct problem.

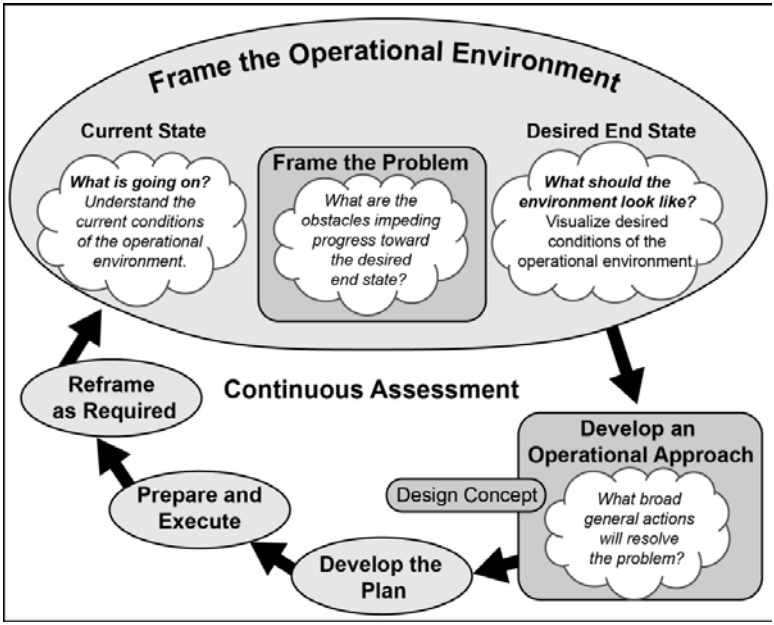


The Red Team's Role

- The Red Team should be represented in the execution of Army Design Methodology (ADM), either as a core

member or by providing critical reviews of the final product of the design.

- Red Teams are an integral part of a critical and creative thinking process about unique situations.
- Red Teams assist the commander and staff to visualize the problem and describe an approach to solve it.
- Red Teams help the design team to capture all perspectives and provide alternative perspectives about the problem.
- Red Teams propose solutions from various perspectives, to include the adversary, partner, and others in the OE.
- Take a breath, step back and to the side, and see what your frame prevents you from seeing.
  Use the divergence-convergence model.



Summary

In the process of decision-making, the group's need to rigorously consider alternatives is at tension with the social pressures to conform to group's norms. Hence, avoiding the lure any 'groupthink' is a penultimate chore in the quest for good decisions. The symptoms of groupthink are observable and groupthink can be mitigated.

To mitigate groupthink, apply the techniques referenced in Chapters V and VI of this handbook, like *Brainstorming*, *Dot Voting*, *My 15%*, and *Troika Consulting (Ad Agency)*. These techniques: eliminate attribution, allow every participants to contribute without the fear of being judged by others, and intercede dynamics [tangential to the process] that might detour the group from its best productivity.

A Red Team or the use of red teaming techniques reinforces the effort to reaching a good decision. The Red Team can have a role in: problem framing, operational design methodology, the MDMP, etc. Moreover, there are rules of thumb for planning sessions.

Endnotes

[1] Carl Von Clausewitz and Michael Howard, *On War,* (Princeton, N.J.: Princeton University Press, 1984), 119.

[2] All quotations in these paragraphs are drawn from Irving, Janis, *Groupthink*, (Boston, MA: Wadsworth Publishing, 1982), 9-10, 13, 174, 262-265 respectively.

[3] Army Doctrine Publication 5-0, The Operations Process, 9.

[4] This is an extract of TRADOC Pam 525-5-500, Commander's Appreciation and Campaign Design, Version 1.0, 28 Jan 08. We deleted certain passages and questions. We retained the most essential ones. http://www.tradoc.army.mil/tpubs/pams/p525-5-500.pdf.

[5] Army Doctrine Publication 5-0, *The Operations Process*, (26 September 2011), 9.

CHAPTER VI: Red Teaming TTP

(Tactics, Techniques and Procedures)

1-2-4-Whole Group

This process is a good way to get a rich conversation and more ideas by using small groups. It involves the principle of pre-commitment, critical thinking, and the clear expression of thought.

Method

One: Individual reflection and pre-commitment. Give participants a short amount of time to reflect on a question or issue. You may use a common issue or have each person choose their own issue. Have them write down their thought or position on the issue. To write is to think again. By writing the participants are pre-committing to their ideas without external influence. Encourage the participants to use the framework of State, Elaborate, Exemplify, and if possible, Illustrate (SEEI). For example, "Here's what I think, here is what I mean by that, let me give an example, and here is a graphic illustration (or analogy)." If you can complete all these steps, you have thought through a problem completely.

Twos: Have the participants find another person and share their ideas. Record any new thoughts or insights.

Small Groups: Invite each of the pairs to join up with another pair to briefly share their issues and any insights gained. Then share observations of the quality of each pair's examination of their issues. How were the issues framed? What was missing from the explanation? Were there biases detected?

Whole Group: Invite everyone back into the whole group. Ask an open question like "What insights emerged from your conversations? What did you learn? How has your understanding/view of the issue changed?" Lastly, ask "What's your 15% of the problem?"

Example

“Most people have about 15-percent control over their work situations. The other 85 percent rests in the broader context, shaped by the general structures, systems, events and culture in which they operate. The challenge rests in finding ways of creating transformational change incrementally: By encouraging people to mobilize small but significant "15-percent initiatives" that can snowball in their effects. When guided by a sense of shared vision, the process can tap into the self-organizing capacities of everyone involved.”

- Gareth Morgan, The Globe and Mail[1]

It doesn’t matter if you’re a General or an enlisted soldier, a senior executive or a member of the team. You still have only your 15 percent. Where do you have freedom to act? What’s in your 15%?

This conversation works very well using the Troika process. Grow from small groups (1 on 1) into larger groups and exchange group representatives. This is a great way to get into a rich conversation with small groups. The steps are:

1. Prepare: Position an issue or problem into one straightforward question.
2. Reflect individually: Give participants two minutes of silence to reflect on the question. They may close their eyes, jot a few notes, etc.
3. Share in pairs: Ask participants to stand, find a partner, and share both ideas in 10 minutes. They may pick the nearest person or move around to mix.
4. Gab in groups: Ask each pair to partner with other pairs in groups of 4-6 for 10 minutes. Suggest that they begin with each sharing items of interest from the previous round and then move to converse as a group.
5. Harvest in whole: Ask everyone back to a ‘whole group’ for 10 minutes. Open with, “What insights emerged from your conversation?” or “How has your understanding/ view of the issue changed?”

1 on 1, 2 on 2, Exchange Emissaries

In this method members of the team are asked to think about ways to address the problem before the group.

1. They first spend time thinking and writing down their ideas.
2. Next, the members form into pairs and exchange ideas. Two groups of two each form a group of four and exchange the ideas each group developed both individually and as a group of two.
3. Each group of four selects a spokesperson for the group. After each group has had sufficient time to explore their options to address the problem, they send their spokesperson to another group of four that addressed the same problem and in turn welcome the spokesperson from the other group to their group.
4. Each spokesperson (emissary) provides the group they have joined a description of the ideas developed by the group they are representing. After they are finished, the group they have joined tries to add to or improve the ideas brought to them by the emissary. After this exchange, the emissary returns to his/her group.
5. Upon return, the emissary shares the feedback from the group visited. In turn, the emissary's group informs him/her of their exchange with the other group's emissary.
6. This concludes with a group out brief of the issue.

4 Ways of Seeing

Examining the situation using the Four Ways of Seeing may show the challenges you face:

1. How you view yourself, your unit, the mission, etc.
2. How the adversary (or indigenous people) views himself; his cause, unit mission, etc.
3. How you view the adversary (or indigenous people)
4. How the adversary (or people) views you
5. Identify disconnects between steps 1 & 4, 2 & 3. These are critical points that analysis and planning must address

Thorough research should be conducted to complete the analysis of these perceptions. It is more complex than the simple model implies, for several reasons:

How X Sees Itself	***How X Sees Y***
How Y Sees Itself	***How Y Sees X***

- Seldom, if ever, will there be only two actors in the system under study.
- All the actors' perceptions and inter-relationships within the system must be considered in order to provide context for the analysis.
- How each actor perceives and defines the OE, legitimate targets and acceptable weapons must also be considered.
- It must be realized that all actors hold values, beliefs, and perceptions that they view as right and rational.
- Perceptions of the external audience(s) to whom we and our adversaries are playing cannot be discounted.

5 Whys

The 5 Whys is a question-asking technique used to explore the cause-and-effect relationships underlying a particular problem. The technique is used to determine the root cause of a defect or problem symptom. However, the process can be used to go deeper to explore questions related to purpose rather than problems.

Method: Pick an issue or pose a question and ask participants to think about it for at least a minute. Pair up or form a small group and choose one person to state their thoughts on the issue. Each participant gets a turn in this role of explaining their thoughts and position on an issue of their choice.

The role of the others in the group is at first to be active listeners. Let the speaker complete their thoughts; do not interrupt for clarification or any other purpose. Once the speaker is done, ask “why?” at least five times, e.g., “Why is that important? Why should my staff section care about that? Why should resources be applied against that effort now?”

You don’t need to stop at 5 whys, several “what” and “who” questions should arise as a result, like “what should do we do now? What are the implications of what is suggested? Who else needs to know?”

It is important to begin with “why” questions. The answers to “why” questions get at causal links behind events and problem symptoms. “What” questions tend toward simple data collection, and are subject to confirmation biases.

5 Will Get You 25

This is a method to tap into the wisdom of the crowd. This is not recommended to make a decision. It is a way to get feedback you might not otherwise get from your staff. *5 Will Get You 25* and *Dot Voting* are two methods of weighted anonymous feedback.

Method

Distribute file cards to everyone. Pose a question: (i.e., *What is the single greatest obstacle to implementation of plan/concept/policy X?*)

Ask the participants to think about it and write their best idea as clearly and in as few words as possible on the card –- a bullet, not an explanation.

When everyone has completed their card, invite the participants to stand up, mill around, and pass the card to someone new. Repeat the process until told to stop, and then each participant reads the card they hold. On the back, rate the idea from 1 to 5; 5 is brilliant, 1, not so much.

Once you grade the card, repeat the process. No one should grade their own card. Emphasize the participants must read the reply without turning the card over and viewing previous scores so they are not influenced.

Repeat the process five times, in five rounds. By round five, each card should have five ratings on the back of the card. Add them up.

Ask “Does anyone have a card with a score of 25…24…23…until you get a “yes.” Ask that person to read the card aloud and record the reply on a piece of butcher paper. Continue with the countdown until you get at least the top five replies.

6 Empathetic Questions

Questions [and difficulty] when looking empathetically from another's perspective:

1. It is difficult to appreciate another's problems.
   What are the "other's" problems?
2. It is difficult to feel another's pain.
   What is the nature of the "other's" pain?
3. It is difficult to understand another's ambitions.
   What are the "other's" ambitions?
4. It is difficult to internalize another's experience.
   What is the "other's" experience?
5. It is difficult to understand how our own actions appear to others.
   How do our own actions appear to "others?"
6. It is difficult to feel how threatened another may feel.
   Why does the other feel threatened?[2]

6 Words

Help people get to the core of an idea by writing a short phrase summarizing their thinking into a set number of words.

This idea is based on a complete short story written by Hemingway "For sale, baby shoes – never worn."

These 6 words communicate a huge degree of information and emotional content. This is an exercise in creating pithy bumper stickers that communicate in a visceral way and are memorable.

Alternative Futures Analysis

Systematically explores multiple ways a situation can develop when there is high complexity and uncertainty.

When to Use

This approach is most useful when a situation is viewed as too complex or the outcomes as too uncertain to trust a single outcome assessment. First, the Red Team must recognize that there is high uncertainty surrounding the topic in question. Second, they, and often their customers, recognize that they need to consider a wide range of factors that might bear on the question. And third, they are prepared to explore a range of outcomes and are not wedded to any preconceived result. Depending on how elaborate the futures project, the effort can amount to considerable investment in time, analytic resources, and money.

A team can spend several hours or days organizing, brainstorming, and developing multiple futures; alternatively, a larger-scale effort can require preparing a multi-day workshop that brings together participants (including outside experts). Such an undertaking often demands the special skills of trained scenario-development facilitators and conferencing facilities.

This technique is a sharp contrast to contrarian techniques, which try to challenge the high confidence and relative certitude about an event or trend. Instead, multiple futures development is a divergent thinking technique that tries to use the complexity and uncertainty of a situation to describe multiple outcomes or futures that should be considered, rather than to predict one outcome.

Value Added

This approach is useful in highly ambiguous situations, when analysts confront not only a lot of “known unknowns” but also “unknown unknowns.” What this means is that the Red Team recognizes that there are factors, forces, and dynamics among key actors that are difficult to identify

without the use of some structured technique that can model how they would interact or behave. Given the time and resources involved, scenario analysis is best reserved for situations that could potentially pose grave threats or otherwise have significant consequences.

Past experience has shown that involving policymakers in the alternative futures exercise is the most effective way to communicate the results of this exploration of alternative outcomes and sensitize them to key uncertainties. Most participants find the process of developing such scenarios as useful as any finished product that attempts to capture the results of the exercise. Policymakers and Red Teams can benefit from this technique in several ways:

- It provides an effective means of weighing multiple unknown or unknowable factors and presenting a set of plausible outcomes.
- It can help to bind a problem by identifying plausible combinations of uncertain factors.
- It provides a broader analytic framework for calculating the costs, risks, and opportunities presented to policymakers by different outcomes.
- It helps anticipate otherwise surprising developments by challenging assumptions and considering possible *wild cards* or discontinuous events.
- It generates indicators to monitor for signs that a particular future is becoming more or less likely, so that policies can be reassessed.

The Method

The most common method used in both the public and private sectors involves the following steps:

- Develop the “focal issue” by systematically interviewing experts and officials who are examining the general topic.

- Convene a group of experts (both internal and external) to brainstorm about the forces and factors that could affect the focal issue.
- Select by consensus the two most critical and uncertain forces and convert these into axes or continua with the most relevant endpoints assigned.
- Establish the most relevant endpoints for each factor; (e.g., if economic growth were the most critical, uncertain force, the endpoints could be “fast” and “slow” or “transformative” and “stabilizing” depending on the type of issue addressed.)
- Form a futures matrix by crossing the two chosen axes. The four resulting quadrants provide the basis for characterizing alternative future worlds.
- Generate colorful stories that describe these futures and how they could plausibly come about. Signposts or indicators can then be developed.

Participants can then consider how current decisions or strategies would fare in each of the four worlds and identify alternative policies that might work better either across all the futures or in specific ones. By anticipating alternative outcomes, policymakers have a better chance of either devising strategies flexible enough to accommodate multiple outcomes or of being prepared and agile in the face of change.

Analysis of Competing Hypotheses (ACH)

Identification of alternative explanations (hypotheses) and evaluation of all evidence that will disconfirm rather than confirm hypotheses.

When to Use

This is an effective technique when there is a large amount of data to absorb and evaluate. While a single analyst can use ACH, it is most effective with a small team that can challenge each other's evaluation of the evidence. Developing a matrix of hypotheses and loading already collected information into the matrix can be accomplished in a day or less. If the data must be reassembled, the initial phases of the ACH process may require additional time.

ACH is particularly appropriate for controversial issues when analysts want to develop a clear record that shows what theories they have considered and how they arrived at their judgments. Developing the ACH matrix allows other analysts (or even policymakers) to review their analysis and identify areas of agreement and disagreement. Evidence can also be examined more systematically, and analysts have found that this makes the technique ideal for considering the possibility of deception and denial.

Value Added

ACH helps analysts overcome three common mistakes that can lead to inaccurate forecasts:

- Red Teams can be susceptible to being unduly influenced by a first impression, based on incomplete data, an existing analytic line, or a single explanation that seems to fit well enough.
- Groups seldom generate a full set of explanations or hypotheses at the outset of a project.
- Groups often rely on evidence to support their preferred hypothesis, but which also is consistent with other explanations.

In essence, ACH helps Red Teams to avoid picking the first solution that seems satisfactory instead of going through all the possibilities to arrive at the very best solution.

The Method

Explicitly identify all the reasonable alternative hypotheses, then array the evidence against each hypothesis—rather than evaluating the plausibility of each hypothesis one at a time. To create a level playing field, the process must:

- Ensure that all the information and argumentation is evaluated and given equal treatment or weight when considering each hypothesis.
- Prevent individuals from premature closure on a particular explanation or hypothesis.
- Protect the individual against innate tendencies to ignore or discount
- Protect information that does not fit comfortably with the preferred explanation at the time.

To accomplish this, the process should follow these steps:

- Brainstorm among analysts with different perspectives to identify all possible hypotheses.
- List all significant evidence and arguments relevant to all the hypotheses.
- Prepare a matrix with hypotheses across the top and each piece of evidence on the side. Determine whether each piece of evidence is consistent, inconsistent, or not applicable to each hypothesis.
- Refine the matrix and reconsider the hypotheses—in some cases, individuals will need to add new hypotheses and re-examine the information available.
- Focus on disproving hypotheses rather than proving one. Tally the pieces of evidence that are

inconsistent and consistent with each hypothesis to see which explanations are the weakest and strongest.

- Analyze how sensitive the ACH results are to a few critical items of evidence; should those pieces prove to be wrong, misleading, or subject to deception, how would it impact an explanation's validity?
- Ask what evidence is not being seen but would be expected for a given hypothesis to be true. Is denial and deception a possibility?
- Report all the conclusions, including the weaker hypotheses that should still be monitored as new information becomes available.
- Establish the relative likelihood for the hypotheses and report all the conclusions, including the weaker hypotheses that should still be monitored as new information becomes available.
- Identify and monitor indicators that would be both consistent and inconsistent with the full set of hypotheses. In the latter case, explore what could account for inconsistent data.

Argument Deconstruction

When to use

Use the argument deconstruction framework when posed with an oral or written argument that requires critical thinking.

Value added

Deconstructing arguments without a framework can lead to insufficient challenging of opinions, value conflicts, statistics, alternative causes and conclusions, and the implications of accepting the argument posed. Critical thinking emphasizes the need to be thorough and systematic, which the argument deconstruction framework facilitates.

The Method

- What is the argument?
  - Argument =
    Issue (or premise, or thesis) + Reasons + Conclusion
  - Premise: a proposition supporting or helping to support a conclusion; a proposition antecedently supposed or proved; something previously stated or assumed as the basis of further argument; a condition; a supposition.
  - Thesis: a proposition stated or put forward for consideration, esp. one to be discussed and proved or to be maintained against objections; an affirmation, or distinction from a supposition or hypothesis
    - ✓ Is the right problem defined?
    - ✓ Is there any use of vague or ambiguous words?
    - ✓ What is the author's point of view?
- Are there any value conflicts?
- Are there any *prescriptive* assumptions? (Statement by author of the way things *should* be, is it a good assumption?)

- Are there any *descriptive* assumptions? (Statement by author of the way things *are*—is it a good assumption?)
- Are there any fallacies in reasoning?
- Does the author use any heuristics (a simplifying strategy, or "rule of thumb") to lay out his information/make his case? (The devil is in the details…)
- How good is the evidence? Does the author use or rely on
    - ✓ Intuition?
    - ✓ Personal experience?
    - ✓ Testimonials?
    - ✓ Appeal to authorities?
    - ✓ Personal observation?
    - ✓ Research studies?
    - ✓ Analogies? (Is the analogy apt?)
- Is there a rival cause? Are there other plausible hypotheses (than the author suggested) which might explain what happened? What are they? Some other way to explain the evidence (reasons) and conclusion?
- Are statistics used?
    - o Are they deceptive?
    - o Use numbers without percentages?
    - o Use percentages without numbers?
- Is there any significant information which is omitted? (Where is the dog that *isn't* barking?)
- Is there any other reasonable conclusion you can draw from the evidence?
- What are the implications of *accepting* the argument?

BATNA

“What is your BATNA – your Best Alternative To a Negotiated Agreement? That is the standard by which any proposed agreement should be measured. That is the only standard that can protect you both from accepting terms that are too unfavorable and from rejecting terms it would be in your best interest to accept.

Your BATNA not only is a better measure but also has the advantage of being flexible enough to permit the explorations of imaginative solutions. Instead of ruling out any solution that does not meet your bottom line, you can compare a proposal with your BATNA to see whether it satisfies your interests.[3]

Develop your BATNA. Vigorous exploration of what you will do if you do not reach agreement can greatly strengthen your hand. Attractive alternatives are not just sitting there waiting for you; you usually have to develop them. Generating possible BATNAs requires three distinct operations: (1) inventing a list of actions you might conceivably take if no agreement is reached; (2) improving some of the more promising ideas and converting them into practical alternatives; and (3) selecting, tentatively, the one alternative that seems best.[4]

Consider the other side’s BATNA. You should also think about the alternatives to a negotiated agreement available to the other side. The more you can learn of their alternatives, the better prepared you are for the negotiation. Knowing their alternatives, you can realistically estimate what you can expect from the negotiation.

Having a good BATNA can help you negotiate on the merits. You can convert such resources as you have into effective negotiating power by developing and improving your BATNA. Apply knowledge, time, money, people, connections, and wits into devising the best solution for you independent of the other side’s assent. The more easily and

happily you can walk away from a negotiation, the greater your capacity to affect its outcome.[5]

Developing your BATNA thus not only enables you to determine what is a minimally acceptable agreement, it will probably raise that minimum. Developing your BATNA is perhaps the most effective course of action you can take in dealing with a seemingly more powerful negotiator."[6]

Brainstorming

Brainstorming is an unconstrained group process designed to generate new ideas and concepts.

When to Use

A technique for stimulating new thinking and it can be applied to virtually all of the other structured analytic techniques as an aid to thinking. Typically, Red Teams will brainstorm when they begin a project to help generate a range of hypotheses about their issue.

Brainstorming, almost by definition, involves a group meeting to discuss a common challenge; a modest investment of time at the beginning or critical points of a project can take advantage of their different perspectives to help structure a problem. This group process allows others to build on an initial idea suggested by a member of the brainstorming session.

Value Added

This technique can maximize creativity in the thinking process, force Red teams to step outside their normal mind-sets, and suspend their typical "good judgment" about the practicality of ideas or approaches. More generally, brainstorming allows organizations to see a wider range of factors that might bear on the topic than they would otherwise consider. Brainstorming gives permission to think more radically or "outside the box."

In particular, it can spark new ideas, ensure a comprehensive look at a problem or issues, raise unknowns, and prevent premature consensus around a single hypothesis.

The Method

Paradoxically, brainstorming should be a very structured process to be most productive. An unconstrained, informal discussion might produce some interesting ideas, but usually a more systematic process is the most effective way to break down mind-sets and produce new insights. In particular, the process involves a divergent thinking phase to generate and collect new ideas and insights, followed by a convergent phase in which ideas are grouped and organized around key concepts. Some of the simple rules to be followed include:

- Never censor an idea no matter how unconventional they might sound.
- Rather find out what prompted the thought, as it might contain the seeds of an important connection between the topic and an unstated assumption.
- Give yourself enough time to do brainstorming correctly. It usually takes one hour to set the “rules” of the game, get the group comfortable, and exhaust the conventional wisdom on the topic. Only then will the truly creative ideas begin to emerge.
- Involve at least one “outsider” in the process—that is, someone who does not share the same educational background, culture, technical knowledge or mindset as the core group but has some familiarity with the topic.

A two-phase, twelve-step, structured process is often used to get the most out of the brainstorming sessions

Divergent Thinking Phase:

- Typically, 10-12 people work best.
- Pose the problem in terms of a "focal question." Display it in one sentence on a large easel or whiteboard.
- Ask the group to write down responses (as many as they can think of) to the question.
- Go sequentially around the room, with each individual giving one idea at a time. Write down the ideas up on the whiteboard. No judgments concerning the ideas are voiced at this time. Continue going around the room until each individual's ideas are exhausted.
- The individuals conducting the brainstorming exercise then will group similar ideas together, forming similar ideas into categories.

Convergent Thinking Phase:

- The individuals conducting the brainstorming exercise then will group similar ideas together, forming similar ideas into categories
- The group can then check/discuss each idea for feasibility as a solution to the problem.
- Assess what the group has accomplished in terms of new ideas or concepts identified or new areas that need more work or further brainstorming.
- The brainstorming group can then use other techniques, such as Dot-voting, to further narrow the field of ideas.

Challenges to Effective Planning

1. Background: Working in groups, especially in the planning process, is fraught with challenges. From an individual perspective, intuitive reasoning often fails under conditions of uncertainty, time pressures and cognitive bias. From an organizational perspective, group structure and conformity can also lead to suboptimal judgments and decision making. This section describes some of the variables and common challenges found in the planning process and what can be done to prevent, mitigate them and improve planning performance.

    a. In addition to exploring alternatives in plans, operations and concepts, Red Teams help commanders and staffs identify and understand flawed organizational processes that contribute to potential errors in planning and decision making.

    b. From an organizational perspective, Red Teams not only provide mitigation and prevention tools but also contribute to improved performance through the use of liberating structures and structured analytical tools. These tools and methods are group combat multipliers that should augment conventional methods such as staff planning meetings and presentations.

2. Factors affecting the planning process: A number of factors can contribute to planning errors, poor decisions and outcomes to include:

    a. Group cohesion and the pull toward conformity: A cohesive staff is a force multiplier but cohesion can exert pressure for group conformity which can lead to the phenomena of groupthink (see Introduction). Excessive conformity stifles professional dissent because hierarchy and relationships are more valued than critical analysis and decision outcomes. If group activity is structured to mitigate hierarchy and conformity, then members are likely to provide feedback and insights that expose invalid

assumptions, ill-conceived plans or flawed courses of action. Red Teamers are trained to interact with the staff to enable structured discussion that balances cohesion with groupthink mitigation. Simultaneously, Red Teams must support the dynamics of staff interaction and avoid 'paralysis by analysis.'

b. Strong directive leadership: Strong leaders under time pressure may direct a course of action thereby limiting options for staff consideration. Doctrine cautions leaders to avoid directing a course of action early in planning process that prevents the staff in identifying other appropriate alternative courses of action.

c. Cognitive biases and heuristics: Research conducted over the past three decades indicate that people are prone to systemic errors in judgment and decision making in predictable ways.[7] These errors are associated with heuristics and biases of our cognitive processes in the context of judgment and decision making. Cognitive biases result in suboptimal actions and beliefs and are generally related with intuitive thinking.[8] Manifestations of these biases in intuitive thinking, are found in heuristics formally defined as, "…a simple procedure that helps find adequate, though often imperfect answers to difficult questions."[9] In high risk, uncertain and complex environments, these imperfections are costly and warrant prevention and mitigation.

d. Relationship and task conflict: Conflict between group members is bound to occur due to difference in leadership styles, personalities, interests and personal agendas. However, not all conflict is bad. Research indicates that "moderate amounts of task conflict (i.e. differences of opinion about the task and how it should be completed) are necessary and valuable for group decision making processes in preventing groupthink. However, relationship conflict in which personal

differences are attacked can distract the group from its purpose and objectives.[10] (see Chapter II)

e. Time constraints and lack of preparation: No matter how cohesive the group, inadequate planning time, inexperience in the operational environment, lead to poor situational understanding and development of flawed plans. Poor preparation and organization for planning further encumber the commander and staff in producing useful and timely plans and orders.

f. Organization for planning: Factors such as a poorly designed physical space and a lack (or excess) of planning standing operating procedures can stifle productive discussion, increase staff friction and hamper effective staff coordination. Poor Information management (e.g., inaccurate or incomplete displays of visualization and dissemination of information) can contribute to a lack of shared situational understanding and degrade staff interactivity.

3. Planning challenges: Many of the variables above manifest themselves in dysfunctional group behaviors that lead to poor planning and decision making outcomes. Red Teams assist the commander and staff in identifying and mitigating these challenges. If left undetected dysfunctional group behaviors may result in bad decisions, lost opportunities, and increased vulnerabilities for the unit. These challenges include:

   a. Complacency: In planning, this often takes the disguise of “we’ve always done it this way” mentality. In a complex environment, the dilemma is to adapt based on prior experience of what works in one situation to another situation. The challenge is understand when continuity and change are decisive and when to discard principles, tactics and strategies that governed past success. As Major Tim Karcher notes in *Understanding the Victory Disease*, the attitude among some staffs could be:

(1) "Why change what has worked in the past?" The greatest danger when using established patterns lies in the enemy's reaction. Setting a pattern is fine as long as the enemy follows with his own patterns and reacts in a predictable fashion. A considerable danger occurs, though, when the enemy deviates from his normal reaction, placing the friendly force at a significant disadvantage and causing the supposed recipe for success to turn into a recipe for failure." [11]

(2) Situations in the OE often change after completion of deliberate planning (e.g., MDMP) but the unit continues executing its' original plan. This behavior is often characterized as "fighting the plan and not the enemy." The staff may adhere to inadequate plans and orders due to the investment in time, pride in ownership, and time. New evidence disconfirming assumptions and tactics may emerge in the interim where new strategies and tactics provide more appropriate solutions to the mission. Red Teams should assist commanders, staff and planning teams in questioning strategies, tactics and plans that claim to be the only solution to a problem when the situation indicates otherwise.

(3) The Red Team's challenge is to help the staff think about "what's next" or "what could potentially occur" – balancing realism with imagination. Red Team tools designed to mitigate complacency are *Alternative Futures Analysis* (p. 80), *Analysis of Competing Hypotheses* (p. 83), and *Shifting the Burden* (p. 184).

b. Mirror Imaging: Richards J. Heuer, who spent 45 years in the CIA working in collection operations, counterintelligence, intelligence analysis, and personnel security, views mirror imaging as "…filling gaps in the analyst's own knowledge by assuming that

the other side is likely to act in a certain way because that is how [your country or organization] would act under similar circumstances."[12] Mirror imaging occurs when you apply your attitudes about trends, capabilities, beliefs, culture onto another. Many American policy makers and analysts fell into this trap during the planning for Operation Iraqi Freedom (OIF). As noted in the report on the miscalculation of Iraqi WMD capabilities, it noted:

(1) "Analysis of Iraq's weapons programs took little account of Iraq's political and social context. While such a consideration would probably not have changed the Community's judgments about Iraq's WMD, the failure even to consider whether Saddam Hussein had elected to abandon his banned weapons programs precluded that possibility.

(2) It seems unlikely to us that weapons experts used to combing reports for tidbits on technical programs would ever have asked: "Is Saddam bluffing?" or "Could he have decided to suspend his weapons programs until sanctions are lifted?" But an analyst steeped in Iraq's politics and culture at least might have asked those questions, and, of course, those turn out to be the questions that could have led the Intelligence Community closer to the truth."

(3) The culture and objectives of others nations and other transnational groups differ from ours. Our assumptions, assessments, and estimates of adversary courses of action need to account for these differences.

(4) While working to avoid mirror imaging American intentions, motivations, thought processes, and capabilities to the enemy. It is just as important

not to apply mirror imaging to partners and others within the operational environment.

(5) Using *4 Ways of Seeing* (p. 76) and *Stakeholder Mapping* (p. 186) are ways to mitigate and prevent mirror imaging.

c. Ethnocentrism: Unlike mirror imaging, this error recognizes the existence of adversary and partner cultural differences but perceives these differences with contempt, disdain and in many cases out of context. Ethnocentrism is "…using the practices of your own 'people' as a yardstick to measure how well the customs of other, different peoples measure up."[13] A common tendency of most individuals is to view one's culture and customs as inherently superior to others. This can lead to a condescending attitude toward other cultures that breeds arrogance. Contempt and arrogance contribute to overconfidence by underestimating the capabilities and motivations of others. One historical example:

(1) "At the tactical level, the 7th Cavalry displayed remarkable overconfidence, clearly demonstrated by how Custer viewed his Indian adversary. During the 1868 Battle of the Washita, when a subordinate speculated they might find more Indians than they could handle, Custer reportedly said, "There are not enough Indians in the country to whip the Seventh Cavalry."[14] Custer's conceit seems to have trickled down to his subordinates, causing them to also believe in their indestructibility."[15]

(2) The challenge for the commander and staff is to understand the culture of the adversary, as well as our partners and others. Then staffs must apply this understanding to the assumptions made and the assessments created.

(3) See Chapter III for a discussion of interpreting, understanding and analyzing cultures and mitigating the effects of ethnocentrism.

d. Mindsets / Patterns of Expectation: Perception is not a passive process that allows us to objectively view the world 'as it is'. Richards J. Heuer notes that, "…experiments have been conducted to show the extraordinary extent to which the information obtained by an observer depends upon the observer's own assumptions and preconceptions." The human brain is designed to 'fill in the blanks' based upon our individual, cultural and social experience. Heuer states, "We tend to perceive what we expect to perceive." In other words, our mission; organizational climate; culture; self-interest; assumptions; prejudices; doctrine; and attitudes influence our thinking. A mindset is a "summation or consolidation of all of our biases about a particular subject."[16]

(1) As individuals receive new information and data, they perceive them in existing images governed by these factors. Continually asking, "What does this mean?" and, "How else can I perceive it?" can offer critical insights.

(2) The challenge is to understand when changes in the operational environment negate the usefulness of past patterns and trends for projecting future developments. Military history contains numerous examples of countries refuting past trends to field new dominating technology or concepts (e.g., development of carrier aviation and the concept of Blitzkrieg to defeat French stationary defenses).

(3) David C. Gompert and Richard L. Kugler note a classic case study of this failure to perceive change. They analyzed Lee's decision to order (on July 3, 1863, the 3rd day of the Battle of

Gettysburg), a frontal assault across a mile of open field against the strong center of the defending Union forces. The authors argue that Lee depended too much on his experience from previous battles such as at Chancellorsville. That when pressed, Union forces would collapse. Lee ignored the fact that the Union forces learned lessons from these battles. Lee underestimated their training and commanders. He ignored the latest information that a significant Union force was entrenched with significant reserves available.

(4) Another challenge of 'patterns of expectation' is when planners believe that "the future will be a linear continuation of the present."[17] This 'planning pitfall' is likely when planners believe their plan can dictate the future. A method for combating this tendency is to use the Premortem technique (p. 165)

e. Oversimplifying or Failure to Think and Decide 'Complexly': In problem solving simulations, cognitive researcher and author, Dietrich Doerner observed that "People court failure in predictable ways" based upon habits of thought that "set failure in motion from the beginning" [18] and an inability to think and decide more 'complexly.' Doerner contends that

- Failure develops gradually according to its own logic.
- When we fail to solve a problem, it is often due to several small mistakes. Small mistakes add up.
- Complicated situations elicit habits of thought that may not measure up to the demands of the system that is generating the problem.
- Apprehensions of failure encourage methods of decision making that may exacerbate the problem

(1) Doerner observed that 'bad' participants:

(a) Acted without prior analysis of the situation.

(b) Failed to anticipate side effects and long term repercussions.
(c) Assumed that the absence of immediately obvious negative effects meant that correct measures had been taken.
(d) Let over involvement in *projects* blind them to emerging needs and changes in the situation.
(e) Were prone to cynical reactions

(2) Good participants:

(a) Made more decisions per task and goal.
(b) Considered of not just the primary goal of any given measure but also its potential effects on other sectors of the system.
(c) Acted more 'complexly' – their decisions took different aspects of the entire system into account, not just one aspect.
(d) Recognized early where [the situation's] real problems lay and attacked them first.
(e) Tested their hypotheses - asked more 'why' than 'what' questions.
(f) Dug deeper in their analysis.
(g) Were interested in causal links behind events and the causal network.
(h) Did not lapse into 'ad hoc-ism.'
(i) Focused on right fields of endeavor and continued to focus on those fields over time.
(j) Were self-critical/ reflective and structured in thinking.

(3) The challenge for any staff is accounting for the myriad variables in a complex problem without oversimplifying the situation. This is even more difficult when planning under time constraints and when a staff lacks organization and integration, (e.g., staff elements and planning teams that "working in their own functional perspective and lanes").

(4) Red Teams can help staffs think more ‘complexly’ by employing Red teaming tools such as *1-2-4-Whole Group* (p. 73), *Shifting the Burden* (p. 184), and *Troika Consulting* (p. 209). Specifically, *Shifting the Burden* fosters close examination of underlying problem(s) and perspective(s) rather than dealing with symptoms manifesting themselves throughout a system.

f. Flawed (historical) or False Analogies: Webster defines analogy as “a form of logical inference, or an instance of it, based on the assumption that if two things are known to be alike in some respects, then they must be alike in other respects.” As one author noted, “When confronted with a novel challenge, the human mind reasons by analogy. We then become prone to reading the world in ways that reaffirm the choice we have made.”[19]

(1) When used successfully, analogies help make sense of a new situation, reduce complexity, and aid in the dialogue with others. However, analogies should be used with caution. Secretary of Defense Robert Gates, quoted American historian Gordon Wood that, “History does not teach lots of little lessons. Insofar as it teaches any lessons, it teaches one big one: that nothing ever works out quite the way its managers intended or expected.”[20]

(2) Decision makers often use history and historical analogies. In Richard Neustadt and Ernest R. May‘s, *Thinking in Time: The Uses of History for Decision Maker*, the authors highlight the challenge and potential errors of using history and historical analogy in decision making without understanding the details and context of events and the differences between the current and past situations (Determining the suitability of an Analogy, p143).

g. Hubris and Overconfidence. Flawed planning takes place when staffs are overconfident in their ability to predict the future, anticipating the actions of adversaries or the consequence of the effects of operations and tactical actions. Some scholars such as Nicholas Taleb contend that it is impractical to predict the future or understand the complexity of the situation. Taleb argues that the only real solution is to have planning systems in place that can react quickly to changes and events.[21]

(1) Overconfidence also stems from faulty reasoning in terms of "attaching high probabilities to low-frequency events" or base rate neglect.[22] Political scientist Philip Tetlock notes that political analysts often base probabilities on "…case-specific hunches about causality that make some scenarios more "imaginable" than others."[23] Tetlock follows that "A plausible story of how a government might suddenly collapse counts for far more than how often similar outcomes have occurred in the past."[24]

(2) The connection between faulty intuition and confidence in improbable but plausible arguments is emphasized in Taleb's notion of the "narrative fallacy." Taleb believes that people are "[vulnerable] to over interpretation and predilection for compact stories over raw truths. It severely distorts our mental representation of the world; it is particularly acute when it comes to the rare event."[25]

Summary: Effective planning in unique, novel, and uncertain situations is difficult. Red Teams help the commander, staff, and planning teams when their reasoning is flawed or when organizational processes impede sound planning. This chapter offers ways to prevent and mitigate challenges in planning and decision making processes. Red Teams must balance *intellectual distance* to observe and highlight potential errors in reasoning against being embedded in the organization as a contributor to the planning process.

Circle of Voices

Circle of Voices is a simple facilitation practice designed to equalize participation and teach students that listening, appreciating, and synthesizing are just as crucial to good discussion as is making brilliant original contributions.

Participants form small groups of five to six seated in a circle. They are given a minute or so in silence to think about what they have to say about an assigned topic. The discussion opens with one person having a period of uninterrupted “airtime” of no more than one minute. During this time the speaker may say whatever they wish about the topic at hand. While the person is speaking no interruptions are allowed. People take their turn to speak by going around the circle in order. This eliminates the stress of other participants having to decide when or whether to jump in, or for the speaker to worry about interruption before they can finish their thoughts.

After the initial *circle of voices* is complete, discussion opens for anyone to speak. The only restriction on this period of discussion is that participants are only allowed to discuss other person’s ideas that have already been expressed. Participants may not expand on their own ideas, only about their reaction to something already said. This prevents a tendency toward *grandstanding*.

Facilitation principles:

- Pre-commitment
- Everyone speaks once before anyone speaks twice.
- Active listening.
- Respectful engagement.

Circular Response

This is a great way to facilitate discussion participation, promote continuity of conversation, and to give people some experience in the effort required for respectful listening.

Participants form groups of six to eight, seated in a circle. They are given a minute or so in silence to think about their response to a discussion topic or question. The conversation begins with one person having a period of uninterrupted “airtime” of no more than one minute. During this time the speaker may say whatever they wish about the topic at hand. While the person is speaking no interruptions are allowed.

After the minute is up, first speaker yields the floor to the person on their left, and that person speaks for a minute. The second speaker is not free, however, to say anything they want. They must incorporate into their remarks some reference to the preceding speaker’s message, and then use this as a springboard for their own comments. This does not have to be an agreement; it may be an expression of dissent from the previous opinion.

After a minute, the second speaker stops talking, and the person on their left becomes the third discussant, following the same ground rules. Following this pattern the discussion moves around the circle. Once everyone has had the opportunity to speak, the floor is opened for unconstrained conversation.

The interesting thing about this facilitation technique is that the last person has no advantage over the second speaker. This is due to the last speaker not having the luxury of mentally rehearsing the perfect contribution because they have no idea what the person immediately before them is going to say until they speak.

Facilitation principles:

- Pre-commitment
- Everyone speaks once before anyone speaks twice.
- Active listening.
- Respectful engagement

Cognitive Biases

Cognitive biases are unconscious beliefs that condition, govern and compel our behavior. Examples include the following:

- Anchoring: Oftentimes, humans are unable to compute an item's true value. Instead, they resort to an overreliance upon an initial "anchor" value provided by someone else, and thereafter bias all subsequent value decisions relative to that initial "anchor."
- Status Quo Bias: Many humans find the status quo comfortable, and avoid changing it.
- Confirmation Bias: A trap that humans often fall into — we tend to look for evidence that supports the conclusion we've made prematurely, not realizing that evidence can often support *several* hypotheses. "No matter what we humans think about, we tend to pay more attention to stuff that fits in with our beliefs than stuff that might challenge them…"[26] In the process, inclined to "see what we expect to see," we actively dismiss evidence that contradicts our conclusion. It is this phenomenon that lends importance to the active search for *disconfirming* evidence: evidence that would disprove the conclusion we've formed.
- Sunk-Cost Bias (aka "Loss Aversion"): A bias in which humans increasingly persist in deciding and acting illogically, based upon decisions they made *previously*. This occurs despite the fact that the *present* context dictates deciding otherwise. Sunk-cost bias occurs because it relieves one of the necessity to admit that preceding decisions might have been made in error. It also may avoid incurring a permanent loss, at least in the short term. It is a *failure to cut bait*, to use a fishing metaphor.

- Framing Trap: The way we frame an issue affects the way we perceive it, and hence, affects a solution's potential options.
- Halo Effect: We tend to select that which we see as more attractive, regardless of actual capabilities or qualities. The opposite of the halo effect is the Pitchfork Effect: we tend to disregard (or put at the bottom of a list) that which we find *unappealing*.
- Narrative Fallacy: The human compulsion to turn a series of connected or disconnected facts into story or pattern; *inventing reality*. This is a human tendency to construe meaning in a completely random situation, where no meaning actually exists.[27]
- Self-Fulfilling Prophecy Bias: A term coined by Robert Merton in 1948. "The self-fulfilling prophecy is, in the beginning, a *false* definition of the situation evoking a new behavior which makes the originally false conception come *true*… the prophet will cite the actual course of events as proof that he was right from the beginning…"[28]

Common Logic Fallacies

Appeal to Emotions, or to Fear. The use of emotionally charged language to distract readers and listeners from relevant reasons and evidence.

Appeal to Popularity, or to the Masses. Occurs when an assertion is made that if something is good for everyone else, it must be good for you too. Marketing and advertisements usually make this claim.

Glittering Generality. The use of vague, emotionally appealing virtue words that dispose us to approve something without closely examining the reasons.

Appeal to Questionable Authority. Occurs when the authority we use to support the premises is actually the wrong authority for the issue at hand. It's akin to "hiding behind" someone/something famous, in the hopes that that alone will sell the argument.

Slippery Slope. Occurs when the conclusion of an argument rests upon an alleged chain reaction and there isn't sufficient reason to conclude that the chain reaction will actually take place.

Red Herring. Occurs when the author diverts the reader's attention with distracting information that is flashy, eye-catching, and generally not relevant to the topic at hand.

Straw man. Stacking the deck by distorting an opponent's point of view so that it is easy to attack; thus we attack a point of view that is weak, irrelevant, or does not truly exist.

False Dichotomy. Occurs when someone presents a complex situation in black and white terms (i.e., they only present two alternatives where many exist). The logic fault here is that there is much more to the argument than the watered-down version presented. Rather than allow watered-down arguments, critical thinkers must think divergently to determine the best possible set of options.

Ad Hominem. Occurs when someone tries to attack a person, and not a position or argument.

Begging the Question. An argument in which the conclusion is sneaked into the premises. “Accept this as true: the premise from which it comes is true!” A fallacy of deductive reasoning.

Hasty Generalization Fallacy. A person drawing a conclusion about a large group based on experiences with only a few members of the group. A fallacy of inductive reasoning.

Faulty or Weak Analogy. Occurs when an author uses an analogy to communicate a concept, but the analogy used is not strong enough to support the conclusion being drawn.

Causal Oversimplification. Explaining an event by relying on causal factors that are insufficient to account for the event, or by overemphasizing the role of one or more of these factors.

Neglect of a Common Cause. Failure to recognize that two events may be related because of the effects of a common third factor.

Post Hoc Ergo Propter Hoc. Occurs when someone argues that because two events occurred, and one followed the other closely in time, then the first event caused the second. It’s an appeal to believe a cause-and-effect relationship that does not actually exist.

Confusion of Cause and Effect. Confusing the cause with the effect of an event or failing to recognize that the two events may be influencing each other.

The False Cause. The presumption that a real or perceived relationship between things means that one is the cause of the other.

Explaining by Naming. Falsely assuming that because you have provided a name for some event or behavior, that you have also adequately explained the event.

Critical MDMP Questions

We discussed the *MDMP* and *Mitigating Groupthink During the MDMP* in Chapter V, p62. This is a consolidated list of considerations from those discussions. Upon receipt of a mission, a planning directive, or commander's guidance, the Red Team Leader must determine the following, often in collaboration with the Commander/Chief of Staff:

- When should the Red Team engage in the planning process? (Most Red Teams will primarily work with Plans.)
- How should the Red Team engage? What are the expected deliverables or outcomes? Are their reporting requirements to the Commander or Chief of Staff?
- What linkage should the Red Team have within the staff? For example, does the chief of staff expect the Red Team to observe or participate in the war gaming process? Does he expect the Red Team to develop alternatives on their own for presentation to the Commander?
- What information does the Red Team need and is it available inside or external to the unit? Are their restrictions on the dissemination of information? What reach-back capability does the team require?
- What is the relationship between other specialized groups on the staff (e.g., Commander's Initiative Group)?

Red Teams face a number of challenges to "provide commanders an independent capability to fully explore alternatives to plans, operations, concepts, organizations, and capabilities in the context of the OE and from the perspectives of our partners, adversaries, and others."

Challenge 1: Remaining *independent* but *accountable*. While independent of the staff as a special staff element, Red Teams rely on the primary and other coordinating staffs to provide them information and must work with

staff members to resolve issues, insights, and observations.

Challenge 2: Inherent tension with the staff. There are inherent tensions with the staff who may view the Red Team's efforts with suspicion. The Commander must endorse the Red Team's effort. Conversely, the Red Team must carefully weigh which items require elevation to the Commander. The Red Team is not a "shadow staff" nor does it replace any of the inherent functions performed by the staff. Success can be judged by quality of the Red Team inputs which provides insights, perspectives, identification of vulnerabilities and unseen opportunities, as well as the team's effort to foster dialogue and communication among staffs.

Challenge 3: "Groupthink versus Pros from Dover." While the Red Team is an independent staff entity, it lives and works within the unit. The team must balance its abilities to be part of the team—cooperatively working to accomplish the mission, while remaining immune to "groupthink." Conversely, the team cannot be aloof or viewed as the "Pros from Dover."

Challenge 4: Cookie-cutter TTP approach. While the deliberate planning system describes a linear thinking process (e.g., Mission Analysis consists of 17 steps), no single red teaming TTP can fit all problems. For example, a red teaming approach to planning consideration for a humanitarian operation will differ from that of planning an offensive operation against a conventional force.

Critical Review Steps

A critical review is an intellectual exercise using various investigative and analytical techniques. The process described here is only a start point for Red Team leaders to formulate their own plan and serves only as baseline to spur thought on how the Red Team will approach a specific critical review.

While the process described here appears as a linear process, in reality many of the steps may overlap. Except for the first and last step, the other steps should be conducted simultaneously or amended based on time, resources, and the initiating authority's guidance.

By definition, a critical review assumes the existence of a concept plan or other document in need of review. If the initiating authority is dissatisfied with the existing courses and desires the Red Team to examine a problem to determine alternative solutions, the Red Team should use the Problem Solving Method rather than the Critical Review.

1. Identification of the Requirement – Receipt of Mission
2. Critical Review Mission Analysis
3. Restatement of the Requirement or Red Team Task to the Initiating Authority
4. Key Issue/Problem Identification and Assessment
5. Initial Research – Formulate Data Collection Plan
6. Conduct Research
7. Determine Critical Review Criteria
8. Contrast and Comparison - Key Questions + Alternative Perspectives
9. Finalize the preliminary assessment and initial report
10. Crosswalk the initial report with requirement
11. Complete report and briefings

Critical Thinking Traits

[Note—this is by no means an "all-inclusive list!"]

Critical thinking is:

- Awareness.
- a process.
- quality of thinking.
- imposing intellectual standards.
- challenging assumptions and exploring alternatives.
- searching for hidden assumptions.
- questioning and arguing logically.
- developing an ever better worldview.
- meta-cognition—thinking about the process of thinking.

Critical thinkers…

- are *active* listeners.
- adopt a skeptical state of mind.
- are open-minded–they never shout down an idea, and they reconsider and revise views where honest reflection suggests that change is warranted.
- abhor absolutes–they realize there is often more than one way.
- think contextually–they gather, assess and interpret *relevant* information, and disregard irrelevant information.
- are dialectical thinkers–they can handle contradictions and opposing ideas.
- identify and question their own assumptions.
- consider points of view, the quality of information, interpretation and inference, assumptions, and implications and consequences.
- are "reflectively skeptical."
- regard problems as exciting, not a hassle.
- understand the constraining role of personal world views.

- demonstrate the intellectual courage required to challenge conventional wisdom.
- search for what s/he doesn't know, rather than being complacent with what s/he does know.
- ask "Why?" "How Do?" "So What," and "What *should* we be doing?"
- are exceedingly curious and inquisitive; driven to determine a more refined version of a given perception.
- are detached emotionally—"reason prevails."
- are disinclined to board the Bus to Abilene—"intellectually independent."
- seek to understand the opinions of others.
- detect attempts to turn concepts into actual entities.
- frame a problem in several ways to consider alternative perspectives.
- evaluate the consequences of various alternatives.
- understand how framing can be used by others to mislead, in order to bias the reader/listener.
- attempt to identify the interconnected variables of a complex situation, and the variables' interrelationships/relative strength of those interrelationships.
- generate hypotheses for given situations, and then test those hypotheses.
- seek disconfirming evidence.
- discern inferences drawn, and looks for faulty inferences.
- distinguish between *causation* and *correlation.*
- recognize the bias in hindsight analysis.
- understand the effects of memory on decision making.
- know of/recognize cognitive biases present in decision making.

- know of/recognize the effects of social conformity/social psychology (including groupthink) present in group decision making.
- discriminate between inductive and deductive reasoning.
- use metaphors and analogies appropriately.
- produce and uses graphics to enhance comprehension.
- judge the credibility of an information source.
- identify premises and conclusions.
- challenge explicit assumptions.
- actively look for implicit assumptions, and challenge them.
- challenge "facts": not all facts are created equal.
- recognize and defend against inappropriate use of emotional/loaded language.
- identify/recognize underlying theories and/or philosophies inherent in an argument.
- detect misuse/abuse of word definitions.
- understand, recognize and avoid common logic fallacies.
- remember to ask "What's missing from the argument?"
- check for adequate sampling size and possible bias in sampling when a generalization is made.
- review statistics used in arguments, and challenge them.
- ask "Are there rival causes that we have overlooked?"
- ask "What are the implications of accepting this argument as-is?"

Finally:

- are systematic and thorough in applying precepts of critical thinking to various situations.
- *defer judgment* to avoid jumping to conclusions or believing false claims.

Critical Variables (CVs)

1. The *Physical Environment* defines the physical circumstances and conditions that surround and influence air, land, sea, and space operations. The defining factors are terrain, weather, topography, hydrology, and environmental conditions. The physical environment has always been a key factor in military operations. History demonstrated that forces able to take advantage of the physical environment have a much higher probability of success. Our opponents understand that less complex and open environments favor the U.S. This is due to our standoff technology, precision guided munitions (PGM), and sophisticated surveillance and reconnaissance capabilities. For this reason, adversaries will seek to use complex terrain, unfavorable weather, and less trafficked sea lanes when confronting U.S. forces.
2. *Nature and Stability of Critical Actors* refers to the internal cohesiveness of actors. It evaluates the population, economic infrastructures, political processes and authority, military forces, goals, and agendas. It also refers to an actor's strength or weakness. It is important to determine where the real strength of the organization lies. It may be in the political leadership, the military, the police, or some other element of the population. Understanding this variable allows US forces to better visualize the nature of the military campaign and the true aims of a threat's campaign. An entity that must commit significant resources to maintain internal control may represent less of a conventional threat and more of a stability and support threat.
3. *Sociological Demographics* concern the characteristics of a human population or part of it. Demographics measure the size, growth, density, and distribution of populations. Demographics also measure statistics regarding birth, marriage, disease, and death. Demographics are a significant factor contributing to likelihood of conflict.

Perceived inequities among sectors of a population can breed envy and resentment. This often results in conflict. Overpopulation and an uneducated, unemployed "youth bulge" can aggravate economic, ethnic, religious, and other rivalries.

4. *Culture* is a system of shared beliefs, values, customs, behaviors, and artifacts that the members of society use to cope with their world and with one another. Understanding a culture requires examining multiple elements, including its core values, history, myths, traditions, and other factors. A culture can change over time. Cultures transmit their shared values and beliefs from generation to generation through learning and social interaction. Finally, a culture in and of itself does not cause a conflict. The friction that comes from the interaction between two different cultures creates the potential for conflict.
5. Nation-states or non-state actors often enter into *Regional and Global Relationships* that can be local, regional, or global. These relationships include political, economic, military, or cultural mergers and partnerships. Membership or allegiance to such a relationship can determine an actor's actions. This can be in terms of support, motivation, and alliance construct. When actors create alliances, they can add to their collective capability and broaden the scale of operations and actions. Regional and global relationships of opponents or allies shape the scale, intensity, and perseverance of antagonists in military operations. In the age of globalization, regional activities will undoubtedly draw global interest and potential involvement. Effects created in one part of the world at the operational or tactical level could have global, cascading outcomes at the strategic level.
6. Existing *Military Capabilities* are the most critical variable for military operations, political aspirations, resolve, and will. It was once easy to define military capabilities.

However, this variable is rapidly becoming one of the most complex. A commander must be able to visualize all military capabilities of the threat. Red Teams must emphasize that our enemies can be flexible and adaptive. They could have the knowledge and ability to use a combination of conventional and unconventional capabilities. The commander must have information on conventional and unconventional capabilities, his ability to use modern technology, and his economic and political ability to affect the mission. Capabilities include equipment, manpower, training levels, resource constraints, and leadership issues. Niche technologies will be increasingly the norm for the near-term. Hybridization, rapid technological advancement, and asymmetric concepts generate constantly changing requirements and needs. In addition, paramilitary organizations, Special Forces, or enhanced police organizations take on greater significance as their capabilities and roles expand.

7. *Information* involves civil and military access, use, manipulation, distribution, and reliance on information technology systems by an entity. Information technology is the systems or mechanisms for preserving or transmitting information. Various actors seek to use perception management to control how the public sees things. The threat will exploit U.S. mistakes. They will also use propaganda to sway the local population to support their cause. Media and other information means can make combat operations visible to the world. The media can influence U.S. political decision making, internal opinion, or the sensitivities of coalition members. The expansion of information technology will greatly assist commanders. Complicated networks provide a vast web of communications capabilities. Redundant communications systems allow for the constant flow of information. Developing countries may have little in the way of communications infrastructure. Information may flow by less sophisticated means—couriers, graffiti,

rumors, gossiping, and local print media. Understanding existing communication infrastructure is important because it ultimately controls the flow of information to the population and the threat.

8. *Technology* reflects the equipment and technological sophistication that an entity could bring to the OE. Technology includes what nations or actors can develop, produce, or import. Global access to technological advances is slowly eroding the U.S.'s advantage. Understanding this variable can determine whether the threat has the technological ability to achieve equality or overmatch in selected areas. The presence of sophisticated technology can indicate where opponents expect to achieve the greatest advantage or perceive the greatest threat.

9. The U.S. military could find a variety of *External Organizations* in a conflict or failed state. These include non-government organizations (NGOs), international humanitarian organizations, multinational corporations, transnational organizations, and other civilian organizations. The organizations can have stated and hidden interests that assist or hinder U.S. mission accomplishment. Each organizational or individual participant pursues its interests in concert or competition with other entities. These actors may have economic, political, religious, cultural, or private motivations that differ from their public organizational mission statements. Defining these variables should inform the commander of the impact external organizations have on mission accomplishment.

10. *National Will and Will of Critical Actor* encompasses a unification of values, morals, and effort between the population, the leadership or government, and the military. Through this unity, all parties are willing to sacrifice individually for the achievement of the unified goal. The interaction of military actions and political judgments, conditioned by national will, further defines

and limits the achievable objectives of a conflict. This determines the duration and conditions of termination of a conflict. The willingness of the people to support threat military, paramilitary, terrorists, or insurgencies can be a significant characteristic of the battlefield. It will influence the type and intensity of resistance the people will pose to U.S. military operations. Most countries view the U.S. national will as a U.S. strategic center of gravity.[29] The degree to which one group can attack its opponent's will and still preserve its own represents its ability to set the conditions for achieving favorable conflict resolution. In a world of transparent military operations, attack on (and defense of) national will has tactical, operational, and strategic implications. A perceived attack on a group's cultural identity will usually serve to bolster its will to fight. This potentially increases both the intensity and duration of a conflict.

11. *Time* is a critical factor and a tool to manipulate tactical, operational, and strategic advantages. It drives the conduct of operations and campaigns. Time is one of the most significant planning factors driving decision-making. How much time is available and how long events might take will affect every aspect of military planning. This includes force package development, force flow rate, quality of intelligence preparation of the AO, need for forward-deployed forces and logistics, etc. Planners need to consider time in the context of the culture that the force is operating. Every culture views time differently. An opponent's view of time might be radically different from ours. This different view of time causes disjointedness in operational tempo.

12. The *Economic* variable establishes the boundaries between the "haves" and the "have-nots." This gap of economic differences among nation-states and other actors can cause conflict. Differences may be significant among nation-states, organizations, or groups regarding how they produce, distribute, and consume goods and

services. Control and access to natural or strategic resources can cause conflict. The ability to affect another actor through economic, vice military means, may become the key to regional hegemonic status or dominance. Economic deprivation is also a major cause of conflict. One actor may have economic superiority over another for many reasons, including access to natural resources or power.

Economic power and the ability to mobilize it represent a nation or actor's ability to rapidly procure, mobilize, and conduct sustained operations. It also reveals external relationships that could result in political or military assistance. For example, potential adversaries understand that the U.S. economy is a center of gravity that is very sensitive to perturbation. American economics and the power that flows from it will be inviting targets. Any disruption of the flow of oil products would have a significant negative impact on our economy. Many of our economic institutions may appear vulnerable to cyber-attack. Economic superiority rather than military superiority may be the key to power or dominance within a region. Analysis identifies those elements of economic power that may be a significant characteristic of the battlefield. In a globalized economy, the threat may leverage its economic power in a manner that affects friendly operations.

13. *Religion* is a variable that affects each of the preceding variables. Religion in itself "is a world view in which people personify cosmic forces and devise ways to deal with them that resemble the ways they deal with powerful human beings in their society. Religion provides man with a way to deal with uncertainty that they otherwise cannot control.[30] Religion is interwoven with a nation's culture. It can be a cornerstone that affects every aspect of culture. It also provides the individual a more worldly connection to other co-religionist outside the boundaries of a particular state. Our understanding of the religion

practiced in a state that U.S. forces operate is crucial to our success. This understanding will shape the way the Army should conduct operations (i.e., belief system of our opponent, key sites, organization of society, interpersonal relationships between our forces and the population).

What Critical Variables inform PMESII+PT		
Politics • Culture • Religion • Nature & Stability of State • Regional & Global Relationships • Sociological Demographics • External Organizations	**Military** • Culture • Religion • Military Capabilities • Nature & Stability of State • Regional & Global Relationships • Technology • National Will	**Economics** • Culture • Religion • External Organizations • Technology • Nature & Stability of State • National Will
Social • Culture • Religion • Sociological Demographics • Technology • External Organizations • Nature & Stability of State • National Will	**Information** • Culture • Religion • External Organizations • Information • National Will	**Infrastructure** • Sociological Demographics • Technology • Regional & global Relationships • Culture • Religion • Nature & Stability of State • Technology
Physical Environment • Culture • Religion • Regional & global Relationships • Physical Environment		**Time** • Time • Culture • Religion • National Will

Critical Variables are relevant to PMESII+PT and METT-TC.

Cultural Perception Framework

When to use

The Cultural Perception Framework is used to assist Red Team members in apperceiving another culture. It complements the 9-Step Cultural Methodology by posing questions of much greater detail. In order to avoid mirror-imaging, its steps lead red teamers through a process of discovering another culture based on its underlying tendencies, habits, values and beliefs. It provides red teams an ability to consider the *kinds* of questions that must be asked of Subject Matter Experts, in order to provide alternative perspectives about that culture.

Value added

Thorough use of the Cultural Perception Framework will ensure an enhanced understanding of a particular culture, by forcing the Red Team members to consider aspects of that culture they might not otherwise have discerned.

The Method

Step 1 – Establish a baseline of understanding by using the 4-Ways of Seeing

- How X views itself
- How Y views itself
- How X views Y
- How Y views X

Step 2 – What does the physical environment offer to the culture? (Water, Land, Food, Climate, Fuel/Power, Natural Resources)

Water

- What is the symbolic significance of water?
- Are there cultural rules about water's use?

- What is the relationship between water use and ritual?
- Who customarily exercises specific functions with respect to water? What are these functions?
- Who, in the culture, has customarily controlled access to water, and how have they used that for power, influence, etc.?
- What roles are expected of U.S. military personnel with respect to water use and provision?

Land

- Has the geography facilitated security, or invite invasion by another culture? How has the security outlook of the people evolved with respect to its geography?
- Who owns the land? Is access open to everyone, or restricted? What are the local conventions of private, communal, and state ownership/use of land? How is the ownership of land related to the power structure of the region?
- Is there sufficient land for agricultural use? Does this land allow for completely feeding the population? Does it provide for agricultural export?
- What land in the area is/is not appropriate for certain groups of people to use? Why?
- Who, locally, has legitimate ability to determine outsiders' access to land?
- Are there symbolic meanings for certain sub-districts in the region, and do groups within the area view this symbolism similarly, or differently? Why?
- What is the relationship between the political national/regional boundaries, and how people living in the nation/region view those boundaries, in terms of politics, economics, genealogy, and security?

- What are the geographic area's principles of division, and is there a relationship between these dividing lines and access to both tangible and symbolic resources?
- Are there particular land formations that are visually striking, with local significance?

Food

- What are the local staples, and what is the required labor to grow, prepare, and serve them?
- What foods are served by whom, to indicate the status of server or guest?
- How do U.S. Military operations or logistics impact the ability of local people to obtain essential foodstuffs?
- What foods have which kinds of ritual significance?
- What are the time- or calendar-related roles of various foods?
- Which foods are strategic commodities, inasmuch as controlling access to them influences one's coercive or political power?
- What, in local terms, is considered food sufficiency, food scarcity, and the proper role of external forces in providing food?
- What kinds of locally-accepted foods are considered strange, dangerous, or not even food (by the U.S. Military)? What foods raise concerns about health or sanitation?

Climate and Seasons

- How does the climate influence local attitudes to—and capabilities for—work, business, and combat?
- What, in local terms, passes for good weather, bad weather, etc?

Fuel and Power

- What are the locally-found, or locally-produced sources of power and fuel?
- What is the relationship between local elites and access to/provision of fuel and power?
- How does the larger government authority provide, or control, access to power?
- What do local people expect of outside forces in terms of power/fuel provision and protection?
- How does the population deal with shortages of power and fuel, and how do U.S. Military operations impact them?

Natural Resources

- What natural resources can be found inside the recognized borders of the nation/region?
- Are these natural resources accessible? Are they nearing depletion? Who controls access to these natural resources?
- Which natural resources are required by the culture, but not available internal to their borders? Where are these locally unavailable resources procured? Who is in the controlling seat for procuring them, and who provides them? What sources of power emanate from this relationship?

Step 3 – How is the economy structured? How do the people make use of what the physical environment offers? (Formal, Informal, As a Means of Exchange, Effect on Social Structure)

The Formal Economy

- What comprises the formal economy?
- On what commodities/services does the formal economy focus?

- What categories of people work in the formal economy?
- How will U.S. Military operations impact the formal economy, and people in it?

The Informal Economy

- How big is the informal economy, as compared to the formal economy? If it is large—why?
- What categories of people work in the informal economy?
- On what commodities/services does the informal economy focus?
- What is the relationship between the informal economy, on the one hand, and unregulated movement of people, crime, and violence, on the other?
- How does the formal economy rely upon the informal economy? Does this cause abuse to the area's population?
- What economic opportunities exist for the population?
- What are formal/informal economic actors' expectations of the state or over-arching political-military authority, with respect to involvement in or disregard for economic activity?
- What is considered an "illegal" good or service in the area, and on what basis? Is what would be termed in the West as "bribery" and "corruption" endemic? If so, what do locals consider corrupt?
- What goods/services are legal, but culturally frowned upon? Who deals in these goods/services?
- What percent of the formal and informal economy is under "foreign" control?
- How will U.S. Military expenditure in the local informal economy, or employment of local informal economic

actors, influence the socio-economic balance of power in the area?

Economy as a Network of Exchange

- How are important physical resources (food, clothing, shelter, cars etc.) obtained by local peoples?
- How do people gain access to critical services such as medical care, transportation, or education?
- Would a specific operational plan improve or block access to critical goods and services?
- What is the degree of (in)equity in the distribution of goods and services among the population?
- Who seems to control the distribution of goods and services, and how? Would a planned operation change this distribution pattern?
- Along with or instead of money, what do local peoples rely on to obtain and exchange goods in the region?
- If money is not the primary economic system, can the U.S. Military effectively use the local method of economic exchange?

Economy as a Way of Structuring Social Relationships

- What are the main economic systems in place in the region (pastoralism, agriculture, industrial production—all three may be present simultaneously)?
- What are the economic rhythms of the community (migration seasons, planting and harvesting, market day, work hours)?
- What are the important features of the environment that determine the economy of the area?
- Who has/controls most of the wealth? What percent of the population lives in poverty, as locally defined?

- How is wealth distributed? Does wealth seem to be concentrated in the hands of certain individuals or groups? On what basis? What power is conferred from such a concentration?
- Does the economy rely on general, balanced, or negative reciprocity?
- Do the elites own wealth, or do they possess power that generates wealth?
- How do local economic structures reflect the relationship of the group to the larger political and state system?

Step 4 – How is the social organization structured? How do the people organize, given the gifts of their physical environment, and their economic choices? (Age, Gender, Kinship, Class, Ethnicity)

Age

- What are the population's demographics? What do they suggest?
- At what age is someone considered a child or adult?
- What specific ceremonies mark the transition to adulthood? Which new social privileges are granted to men and women when they pass these manhood or womanhood rituals?
- What are locally accepted or expected economic roles for what U.S. society considers children?
- How should the U.S. Military prepare to respond to children that act as soldiers in militaries or insurgencies, or participate in violent activities against U.S. forces?
- What special status or roles are accorded to the elderly?

- Is there an age grading system that stratifies people according to their age and stage in the life cycle? And if so, what rights, roles, and duties do people have at each stage?

Gender

- What are the common child rearing practices, and how do they differ by gender and class?
- What are the roles assigned to men? What are the roles assigned to women?
- What work, activities, and spaces are assigned predominantly to men and women?
- Who undertakes which tasks and where?
- How must operational plans change to account for different work, roles, and spaces assigned to men and women?
- What roles do women play in local militaries and insurgencies? Do they engage in armed combat?
- If women are not visibly observable, what roles and tasks do they undertake “behind the scenes?”
- How can operational plans and assignment of manpower include gender to maximize effectiveness of the unit?

Kinship and Tribal Membership

- Does some form of “tribe”- or “clan”-related social structure exist, and play a role in society? To what degree?
- From which side of the family does descent originate? Is the society a matriarchal or patriarchal one? Do members of a family identify with the father’s side/relatives, the mother’s side/relatives, or both?
- What is the nature of marriage in society: who decides, what are the power relationships internal to, and

external to the married couple? Does the society practice monogamy or polygamy?

- To what degree does the society believe in collective unity, vice individualism? What degree of egalitarianism is prevalent in society?
- What are the reasons underlying social unity? What is it that holds the society together? What provides "meaning" to this society?
- Does the society rely upon "fictive" kinship? What is the essence of this fiction—which segments of society does it uphold, and which segments does it suppress?
- Does the society rely upon extended family units, or nuclear families? Why?
- How are land, water, or access to certain goods and resources concentrated in the hands of specific kin groups or tribes?
- How will our operations in the region support certain kin groups and enhance their power; or conversely undermine these groups?
- What are the possible outcomes of an operation that will challenge the power or control of resources by certain kin groups in the region (war, insurgency, increased stability, greater/lesser access to important goods and services)?
- How does a U.S. Military's choice of local points of contact interact with or disturb local kin relationships, thus influencing the degree of success of U.S. Military initiatives?

Class

- Does class play a role in society? To what degree?
- How is class defined in the area: on the basis of wealth, education, region of origin, inheritance, or other factors?

- Is status acquired through birth, or achieved through action?
- What are the privileges (economic, political, social, and religious) of members of the upper class?
- What are the key institutions in the social structure, and how did the leaders of those institutions acquire their roles?
- How is access to essential resources for survival (food, shelter, clothing, water) determined by class?
- How does the concentration of wealth (through corruption, graft, or legitimate means) in the hands of an elite upper class relate to resource or power access?
- If creating a plan to support lower class groups, will funds and resources have to pass through the hands of the upper class first (and consequently disappear)?
- What is the reality of upward mobility in the area's class system, and what do local people consider to be their potential for in-system upward mobility?
- How will U.S. Military measures that influence different groups' social mobility be viewed by those groups, or by other, competing groups?

Ethnicity

- Does ethnicity play a role in society? To what degree?
- What is the relationship between particular ethnic groups and control of professions or positions of power?
- How do groups that are barred from these positions of power challenge the system (breeding grounds for insurgents, theft and bribery, civil war)?

- What are local assumptions about U.S. and western biases and partisanship with respect to ethnic group struggles?
- How will a US Military alliance or dealings with a particular ethnic group affect those in power? What are possible reactions of those groups that are ignored?
- In this area, what kinds of processes have historically activated which ethnic identities and feelings of group membership?

Step 5 – What defines the political structure? Who makes the decisions concerning power distribution and resource usage? (leadership, conflicts over power)

Leadership

- What types of leaders does the society support? Charismatic? Violent? Legally elected?
- Who are the central players in the leadership? What are their histories, and what are their ideologies and beliefs? What networks do they belong to?
- Do the members of the leadership "live for politics," or make a living "off of politics?" What are their motives in doing so?
- How is decision-making organized, and who makes decisions?
- What particular social and political ideologies are prevalent? What narratives is the leadership using?
- What are the principles and processes governing policy deliberations and decision-making?
- Whom do leaders have to consult; to whom must they answer?

- How is leadership obtained and passed on (by election, inheritance, demonstration of skill, and membership in a certain age or social group, by force)?
- Who are the official formal leaders and what symbols indicate their status?
- To whom do people turn to actually get something done?
- What is the relationship between the formal and informal leader?
- Which institutions wield power? Particular social structures (tribes, clans, etc.)? Religious entities? Labor unions? Political parties? Courts? Criminal organizations?

Conflicts over Power

- What motivates the society? This may be political in nature, as well as economic, or even based on desires for social change. What tensions are inherent in the society?
- How does the society handle the inequity of power? Do members of society revile others who exert power upon them? Or are members of society inclined to accept this inequitable power structure submissively? Are members who accept inequitable power relationships submissively inclined to "wait until told what to do?" In other words, are they overly dependent on what the boss says—as opposed to a society in which the people feel inclined toward a high degree of interdependence, and use initiative?
- To what degree are the members of society comfortable with uncertainty (exhibited in low stress and low anxiety—what is different is curious)? To what degree do they attempt to avoid uncertainty (exhibited in high stress and high anxiety—what is different is dangerous)?

- Is this a society that relies on harsh power, or rule of law?
- What are the most important cultural characteristics that determine one's position and power in the community (age, class, gender, tribal identity, ethnicity, religion)?
- What is the degree of polarization in the region with respect to religious/ethnic/tribal identities?
- What is the amount of flexibility and interaction between religious/ethnic/tribal groups?
- Which groups hold power, and to what degree of concentration?
- Which groups are excluded, and along which axes?
- What is their degree of consciousness of exclusion?
- What is the nature of the bureaucracy? Is it efficient, and easy for the society to navigate? Or do the members of the bureaucracy exact tribute from society as a way of conducting business, or exercising power? To what degree is it necessary to find someone who can deal with this inefficient bureaucracy (someone who has "wasta") quickly?
- What is the role of patronage, and what characterizes a "patron?"
- Are politics used for religious purposes, or is religion used for political purposes?
- How do state bureaucracies relate to other elements of the social structure?
- Do these groups' leaders think it is possible to challenge the system?
- How do marginalized and losing groups gain access to valued goods, resources, and opportunities (black market, theft, raids, and insurgency)?

- How will allying with one group affect U.S. Military relationships with the other groups?

Step 6 – What are the belief systems? (History, Folklore, Rituals, Norms, Imagined Memory, Icons, Symbols and Communication, Taboos, and Religion)

History, Imagined Memory, Folklore

- What are the critical narratives of the cultural history? What are the pivotal historical stories that all people in the community share?
- What do people believe about themselves, and where they came from? What are the stories taught in school?
- How do the people learn in school? Via rote memory? Socratic dialogue? Other? Are they taught to challenge authority and conventional wisdom, or follow the party line?
- What are the daily sayings and folktales that everyone refers to in common conversation?
- How are these (remembered histories, folktales, and sayings) used to emphasize or teach important values and ideals?
- How do different groups in the area give different significance to the same historical stories?
- How does the society perceive current and past events?
- What are the key myths associated with social control?
- Does this society defer to ethnocentric beliefs, or does it display cultural relativity in its views of outsiders?
- Are there any myths explaining the essence of the "nation?" To what degree do the people identify with a "national" myth? How does this national myth conflict

with other social structure bases—ethnicity conflicts, tribal conflicts, etc.?

- Are there any significant emotional events in the life of the people? How recent/how far back in time are these events? To what degree has myth embraced these events, and what are the myths? Which leadership groups within the area support these myths to their own ends?
- Has the area been historically invaded or isolated? What is the significance of this?
- How are these histories, folktales, and sayings used to support propaganda for or against U.S. Military and U.S. activities in the region?
- How has the society accommodated cultural change in the past? Is it a society that relies upon pluralism? Syncretism? Or Assimilation?

Icons

- Who are the local heroes? What important qualities do these heroes embody?
- Who are the local villains? Why are they villainous (what makes them evil)?
- Are the heroes or villains compared to the U.S. Military or Americans?
- What do the comparisons illustrate about local attitudes towards the U.S. and the military?

Symbols and Communication

- What physical symbols (clothing, headdress, insignia, and scarification) indicate membership or status in the ethnic, religious, and social groups of the region?
- What physical and written symbols (graffiti, fences, signs, and spiritual markers) are important to be able to

recognize in order to navigate and understand what is happening in the region?

- What is the nature of routine greetings and farewells? What do they mean?
- What are the hand signals and predominant body language actions that members of the population use? What do they mean?
- How do the people communicate? Word of mouth? Gossip and rumor? In written form? Via television? Via texting and cell phone? Via Internet?
- What are the society's proverbs? For those which translate only with difficulty—what do they mean?
- What words or phrases are essential for basic communication with local people?
- What non-verbal behaviors may be misinterpreted by local people? Which non-verbal behaviors are important to understand in meetings and negotiations?

Rituals

- What are the rites of passage? Rites of enhancement?
- What behaviors and actions are important in the ritual or ceremony, and what does this reveal about cultural ideals and values?
- Who participates in the ritual, and what roles do the participants play?
- What does presence of participants, or the nature of their participation, say about their membership and status in the group?
- What does the public performance of the ritual communicate to outsiders?
- How is this performance potentially a politically charged statement about the group's status and rights within the larger society?

- What activities, not related to the ritual or ceremony itself, occur at ceremonial gatherings, due to the social status of the participants?

Norms, Mores, and Taboos

- What does the society value? Are its values predicated on dualism (e.g., absolutes, “evil versus good”), or on relativism (right versus wrong depends upon context)?
- How does society sanction its members? Does it allow for criticism and alienation?
- What is the role of emotional outburst—is it restrained? Accepted? Gender specific?
- To what degree do the members of society value human life? For what reasons would people in the society kill someone else? Why—as a measure on behalf of the state? To restore personal or family honor? To appropriate vengeance?
- What underlying allegiances or codes of honor could influence the success of an operation?
- What activities in the area are considered serious violations of social mores and could carry serious punishments, including death?
- What food and behavioral taboos exist in the region?
- What norms should the U.S. Military observe, even if they are foreign to the area?
- What beliefs or assumptions exist locally about American practices as regards local norms, mores, and taboos?
- What might the local people think (or have been propagandized to think) that the U.S. Military is likely to disregard in terms of local norms, mores, and taboos?

Religious Beliefs

- What are the predominant religions in the area?

- What are the key religious narratives? What do they signify, and whom do they support?
- Are the practiced religions focused on the social welfare of the people, in the hereafter, or both?
- What are the actual (versus theoretical/textual) religious practices in the specific area where the U.S. Military operates? Are these religions affected by local culture?
- How do local practices of a religion the U.S. Military has encountered elsewhere differ from what the U.S. Military thinks the religion is "supposed" to look like?
- Who is the actual leader of the local religious community?
- How do religious leaders relate to the educated elite vs. popular groups, etc?
- What is the basis of authority for a "religious" leader in the area: book learning, lineage, charisma, etc.?
- What power and role, if any, does the formal religious system play in local peoples' daily lives?
- What conflicts or disagreements exist between the formal religious system and the local religious practices of the area?
- How prominent is "religion" as an explanatory factor for people in current events, and in reference to history, or historical trajectories?
- What is "the way the world is supposed to be" according to locally-held religious beliefs, and how does the U.S. Military presence impact that?

Religious Membership

- How do people define and express their religious membership in the region?
- What roles and status do the various religious groups or sects hold in the larger society?

- What is the meaning of geography for religious groups in the area?
- What effects would a planned U.S. Military operation in the region have upon the power, status, and access to critical resources of the various religious groups or sects?
- How will the U.S. Military operations influence indigenous peoples' views of U.S. Military or U.S. biases towards different religious groups of the social structure?

Step 7 –

A. Conduct an analysis, based on the results of all information acquired. What particular deductions can you come to, based on the aggregate of the collected information?

B. Synthesize the results. Given the particular reason/motive for conducting the analysis, what is the "so what?" How does the information provide insight as to how another culture might react to U.S. Military presence? In what ways does the information illuminate "how they might think" about various issues?

Deception Detection

Systematic use of checklists to determine when deception actually may be present and how to avoid being deceived.

When to Use

In reality, analysts too seldom check for the possibility of deception, even when there is a well-known history of its use. The search for clues that deception is being conducted is often time consuming and requires extensive fact checking and hypothesis testing. Nonetheless, it can be critical in cases where the stakes are high. Analysts should be concerned about the use of deception when the deceiver would have a lot to gain through his efforts and has strong capabilities to deny or manipulate U.S. intelligence collection assets.

Value Added

Deception Detection can add rigor to analysis and reinforce the effectiveness of other analytic techniques covered in this primer. There may be times when analysts will place too much confidence in the effectiveness of other techniques covered in this primer, if they have not considered the possibility that deception may be present as well. For example, a well-developed set of indicators might actively mislead analysts, if they were partly developed from information purposely designed or fabricated by an adversary to mislead its opponents. While most analysts know they cannot assume every piece of collected intelligence is valid, few know how to adapt their daily work habits to adjust for the possibility of deception. Posing the hypothesis of deception places a considerable cognitive burden on analysts. Once accepting this possibility, it places in question all the evidence and makes it difficult to draw any inferences from the evidence with high confidence. A checklist of questions to detect possible deception can prevent the analyst from becoming paralyzed.

The Method

Analysts should routinely consider that their information base is susceptible to deception. If there is any possibility that deception could be present, a small group of analysts should assess key reporting based on four sets of criteria:

- Does a foreign actor have the motive, opportunity, and means (MOM) to deceive?
- Would this potential deception be consistent with past opposition practices (POP)?
- Do we have cause for concern regarding the manipulability of sources (MOSES)
- What can be learned from the evaluation of evidence (EVE)?

In addition to using this deception detection technique, analysts can also employ the technique of analysis of competing hypotheses (ACH). In this case, analysts would explicitly pose deception as one of the multiple explanations for the presence or absence of information. In the counterintelligence field, the use of ACH as well as Deception Detection techniques has proven very useful.

Determining the Suitability of an Analogy

An analogy is a comparison, used to improve our ability to comprehend one situation by comparing it to a previous situation about which we know something. It is a form of inductive reasoning, in which we proceed from one general premise to another. Like all inductive thinking, however, there is no certainty whether the analogical conclusion is warranted—at best the conclusion could be probable.

The manner to determine an analogy's suitability is to compare the ways in which both situations are *similar* to each other, and the ways in which both situations are *dissimilar*. For example, given the analogy "Going into Iraq will be our next Vietnam," the person making the statement presumes that one will be like the other. In some ways, perhaps it might. In others, however, there may be significant differences.

As such—given the analogy stated above, first determine the criteria around which you make the "similar/dissimilar" assessment. List the broadest and most expansive set of criteria you can possibly think of; the assessment of an analogy's suitability rests in large measure on the number of different criteria you can possibly site. Just a few of the criteria for our scenario could be as follows:

- Nature of the enemy
- Nature of the environment in which we will operate
- Nature of the regional allies or antagonists which may help/hinder either side
- Size and composition of enemy forces we will fight against
- Size and composition of our own enemy forces
- Whether or not the population will tend to rally around one side or the other
- Duration of the conflict
- Professional state of the enemy forces
- Professional state of the U.S. forces

Next, carefully consider our situation in Vietnam for each criterion. Make a list.

Thereafter, carefully consider our situation in Iraq for each criterion. Make a list.

Now compare the two lists, criteria-by-criteria. Are those two lists more similar or dissimilar? If they are mostly similar, perhaps you have a *strong* analogy/inductive argument. However, if they are mostly dissimilar, you have a *weak* analogy/inductive argument, and whomever uttered the statement most likely didn't think through the ramifications of his/her remarks. Instead, they were likely focused on a narrow subset of the criteria you have considered, in a way that frames their conclusion.

Devil's Advocacy

Challenging a single, strongly held view or consensus by building the best possible case for an alternative explanation.

When to Use

Devil's Advocacy is used to consider whether stated beliefs or assertions have been formed prematurely, without first considering alternative perspectives. It is a technique designed to help expose *implicit* assumptions and faulty reasoning.

The logic behind Devil's Advocacy stems from the cognitive challenges of decision making discussed by Richards Heuer (*The Psychology of Intelligence Analysis*) and Morgan D. Jones (*The Thinkers Toolkit*):

- We commonly solve problems by first forming a conclusion, and *then* using available evidence to support it. "[We tend to] favor a particular outcome or solution early on in the analytic process...long before we can objectively analyze the evidence and reach a conclusion." (This is the cognitive bias known as confirmation bias.)
- We tend to perceive what we *expect* to perceive
- We tend to value information that is *consistent* with our views, and reject or overlook information *that is not*
- We can easily become wedded to a pre-existing plan, person's reputation, etc., which precludes us from continuing to think critically about that plan, person, etc.

Value Added

Devil's Advocacy helps red teamers expose faulty reasoning, especially when the beliefs or assertions in question are the result of "conclusions jumped to." The tool will help establish additional evidence which should have originally been considered; it helps illuminate evidence which was either intentionally or unintentionally disregarded or ignored.

The Method

Conducting Devil's Advocacy is fairly straightforward: for a stated belief or assertion, *prove its opposite*. Do this by 1) considering the same evidence, some of which may have been disregarded or ignored, and by 2) finding new and disconfirming evidence originally unavailable.

Example. Given a stated position: "The U.S. Federal Government should *not directly* fund private schools"

- State and prove the position in its opposite form: "The U.S. Government *should* directly fund private schools, because…"
    - Enumerate reasons why this should be so. Consider all evidence originally available, especially that which was disregarded or ignored. Oftentimes, evidence can support several hypotheses, based upon its interpretation.
    - *Actively search* for new evidence which proves this opposite assertion.
- Disprove the *original* belief or assertion:
    - Reasons in the "stated position" which are *faulty*
    - Reasons in the "stated position" which were *ignored/overlooked*
    - Reasons *which are missing* from the "stated position"
    - Consider any implicit assumptions upon which the "stated position" rests

Divergence - Convergence

Think - Write - Share - This is the single most important idea to enable critical thinking. Before tackling any issue, we should think independently and reflectively first, then write down our thought–which helps us to shape and refine them, and finally share them in a disciplined fashion. Divergence-convergence is a form of ‘think-write-share’ – method:

- Everyone writes down as many ideas as they can about the problem or issue – they do not self-censor.
    - Facilitator goes around the room taking only one idea from each member of the group. Everyone speaks once before anyone speaks twice. Ideas are collected without commentary or criticism. If someone else offers something on your list, then scratch it out and offer something not yet raised.
- This goes on until all lists are exhausted.
- Once everyone’s list is exhausted and captured on the board, the group, aided by the facilitator, bins the ideas into a set of unique and distinguishable approaches so ideas bleed over on each other to the minimum extent possible. This sets the table for ‘dot voting’.

Dot Voting

Frequently, planning teams must prioritize their efforts as there is simply not enough time to address all legitimate issues. Dot voting is a method designed to anonymously collect the groups' perspective about the most urgent issues needing to be addressed. *Dot Voting* and *5 Will Get You 25* are two methods of weighted anonymous feedback.

- Identify the largest possible universe of issues using divergent thinking and collect them in a macro list
- Group the input in the broadest possible way so that no two topics remaining on the list overlap with each other (i.e., each topic is distinguishable from each other)
- Number the remaining distinguishable issues (for the sake of this illustration let's assume there are 12 different and legitimate issues worthy of the groups energy and attention)
- Each member writes a list of the numbers 1-12 in a column on a 3x5 card
- Each member then 'dot votes' 7 times (place a dot next to the number of the topic that s/he wants to vote for. All 7 votes can be given to a single topic, 7 topics one vote each, or divided 3 and 4, 1 and 6, 2 and 5, etc.
- Collect the 5x8 cards and total the number of votes for each idea or issue

The value of this approach is as follows:

- forces each person to prioritize by having a little more than 50% votes of the total number of issues (7 of 12) but also gives them the opportunity to vote for more than one compelling issue
- gives some indication of the weight of each idea with respect to each other (a group score of 40 is significantly higher than a group score of 20 even though 20 may be the second highest score). This can

be used to develop what the weighted/ priority factors for a COA should be

Note - for this to work properly it is absolutely critical that ideas don't compete against each other during dot voting so creating distinguishable issues is a key part of the process.

Fishbowl

“Fishbowl” is a liberating structure aimed at developing active reflection, listening, and fresh perspectives.

Create a circle of chairs in the center of a larger circle. Five-six is a good number. If you have a very large group, there may be multiple outer circles.

Invite a small group of people that have direct experience with the challenge into the small circle of chairs at the center. Ask this group to talk about the challenge together, sharing stories of their direct experience and insights as they might do if they were sitting in a coffee shop or at dinner together. They talk to each other, NOT the audience.

Invite the audience to ask questions and share their insights about the conversation while those in the center circle just listen. Gather all the questions. You might want to use file cards or have someone capture all the questions on chart paper.

Then invite the group to dialogue with each other between the two circles.

Some good questions for the debrief:

- What did you hear that surprised you?
- How has your perspective on the issue changed?
- What questions are still open for you?

Frame Audit

Use the Frame Audit to help uncover less than successful frames and faulty logic, as well as potentially reframe an issue in more helpful ways. Given a situation and frame, do the following:

- Ask yourself: what matters most to whomever uses this frame? What do they tend to talk about the most? Why?
- Also ask: given the frame we are using, how do others tend to see/frame the same issue? What is it they consider that we don't consider?
- For the frame you are using, consider further:
    - What issue(s) does the frame address most? Why?
    - What boundaries do we put on the question? (Boundaries are what we include within the frame, versus what we leave out.)
    - What yardsticks (how we measure the question) and reference points (key measurement benchmarks) do we use to measure success?
    - What metaphors do we use in thinking about this issue? Why?
    - Why do we think about this question this way? What training or experience frames the way we view the world?
    - What does the frame emphasize? Minimize? Why?
    - Do other people in our profession think about this question differently? How? Why? Are their frames successful?
- Finally, ask whether your frame is effective:
    - Does the frame prompt you to ask the right questions most of the time?

- Have you tested or challenged the frame, or have others tried to do so?
- Is your frame decisive in the sense of helping you resolve tough issues?
- Is your frame easily communicated to and understood by others?
- Do key stakeholders accept your frame as a guide to joint action?
- Does your frame achieve sufficient simplicity without being too simple?
- Is your frame adaptive and up-to-date with respect to changing times?
- Does your frame generate solutions that achieve desired results?
- What are some notable failures of the frame? Where has it led you astray?
- What are some of the deeper assumptions which underlie your frame?
- What are some of the origins of the assumptions in your past experience?[31]

High-Impact/ Low-Probability Analysis

Highlights a seemingly unlikely event that would have major policy consequences if it happened.

When to Use

A contrarian technique that sensitizes analysts to the potential impact of seemingly low probability events that would have major repercussions on U.S. interests. Using this technique is advisable when policymakers are convinced that an event is unlikely but have not given much thought to the consequences of its occurrence. In essence, this can be a warning that the intelligence and policy communities must be alert to an unexpected but not impossible event.

Value Added

Mapping out the course of an unlikely, yet plausible, event can uncover hidden relationships between key factors and assumptions; it also can alert analysts to oversights in the mainstream analytic line. In addition, an examination of the "unthinkable" allows analysts to develop signposts that may provide early warning of a shift in the situation. By periodically reviewing these indicators a Red Team is more likely to counter any prevailing mind-set that such a development is highly unlikely.

The Method

If there is a strongly held view that an event is unlikely, then postulating precisely the opposite should not be difficult.

- Define the high-impact outcome clearly. This process is what will justify examining what most analysts believe to be a very unlikely development.
- Devise one or more plausible explanations for or "pathways" to the low probability outcome. This should be as precise as possible, as it can help identify possible indicators for later monitoring.
- Insert possible triggers or changes in momentum if appropriate. These can be natural disasters, sudden

health problems of key leaders, or new economic or political shocks that might have occurred historically or in other parts of the world.

- Brainstorm with individuals having a broad set of experiences to aid the development of plausible but unpredictable triggers of sudden change.
- Identify for each pathway a set of indicators or “observables” that would help you anticipate that events were beginning to play out this way.
- Identify factors that would deflect a bad outcome or encourage a positive outcome.

Indicators or Signposts of Change

Periodically review a list of observable events or trends to track events, monitor targets, spot emerging trends, and warn of unanticipated change.

When to Use

An analyst or team can create an indicators or signposts list of observable events that one would expect to see if a postulated situation is developing; (e.g., economic reform, military modernization, political instability, or democratization). Constructing the list might require only a few hours or as much as several days to identify the critical variables associated with the targeted issue. The technique can be used whenever a Red Team needs to track an event over time to monitor and evaluate changes. In those instances, a Red Team would be watching for mounting evidence to support a particular hypothesis, low probability event, or scenario.

When there are sharply divided views on an issue, an indicators or signposts list can also “depersonalize” the argument by shifting analytic attention to a more objective set of criteria. Using an indicators list can clarify substantive disagreements, once all sides agree on the set of objective criteria used to measure the topic under study.

Value Added

By providing an objective baseline for tracking events or targets, indicators instill rigor into the analytic process and enhance the credibility of analytic judgments. An indicators list included in a finished product also allows the policymaker to track developments and builds a more concrete case for the analytic judgments. By laying out a list of critical variables, analysts also will be generating hypotheses regarding why they expect to see the presence of such factors. In so doing, the Red Team can make the analytic line much more transparent and available for scrutiny by others.

The Method

Whether used alone, or in combination with other structured analysis, the process is the same:

- Identify a set of competing hypotheses or scenarios
- Create separate lists of potential activities, statements, or events expected for each hypothesis or scenario
- Regularly review and update the indicators lists to see which are changing
- Identify the most likely or most correct hypotheses or scenarios, based on the number of changed indicators that are observed

Developing two lists of indicators for each hypothesis or scenario may prove useful to distinguish between indicators that a development is or is not emerging. This is particularly useful in a “What If?” Analysis, when it is important to make a case that a certain event is unlikely to happen. Checklist of questions to detect possible deception can prevent the analyst from becoming paralyzed.

Key Assumption Check

List and review the key working assumptions on which fundamental judgments rest.

When to Use

Most useful at the beginning of an analytic project. An individual analyst or a team can spend an hour or two articulating and reviewing the key assumptions. Rechecking assumptions also can be valuable at any time prior to finalizing judgments, to ensure that the assessment does not rest on flawed premises. Identifying hidden assumptions can be one of the most difficult challenges an analyst faces, as they are ideas held—often unconsciously—to be true and, therefore, are seldom examined and almost never challenged.

Value Added

Explicitly identifying working assumptions during an analytic project helps:

- Explain the logic of the analytic argument and expose faulty logic.
- Understand the key factors that shape an issue.
- Stimulate thinking about an issue.
- Uncover hidden relationships and links between key factors.
- Identify developments that would cause you to abandon an assumption.
- Prepare analysts for changed circumstances that could surprise them.

The Method

Consider how their analysis depends on the validity of certain premises, which they do not routinely question or believe to be in doubt. A four step process will help analysts:

1. Review what the current analytic line on this issue appears to be; write it down for all to see.
2. Articulate all the premises, both stated and unstated in finished intelligence, which are accepted as true for this analytic line to be valid.
3. Challenge each assumption, asking why it "must" be true and whether it remains valid under all conditions.
4. Refine the list of key assumptions to contain only those that "must be true" to sustain your analytic line; consider under what conditions or in the face of what information these assumptions might not hold.

Questions to Ask During this Process Include:

- How much confidence exists that this assumption is correct?
- What explains the degree of confidence in the assumption?
- What circumstances or information might undermine this assumption?
- Is a key assumption more likely a key uncertainty or key factor?
- Could the assumption have been true in the past but less so now?
- If the assumption proves to be wrong, would it significantly alter the analytic line? How?
- Has this process identified new factors that need further analysis?

Liberating Structures

A liberating structure (LS) is any approach/technique/effort that liberates good ideas from group constraints. Liberating structures intercede factors [tangential to the process, i.e., group dynamics] that otherwise detour the group from their best productivity. Liberating structures release a group in deliberation [i.e. problem-solving or decision-making] from constraints unrelated to the problem itself.

Useful techniques are detailed throughout this chapter and at http://www.liberatingstructures.com.

Liberating structures can:

- Buy time.
- Suspend rank.
- Afford anonymous input.
- Vocalize opportunity costs.
- Enjoy life, suspend stressors.
- Lead a person out of logical habits.
- Take people out of their comfort-zone.
- Test prevalent wisdom as though it were wrong.
- Summons diversity; contributions with differing expertise, backgrounds, perspectives, etc.
- Invites dichotomy; from those closest to the problem to farthest from the bias or a view on the other side.

Mitigating Groupthink

- The leader should refrain from stating up front any preferences or expectations.
- Establish an *expectation of conflict* in deliberation—but focused on the issues, not between personalities. Conflict can foster creativity and learning.
- Prior to beginning, have all individual "pre-commit" by writing down their initial answers to the issue being discussed—this helps establish ideas prior to deliberation and mitigate a pull toward conformity. Demand several options from each member.
- Each member of a decision-making group should have the *responsibility* to air objections and doubts, and be reinforced by the leader's acceptance of criticism from the group at large.
- *Leverage anonymity of ideas and responses* where possible.
- The group should consciously construct alternative perspectives of the situation. Alternative perspectives force the group to form options in the case they occur.
- The group should set up several independent sub-groups to work on the same issues. *Seek diversity in assembling these groups*.
- The group should assign individuals to act as a devil's advocate vis-à-vis options, policies, etc., that the group is assembling.
- The group's individuals should seek outside expertise and input on the question(s) at hand.
- The group should bring in expertise to challenge the views being developed by the group itself.
- Once the group has reached a conclusion on the best option, a "second chance" meeting should be held at which

every member restates any and all reservations he/she may have concerning the chosen option.

My 15%

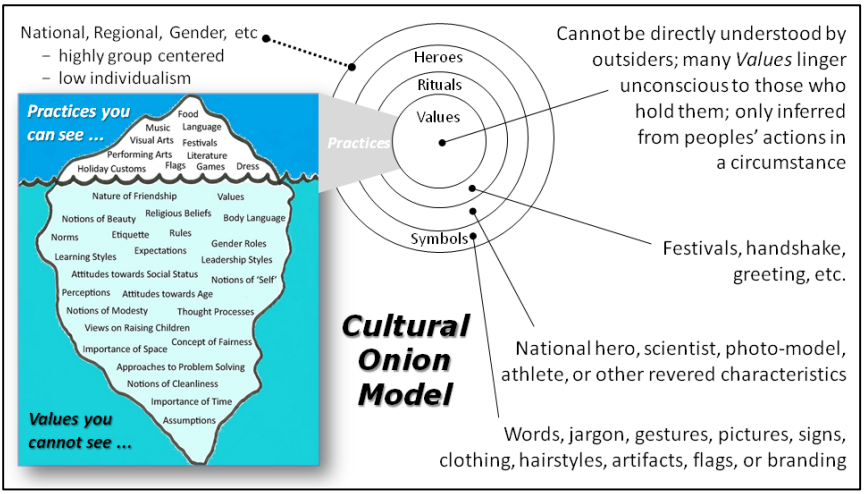
Most people have about 15 percent control over their work situations. The other 85 percent rests in the broader context, shaped by the general structures, systems, events and culture in which they operate. The challenge rests in finding ways of creating transformational change incrementally: By encouraging people to mobilize small but significant "15 percent initiatives" that can snowball in their effects. When guided by a sense of shared vision, the process can tap into the self-organizing capacities of everyone involved.

It doesn’t matter if you’re a General Officer or an enlisted soldier, a Senior Executive or a member of the team. You still have only your 15 percent.

Where do you have freedom to act? What’s in your 15%?

Onion Model

Hofstede's "Onion" Model: Manifestations of Culture at Different Levels of Depth (p. 30). In Hofstede's model we find *Values* at the core, wrapped by *Rituals*, *Heroes*, and *Symbols.* Each layer is influenced by the core and subsumed under the term *Practices*. As with most red teaming tools, the "onion model" should be used to prompt better questions, create a more comprehensive perspective, and expose ignorance. Notionally, it is possible to learn about, train on, or emulate each layer through concentrated practice; but not the core. Core values are learned culture, and deeply contextual. This is what Connerley and Pederson meant when they said "Culture may be learned, but it cannot be taught."[32]



When to Use

Like *4-Ways of Seeing*, use this tool early in any cultural review. Many people belong to several different groups at the same time, unavoidably carrying within them layers of mental programming that corresponds to different levels of culture. Refer to Chapter III for additional insight.

Value Added

This model helps to surface manifestations, similarities, and differences among or within the culture of a country, region, or group.

The Method

Interview and observe subjects. Postulate values and layers within the group(s). Populate the layers. Compare and contrast against the other selected groups, as needed.

For example:

- a *National* level according to one's country (or countries for those who migrated during their lifetime)
- a *Regional* and/or *Ethnic* and/or *Religious* and/or *Linguistic Affiliation* level; most nations are composed of culturally differing groups: regions, ethnicities, religions, and language
- a *Gender* level, according to whether a person was born as a girl or as a boy
- a *Generation* level, according to whether a person is a grandparent, parent, or child
- a *Social Class* level, according to opportunities linked with educational, occupational, or social standings
- an *Organizational* or *Corporate* level, according to how employees are/were socialized in their workplace

Outside-In Thinking

Used to identify the full range of basic forces, factors, and trends that would indirectly shape an issue.

When to Use

At the conceptualization of an analytic project, when the goal is to identify all the critical, external factors that could influence how a particular situation will develop. It would work well for a group of analysts responsible for a range of functional and/or regional issues. When assembling a large database that must identify a number of information categories or database fields, this technique can aid in visualizing the entire set of categories that might be needed in a research effort. Often analysts realize only too late that some additional information categories will be needed and then must go back and review all previous files and recode the data. With a modest amount of effort, “Outside-in Thinking” can reduce the risk of missing important variables early in the analytic process.

Value Added

Most analysts spend their time concentrating on familiar factors within their field or analytic issue. That is, they think from the “inside”—namely, what they control—out to the broader world. Conversely, “thinking from the outside-in” begins by considering the external changes that might, over time, profoundly affect the analysts’ own field or issue. This technique encourages analysts to get away from their immediate analytic tasks (the so-called “inbox”) and think about their issues in a wider conceptual and contextual framework. By recasting the problem in much broader and fundamental terms, analysts are more likely to uncover additional factors, an important dynamic, or a relevant alternative hypothesis.

The Method

Develop a generic description of the problem or the phenomenon under study. Then:

- List all the key forces (social, technological, economic, environmental, and political) that could have an impact on the topic, but over which one can exert little influence (e.g., globalization, social stress, the Internet, or the global economy).
- Focus next on key factors over which an actor or policymaker can exert some influence. In the business world this might be the market size, customers, the competition, suppliers or partners; in the government domain it might include the policy actions or the behavior of allies or adversaries.
- Assess how each of these forces could affect the analytic problem.
- Determine whether these forces actually do have an impact on the particular issue based on the available evidence.

Premortem Analysis

This is a method for helping decision makers anticipate problems. The purpose of a Premortem is to find key vulnerabilities in a plan. In contrast to risk analysis, the Premortem begins with the assumption that the plan *has failed*. The pull of groupthink, consensus, and a false sense of security is punctured, and is replaced by an active search aimed at preventing trouble later on. The premise for the Premortem exercise is that people may feel too confident once they have arrived at a plan. Premortem analysis empowers the participants to question the premise of a proposed course of action, its assumptions, and tasks. It breaks ownership of a course of action through a divergent process that encourages objectivity and skepticism.

Dr. Gary Klein developed the concept of the Premortem analysis.[33] This is a powerful red teaming tool as it is 1] simple to use, 2] simple to understand, 3] and when used during the decision-making process will empower the red team and members of the larger plans team to question the premise of a proposed course of action, assumptions, or specified tasks.

When to Use

The ideal time to use a Premortem analysis is just before the war gaming step in the decision making process, either the war game that analyzes proposed COAs or the war game that refines the selected COA into the concept of the operation.

Value Added

The use of a Premortem analysis will break the ownership of a particular course of action by a thorough, if rapid, session of answering the question, what would cause this course of action to fail if it is the basis for the operations plan?

The Method

Premortem analysis is an application of mental simulation. The premise for Premortem analysis is that people may feel too confident once they have arrived at a plan, especially if they are not highly experienced. The Premortem analysis requires one person to act as the scribe and must be limited in duration to no more than 30 minutes, ideally 20.

Step 1 Preparation. All members should be familiar with the base plan, at a minimum.

Step 2 Imagine a fiasco. Imagine that the plan failed. Ask, why did this happen? What could have caused this? Specifically, what are the *reasons*?

Step 3 Generate the reasons for failure. Participants individually spend several minutes writing down all the possible reasons for failure. It is important to do this individually first, so that the insights and experience of each participant are brought to bear.

Step 4 Consolidate the lists. Go around the room in round-robin fashion and solicit input from the participants, one at a time. Record the ideas on a whiteboard or poster paper. Continue until all ideas are exhausted. This is a divergent process in which four rules must be followed:

Rule 1: The more ideas, the better

Rule 2: Build one idea upon another. In other words, if someone else's idea prompts a new one from you, write it down.

Rule 3: Wacky ideas are okay. This rule bothers most people. Conventional wisdom dictates that "new" ideas must be sensible, reasonable, constructive, and practical. Wacky, silly, and foolish are subjective modifiers that people tend to apply to any idea that does not conform narrowly to a risk-free standard of sensible, reasonable,

constructive, or practical. Although wacky ideas may seem foolish, they can generate serious thought.

Rule 4: Don't evaluate ideas, neither yours nor someone else's. This includes body language, eye rolls, nods or groans. This rule liberates people from their self-imposed restraints in generating ideas, and eliminates fear of criticism and ridicule.

Step 5 Revisit the plan. Based on the list of concerns, revisit the plan and determine what to mitigate. Determine "ownership" and develop concepts for modifications to the plan.

Step 6 Keep and periodically review the list. This helps keep the possibility of different types of failure fresh in everyone's mind as the plan develops or is implemented.[34]

Problem Restatement

When to use

Problem Restatement is a process ideally conducted during the early stages of the problem solving process (Defining the Problem). Too often, humans uncritically accept a problem statement as given, without critically reflecting on whether the problem has been adequately framed. This happens because we are usually too eager to jump in and solve the problem as stated —believing that "the authorities know what they want"—rather than first considering various ways the problem could be framed. Several examples of poorly framed problems include those that:

- Are too *vague or broad* in definition
- Are too *narrow* in definition
- Contain inherent assumptions
- Contain a presumed solution

Since the manner in which we frame a problem directly affects its solution, poor problem framing leads to solutions which don't solve the real problem at hand.

Value added

Problem Restatement tool allows red teamers a way to ensure that the commander and staff have adequately considered how to best frame their problems, before solving those problems.

The Method

Problem Restatement consists of conducting several tasks related to the "proposed problem statement" in a *divergent* thinking mode, before settling on the best frame of the problem. Do each of the following; any or all of these may lead to alternative perspective in improving the framing of the problem:

- Paraphrase the problem statement—restate it using different words without losing the original meaning.

"Trying to say the same thing with different words puts a slightly different spin on the meaning, which triggers new perspectives and informative insights."

- Turn the problem on its head—by stating it in an opposite manner. (This is similar to Devil's Advocacy: stating the given problem in the opposite manner. This provides a different perspective in which to consider the problem.)
- Broaden the focus—restate the problem in a larger context. This may reveal a narrowly-defined problem statement.
- Redirect the focus—boldly, consciously change the focus of the problem. If the original focus concerned boosting sales, consider framing the problem instead in terms of cutting costs. This task involves looking for unexamined variables affecting the problem frame.
- Ask "Why?" Formulate a "why" to the initial question, then answer it, then do it again, etc. Conducting this task may reveal insights obscured in the original framing of the problem statement, as well as murky, unclear thinking.

Quality of Information Check

Evaluate completeness and soundness of available information sources.

When to Use

Weighing the validity of sources is a key feature of any critical thinking. Moreover, establishing how much confidence one puts in analytic judgments should ultimately rest on how accurate and reliable the information base is. Hence, checking the quality of information used in intelligence analysis is an ongoing, continuous process. Having multiple sources on an issue is not a substitute for having good information that has been thoroughly examined. Analysts should perform periodic checks of the information base for their analytic judgments. Otherwise, important analytic judgments can become anchored to weak information, and any “caveats” attached to those judgments in the past can be forgotten or ignored over time.

Value Added

A thorough review of information sources provides analysts with an accurate assessment of “what we know” and “what we do not know.” It is also an opportunity to confirm that sources have been cited accurately. In the case of HUMINT, this will require extensive review of the sources’ background information and access as well as his or her motivation for providing the information. Similarly, reviewing technical sourcing can sometimes reveal inadvertent errors in processing, translation, or interpretation that otherwise might have gone unnoticed. In addition, a quality of information check can be valuable to both collectors and policymakers:

- It can help to detect possible deception and denial strategies by an adversary.
- It can identify key intelligence gaps and new requirements for collectors.
- It can assist policymakers in understanding how much confidence analysts are placing on analytic judgments.

The Method

An analyst or a team might begin a quality of information check by developing a database in which information is stored according to source type and date, with additional notations indicating strengths or weaknesses in those sources. Ideally, analysts would have retrieval and search capability on the database, so that periodic reviews are less labor intensive and result in a more complete review of all sources used in past analysis. For the information review to be fully effective, analysts will need as much background information on sources as is feasible. Knowing the circumstances in which reporting was obtained is often critical to understanding its validity. With the data in hand, analysts can then:

- Review systematically all sources for accuracy.
- Identify information sources that appear most critical or compelling.
- Check for sufficient and strong corroboration of critical reporting.
- Reexamine previously dismissed information in light of new facts or circumstances that cast it in a different light.
- Ensure that any recalled reporting is identified and properly flagged for other analysts; analysis based on recalled reporting should also be reviewed to determine if the reporting was essential to the judgments made.
- Consider whether ambiguous information has been interpreted and caveated properly.
- Indicate a level of confidence that analysts can place in sources, which are likely to figure in future analytic assessments.

Red Team Analysis

Models the behavior of an individual or group by trying to replicate how an adversary would think about an issue; UFMCS also refers to this method as the *Initiatives Group*.

When to Use

Frequently, analysts face the challenge of forecasting how a foreign leader or decision-making group may behave when it is clear that there is a risk of falling into a "mirror-image" problem. That is, analysts can sometimes impute to a foreign actor the same motives, values, or understanding of an issue that they hold. Traditional analysis sometimes assumes that foreign leaders or groups will behave "rationally" and act as the analysts would if faced with the same threats or opportunities. History has shown that foreign leaders often respond differently to events because of different cultural, organizational, or personal experiences. Red teaming analysis tries to consciously place analysts in the same cultural, organizational, and personal setting ("putting them in their shoes") in which the target individual or group operates. Whereas analysts normally work from the position of the "blue" (friendly forces), a "red" team of analysts attempts to work in the environment of the hostile forces.

Value Added

Like Devil's Advocacy and Team A/Team B techniques, red teaming analysis is aimed at freeing the analyst from the prison of a well-developed mind-set; in this case, the analyst's own sense of rationality, cultural norms, and personal values. Whereas analysts usually operate as "observers" of a foreign adversary, the red teaming technique transforms the analyst into an "actor" operating within the adversary's culture and political milieu. This form of "role playing" is useful when trying to replicate the mind-set of authoritarian leaders, terrorist cells, or other non-Western groups that operate under very different codes of behavior or motivations. Often this technique can introduce new or different stimuli that might not have been factored

into traditional analysis—such as the target's familial ties or the international political, economic, and military pressures felt by the individual. For example, Red Team participants might ask themselves: "What would my peers, family, or tribe expect me to do? Alternatively, a Red Team analyst might pose the question to his colleagues: "How do we perceive the external threats and opportunities?" Finally, the red teaming technique can factor into its analysis the way in which personal power and status might influence a target's behavior.

The Method

Build a team of experts with in-depth knowledge of the operating environment, the target's personality, and the style of thinking used. The team should be populated not just with those who understand the language, but also with people, who might have experienced the culture, share the ethnic background, or have worked in a similar operational environment. Once established and separated from traditional analysis, the team members should:

- Put themselves in the adversary's circumstances and react to foreign stimuli as the target would.
- Develop a set of "first-person" questions that the adversary would ask, such as: "How would I perceive incoming information; what would be my personal concerns; or to whom would I look for an opinion?"
- Draft a set of policy papers in which the leader or group makes specific decisions, proposes recommendations, or lays out courses of actions. The more these papers reflect the cultural and personal norms of the target, the more they can offer a different perspective on the analytic problem.

Red teaming analysis is not easy to conduct. It requires significant time to develop a team of qualified experts who can think like the adversary. The team has to distance itself from the normal analysis and work as though living in the

target's world. Without a sophisticated understanding of the culture, operational environment, and personal histories of the foreign group, analysts will not be able to behave or think like the enemy. Analysts can never truly escape their own experiences and mindsets, but this technique can at least prevent them from falling into "mirror-imaging" unconsciously.

The most novel feature of red teaming analysis is its presentation.

- The analysis is often in a "first person" format—that is, drafted as memos to or from a leader or group.
- Red teaming analysis avoids the use of caveats or qualifications and assumes that the recipient understands that the paper is aimed more at provoking thought or challenging the conventional understanding of how an adversary thinks.
- Such papers are rarely coordinated among other experts and do not purport to represent the consensus view on an issue.

Red teaming papers do not plot out all possible courses of action but seek to give a prediction based on the target's special personal, organizational, or cultural experiences.

Red Teaming – Assessment Questions

- Are the proposed measurements of effectiveness clearly linked to the strategy, mission, or end state?
- Does the measurement have a clear start point (baseline) in which to measure progress?
- Does the measurement system incorporate higher headquarters metrics? Are the unit's tasks developed to local conditions?
- What is the level of coalition or interagency agreement to the assessment measures? If no agreement, what are the implications?
- Who has primary responsibility for assessment? Has the task (who, what, when, where) been established?
- Has key assessment measures been included in the unit's CCIR?
- Do the metrics reflect a cultural sensitivity, whereby important things are measured? From the civilian population perspective, does the U.S. MOE matter (e.g., Maslow Theory - electricity vice elections)? What are the expectations of the people in terms of patience for process?
- From the enemy's perspective, what are their measures of effectiveness? Does our MOE's measure what is important to him?

Red Teaming – Assumption Questions

When to Use

An individual analyst or a team can spend an hour or two articulating and reviewing the key assumptions. Rechecking assumptions also can be valuable at any time prior to finalizing judgments, to ensure that the assessment does not rest on flawed premises. Identifying hidden assumptions can be one of the most difficult challenges an analyst faces, as they are ideas held—often unconsciously—to be true and, therefore, are seldom examined and almost never challenged.

Value Added

Explicitly identifying working assumptions during an analytic project helps:

- Explain the logic of the analytic argument and expose faulty logic
- Understand the key factors that shape an issue.
- Stimulate thinking about an issue
- Uncover hidden relationships and links between key factors
- Identify developments that would cause you to abandon an assumption
- Prepare analysts for changed circumstances that could surprise them

The Method

Consider how their analysis depends on the validity of certain premises, which they do not routinely question or believe to be in doubt. A four step process will help analysts:

- Review what the current analytic line on this issue appears to be; write it down for all to see.

- Articulate all the premises, both stated and unstated in finished intelligence, which are accepted as true for this analytic line to be valid.
- Challenge each assumption, asking why it “must” be true and whether it remains valid under all conditions.
- Refine the list of key assumptions to contain only those that “must be true” to sustain your analytic line; consider under what conditions or in the face of what information these assumptions might not hold.

The List

- Does the assumption meet the standards for an assumption; fact or opinion?
- Is the assumption based on preconception, bias, or historical analogy; are they relevant and/or accurate?
- Is the assumption logical, given what is known about the enemy (equipment, doctrine, and TTP), weather, and terrain; does the assumption reflect reality found in the OE?
- Does the staff use a defined procedure throughout the planning and preparation (and potentially portions of the execution phase) that continually examines whether assumptions are valid?
- Is the assumption appropriate to the level of planning?
- Are there assumptions made implicitly during planning but not stated or assumptions made by the staff but not included in the plan?
- How is the staff addressing assumptions included in higher headquarters plans?
- How many assumptions are acceptable?

Red Teaming – Key Questions

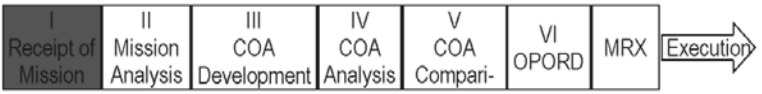
Red Teams continually and constructively challenge the staff's thinking processes during planning and operations:

Question	**Result in**
• What if….?	• Alternative analysis
• What are the objectives of….?	• Consideration of enemy, partner, and others on the battlefield
• What about….?	• Identification of gaps, seams, vulnerabilities
• What are we missing?	• Identification of gaps, seams, vulnerabilities
• What happens next?	• Identification of branches and sequels
• What should we assess?	• Identification of measures of effectiveness
• How can we assess…?	• Description of the assessment
• How do we know success?	• Description of a desired end-state
• What worked and why?	• Enables a learning organization
• What didn't work and why?	• Avoid patterns of operation

Red Teaming – MDMP Actions

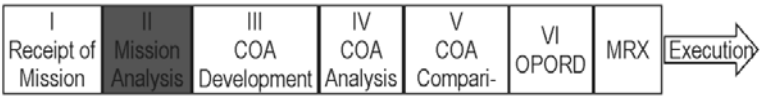
The military decision making process (MDMP) combines the conceptual and detailed aspects of planning and integrates the activities of the players throughout the planning process. The MDMP begins with *Receipt of the Mission* and ends with *Execution*. Staff actions are outlined in doctrine and the following are recommendations for the Red Team.

Receipt of the Mission



1. Based on the mission brief, construct a simple matrix using the *S-W-O-T* (p. 204) formula identified in the briefing which are found in the operational environment from the US, adversary, and other perspectives. From this matrix, what are glaring omissions/gaps in the briefings/products provided?
2. What are the timelines associated with the plan?
3. Did the mission brief provide sufficient details to support the planning for all phases of the operation?
4. Were higher headquarters assumptions identified?

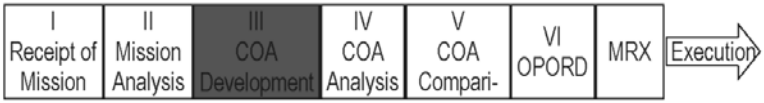
Mission Analysis



5. Assist the staff in the identification of specified, implied, and essential tasks.
6. Identify higher headquarters assumptions and challenge assumptions used by the staff.
7. Attend mission analysis brief.
8. Identify the enemy and US/coalition centers of gravity from their perspectives.

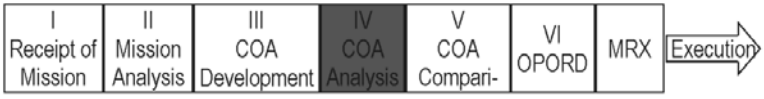
9. Identify potential end state definitions for adversaries, coalition, and other major stakeholders.
10. Continue OE/cultural analysis for use in COA Development.
11. Red Teaming Tools/Questions include:
    - Was the U.S./coalition end states clearly stated? Are there differences between the partners? Did we identify the enemy end state?
    - Does the information about the OE provide sufficient detail and linkages among the variables?
    - Has the higher headquarters provided any "assessment" measures that would affect formulation of the unit's assessment system

COA Development



- Is there sufficient focus and identification of requirement for all phases of the operations (e.g., stability and support)
- Does the COA account for all variables found in the OE (e.g., PMESII-PT)?
- Are the assessment tasks sufficiently identified?
- Continually examine assumptions for validity. Is there a plan to confirm/deny them? What consequences or branches are required? Did we consider key assumptions as potential CCIR? ISR Implications?
- Conduct a *Premortem Analysis* (p. 165) of the COAs.

COA Analysis



- Assist staff by serving as the unbiased "umpire" for the war game to arbitrate disputes.
- Help staff determine if adequate measures are in place to measure success and how/who will provide input to the measurement.
- Monitor the war game to help insure accuracy, for:
  - Realistic friendly and enemy capabilities.
  - Appropriate actions and results.
- Review the war game procedures and questions.
- Does the war game account for the involvement, reaction, or counteraction by significant stakeholders? (*4 Ways of Seeing* p. 76, *Stakeholder Mapping* p. 186)

(DOD) Wargaming is a conscious attempt to visualize the flow of an operation, given own strengths and weaknesses and dispositions, enemy assets and possible COAs. It attempts to foresee the action, reaction, and counteraction dynamics of an operation. This process highlights tasks that appear to be particularly important to the operation and provides a degree of familiarity with operational-level possibilities that might otherwise be difficult to achieve. **(JP 5-00.2)**

War games succeed or fail due for a variety of reasons. Red Teams can help the staff review the following with them:

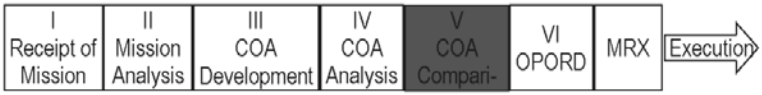
12. What are the standing operating procedures for the war game?
13. Who's in charge? XO or Chief of Staff according to doctrine – Is this reality?
14. What is the role of the G5/G3 Planner – who has ownership of the plan?
15. Who's the umpire? Who decides and arbitrates disputes?
16. Is there sufficient time available for war gaming?

Does the war game account for the most difficult phase or aspect of the planned operation? (e.g., for a conventional fight – river crossing/passage of lines are considered among the most difficult).

Who fights the enemy? G2? Is there significant seniority/expertise of the enemy team?

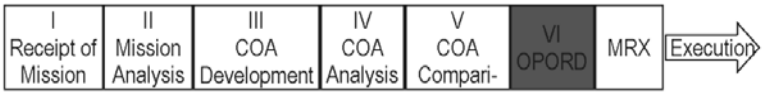
- Is the enemy's "aim and concept" placed within a larger context to see the "big picture"?
- Is the range of alternatives available broad enough for consideration (e.g., prevent deployment of US forces)?
- Are enemy capabilities wished away through the application of joint capabilities (e.g., airpower)
- Does the enemy fight realistically? What doctrine/TTP?
- What is the cultural mindset and how does it influence the ECOA?
- Based on lessons from the war games, which intelligence estimates require changes?
- What assumptions are used? What unstated assumptions are used?
- What procedures or "plays" are used based on SOP? TTP from experience? How is the OE for the current operation different from previous experience?
- Who role plays the others on the battlefield? Civilian factions, militias, NGOs, corporations?
- Who role plays the coalition or interagency partners?

<u>COA Comparison</u>



- Monitor development of COA comparison and subsequent briefings to ensure the COA accounts for critical items to include:
    - the OE variables
    - assumptions
    - perspectives of coalition partners and others

OPLAN/OPORD Production & Briefing



17. If directed, conduct order's crosswalk to identify gaps, disconnects, or vulnerabilities to the plan based on critical review of the prepared order and staff annexes and appendices.
18. Review the assessment plan to insure adequacy and it reflects the cultural implications associated with assessing progress.
19. Review timelines for release of the order/plan for a review whether sufficient planning time is available for subordinate units.

Key Points

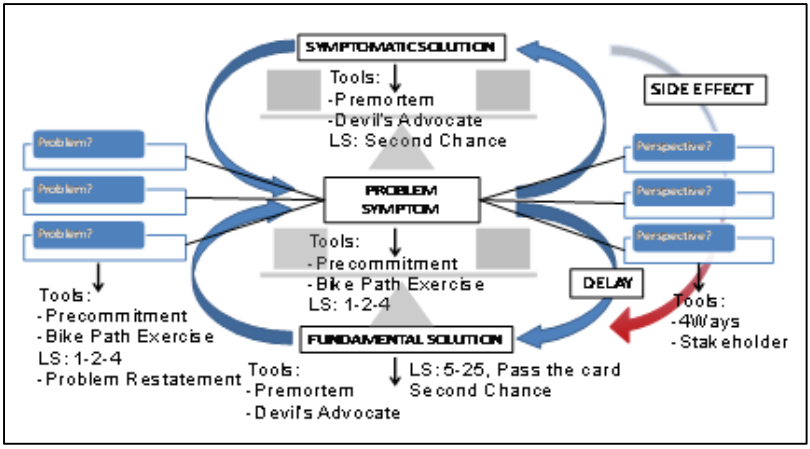
- Red Teams do not normally produce a separate staff product for inclusion in the order or plan.
- The best measure of Red Teams value is the staff producing a better staff product and identification of alternatives to the Commander.
- Red Teams depend on the Commander's or Chief of Staff's guidance, the negotiations/communication skills of the Red Team, and the culture of the unit.

Shifting the Burden

The “Shifting the Burden” model structure as Peter Senge calls it is composed of two balancing (stabilizing) processes. Both balancing loops try to correct the same problem symptom, but one addresses symptoms while the other addresses the underlying problem(s). Efforts directed only at symptomatic solutions which appear beneficial at first only serve to exacerbate the problem over time, often with debilitating side effects.

While Senge addresses the underlying problem indirectly in “Understanding and Using the Model” on page 105 of *The Fifth Discipline*, (revised 2006 edition), the problem is not part of the model, only the problem symptom. He talks about a problem again in “How to Create Your Own Shifting the Burden Model” on page 111, but does not address how to determine what the problem is or how it is perceived.

Senge’s approach is symptom/solution centric. The addition of problem and perspective elements to the structure along with Red Team tools and Liberating Structures to diagnose them, make Senge’s structure a richer framework for Red Teamers to develop alternative perspectives and options. To start with identifying the problem symptom as Senge suggests is a good place to begin, but rather than proceeding from there to identifying the fundamental solution (convergent thought process), this model recommends a close examination of the underlying problem(s) and perspective(s) before moving on to the solution(s). Sometimes restating a problem shows there is more than one problem. Several tool recommendations are included in the illustration on the next page.



Operating Assumption is an alternate term for Perspective. JJ O'Boyle explains operating assumptions and cultural logic in *The Culture of Decision Making*; http://www.winstonbrill.com/bril001/html/article_index/articles/251-300/article251_body.html.

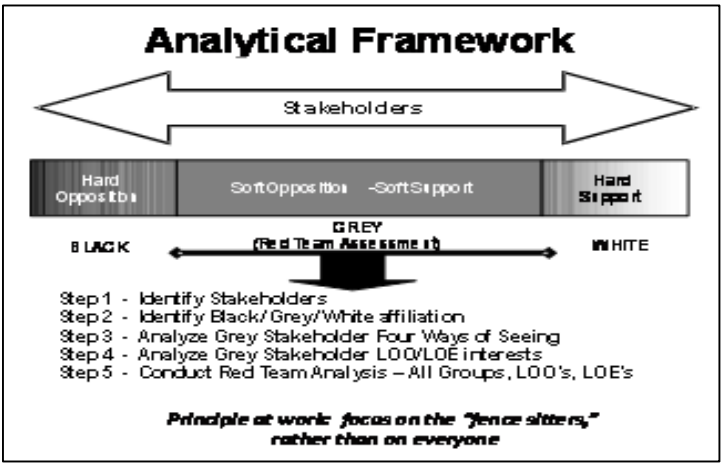
Stakeholder Mapping

When to Use

Stakeholder Mapping is a diagnostic tool for use in analysis, influence, negotiation, and decision support. It should be used when the Red Team needs to demonstrate the breadth of effects a planned operation can have within an operating area. Using intelligence and information available, the Red Team can develop a perspective on operations that will enhance the appreciation of the staff on potential unintended consequences of operations. The Red Team can also suggest methods of improving the impact of an operation on groups that are "on the fence" regarding their support for US/coalition/host nation operations.

Value Added

Stakeholder Mapping's greatest value is in the campaign design phase of decision making, specifically in framing the problem. In developing the commander's appreciation for the mission and operating area that precedes mission analysis Stakeholder Mapping provides understanding and viewing the operational environment from a systemic perspective. The analysis that occurs in the Stakeholder Mapping provides commander and planners insights into how the stakeholders view operations in the battle space.

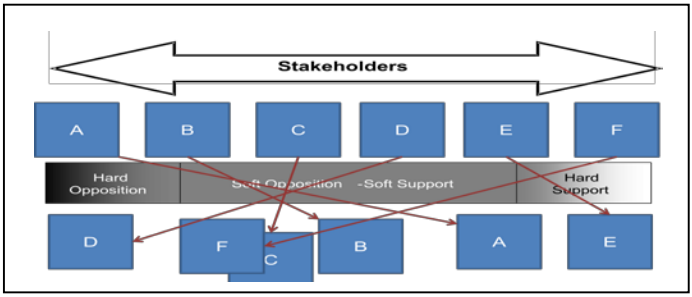


The Method

Step 1: Identify Stakeholders. They can be:

- Internal or external
- Individual, organization, or entity
- Strategic, Operational, or Tactical
- Senior or subordinate, or horizontal levels

Step 2: Identify Stakeholder Black/White/Grey Affiliation

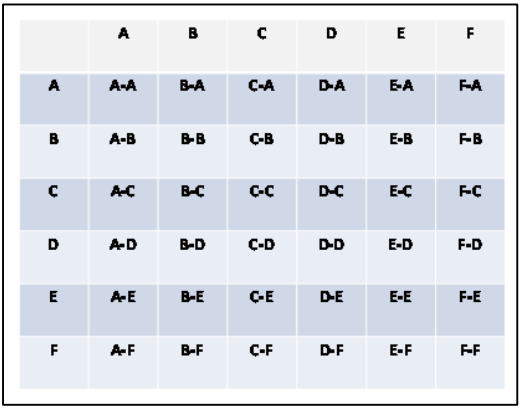


Step 3: Analyze Grey Stakeholder *4-Ways of Seeing*

Conduct thorough research to complete the analysis of these perceptions as it is more complex than the simple model implies, for several reasons:

- Seldom, if ever, will there be only two actors in the system under study.
- All the actors' perceptions and inter-relationships within the system must be considered in order to provide context for the analysis.
- How each actor perceives and defines the organizational or Operational Environment, strategic goals, and plans must be considered.
- It must be realized that actors and organizations may hold perceptions, both accurate and inaccurate.

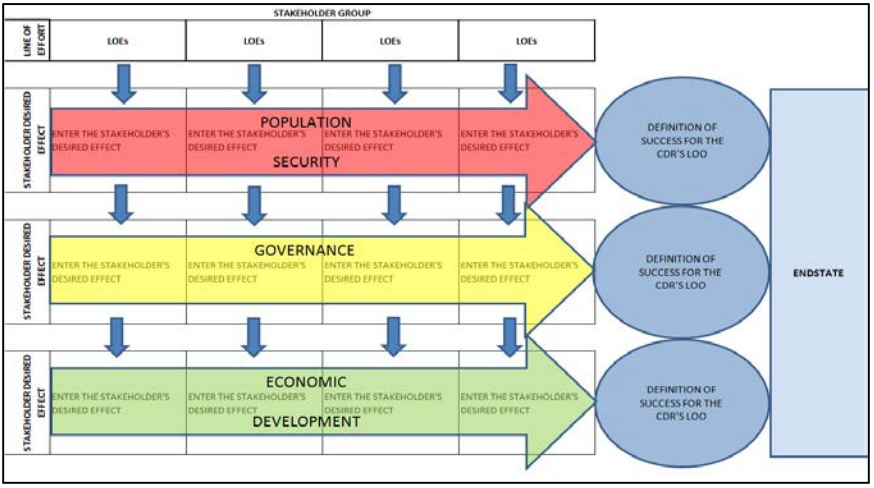
- Perceptions of the external audience(s) to whom we and our allies are playing cannot be discounted.



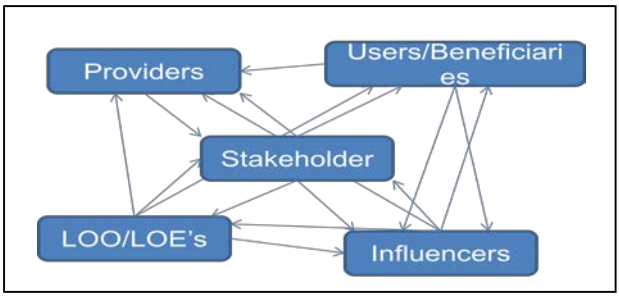
	A	B	C	D	E	F
A	A-A	B-A	C-A	D-A	E-A	F-A
B	A-B	B-B	C-B	D-B	E-B	F-B
C	A-C	B-C	C-C	D-C	E-C	F-C
D	A-D	B-D	C-D	D-D	E-D	F-D
E	A-E	B-E	C-E	D-E	E-E	F-E
F	A-F	B-F	C-F	D-F	E-F	F-F

Step 4: Analyze Stakeholders Lines of Effort (LOE) Interests.

- After a thorough assessment of the Stakeholder, the Red Team defines the Stakeholder's LOEs. Begin with the "fence sitters."
- Determine what the Stakeholder's Desired effect is within each LOE.
- Next, the Stakeholder's desired effect in the Lines of Effort (LOE) is assessed within the Commander's LOOs.



Step 5: Red Team Analysis: Organizational Mind Mapping. There is no one way to conduct Red Team analysis. Mind Mapping may be useful in organizational analysis: after identification of stakeholders, categorization is required. This is done by using a whiteboard or flip chart.

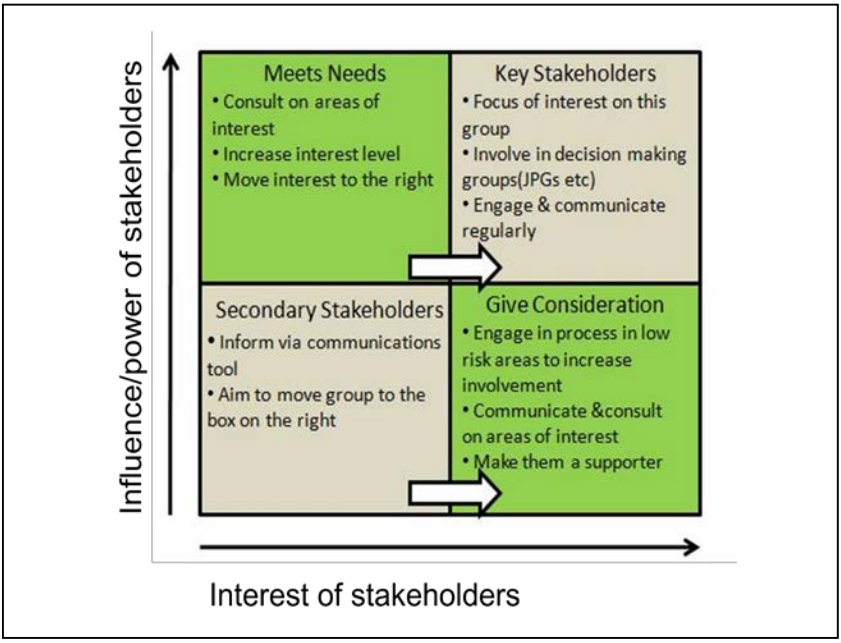


The arrows are representative of potential links between stakeholders, e.g., command relationships, habitual collaboration, common interests, etc.

Step 6: Another method for Analysis

- Once stakeholder interests have been mapped, they must be prioritized. A common approach is to map the interest and influence of each stakeholder group based on a chart like this one:

- Once the stakeholders have been mapped, focus of effort can be placed on the highest priority groups while providing sufficient information to keep the less influential groups happy.



Strategies for Structured Analysis

These structured analytic techniques can be used in a variety of ways when analysts begin a new assessment. Some can be used equally effectively at multiple points in the process and can promote an analyst's ability to keep an open mind, to consider multiple—including highly unlikely—hypotheses, to challenge conventional wisdom, and to assess the impact of important information gaps or deception on analytic judgments and confidence levels. The Timeline for Using Analytic Techniques provides some thoughts on when to use one or more of them during the course of an analyst's research and writing.

Starting Out

At the beginning of an analytic project, analysts are always wise to consider brainstorming and assumptions checks to ensure that important factors are not being missed or taken for granted. Similarly, outside-in-thinking can sometimes put an analytic project into a broader international context, in which factors outside the lead analyst's area of responsibility might impact on his or her analytic judgments. For instance, economic assumptions about the price of oil might be key to a regional political analyst's understanding the prospects for political stability in an oil-exporting country or an underdeveloped country entirely dependent on expensive energy imports. A High Impact/Low Probability assessment can also sensitize analysts early on to the significance of dramatic events that might affect their analytic lines.

Some techniques like Indicators and Signposts or Analysis of Competing Hypotheses (ACH) can be useful throughout a project and revisited periodically as new information is absorbed and analyzed. ACH, in particular, is a good tool to use throughout a project to prevent premature closure and to highlight evidence that is most "discriminating" in making an analytic argument. Alternative Futures analysis is similarly useful at the beginning of a project, but can amount to the structure for the entire project.

Hypothesis Testing

As an analytic project takes shape, and hypotheses are being formed about the key intelligence question, it can be appropriate to use one or another contrarian technique to challenge the conventional analytic line that is being developed. If the assessment contains strong judgments about an adversary's behavior, then challenging this view with a "Red Team" effort might be a good corrective to too much of a rational actor approach. In addition, a review of intelligence gaps at this juncture can also help give the analysts a better degree of confidence in the information base and judgments reached in the assessment.

A Final Check

As the assessment is being finalized, it can still be useful to review key assumptions as a sanity check on the underlying logic of the analysis. A brainstorming session also may be helpful to ensure that no plausible hypothesis has been dismissed or left unaddressed. If a firm consensus has formed around an analytic line and has not been seriously questioned in some time, then a Devil's Advocacy exercise could be useful. Analysts might also use a final review to decide if they have identified a list of key indicators for future developments. This can be an important guide to include in the assessment as a way to track future developments and monitor whether the analytic judgments reached are being realized or in need of revision.

String of Pearls

The Army Directed Studies Office developed the Task Concept Analysis technique, often called the “string of pearls” as a technique to link a rigorous analysis of assumptions with consideration of unintended consequences. This is a time consuming analysis best suited to a structured planning process. Use of the tool provides a way to visualize the cumulative effects that result from “wishful thinking” and failure to consider the many possible outcomes in a friendly plan or order. This analysis will show if the plan is vulnerable to faulty assumptions; dependencies that may not remain in place when the plan is executed; or the effects of unmitigated, unintended consequences (cascade or 2nd & 3rd order effects).

Identifying critical vulnerabilities in the plan allows planners to reinforce or mitigate these critical vulnerabilities. At a minimum, it informs the commander that there is a risk associated with a particular area in the plan. There are an infinite number of unintended consequences for any action. This technique will help identify those that are most likely to occur and most likely to generate results which may need to be mitigated by branch and sequel planning.

This analysis of the plan can stand alone or be used in a comparison with an emulative analysis of an enemy plan in order to see where differing strategies match up. The staff may identify an enemy strategy that is “unanswered” by a friendly course of action.

When to Use

String of Pearls is a time consuming process. It is best used when the Red team is asked to do an independent assessment of an existing plan. Red Teams can also use the method in a focused manner for analyzing and challenging assumptions associated with a plan, as well as showing the cumulative effect of failed assumptions on the entire plan.

Value Added

The methodology is a rigorous process of analyzing the plan:

- help prevent "assuming away the problem"
- identify weaknesses in a plan
- force consideration of unintended consequences
- highlight the need for focused branch &/or sequel plans

The Method

There are four basic steps to conducting a concept analysis.

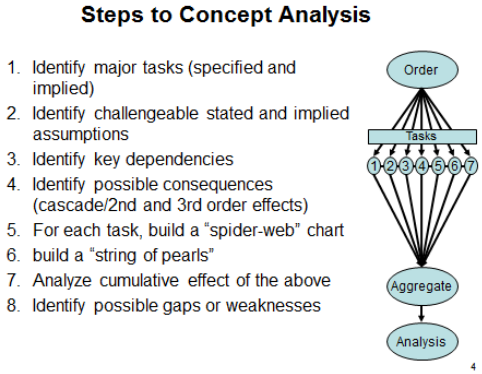
Step one is to identify all the major tasks.

Step two is to identify three elements of each major task:

- Identify challengeable stated and implied assumptions
- Identify key dependencies in each task
- Identify the potential unintended consequences (cascade and 2nd & 3rd order effects) for each task

Step three is to depict how the combined assumptions, key dependencies, and possible unintended consequences for each task accumulate across the entire plan.

Step four is to analyze how the cumulative effect [depicted above] might indicate any gaps or weaknesses in the plan.



The key to this *concept analysis* is the graphics rendered in *PowerPoint*, e.g., the source of the phrase *String of Pearls*. It is this representation which allows the decision maker to

"see" and understand the cumulative effects which are often hidden when considered separately.

Assumptions & Dependencies

Appropriate assumptions have two characteristics:

- They are valid, that is, they are likely to be true, and
- They are necessary, that is, they are essential to continuing the problem solving process.

The staff is most concerned about the validity of each assumption. If planners are considering assumptions that are valid but not necessary, they are creating extra work for themselves. If they are creating a roadblock in the planning process for themselves by identifying an assumption that is not necessary but can't be shown to be valid, that is a concern and should be pointed out. It is important to distinguish between assumptions and dependencies.

- Assumptions replace unknown facts in order to enable continued planning.
- If an assumption is invalid, the task associated with it may fail or may be at risk of failure.
- A dependency is a critical condition or precursor action necessary for successful execution of the task.
- Another task can be a dependency.

Let's talk about the difference between an assumption and a dependency. By re-wording a dependency, you can turn it into an assumption but that defeats the purpose of this analysis. For example, you could say either that execution of a task is dependent on fuel being available or that a planning assumption is that fuel will be available.

The difference is temporal, (i.e. whether or not you actually know the answer "at the time" of the analysis). An assumption is a fact that you don't know, but must "assume" in order to continue planning a specific course of action. If the staff assumes fuel will be available, then the staff can plan a road movement or helicopter assault.

A dependency is necessary to execute the task successfully and is a fact at the time of planning. For example the staff may know that fuel is available for a planned helicopter assault and plans accordingly, but if the fuel is destroyed or diverted to other uses, then the task cannot be executed.

Remember, a task can also be a dependency. Relationships between tasks can create dependency; the start or end date of the 2nd task (successor) is constrained by the start or end date of the 1st (predecessor). Differentiate the assumption from the dependency by asking, "Where is it listed during mission analysis, under 'facts' or 'assumptions'?"

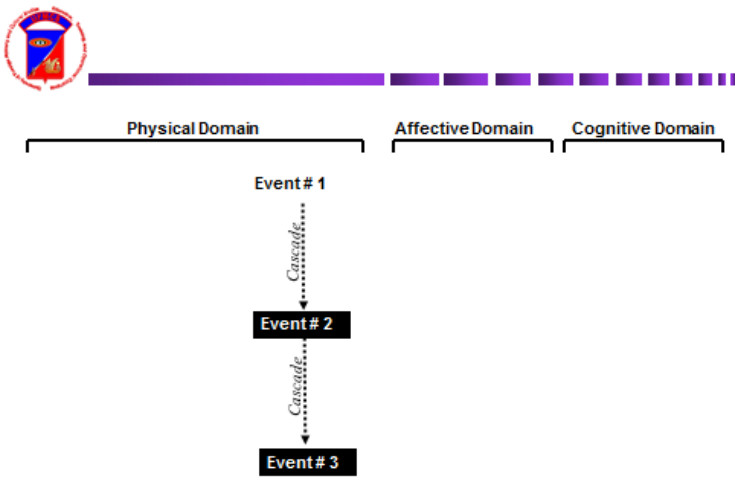
Unintended Consequences

An understanding of unintended consequences must begin with a discussion of an adaptation of Bloom's Taxonomy.[35] Bloom postulated that learning occurs in three Domains and for our purposes, so do effects. So, what are domains?

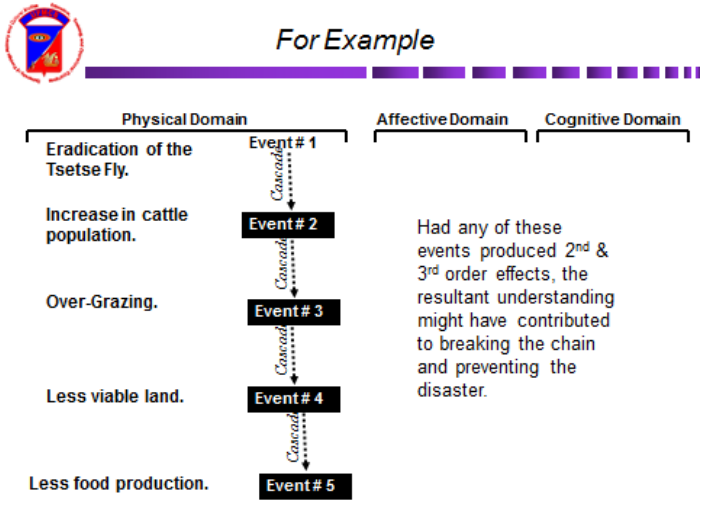
Domains are a particular sphere of influence, concern, or activity.[36] Bloom offers three domains. The cognitive domain reflects *knowledge*. In this domain, the mind completes levels of understanding a concept; building to next higher *level of understanding*. The affective domain reflects *emotion*: attitude, awareness, and integration; one feels *levels of feeling* about recognizing and synthesizing the information. The psychomotor [physical] domain reflects the *body*; one connects mind to body events in a way that generates particular *muscle memory for an action*.

Events or actions are sometimes called 1st order effects as they actually *occur* in the physical domain. 2nd order effects represent how individuals *feel* about the event; emotions in the affective domain. 3rd order effects represent *thoughts* about the event; thinking in the cognitive domain.

On the other hand, cascading effects follow a chain of actual causality (*If-then* or *Cause-in-fact*) as they occur exclusively in the physical domain. Cascade effects are mechanical, as one event *precipitates* the next.



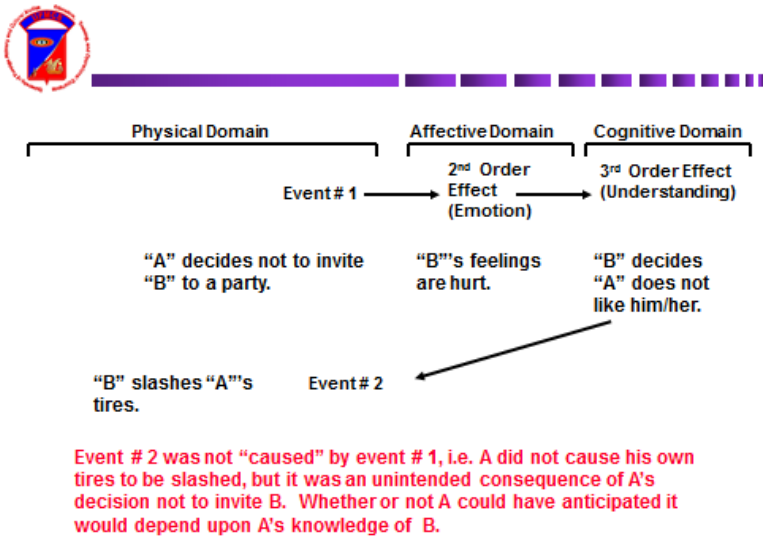
Consider the unintended disaster in southern Africa which resulted from a project to combat hunger in the Okavango delta.[37] A simple plan to repress the Tsetse Fly and increase cattle production resulted in over-grazing which after several years turned originally habitable land into barren desert, ultimately resulting in more starvation than in the beginning.



Theoretically, in this scenario, one could call *starvation* a "6th Order Effect", however such an analysis renders the terms meaningless since an infinite number of events could result.

Contrast this against the causality associated with 2nd & 3rd order effects and its concept of "free will" (remember the distinction between *complicated* and *complex*). 2nd & 3rd order effects result in what is commonly called *but for* causation. For example, in the scenario, individual "A" decides not to invite individual "B" to a party. B decides A dislike him and gets angry, slashing the tires on A's car.

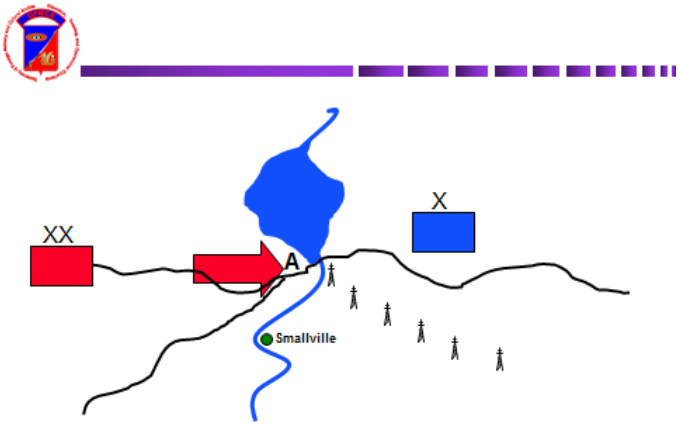
We could say that *but for* A's decision, his tires would not have been damaged, but one should not accuse A of *causing* the damage to his own tires.



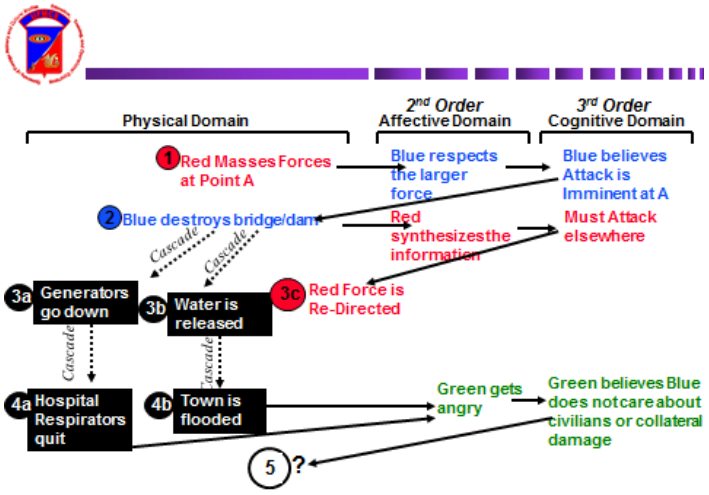
Events subsequent to 2nd & 3rd order effects which precede them are often "*unintended*" consequences of the first event or decision, but they are not caused by the original event. 3rd order effects do NOT produce 4th order effects, they merely introduce the element of choice into the equation. They become the catalyst for the new event.

2nd & 3rd Order Effects are a "term of art", used to focus the planner's attention on the OE (especially Culture) and the way in which it affects how people (friendly, enemy, or others) may "feel" and "think" about the results of the plan.

Considering unintended consequences, both cascade and 2nd & 3rd order effects, will minimize the likelihood that one or the other will be overlooked in the analysis. For example:



In image, a smaller Blue Force, observes a larger Red Force massing at Point "A". The movement occurs in the physical domain, but Blue's thoughts (i.e. is attack imminent, is this a feint or ruse?) influence Blue's action. For example, if Blue decides an attack is imminent and decides to destroy the Bridge/Dam in order to prevent Red from crossing, the unintended consequences might be illustrated like this:



To identify *cascade effects* requires a knowledge of physics, a *hard science* question. To identify 2nd & 3rd order effects and predict their consequences requires an understanding of culture, history, and sociology among other social, or "soft" sciences. The Red Teamer must be adept at both of these skills or enlist the aid of "ad hoc" members to do so. Ask:

- Will the plan you are contemplating produce a cascade of other events and if so, what could they be?
- What message or "information" is being conveyed by the plan and to whom is it being conveyed? (See also Stakeholder Analysis).
- How will it be "interpreted" by your adversary, friends, partners or others?

Build the "String of Pearls"

This image is key to understanding (or demonstrating) the final analysis. Group the tasks by objective, phases, layers, or any other way the planners related them. At the end, the grouping will surface tasks that need a closer look and show the cumulative effect on each objective, phase, or layer. To build the graphic, take the following steps:

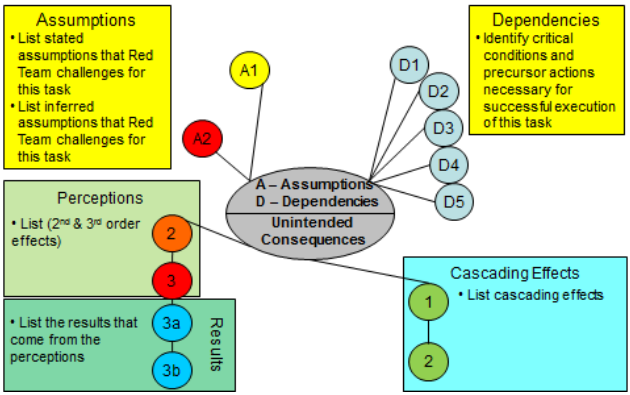
Examine the assumptions (specified & implied) in the plan.

- Determine whether they are valid.
- Associate each assumption that you do not consider valid with a specific task or tasks that you have previously identified.
- For each task, determine whether a dependency should be implied as necessary in order for that task to be executed.
- Decide whether these are "risky" dependencies.
- List these assumptions & dependencies for inclusion in the spider chart you will build for each task.
- Characterize each based upon whether it places the plan at "risk" or if invalid will cause the plan to "fail".

Consider the potential for unintended consequences associated with each task.

- Determine if there are likely to be cascading effects.
- Consider what message is being sent to each of the major stakeholders and how they may feel about it.
- Determine the spectrum of beliefs that may be engendered by the message (i.e. their perceptions).
- Consider what actions they may take as a result.

Build a "Spider-Chart" For Each Task



Next, build a spread sheet to help determine how frequently each assumption, dependency, or unintended consequence appears, i.e. how many other tasks may not be completed as a result of a particular assumption or action. The more tasks that may not get completed, the greater risk of failure.

Build a Spreadsheet

- Spreadsheet lists assumptions, dependencies, and consequences (effects) for each task.
- Fill in the spreadsheet with the same information which you compile for the spider charts as you complete them. This will help you identify the frequency with which they occur throughout the plan or order.
- Use exactly the same language for similar ideas
  - Example: "The enemy changes tactics" is similar to "The enemy adjusts his tactics" but will be counted as two separate ideas by excel
- This spreadsheet will help count the frequency of events

	A	B	C	D	E
1	**Task**	**Assumption**	**Dependencies**	**CONSEQUENCE**	**CONSEQUENCE**
2	Displace Command Post	Trucks available (ground movement)	Jump CP is operational	Fuel will be consumed	Fuel depot will need to be replenished
3		Helicopters available (air movement)			

19

From the spreadsheet or a manual count:

- Count how many times each assumption occurs throughout the entire plan or order.
- Count how many times each dependency occurs throughout the entire plan or order.
- Count how many times each unintended consequence occurs throughout the entire plan or order.

A thorough analysis of the data will reveal that some events occur repeatedly across multiple tasks—this should be of concern to the commander.

For Example:

If the same dependency is necessary for 15 of 20 tasks, it is significant for this analysis. If the same unintended consequence might occur as a result of only 7 of 20 tasks, it may not be significant for this analysis.

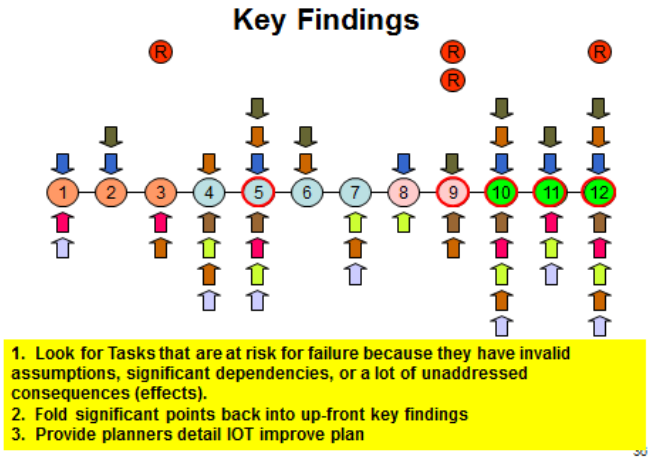
Now Build The PowerPoint Images.

The aggregate effect of the identification of possibly invalid assumptions, dependencies, and unintended consequences for each task can be viewed in a graphic representation. This representation indicates which tasks are most sensitive to other events and helps planners determine and prioritize which tasks should be revisited or what branch plans should be written to mitigate unintended consequences.

- Step 1: Draw “failure” and “risk” assumptions over the tasks on the “string of pearls”
- Step 2: Draw dependencies over the tasks on the “string of pearls”
- Step 3: Draw 2nd & 3rd order effects under the tasks on the “string of pearls”
- Step 4: Draw cascade effects under the tasks on the “string of pearls”.
- Step 5: Combine all elements in one slide, except for “at risk” assumptions

Analysis/Key Findings

- Note which tasks are most sensitive to the aggregate effect of the different elements you have identified
- Recommend that planners revisit these tasks or write branch plans to mitigate the consequences of the attempted or successful execution of the tasks
- In the chart below tasks 5 and 9-12 were identified as especially sensitive tasks given the number of dependencies and unintended consequences. Each staff group should then provide its analysis and guidance back to the plans staff section (G5/S5) for its final efforts in writing the operations plan. The steps of this process, much like the steps of the decision making process, can be adapted to the time available.



LIMITATIONS

Remember, the different elements that are identified are not weighted. For example:

- An unintended consequence might be *igniting a civil war*. This is more important than another identified unintended consequence like *running out of fuel*.
- However, both effects would get one arrow in this analysis; identify in both the analysis and the brief.

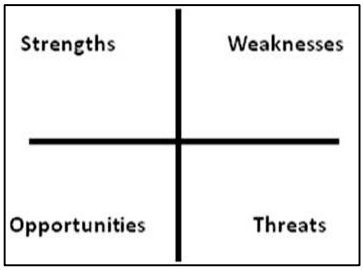
S-W-O-T Analysis

When to use

SWOT (Strengths, Weaknesses, Opportunities and Threats) is a red teaming framework designed to view a situation from four different perspectives. While SWOT can be used at any time, it is especially beneficial when used early in the red team's analysis of a problem, in conjunction with the 4 Ways of Seeing. Doing so helps the red team step away from its personal and cultural biases early-on, in order to attain alternative perspective. Combining S-W-O-T Analysis with 4-Ways of Seeing can become a powerful process to help stimulate the red team's effort.

Value added

SWOT is a framework that adds value by essentially forcing the red team to think through the various perspectives of a given situation.



The Method

Red teams using SWOT should establish a four-quadrant diagram, and label each quadrant as "Strengths," "Weaknesses," "Opportunities," and "Threats."

Thereafter, the team brainstorms to identify entries for each of the four quadrants, based upon the situation being red teamed. For example a red team could conduct a SWOT analysis on the potential implications of actively affecting the economic situation in a given region. When using SWOT in a situation of various actors (e.g., Division red team recognizing and dealing with various political leaders within its area, or a theater-strategic red team considering the interaction between the various entitles within the theater), conducting multiple SWOT analyses (one for each actor that views the other actors) would help the red team "see" the situation in a more holistic light. Finally, when SWOT used in conjunction with the 4 Ways of Seeing, some consideration should be given to which of the two tools is used first, and which follows.

Team A / Team B Analysis

Use of separate analytic teams that contrast two (or more) strongly held views or competing hypotheses.

When to Use

If there are at least two competing views within a Red Team or perhaps competing opinions within the policymaking community on a key issue, then Team A/Team B analysis can be the appropriate technique to use. Developing a full-blown Team A/Team B exercise requires a significant commitment of time and resources, so it is worthwhile considering if the issue merits this kind of attention. A longstanding policy issue, a critical decision that has far-reaching implications or a dispute within a community that has obstructed effective cross-agency cooperation would be grounds for using Team A/Team B. If those circumstances exist, then the Red team will need to review all of the data to develop alternative papers/briefing that can capture the essential differences between the two viewpoints.

Value Added

For the policymaker, this technique helps to surface and explain important analytic differences within the expert community. Often senior officials can learn more by weighing well-argued conflicting views than from reading an assessment that masks substantive differences or drives analysis to the lowest common denominator. By making the key assumptions and information used for each argument more transparent, a policymaker can judge the merits of each case, pose questions, and reach an independent judgment on which argument is the strongest. Moreover, highlighting alternative views puts individuals on notice that they need to be searching for new information that can confirm or disconfirm a range of hypotheses.

If opposing positions are well established, it can be useful to place individuals on teams that will advocate positions they normally do not support; forcing Red Teamers to argue “the other side” can surface an awareness to their own mind-set.

The Method

Analysis Phase: A Team A/Team B exercise can be conducted on an important issue to:

- Identify the two (or more) competing hypotheses or points of view.
- Form teams or designate individuals to develop the best case that can be made for each hypothesis.
- Review all pertinent information that supports their respective positions.
- Identify missing information that would buttress their hypotheses.
- Structure each argument with an explicit presentation of key assumptions, key pieces of evidence, and careful articulation of the logic behind the argument.

Debate Phase: An oral presentation of the alternative arguments and rebuttals in parallel fashion can then be organized for the benefit of other analysts:

- Set aside time for an oral presentation of the alternative team findings; this can be an informal brainstorming session or a more formal “debate.”
- Have an independent “jury of peers” listen to the oral presentation and be prepared to question the teams regarding their assumptions, evidence, or logic.
- Allow each team to present their case, challenge the other team’s arguments, and rebut the opponent’s critique of its case.
- Let the jury consider the strength of each presentation and recommend possible next steps for further research and collection efforts.

Telling Stories

The most conservative estimates of linguists and anthropologists put the evolution of oral language a minimum of 175,000 years prior to the development of written languages. As a consequence humans are wired to learn things through the use of storytelling.

When remembering or telling a personal story humans are more connected to the information being described. There is a difference in the quality of discussions and learning when stories are personal. An illustration follows:

Recently the author was asked to facilitate a discussion of desirable leadership qualities with a group of Majors at CGSC. Rather than ask them to regurgitate a list of established desirable qualities of leaders they were asked to remember the best leaders they had ever worked for and write down the qualities that made them such good leaders. The group then collected a comprehensive list, the number of qualities collected was staggering (group of 11 in 5 minutes of this exercise named 80 independent leadership qualities) and very personal. While well accepted qualities such as ‘setting the example’, treating others with respect, etc., were on the list so were much less noted qualities such as ‘being respectful of their subordinates time’, ‘a sense of humor’, ‘empathy,’ etc.

Telling stories is a powerful way to generate conversation and have people learn and remember.

TRIZ

TRIZ is "a problem-solving, analysis and forecasting tool derived from the study of patterns of invention. It was developed by the Soviet inventor and science fiction author Genrich Altshuller and his colleagues in the 1940s. In English it is typically translated as “the Theory of Inventive Problem Solving.” It is sometimes used in Six Sigma processes, in project management and risk management systems, and in organizational innovation initiatives. The full TRIZ process includes many problem-solving strategies. For our purposes we’re only going to use one piece of the TRIZ approach.

Ponder a difficult and complex problem you need to solve by walking through.

Describe the key elements of the desired result, and be specific.

Design a complete system that makes it impossible to achieve that result.

Then ask:

- What policies, practices, and ways of operating could eliminate any possibility of any requisite events occurring?
- What does this system have in common with the current state of affairs?

What will eliminate similarities between the current system and the new design?

Troika Consulting (Ad Agency)

This is a great process to help participants get started thinking about applications and action planning.

Invite participants to find two partners and sit down in a group of three (or four, but no more than four). Suggest that one member of the group be a time keeper to keep the group on track and to ensure everyone gets equal time. Give everyone time to reflect individually on a gnarly question. It may be very useful for them to take some notes.

Think about a challenge you are facing in your staff section.

- What's the question you most need to answer in order to move forward?
  How can you get that question answered?
- What's the biggest obstacle to making the changes you want to make?
  What must be done to move beyond that obstacle?

In each round of 10 minutes, one participant will share their challenge and ideas for next steps.

The role of the partners is first to ask questions to help them hone and improve their ideas.

Next, the partners engage with each other and, finally, with the participant about how they might handle the challenge and what possibilities might contribute to moving forward.

Switch roles so that each member of the Troika has a turn. After each member of the Troika has had their turn, the group can spend some time in conversation about insights and patterns they noticed across the three rounds.

This is a method to tap into the wisdom of the crowd. This is not recommended to make a decision. It is a way to get feedback you might not otherwise get from your staff.

Validating Assumptions

How many times have we encountered situations in which completely plausible premises, based on solid expertise, have been used to construct a logically valid forecast—with virtually unanimous agreement—that turned out to be dead wrong? In how many of these instances have we determined, with hindsight, that the problem was not in the logic but in the fact that one of the premises—however plausible it seemed at the time—was incorrect?

In how many of these instances have we been forced to admit that the erroneous premise was not empirically based but rather a conclusion developed from its own model (sometimes called an assumption)?

And in how many cases was it determined after the fact that information had been available which should have provided a basis for questioning one or more premises, and that a change of the relevant premise(s) would have changed the analytic model and pointed to a different outcome?[38]

-- Douglas MacEachin
Former CIA Deputy Director of Intelligence

No plan of operations extends with certainty beyond the first encounter with the enemy's main strength.[39]

-- Helmuth von Moltke
Chief of the Prussian General Staff, 1857-1887

1. <u>What is an assumption?</u> An assumption is an implicit or explicit belief about a past, current or future situation, issue or state of affairs. Planning and problem solving rely on assumptions because commanders, staffs and planning teams often lack relevant information about a situation and habitually rely on their beliefs to interpret a situation. Assumptions also help simplify and interpret factors related to 'what ought to be done' or 'how the world works'. From a cognitive perspective, humans are persistently on "cognitive autopilot" enabling us to accomplish routine tasks efficiently but unreflectively (without costly mental effort) (See Chapter III). Hence, it is often the case that assumptions are overlooked or

accepted uncritically, even when matters are complex and entail high risk under conditions of uncertainty.

a. Assumptions are often hidden from view. In solving or managing problems we often act based upon intuition and if questioned, rationalize our actions after the fact. If there is a degree of risk associated with taking action it is prudent to understand the assumptions underlying that decision. In matters involving high risk, it is essential to understand assumptions behind that decision. The latter is important in anticipating the consequences of those actions.

b. Assumptions can also constrain us as we attempt to deal with an issue. If we critically assess assumptions we might be able to gain additional insight and generate options that would not otherwise be apparent. Identifying and assessing assumptions, when working in groups, is also useful in preventing misunderstanding, aligning interests and reducing conflict within the group.[40]

2. Assumptions and Red Teaming: Red teaming tools and techniques provide a critical capability for checking, challenging and validating assumptions in planning, problems solving and decision making. Specifically, Red Teams assist Commanders, staffs and planning teams in checking, challenging and validating assumptions by:

   a. Helping the staff identify invalid and unneeded assumptions.

   b. Identifying needed assumptions to further the planning process.

   c. Identifying when the staff has defaulted to an unstated assumption – during design, mission analysis and course of action development and analysis.

   d. Offering alternatives and insights to assumptions about the operational environment, adversaries and other actors in the operational environment.

e. Identifying when the staff needs to develop a branch plan in case a key assumption proves invalid.

3. Assumptions in military planning: Joint Publication (JP) 5-0, *Joint Operation Planning* defines an assumption as "…a supposition about the current situation or future course of events, assumed to be true in the absence of facts…[or] a presupposition on the future course of events, either or both assumed to be true in the absence of positive proof, necessary to enable the commander in the process of planning to complete an estimate of the situation and make a decision on the course of action."[41],[42]

   a. Commanders, staffs and planning teams employ assumptions to "…address gaps in knowledge critical for the planning process to continue."[43]

   b. Commanders and staffs and planning teams "…must either validate the assumptions (turn them into facts) or invalidate the assumptions (alter the plan accordingly) as quickly as possible." Rules of thumb are "…never assume away adversary capabilities or assume that unrealistic friendly capabilities would be available."[44]

4. Assumptions in the context of oral and written statements and arguments: Authors M. Neil Browne and Stuart M. Keeley define an assumption as "…an unstated belief that supports…explicit reasoning."[45] The authors emphasize the importance of identifying implicit assumptions because, "hidden or unstated beliefs may be at least as significant in understanding [an] argument."[46] (See assumptions in arguments)

   a. Browne and Keeley further define assumptions into two categories: value and descriptive assumptions.

      (1) A value assumption "is an implicit preference for one value over another in a particular context."[47]

These are prescriptive in nature and imply how the world 'ought to be.'

(2) A descriptive assumption "is an unstated belief about how the world was, is, or will become."[48]

b. Browne and Keeley believe that questioning assumptions not only benefits individual reasoning but contributes to the quality of group reasoning and decision outcomes. Underlying this is their observation that assumptions are often, "hidden or unstated; taken for granted; influential in determining the conclusion; and potentially deceptive."[49]

5. Sources of Assumptions:

a. Mental models, mindsets, values, beliefs and world views: These are ideas that help us frame and interpret how the world works. These are similar to heuristics which help us navigate and engage our environment. As guiding patterns, these are valuable from an efficiency perspective but often hinder us when the environment changes or when the world does not conform to our expected pattern (See Chapter III).

b. For military operations, assumptions often relate to:

(1) Policy and strategic aims that direct the use of military action.
(2) Narratives describing the nature of the operation.
(3) Characteristics of the OE — the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander.
(4) Descriptions of adversary capabilities and will, critical links, key nodes, high value targets (HVTs) and centers of gravity (COG).
(5) Adversary probable intentions and likely courses of action (COA).[50]
(6) Weather.

(7) Specific terrain considerations that significantly affect the feasibility of the course of action.
(8) Deployment time, assets, availability, and access to airfields and ports.
(9) Risk.
(10) Date and level of mobilization for reserve and National Guard forces.
(11) Cultural implications (e.g., how the population views US/coalition involvement).
(12) Post conflict conditions.

c. For problem solving, assumptions often deal with resources, support, and relationships.

d. In concept development, specifically in the force development arena, assumptions often address conditions anticipated to be prevalent in the future, 5 to 15 years.[51]

6. Checking, Challenging and Validating Assumptions: Commanders, staffs and planning teams should question whether their assumptions are valid throughout planning and the operations process. Assumptions must be continually reviewed to ensure validity.[52]

a. Challenging assumptions helps identify stakeholder perspectives and their implications to the planning process.

b. JP 2-0, Joint Intelligence states, “Red teams assist joint operation planning by validating assumptions about the adversary, participating in the war-gaming of friendly and adversary COAs, and providing a check on the natural tendency of friendly forces to “mirror image” the adversary (i.e., to ascribe to an adversary the same motives, intent, and procedures that guide friendly forces).”[53]

c. In conceptual planning or Army Design Methodology (ADM), planning teams develop assumptions in the lack of factual evidence as they frame an OE and

problems. Planning teams record their assumption and challenge them while planning.

d. A structured analytical technique for identifying assumptions is listing and reviewing key working assumptions on which fundamental judgments rest, *Red Teaming – Assumption Questions* (p. 176).

(1) Broad assumptions without an understanding of their sub-level components may lead to faulty assumptions.

(2) For example, given sufficient preparation, load, and travel time, a staff can only assume a Brigade Combat Team (BCT) will be available to a theater commander in 30 days. Airfields and ports must have favorable weather unfettered by the enemy. The staff should continually question whether their assumptions are valid using the variables found in the OE or a similar construct.

(3) Past operations illustrate the challenges inherent to any operation when planning assumptions prove false. It appears that most senior civilian and military leaders failed to review the historical records of military occupations and of Middle Eastern or Iraqi history, and also failed to listen and evaluate outside views about potential weaknesses with their planning assumptions. Even the most senior staffs can fall into this trap, noted in ON POINT II:

"In the case of OIF, the postwar situation in Iraq was severely out of line with the suppositions made at nearly every level before the war. The V Corps commander, Lieutenant General Wallace, asserted that the assumptions made by planners about the Iraqi infrastructure and society after the conflict were particularly damaging to the PH IV plan:

I believe the things that we assumed would be in place on the ground that make Phase IV operations extraordinarily easy if they are there or extraordinarily hard if they are not had most to do with Iraqi institutions and infrastructure. We made the

assumption that some of those institutions and some of that infrastructure would be in place upon our arrival, regardless of the presence of the regime or not. The criticality of those assumptions was such that when the regime ceased to exist or ceased to dominate the areas in which we were operating, then all of those institutions and all of that infrastructure ceased to operate at the same time.

Wallace succinctly concluded, "We had the wrong assumptions and therefore we had the wrong plan to put into play."
-- ON POINT II[54]

Another example, assumed access by a friendly nation to ports and airfield to support closure into a region – requires continual checks to insure the assumption isn't wishful thinking but is grounded in reality. Throughout the lengthy planning effort for Operation Allied Force in 1998-99, allied leaders and planners widely adhered to a significant assumption. When the order arrived to execute the operation – on the very eve of hostilities – that assumption continued to prevail. But as the days of the aerospace campaign stretched into weeks and then months, the allies recognized their assumption for the fallacy it was – namely, that President Slobodan Milosevic of Yugoslavia would capitulate after a "modest set of punitive air strikes…"
-- COL Malone, USAF
OPERATION ALLIED FORCE[55]

(4) Are the assumptions logical, realistic, and considered likely to be true?
(5) Are there too many assumptions? How many assumptions are acceptable? There is no rule that defines the correct number of assumptions but an excessive amount of assumptions may correlate with higher risk and an increased probability of a faulty plan. General (ret) Anthony Zinni USMC offers, "I would always challenge assumptions very vigorously as the commander in chief (CINC). We have too many (assumptions). Many are pointless and some assume away problems."[56]

(6) Are there branches and sequels to execute if one or more key assumptions prove false?
(7) Why must this assumption “be true”?
(8) How much confidence exist that this assumption is true?
(9) What is the explanation for the degree of confidence for this assumption to be true?
(10) Could the assumption have been true in the past but less so now?
(11) If the assumption proves to be wrong, would it alter the line of thinking?
(12) Has checking assumptions identified new factors that need future analysis?
(13) What circumstance or information might underline this assumption?

e. Planning team and planning process considerations in challenging assumptions: A system must be in place that enables continual examination of the accuracy of the assumptions. Planners must also establish branch plans in case key assumptions prove invalid. The planning team works on these questions as a group, assigns a sub-team to work on these questions, or solicits support from the unit’s red team to help with challenging assumptions.

(1) Is there a procedure that is used throughout the planning and preparation (and potentially portions of the execution phase) that continually examines whether assumptions are valid? A technique is to establish validation points throughout the planning process to insure:
(a) Assumptions remain valid
(b) Assumptions proven as facts are deleted
(c) Assumptions proven invalid are discarded - requiring re-examination of the feasibility of the plan or development of branches.
(2) Is the assumption appropriate to the level of planning?

(3) Are there assumptions made implicitly during planning but not stated or assumptions made by the staff but not included in the plan? Unstated assumptions (explicit or implicit) can fault a plan from the beginning and do a disservice to the commander and the planning process.

(4) How are assumptions in higher headquarters plans addressed? Joint planning doctrine states, "For planning purposes, subordinate commanders can treat assumptions made by higher headquarters as true in the absence of proof to the contrary. However, they should challenge those assumptions if they appear unrealistic."[57]

(5) In deliberate planning there likely assumptions that cannot be verified until a crisis develops. In Crisis Action Planning (CAP), "…assumptions should be replaced with facts as soon as possible."[58]

(a) The staff accomplishes this by identifying the information needed to convert assumptions to facts and submitting an information request to an appropriate agency as an information requirement.

(b) If the commander needs the information to make a key decision, the information requirement can be designated a commander's critical information requirement (CCIR). Although there may be exceptions, the staff should strive to resolve all assumptions before issuing the Operations Order (OPORD).

f. Argument Deconstruction: For evaluating assumptions in statements and oral arguments, we can employ critical questioning to expose hidden assumptions. For example questions see Challenging Assumptions below. Authors M. Neil Browne and Stuart M. Keeley refer to critical thinking as:

(1) Awareness of a set of interrelated critical questions;
(2) Ability to ask and answer critical questions at appropriate times; and the
(3) Desire to actively use the critical questions.[59]

g. 5 Whys is important to begin with “why” questions. The answers to “why” questions get at causal links behind events and problem symptoms. “What” questions tend toward simple data collection, and are subject to confirmation biases. The 5 Whys is a question-asking technique used to explore the cause-and-effect relationships underlying a particular problem. The technique is used to determine the root cause of a defect or problem symptom. However, the process can be used to go deeper to explore questions related to purpose rather than problems.

h. Four Ways of Seeing is a flexible tool; a technique available to planning teams to develop and compare how other actors within an OE view a situation or problem. The planning team can compare the friendly force with an enemy force or other actors or compare multiple actors with each other.

(1) To develop a richer understanding of an OE and problems, it is helpful for the planning team to examine the situation from the perspectives of other actors within the OE in order to appreciate their respective assumptions. For example:
(2) How does an enemy view the causes of conflict?
(3) What are the goals of the enemy force within an area?
(4) How does the enemy force perceive the goals of coalition forces in the area.

i. Premortem is another means of identifying and challenging assumptions is to apply the Premortem Analysis to a plan or COA. Premortem Analysis is a form of mental simulation in which you imagine an

outcome that results in failure. The premise for the Premortem exercise is that people may feel too confident once they have arrived at a plan. Premortem analysis empowers the participants to question the premises of a plan or proposed course of action, its assumptions, and tasks. The pull of groupthink, consensus, and a false sense of security is punctured, and is replaced by an active search aimed at preventing trouble later on. It breaks ownership of a plan or COA through a divergent process that encourages objectivity and skepticism.

j. Frame Analysis Audit: The frame audit is useful for uncovering built in biases and blind spots in mental models, beliefs or worldviews.[60]

7. Intelligence and Assumptions: Intelligence analysts often have to fill in gaps in knowledge with assumptions about adversary will, capabilities, probable intentions and visualization of the OE (e.g., PMESII-PT). The intelligence estimate supporting the operation should clearly identify these assumptions. The intelligence staff should identify and tap into any ongoing or existing information collection activities or joint intelligence, surveillance, and reconnaissance (ISR) collection that may offer relevant information to fill gaps.[61] The challenges for the intelligence professional are threefold:

   a. Avoid confusing assumptions as facts.

   b. Keep assumptions to a minimum, challenge them continually, and assumptions must reflect the culture, doctrine, TTP, and realistic adversary capabilities.

   c. The Information Collection or intelligence, surveillance, and reconnaissance (ISR) plan must reflect the requirements to confirm or deny these assumptions using available ISR assets.[62]

8. Key Points:

   a. An assumption is an implicit or explicit belief about a past, current or future situation, issue or state of affairs. Assumptions help simplify and interpret factors related to ‘what ought to be done’ or ‘how the world works’

   b. It is often the case that assumptions are overlooked or accepted uncritically, even when matters are complex and high risk under conditions of uncertainty.

   c. Assumptions are often hidden or unstated; taken for granted; influential in determining the conclusion; and potentially deceptive.

   d. Assumptions must be continually reviewed to ensure validity. Commanders, staffs and planning teams should question whether their assumptions are valid throughout planning and the operations process.

   e. In joint planning, a valid assumption has three characteristics: logical, realistic, and essential for the planning to continue.

   f. An excessive amount of assumptions may correlate with higher risk and an increased probability of a faulty plan.

   g. The use of assumptions requires the staff and planning teams to develop branches and sequels if the assumptions prove invalid.

   h. Often an unstated assumption may be more dangerous than stated assumptions proven wrong.

What if? Analysis

Assumes that an event has occurred with potential (negative or positive) impact and explains how it might come about.

When to Use

A technique for challenging a strong mindset that an event will not happen or that a confidently made forecast may not be entirely justified. It is similar to a High- Impact/Low-Probability analysis, but it does not dwell on the consequences of the event as much as it accepts the significance and moves directly to explaining how it might come about.

Value Added

By shifting the focus from whether an event could occur to how it may happen, analysts allow themselves to suspend judgment about the likelihood of the event and focus more on what developments—even unlikely ones—might enable such an outcome. An individual or team might employ this technique and repeat the exercise whenever a critical analytic judgment is made.

Using this technique is particularly important when a judgment rests on limited information or unproven assumptions. Moreover, it can free analysts from arguing about the probability of an event to considering its consequences and developing some indicators or signposts for its possible emergence. It will help analysts address the impact of an event, the factors that could cause—or alter—it, and likely signposts that an event is imminent.

A *What If? Analysis* can complement a difficult judgment reached and provide the policymaker a thoughtful caution to accepting the conventional wisdom without considering the costs and risks of being wrong. This can help decision makers consider ways to hedge their bets, even if they accept the analytic judgment that an event remains unlikely.

The Method

What If? Analysis must begin by stating clearly the conventional analytic line and then stepping back to consider what alternative outcomes are too important to dismiss, even if unlikely. Brainstorming (p. 223) over a few days or weeks can develop one or more plausible scenarios by which the unlikely event occurs:

- Assume the event has happened.
- Select some triggering events that permitted the scenario to unfold to help make the "what if" more plausible; for example, analysts might postulate the death of a leader, a natural disaster, or some economic event that would start a chain of other events.
- Develop a chain of argumentation based as much on logic as evidence to explain how this outcome could have come about.
- "Think backwards" from the event in concrete ways– that is, specifying what must actually occur at each stage of the scenario is often very useful.
- Identify one or more plausible pathways or scenarios to the unlikely event; very often more than one will appear possible.
- Generate a list of indicators or "observables" for each scenario that would help to detect the beginnings of the event.
- Consider the scope of the positive and negative consequences of each scenario and their relative impacts.
- Monitor the indicators developed on a periodic basis.

Why Assess?

"Nothing is more wasteful than doing with great efficiency, that which is totally unnecessary!"[63]

Assessment is a process that measures progress toward accomplishing a task, creating an effect, or achieving an objective.

Assessment Considerations:

- Effective assessment systems focus on the end state and objectives.
- Measures of effectiveness are usually more important than measures of performance.
- Assessment's applicability transcends the spectrum of conflict and all phases of an operation.
- Effective assessment planning is not an afterthought, but built up front in planning.
- Assessment processes and metrics should be nested with the higher headquarters but designed and tailored to assess the specific objective of the unit.
- A good assessment system enables commanders to make timely shifts in resources to reinforce efforts.
- Assessment measures can be either quantitative or qualitative.
- Objectives, effects, and measures of effectiveness are interrelated.
- Assign responsibility for assessment.
- Understand other stakeholder's interests in an assessment system (coalition, interagency, enemy).

Assessment measures must be:

- Relevant: Assessment measures should directly relate to the envisioned operational end-state, objective, or mission. The less precise an end state the more difficult it is to define assessment measures.
- Appropriate: Should reflect the OE; be realistic and appropriate for the echelon.

- Measurable: Assessment measures can be qualitative or quantitative. To be measurable, a baseline must be established which accurately states the current situation in order to determine progress. Objective, quantitative criteria (metrics) are less subjective to error than qualitative or subjective criteria (metrics).
- Timely: Good assessment systems provide commanders timely feedback. Timeliness not only determines success or failure of efforts, but it also helps to reprioritize and reallocate resources as needed. Good assessment systems should be reasonable in the time required to input and use the system.
- Numerically Reasonable: Keep measures to a minimum to maintain focus on the most important and to enable recognition of success or failure to reallocate resources.
- Resourced: For any effective assessment system, planners must establish:
  - Who will observe?
  - When will we observe
  - How often will we observe?
- Nested (when appropriate) with Higher Headquarters Assessment Measures.
- Systemically (and graphically when appropriate) Displayed and Reviewed.
- Account for the "culture and expectations" found in the OE.

It should be emphasized that both MOE and MOP must be "measurable." If you can't Measure it, it can't be an MOE or an MOP. This means it must be stated in terms of "numbers." It should also be emphasized that while MOE are usually more important, if we don't look at MOP and we are not achieving the desired effect, we won't know if it's because we aren't doing the right thing or if it's because we're not doing things right. MOP must be looked at to rule out execution if the tasks aren't achieving the desired effect.

Measures of Performance (MOP)

- Criteria used to evaluate accomplishment of our actions.
- Should answer “Are we doing things right?”
- The criterion to assess friendly actions that is tied to measuring task accomplishment?
- Sometimes called a Measure of “EFFORT”

Example

Desired Effect: Reduction in popular support to criminal elements

Task: Influence populace to report crime &criminals

MOP: Number of face-to-face engagements with local leaders

Number of advertisements for tip-line numbers

Common Measures of Performance (MOP)

- Quantity
- Cost
- Schedule
- Productivity

Measures of Effectiveness (MOE)

- The criteria used to evaluate how actions have affected (changed) system behavior or capabilities.
- Should answer “Are we doing the right thing?”

Example

Desired Effect: Reduction in popular support to criminal elements

Task: Influence populace to report crime &criminals

MOE: Number of valid citizen reports of criminal elements

Number of valid citizen reports of criminal activities

Endnotes

[1] Gareth Morgan, “The 15-% solution,” The Change Page of the *Globe and Mail* (Toronto, ON: Philip Crawley, 1994).

[2] From Ken Booth’s book, *Strategy and Ethnocentrism*.

[3] Fisher, R., Ury, W. and Patton, B. (1991). *Getting to Yes: Negotiating Agreement Without Giving In.* Second Edition. New York: Penguin Books.102.

[4] Fisher, R., Ury, W. and Patton, B. (1991). *Getting to Yes: Negotiating Agreement Without Giving In.* Second Edition. New York: Penguin Books. 105.

[5] Fisher, R., Ury, W. and Patton, B. (1991). *Getting to Yes: Negotiating Agreement Without Giving In.* Second Edition. New York: Penguin Books. 107.

[6] Fisher, R., Ury, W. and Patton, B. (1991). *Getting to Yes: Negotiating Agreement Without Giving In.* Second Edition. New York: Penguin Books. 108.

[7] Daniel Kahneman, *Thinking, Fast and Slow* (New York: Farrar, Straus and Giroux, 2011), 4.

[8] *Thinking, Fast and Slow*, 8.

[9] Ibid., 98.

[10] J. Edward Russo and Paul J. H. Schoemaker, *Winning Decisions: Getting It Right the First Time* (New York: Currency, 2002), 165.

[11] Timothy Karcher, *Understanding the "victory Disease" from the Little Bighorn to Mogadishu and beyond* (Fort Leavenworth, Kan.: Combat Studies Institute Press, 2004), 2.

[12] Richards J. Heuer, *Psychology of Intelligence Analysis*. 2nd ed. (Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency, 1999), 70.

[13] Robert H. Lavenda and Emily A. Schultz, *Core Concepts in Cultural Anthropology*. 3rd ed. (Boston: McGraw-Hill, 2007), 21.

[14] Robert M. Utley, *Cavalier in Buckskin: George Armstrong Custer and the Western Military Frontier* (Norman: University of Oklahoma Press, 1988), 65 cited in Karcher, *Understanding the “Victory Disease,” From the Little Bighorn to Mogadishu and Beyond*, 40.

[15] Walter, Mason Camp and Kenneth M. Hammer, *Custer in '76: Walter Camp's Notes on the Custer Fight* (Provo, Utah: Brigham Young University Press, 1976), 107 cited in *Understanding the “Victory Disease,” From the Little Bighorn to Mogadishu and Beyond*, 40.

[16] Heuer, *Psychology of Intelligence Analysis*, 7-8.

[17] Army Doctrine Reference Publication (ADRP) 5-0, *The Operations Process*, (17 May 2012), 2-24.

[18] Dietrich Doerner, *The Logic of Failure: Recognizing and Avoiding Error in Complex Situations* (New York: Basic Books, 1996), 10.

[19] Evan Thomas in his book, *Sea of Thunder*, describes the naval actions in the Pacific during World War II between US commanders and their Japanese counterparts culminating in the Battle of Leyte Gulf. In particular the narrative describes how an experienced American commander was wedded to a preconception shaped by U.S. military culture, past experience fighting the Japanese, and a failure to consider other possibilities. Evan Thomas, *Sea of Thunder: Four Commanderes and the Last Great Naval Campaign 1941-1945* (New York: Simon and Schuster, 2006).

[20] Jim Garamone, "Gates Urges Restraint, Resolve for NATO," American Forces Press Service, 19 September 2008. Available at http://www.defense.gov/news/newsarticle.aspx?id=51250 (Accessed 29 August 2014). In his speech to the Oxford Analytica in Blenheim Place, England, Secretary of Defense Gates juxtaposed lessons of miscalculations, nationalism and hubris which led to WW I and the Munich 'appeasement.' He concluded "For much of the past century, Western psychology, rhetoric and policy-making on matters of war and peace has been framed by, and often lurched between, these two poles – between excessive pressures to take military action and excessive restraint, between a too eager embrace of the use of military force and an extreme aversion to it." Thus he concludes that the "lessons of history" may be over learned.

[21] Nassim Nicholas Taleb, T*he Black Swan: The Impact of the Highly Improbable* (New York: Random House, 2007).

[22] J. Koehler, "The Base-Rate Neglect Fallacy Reconsidered: Descriptive, Normative, and Methodological Challenges," *Behavioral and Brain Sciences* 19 (1996): 1-53 cited in Philip E. Tetlock, *Expert Political Judgment: How Good is It? How Can We Know?* (Princeton, NJ: Princeton University Press, 2005), 40.

[23] Philip E. Tetlock, *Expert Political Judgment How Good Is It? How Can We Know?* (Princeton, N.J.: Princeton University Press, 2005), 40.

[24] Ibid.

[25] Nassim Nicholas Taleb, *The Black Swan: The Impact of the Highly Improbable*, 2d Ed. (New York: Random House, 2010), Kindle Edition location 1653.

[26] Gary F. Marcus, *Kluge: The Haphazard Construction of the Human Mind* (Boston: Houghton Mifflin, 2008), 53.

[27] Taleb, *The Black Swan*, Chapter 6.

[28] Scott Plous, *The Psychology of Judgment and Decision Making* (Philadelphia: Temple University Press, 1993), 234-235.

[29] Wayne Michael Hall, *Stray Voltage: War in the Information Age. (*Annapolis, MD: Naval Institute Press, 2003). Mr. Hall defines will as "the resolution, sacrifice, and perseverance of individuals and groups of people to win in a competitive struggle."

[30] Drawn from Robert H. Lavenda and Emily A. Schultz, *Core Concepts in Cultural Anthropology* (Boston, Mass: McGraw Hill, 2007).

[31] The information from the Framing Audit Tool is derived from pages 30-31 and 45 of Winning Decisions, by J. Edward Russo and Paul J.H. Schoemaker.

[32] Mary L. Connerley and Paul Pedersen, *Leadership in a Diverse and Multicultural Environment: Developing Awareness, Knowledge, and Skills* (Thousand Oaks, Calif.: Sage Publications, 2005), xii.

[33] Gary Klein, *Sources of Power: How People Make Decisions* (Cambridge, Mass.: The MIT Press, 1998), 71.

[34] Ibid.

[35] Benjamin S. Bloom, *Taxonomy of Educational Objectives; the Classification of Educational Goals* (New York: Longmans, Green, 1956).

[36] Bloom.

[37] Doerner, *Logic of Failure*.

[38] Douglas MacEachin, Forward to *Psychology of Intelligence Analysis* (Washington, DC: CSI Publications, 1999). Available at https://www.cia.gov/library/center-for-the-study-of-intelligence/csi-publications/books-and-monographs/psychology-of-intelligence-analysis/index.html

[39] Helmuth von Moltke, *Militarische Werke*, vol. 2, part 2, pp. 33-40, translated and cited in Daniel J. Hughes (ed.), *Moltke on the Art of War: Selected Writings* (New York: Presidio Press, 1993), 45. Compare to the often quoted paraphrase, "No plan survives first contact with the enemy."

[40] Adapted from Lieutenant Colonel Richard King, *Thinking Skills Resources*. Unpublished draft, 2009, 69.

[41] Ibid., GL-5.

[42] Joint Publication (JP) 5-0, *Joint Operation Planning,* 11 August 2011, IV-7. See also the JP 5-0, GL-5. Available online from the Joint Electronic Library at http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf

[43] Ibid.

[44] Ibid., IV-8.

[45] M. Neil Browne and Stuart M. Keeley, *Asking the Right Questions: A Guide to Critical Thinking* (Upper Saddle River, NJ: Pearson Prentice Hall, 2007), 55.

[46] Ibid., 53.

[47] Ibid., 59.

[48] Ibid., 73.

[49] Ibid., 54-55.

[50] JP 2-0, I-26.

[51] A good example of how an analyst critically questioned a concept based upon its assumptions is found in, Antulio J. Echevarria II, *Rapid Decisive Operations – An Assumptions-Based Critique* (Carlisle: Strategic Studies Institute, 2001). Available at http://www.strategicstudiesinstitute.army.mil/pubs/display.cfm?pubID=218, accessed 8 August 2014.

[52] JP 5-0, IV-8.

[53] JP 2-0, I-26.

[54] Donald P. Wright, Timothy R. Reese with the Contemporary Operations Study Team, *ON POINT II: Transition to the New Campaign: The United States Army in Operation IRAQI FREEDOM May 2003–January 2005*, Fort Leavenworth, KS: Combat Studies Institute, 2008, pages 79 – 80.

[55] Timothy G. Malone, "The Red Team" Forging a Well-Conceived Contingency Plan, *Aerospace Power Journal*, Summer 2002, page 22.

[56] Peter D. Woodmansee, Timothy L. Faulkner and Wayne C. Blanchette, "The Need to Validate Planning Assumptions," *Military Review*. January – February 2005, pgs 58 - 62.

[57] JP 5-0, pgs IV-7 to IV-8.

[58] Ibid., pg IV-8.

[59] *Asking the Right Questions*, pg 2.

[60] J. Edward Russo and Paul J.H. Schoemaker, *Winning Decisions: Getting it Right the First Time* (New York: Doubleday, 2002), 21-33.

[61] Field Manual (FM) 3-55, *Information Collection*, 23 April 2012, pg 3-2.

[62] Information collection is… the Army's replacement [term] for intelligence, surveillance, and reconnaissance (ISR). ISR is a joint term, for which the Army revised to meet Army needs. FM 3-55, iii.

[63] Will Kaydos, *Measuring, Managing, and Maximizing Performance* (Cambridge, Mass.: Productivity Press, 1991), 17.

Bibliography

Army Doctrine Publication 5-0, *The Operations Process*. Washington, D.C.: Department of the Army, May 2012.

Barnet, Sylvan. *Critical Thinking, Reading, and Writing: A Brief Guide to Argument*. 7th ed. Boston, MA: Bedford/St. Martins, 2011.

Berens, Linda. *Understanding Yourself and Others: An Introduction to the 4 Temperaments, 4.0*. Los Angeles: Radiance House, 2010.

Bloom, Benjamin S. *Taxonomy of Educational Objectives*. New York: Longmans, Green, 1956.

Booth, Ken. *Strategy and Ethnocentrism*. New York: Holmes & Meier, 1979.

Brookfield, Stephen. *Developing Critical Thinkers: Challenging Adults to Explore Alternative Ways of Thinking and Acting*. San Francisco: Jossey-Bass, 1987.

Brookfield, Stephen. *The Skillful Teacher: On Technique, Trust, and Responsiveness in the Classroom*. San Francisco: Jossey-Bass Publishers, 1990.

Browne, M. Neil. *Asking the Right Questions: A Guide to Critical Thinking*. 8th Ed. Upper Saddle River, NJ, Pearson, 2007.

Burnet, John. *Plato's Euthyphro, Apology of Socrates, and Crito*. Oxford: Clarendon Press, 1977.

Camp, Walter Mason, and Kenneth M. Hammer. *Custer in '76: Walter Camp's Notes on the Custer Fight*. Provo, Utah: Brigham Young University Press, 1976.

"Carl Jung: Books." Carl Jung: Books. Accessed November 20, 2014. http://www.carljung.co/p/carl-jung-books.html.

CHAIRMAN OF THE JOINT CHIEFS OF STAFF INSTRUCTION 3126.01A. *Language, Regional Expertise, and Culture (LREC) Capability Identification, Planning and Sourcing*. 2013.

Claude Levi-Strauss, The Elementary Structures of Kinship. (Boston: Beacon Press, 1967), 10

Clausewitz, Carl Von, and Michael Howard. *On War*. Princeton, N.J.: Princeton University Press, 1976.

Ronald Cohen, "The Political System," in A Handbook of Method in Cultural Anthropology, eds. Raoul Naroll and Ronald Cohen, pp. 484-499. New

York & London: Columbia Press, 1970.

Connerley and Pedersen. *Leadership in a Diverse and Multicultural Environment: Developing Awareness, Knowledge, and Skills*. Thousand Oaks, CA: Sage Publications, 2005.

Cox, Taylor. *Cultural Diversity in Organizations: Theory, Research, and Practice*. San Francisco: Berrett-Koehler, 1993.

Demarest, Geoff. *Winning Irregular War*. Leavenworth, Kansas: Foreign Military Studies Office, 2014, pp. 153-154.

Dept of the Army of the US of America, ADP 5-0, *The Operations Process*. Washington, DC: GPO, 2012.

Dept of the Army of the US of America, Field Manual (FM) 3-55, *Information Collection*. Washington, DC: GPO, 2013

Dept of the Army of the US of America, *The United States Army Commander's Appreciation and Campaign Design*, 1st Ed, Ft Monroe VA, Washington, DC: GPO, 2008

Doerner, Dietrich. *The Logic of Failure: Why Things Go Wrong and What We Can Do to Make Them Right*. New York: Metropolitan Books, 1996.

Echevarria, Antulio Joseph. *Rapid Decisive Operations: An Assumptions-based Critique*. Carlisle Barracks, PA: Strategic Studies Institute, U.S. Army War College, 2001.

Elder, Linda, and Richard Paul. *The Miniature Guide to Critical Thinking: Concepts and Tools*, 6th Ed, Dillon Beach, CA, 2009.

Ennis, Robert Hugh. *Critical Thinking*. Upper Saddle River, NJ: Prentice Hall, 1996.

Facione, Peter A. *Critical Thinking: What It Is and Why It Counts*. Millbrae, CA: California Academic Press, 1998.

Fisher, R., Ury, W. and Patton, B. (1991). *Getting to Yes: Negotiating Agreement Without Giving In.* Second Edition. New York: Penguin Books.

Garamone, Jim. "Gates Urges Restraint, Resolve for NATO." *Armed Forces Press Service* (19 September 2008): Armed Forces Press Service, accessed 29 August 2014, http://www.defense.gov/news/newsarticle.aspx?id=51250 .

Geertz, Clifford. *The Interpretation of Cultures: Selected Essays*. New York: Basic Books, 1973.

Goodenough, Ward Hunt. *Culture, Language, and Society*. 2d ed. Menlo Park, Calif.: Benjamin/Cummings Pub., 1981.

Haight, G. "Managing Diversity." *Across the Board* 27, no. 3 (1990): 22-29.

Hall, Wayne M. *Stray Voltage: War in the Information Age*. Annapolis, Md.: Naval Institute Press, 2003.

Harris, Marvin. *Cows, Pigs, Wars & Witches: The Riddles of Culture*. New York: Random House, 1989.

Heuer, Richards J. *Psychology of Intelligence Analysis*. 2nd ed. Washington, D.C.: Center for the Study of Intelligence, Central Intelligence Agency, 1999.

Hofstede, Geert H., and Gert Jan Hofstede. *Cultures and Organizations: Software of the Mind: Intercultural Cooperation and Its Importance for Survival*. Rev. and Expanded 3rd ed. New York: McGraw-Hill, 2010.

Janis, Irving L. *Groupthink: Psychological Studies of Policy Decisions and Fiascoes*. 2nd ed. Boston: Houghton Mifflin, 1982.

Jason, Gary James. *Critical Thinking: Developing an Effective Worldview*. Belmont, CA: Wadsworth Thomson Learning, 2001.

Joint Chiefs of Staff, Joint Publications (JP) 2-01.3. *Joint Intelligence Preparation of the Operational Environment*. Washington D.C., 2009.

Joint Chiefs of Staff, Joint Publications (JP) 5-0, *Joint Operation Planning*, Washington D.C, 11 August 2011.

Jones, Morgan D. *The Thinker's Toolkit: Fourteen Skills for Making Smarter Decisions in Business and in Life*. New York: Times Business, 1995.

Jowett, Benjamin. *Six Great Dialogues*. Mineola, N.Y.: Dover Publications, 2007.

Jung, C. G. *Memories, Dreams, Reflections*. New York: Pantheon Books, 1963.

Kahneman, Daniel. *Thinking, Fast and Slow*. New York: Farrar, Straus and Giroux, 2011.

Karcher, Timothy. *Understanding the "victory Disease" from the Little Bighorn to Mogadishu and beyond*. Fort Leavenworth, Kan.: Combat Studies Institute Press, 2004.

Kaydos, W. J. *Measuring, Managing, and Maximizing Performance: What Every Manager Needs to Know about Quality and Productivity to Make Real Improvements in Performance*. Cambridge, Mass.: Productivity Press, 1991.

Keesing, Roger. "Toward a Model of Role Analysis." In *A Handbook of Method in Cultural Anthropology*, edited by Raoull Naroll and Ronald Cohen, 423-453. New York: Columbia University Press, 1970.

"Keirsey Temperament Website." Keirsey Temperament Website. Accessed November 20, 2014. http://keirsey.com/keirseybooks.aspx.

King, Richard. *Thinking Skills Resources*, unpublished draft. 2009.

Klein, Gary A. *Sources of Power How People Make Decisions*. 2nd MIT Press Pbk. ed. Cambridge, Mass.: MIT Press, 1999.

Kluckhohn, Florence Rockwood, and Fred L. Strodtbeck. *Variations in Value Orientations*. Evanston, Ill.: Row, Peterson, 1961.

Koehler, J. "The Base-Rate Neglect Fallacy Reconsidered: Descriptive, Normative, and Methodological Challenges." *Behaviorial and Brain Sciences*, 19 (1996): 1-53.

Lavenda, Robert H., and Emily A. Schultz. *Core Concepts in Cultural Anthropology*. 3rd ed. Boston: McGraw-Hill, 2007.

Malone, Timothy. "The Red Team Forging a Well-Conceived Contingency Plan." *Aeorspace Power Journal* Summer 2002 (2002): 58-62. Accessed January 1, 2014. http://www.airpower.maxwell.af.mil/airchronicles/apj/apj02/sum02/malone.html .

Marcus, Gary F. *Kluge: The Haphazard Construction of the Human Mind*. Boston: Houghton Mifflin, 2008.

Moltke, Helmuth Von. *Militärische Werke*. Vol. 2. Berlin: Mittler, 1904.

Moltke, Helmuth, and Daniel J. Hughes. *Moltke on the Art of War: Selected Writings*. Novato, CA: Presidio Press, 1993.

Morgan, Gareth. “The 15-% Solution” from the Change page of the *Globe and Mail.* Toronto, Ontario: Philip Crawley, 1994.

"Personality Dimensions®." Personality Dimensions®. Accessed November 20, 2014. http://www.personalitydimensions.com/.

Plous, Scott. *The Psychology of Judgment and Decision Making*. Philadelphia: Temple University Press, 1993.

"Quotations by Author." Bertrand Russell Quotes. Accessed November 24, 2014. http://www.quotationspage.com/quotes/Bertrand_Russell/ .

"Ralph Waldo Emerson Quote :." "Most of the Shadows Of..." Accessed November 24, 2014. http://www.wisdomquotes.com/quote/ralph-waldo-emerson-162.html .

Roger Fisher & William Ury. *Getting to Yes.* 102, 105, 107, 108.

Rotkoff, Steven. "Introspection and Emotional Vulnerability as Leader Development and Team Building Tools." *Small Wars Journal*. May 31, 2011. Accessed November 20, 2014. http://smallwarsjournal.com/blog/journal/docs-temp/777-rotkoff.pdf.

Russo, J. Edward, and Paul J. H. Schoemaker. *Winning Decisions: Getting It Right the First Time*. New York: Currency, 2002.

Salmoni, Barak A., and Paula Eber. *Operational Culture for the Warfighter: Principles and Applications*. 2nd ed. Quantico, Va.: Marine Corps University ; Washington, DC :, 2012.

Senge, Peter M. *The Fifth Discipline: The Art and Practice of the Learning Organization*. New York: Doubleday/Currency, 2006.

Stewart, Kate. *Interpersonal Communications Skills Workbook*.

Taleb, Nassim Nicholas. *The Black Swan: The Impact of the Highly Improbable*. New York: Random House, 2007.

Tetlock, Philip E. *Expert Political Judgment How Good Is It? How Can We Know?* Princeton, N.J.: Princeton University Press, 2005.

Thomas, Evan. *Sea of Thunder: Four Commanders and the Last Great Naval Campaign, 1941-1945*. New York: Simon & Schuster, 2006.

University of Foreign Military and Cultural Studies. *Red Team Handbook*, v. 5. Fort Leavenworth, KS: UFMCS, 15 April 2011.

Utley, Robert M. *Cavalier in Buckskin: George Armstrong Custer and the Western Military Frontier*. Norman, OK: University of Oklahoma Press, 1988.

Williams, Scott. "Self-Awareness and Personal Development." Self-Awareness and Personal Development. Accessed November 20, 2014. http://www.wright.edu/~scott.williams/LeaderLetter/selfawareness.htm.

Wright, Donald P., and Timothy R. Reese. *The United States Army in Operation Iraqi Freedom, May 2003-January 2005: On Point II : Transition to the New Campaign*. Fort Leavenworth, KS: Combat Studies Institute Press, 2008.

Zinni, Anthony, and Joe Strange. "Non-Traditional Military Missions: Their Nature, and the Need for Cultural Awareness & Flexible Thinking." In *Capital "W" War: A Case for Strategic Principles of War : (because Wars Are Conflicts of Societies, Not Tactical Exercises Writ Large)*, 282. Quantico, VA: Marine Corps University, 1998.

Abbreviations

Abbreviations

ACH	Analysis of Competing Hypothesis
ADM	Army Design Methodology
ADP	Army Doctrine Publication
ADRP	Army Doctrine Reference Publication
AO	Area of Operations
BCT	Brigade Combat Team
CAP	Crisis Action Planning
CCIR	Commander's Critical Information Requirement
CGSC	Command & General Staff College
CINC	Commander In Chief
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
COA	Course of Action
COG	Centers of Gravity
CVs	Critical Variables
DOD	Department of Defense
ECOA	Enemy Course of Action
ESP	Extrasensory Perception
EVE	Evaluation of Evidence
HUMINT	Human Intelligence
HVT	High Value Targets
ISR	Intelligence, Surveillance, and Reconnaissance
JIIM	Joint Interagency, Intergovernmental, and Multinational
JP	Joint Publication
LOE	Lines of Effort
LOO	Lines of Operation
LREC	Language Regional Expertise and Culture
MDMP	Military Decision Making Process
MOE	Measures of Effectiveness
MOM	Motive, Opportunity and Means

MOP	Measures of Performance
MOSES	Manipulability of Sources
MRX	Mission Rehearsal Exercise
OE	Operational Environment
OEF	Operation Enduring Freedom
OEL	Operational Environment Laboratory
OIF	Operation Iraqi Freedom
OPLAN	Operations/Operational Plan
OPORD	Operations Order
OPT	Operational Planning Team
PGM	Precision guided munitions
PMESII	Political, Military, Economic Social, Infrastructure, Information
PT	Physical Environment and Time (US Army)
POP	Past Opposition Practices
REC	Regional Expertise and Culture
RT	Red Team or Red Teaming
RTHB	Red Team Handbook
SEEI	State, Elaborate, Exemplify, Illustrate
SME	Subject Matter Expert
SOP	Standard Operating Procedure
SWOT	Strengthens, Weakness, Opportunities & Threats
TRADOC	United States Army Training and Doctrine Command
TTP	Tactics, Techniques and Procedures
UFMCS	University of Foreign Military and Cultural Studies
USAFAS	United States Army Field Artillery School
WMD	Weapons of Mass Destruction
XO	Executive Officer

Index

2nd & 3rd order 193, 198
alternative futures 80
analysis 113
apperception 32, 38
assessment 143
assumption .. 112, 114, 151
assumptions check 156
Bloom 196, 229, 231
Booth 41, 227, 231
brainstorming 89
Browne ... 45, 56, 212, 213, 218, 229, 231
center of gravity .. 119, 186
Clausewitz 57, 231
critical actors 115
culture 116
deductive. 52, 53, 108, 114
demographics 115
devil's advocacy 145
Doerner ... 54, 99, 227, 232
Douglas 210, 229
economics 119
empathy 28, 36, 207
external organizations . 118
Hall 228
Hofstede .. 29, 42, 161, 233
hypotheses, competing . 83
hypothesis testing 192
indicators or signposts 154
inductive 53, 108, 114, 143
information 117
initiatives group 172
Janis ... 57, 58, 59, 72, 233
Jung 9, 20, 21, 231, 233
Klein 165
Lavenda 228
listening 17
Malone 230
mental simulation 166
military capabilities 116
national will 118
personality ... 6, 10, 19, 173
physical environment ... 115
PMESII 27, 34, 180, 220
receipt of mission 111
Reese 230
relationships 116
religion 120
Russo 50, 56, 227, 229, 230, 235
Schoomaker 1, 8
Schultz 228
self, core 20
Senge 54, 184, 235
stakeholder mapping ... 186
strategic questioning 16
system 32, 54, 76, 100, 208, 224
System 6
team A/team B 205
technology 118
Thomas 6, 228, 235
time 119
what if? analysis .. 222, 223
Zinni 22, 216, 235

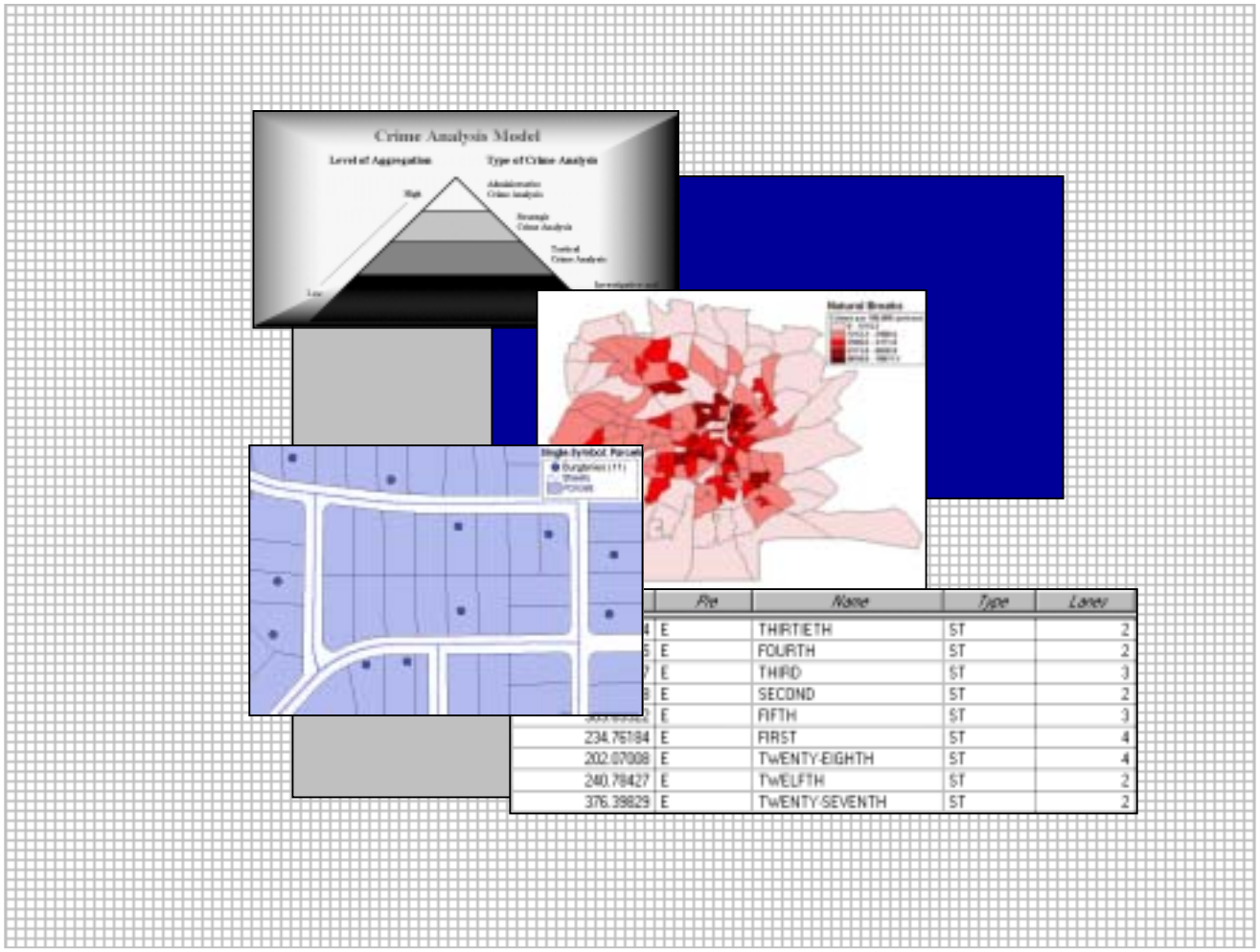
My Notes

This Page Is Intentionally Left Blank

COPS

COMMUNITY ORIENTED POLICING SERVICES
U.S. DEPARTMENT OF JUSTICE

INTRODUCTORY GUIDE TO CRIME ANALYSIS AND MAPPING



Introductory Guide to Crime Analysis and Mapping

Written by:
Rachel Boba, Ph.D.
Director, Crime Mapping Laboratory
Police Foundation

November 2001
Report to the Office of Community Oriented Policing Services
Cooperative Agreement #97-CK-WXK-004

The opinions, findings, and conclusions or recommendations expressed in this document are those of the authors and do not necessarily represent the official position or policies of the U.S. Department of Justice.

Acknowledgements

The author would like to thank Kristin Quayle for transcribing our training session during her summer here at the Police Foundation, as well as Mary Velasco and Erin Lane, Research Associates at the Police Foundation, for their careful review and comments.

Page

I. Introduction 8

II. Introduction to Crime Analysis 9

Definition of Crime Analysis 9

Types of Crime Analysis 11
- ***Intelligence Analysis*** *11*
- ***Criminal Investigative Analysis*** *12*
- ***Tactical Crime Analysis*** *13*
- ***Strategic Crime Analysis*** *13*
- ***Administrative Crime Analysis*** *14*

Crime Analysis Model 15

III. Introduction to Crime Mapping 17

Historical Overview 17

Types of Mapping 18
- ***Manual Pin Mapping*** *18*
- ***Computer Mapping*** *19*
- ***Geographic Information System (GIS)*** *19*
- ***Crime Analysis Mapping*** *20*
- ***GIS Components*** *20*
  - *Data representation* *20*
    - *Point feature* *20*
    - *Line feature* *21*
    - *Polygon feature* *21*
    - *Image feature* *22*
  - *Data of geographic features* *23*
    - *Point data* *23*
    - *Line data* *24*
    - *Polygon data* *24*

Page

GIS toolbox *25*
Connectivity *25*
Contiguity *26*
Geometry *26*
Visual display/mapping *27*
Thematic approach *27*
Scale *28*
Querying GIS data *31*
Tabular queries *31*
Spatial queries *32*

IV. Introduction to Problem Solving 34

Definition of Problem Solving 34

SARA Approach to Problem Solving 34
Scanning ***34***
Analysis ***34***
Response ***35***
Assessment ***35***

Crime Analysis and Problem Solving 36

V. Data and Geocoding 37

Types of Data 37
Tabular Data ***37***
Geographic Data ***37***

General Data Integrity Issues 38
Data Entry ***38***
Timeliness ***38***
Data Validity ***38***
Reliability ***39***
Data Transfer Process ***39***
Data Confidentiality/Privacy ***39***

Page

Data Management **40**
Metadata ***40***
Geocoding ***40***
Introduction *40*
The geocoding process *41*
Step 1: Prepare the geographic and tabular files for geocoding *41*
Step 2: Specify geocoding parameters *45*
Step 3: Geocode *46*
Step 4: Review results *48*
Step 5: If necessary, respecify parameters and geocode again *50*
Conclusion *51*

VI. Spatial Analysis Techniques 52

Single Symbol Mapping **52**

Graduated Mapping **55**
Graduation By Size ***55***
Graduation By Color ***57***
Classification Methods ***59***
Natural breaks *59*
Quantile *60*
Equal area *61*
Equal interval *62*
Standard deviation *63*
Custom *65*

VII. Crime Analysis Product Format and Dissemination 67

Factors to Consider **67**

Methods of Dissemination **67**

Components of Crime Analysis Products **68**

Page

Types of Crime Analysis Products 68

General Crime Analysis Product Elements 70

Map Design Elements..... 71

Evaluating the Utility of Crime Analysis and Mapping Products 73

VIII. References 74

I. Introduction

The following guide was developed from the curriculum for the "Introduction to Crime Analysis Mapping and Problem Solving" training course conducted by members of the Police Foundation's Crime Mapping Laboratory in 2001 and funded by the Office of Community Oriented Policing Services (COPS). The purpose of this document is to convert the information presented in the training into a succinct and readable report that makes it available to a larger audience than was reached through the training sessions. It is not intended to be a comprehensive document on crime analysis, crime mapping, and problem solving, but rather a "starter" guidebook for someone just entering the field or a reference manual for current crime analysts or other law enforcement analysts. The format of the document follows the format of the training slides loosely, but it is not necessary to read them together. This document stands on its own. For further reading on crime analysis and mapping, see other relevant documents written by the Police Foundation at www.policefoundation.org or www.cops.usdoj.gov.

II. Introduction to Crime Analysis

As an introduction to crime analysis, this section provides the definition of crime analysis as a general concept as well as definitions of five types of crime analysis. These definitions are used in the Police Foundation's "Introduction to Crime Analysis Mapping and Problem Solving" course and have been created to synthesize current concepts and ideas in the field of crime analysis. These definitions are meant to enhance the understanding of crime analysis and to help create commonly understood terminology. The latter part of this section includes a hierarchical model by which all five types of crime analysis are related to one another.

Definition of Crime Analysis

> *The qualitative and quantitative study of crime and law enforcement information in combination with socio-demographic and spatial factors to apprehend criminals, prevent crime, reduce disorder, and evaluate organizational procedures.*

Qualitative and quantitative. Crime analysis uses both qualitative and quantitative data and analytical techniques. Qualitative data and analytical techniques refer to non-numerical data as well as the examination and interpretation of observations for the purpose of discovering underlying meanings and patterns of relationships. This is most typical of field research, content analysis, and historical research. Quantitative data are data primarily in numerical or categorical format. Quantitative analysis consists of manipulations of observations for the purpose of describing and explaining the phenomena that those observations reflect and is primarily statistical. Crime analysis employs both types of data and techniques depending on the analytical and practical need. For example, crime data can be used in various ways, both quantitatively and qualitatively. The information such as date, time, location, and type of crime is quantitative in that statistics can be used to analyze these variables. On the other hand, narratives of crime reports are considered qualitative data in that a large number of narratives are nearly impossible to analyze statistically and are primarily examined to determine general themes and patterns.

Study. Study is a systematic way of looking at crime and law enforcement information. That is, crime analysis is not examining information haphazardly but rather is applying formal analytical and statistical techniques as well as research methodology to law enforcement information according to the rules of social science.

Crime. In a law enforcement agency, the central focus is crime, both those reported to the police and those that are not. Thus, the central type of data analyzed is crime and the information surrounding it, such as arrests, offenders, victims, property, and evidence.

Law enforcement information. In addition to crime, law enforcement agencies address many other issues and thus collect many other types of data. Examples of law enforcement data that are often available for crime analysts are calls for service (e.g., noise complaints, burglary alarms, suspicious activity), traffic information (e.g., accidents and citations), citizens' perceptions (e.g., fear of crime, crime prevention behavior, satisfaction with the police), victimization, probation records, and parole information.

In combination with… This phrase refers to identifying patterns and studying relationships of crime and law enforcement data with other types of information, such as those listed below.

Socio-demographic. This type of information refers to characteristics of individuals and groups such as sex, race, income, age, and education. On an individual (micro) level, socio-demographic information is used in law enforcement to search for and identify crime suspects. On a macro level, socio-demographic information is used to determine the characteristics of groups and how they relate to crime. For example, the information may be used to answer the questions, "Where can we find the suspect who is a white male, 30-35 years of age with brown hair and brown eyes?" or "Can demographic characteristics explain why one neighborhood has a higher rate of crime than another?"

Spatial. The location where crimes or activities occur and the relationship of those places to one another and to other information is an important factor in the analysis of crime. It is not only important where a crime takes place but also the characteristics of those places and the environment in which the crime occurs. Thus, examination of spatial data such as streets networks, parcel information, orthophotographs, school locations, business and residential zoning, among others, is imperative for effective crime analysis.

The last four key points describe the four goals of crime analysis.

Apprehending criminals. The main function of crime analysis is to support law enforcement endeavors. One of the primary goals of law enforcement is the apprehension of criminals; consequently, one of the primary goals of crime analysis is to assist in the apprehension of criminals. For example, a detective may have a robbery incident in which the suspect has a snake tattoo on his left arm. The crime analysts may assist by searching a database of field incident cards to identify

individuals with such a tattoo. Also, a crime analyst may conduct a time of day/day of week analysis of burglary incidents that would assist officers in surveillance of an area to catch offenders.

Prevent crime. Another primary goal of law enforcement is to prevent crime through methods other than apprehension. This goal lends itself particularly well to assistance from crime analysis. For example, members of the police department are conducting a crime prevention campaign about residential burglary and would like to target their resources in the areas that need it the most. Crime analysis can assist in planning community education and patrol response tailored to the problem by providing spatial analysis of residential burglary, analysis of how, when, and where the burglaries occurred, and analysis of what items were stolen. This information could be used to develop crime prevention suggestions such as closing and locking a garage door.

Reduce disorder. Many criminologists contend that social disorder can lead to crime; that is, blight and other indicators of social decay left unchecked can attract crime and accelerate further decay. Thus, reducing disorder is a law enforcement objective and, by extension, one for crime analysis as well. Crime analysis can assist with these efforts by providing research and analysis of disorder indicators such as traffic accidents, noise complaints, or trespass warnings that can assist officers in addressing these issues before they become more serious problems.

Evaluate organizational procedures. The fourth goal of crime analysis is assisting with the evaluation of organizational procedures. Several examples include resource allocation, the assessment of crime prevention programs, realigning geographic boundaries, forecasting staffing needs, and developing performance measures for the police department.

Types of Crime Analysis

The following are five types of analysis that fall under the umbrella of crime analysis. As you will see, each contains characteristics of crime analysis in general, but each is specific in the type of data and analysis used as well as in its purpose.

Intelligence Analysis

> *The study of "organized" criminal activity, whether or not it is reported to law enforcement, to assist investigative personnel in linking people, events, and property.*

The purpose of intelligence analysis is to assist sworn personnel in the identification of networks and apprehension of individuals to subsequently prevent criminal

activity. A related goal is to link information together, prioritize information, identify relationships, and identify areas for further investigation by putting the analysis in a framework that is easy to understand. Much of the information analyzed in the field of intelligence analysis is not reported to the police by citizens but is gathered by law enforcement. Examples of data collection methods include surveillance, informants, and participant observation. In addition, the type of information is not limited to criminal information but can include telephone conversations, travel information, financial/tax information, and family and business relationships. Intelligence analysis has traditionally focused more or less on organized criminal activity, which includes drugs and prostitution syndicates. The data analyzed are plentiful and primarily qualitative, and thus are usually analyzed through qualitative methods. In light of the events of September 11, 2001, intelligence analysis has most recently begun to focus on terrorist activity at the local level as well.

Criminal Investigative Analysis

> *The study of serial criminals, victims, and/or crime scenes as well as physical, socio-demographic, psychological, and geographic characteristics to develop patterns that will assist in linking together and solving current serial criminal activity.*

This type of analysis has also been called "profiling," which is the process of constructing a "profile" of an unknown offender based on the nature of the crime, the facts of the case, and the characteristics of the victim. As with intelligence analysis, this type of analysis focuses primarily on qualitative data surrounding serious serial crimes such as murder and rape. Data are collected and analyzed on an individual level for those persons primarily or peripherally involved with the incidents. The spatial nature of the incidents and related locations such as the body dump sites or the encounter sites is also considered. The primary purpose of criminal investigative analysis is to develop patterns of serial crimes crossing city, state, and even national boundaries by linking behavior and evidence within and among incidents in order to catch the offender and/or clear cases. This is a very specific type of crime analysis that is primarily done on the federal law enforcement level since these types of crime occur infrequently and cross jurisdictional boundaries.

Tactical Crime Analysis

> *The study of recent criminal incidents and potential criminal activity by examining characteristics such as how, when, and where the activity has occurred to assist in problem solving by developing patterns and trends, identifying investigative leads/suspects, and clearing cases.*

Tactical crime analysis focuses on information from recent crimes reported to the police. "Recent" can refer to the last few months or longer periods of time for specific ongoing problems. Tactical crime analysis also focuses on specific information about each crime such as method of entry, point of entry, suspects actions, type of victim, type of weapon used, as well as the date, time, location, and type of location. Field information such as suspicious activity calls for service, criminal trespass warnings, and persons with scars, marks, or tattoos collected by officers is also considered in the analysis. Although quantitative analysis is often conducted once a pattern has been identified, qualitative analysis, (i.e., critical thinking and content analysis) is used to identify patterns and trends initially. Three purposes of tactical crime analysis are 1) linking cases together and identifying the notable characteristics of the patterns and trends, 2) identifying potential suspects of a crime or crime pattern, and 3) clearing cases. The focus of tactical crime analysis is examining data daily in order to identify patterns, trends, and investigative leads for recent criminal and potential criminal activity. Once a crime pattern, suspect, or investigative lead is identified, the information is compiled and disseminated to patrol officers and detectives.

Strategic Crime Analysis

> *The study of crime and law enforcement information integrated with socio-demographic and spatial factors to determine long term "patterns" of activity, to assist in problem solving, as well as to research and evaluate responses and procedures.*

Strategic crime analysis consists primarily of quantitative analysis of aggregate data. Monthly, quarterly, and/or yearly compilations of criminal and non-criminal information such as crime, calls for service, and traffic information are analyzed in aggregate form. That is, general categories such as date, time, location, and type of incident are analyzed instead of qualitative data such as narrative descriptions of incidents. Variables including race, class, sex, income, population, location, and location type are examined along with law enforcement information in the analysis process. The two primary purposes of strategic crime analysis are 1) to assist in the identification and analysis of long-term problems such as drug activity or auto theft and 2) to conduct studies to investigate or evaluate relevant responses and procedures. Both of these purposes correspond very well to the problem solving process (see

Section IV for a discussion of crime analysis and problem solving specifically). These types of studies include evaluation of crime prevention programs, in depth examination of a particular crime problem, and implementation of a survey of citizens' perceptions of crime and the police. They incorporate pre- and post-measurement as well as both impact and process evaluation methodology. Procedures examined include such activities as deployment and staffing, redistricting of beats or precincts, data entry and integrity, and the reporting process. In sum, strategic crime analysis uses statistical techniques and research methods to investigate long-term problems and evaluate organizational procedures. Analysts who primarily conduct strategic crime analysis are also called problem or research analysts.

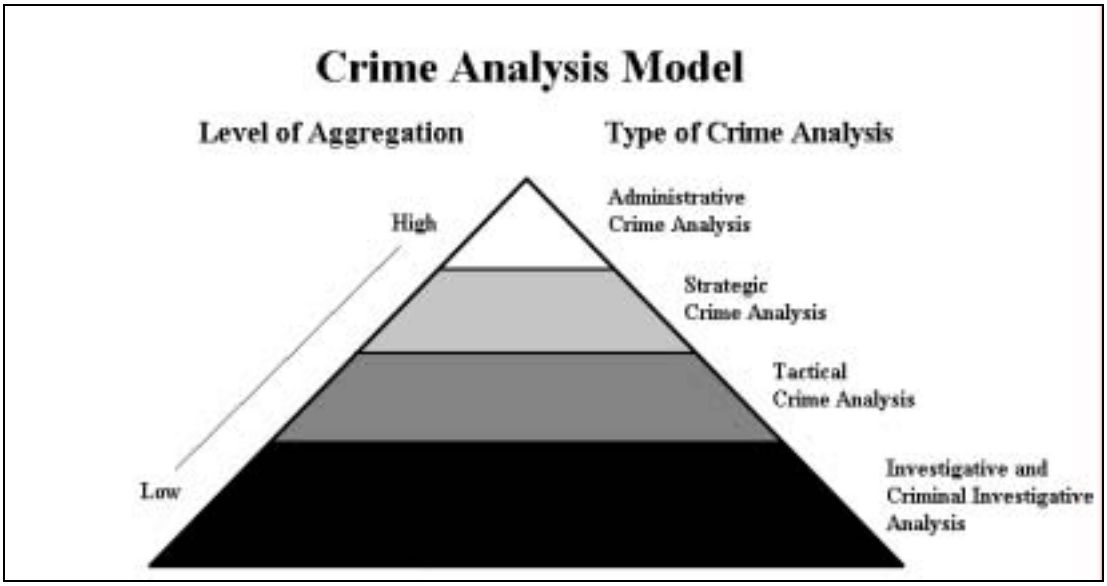
Administrative Crime Analysis

> *The presentation of interesting findings of crime research and analysis based on legal, political, and practical concerns to inform audiences within law enforcement administration, city government/council, and citizens*.

Administrative crime analysis is different from the previous types of analysis in that it refers to presentation of findings rather than to statistical analysis or research. The decision of what and how to present information is the primary focus of administrative crime analysis. Often, the type of information that is presented represents the "tip of the iceberg" of all the work and analysis that has previously been done, for example, an executive summary of a report. The purpose and the audience of the information determine "what" is presented along with legal (e.g., privacy and confidentiality), political (e.g., union issues, election concerns), and practical concerns (e.g., complexity of the information presented). The primary purpose of administrative crime analysis is to inform audiences. These audiences may vary from one situation to the next, which is why the type and quantity of information should vary as well. Audiences can be police executives, city council, media, citizens, and neighborhood groups or a combination. An excellent example of administrative crime analysis is the use of the Internet to provide information to the general public. Audiences of a police Internet site include citizens, police personnel, businesses, victims, criminals, and media—essentially everyone; therefore, the type of information published should be appropriate for an array of diverse customers. The information provided should be simple, clear, and concise and should not disclose sensitive information. One rule of thumb would be to only publish information that one would be comfortable seeing on the evening news.

Crime Analysis Model

The following figure displays how all of these types of crime analysis relate to one another in terms of the level of aggregation of the information. That is, types with low levels of aggregation focus on individual cases and used qualitative data and analysis techniques and those with high levels of aggregation focus on a limited scope of larger amounts of data and information. At the top of the figure, criminal investigative analysis and intelligence analysis utilize the least aggregated and most qualitative data. The data consist of information about informal networks of criminals and their non-criminal acquaintances and relatives as well as where individuals live, work, and "play." The focus here is on the specifics of criminals, the nature of their crimes, their relationships, and their lives in general.



Tactical crime analysis utilizes only crimes and activity reported to the police so the data are more aggregate and somewhat less abundant than those used for criminal investigative and intelligence analysis. Tactical crime analysis is primarily qualitative in nature but depending on the data, quantitative techniques can be used to describe characteristics of a given pattern such as the most common time the crimes occur (time series) or where the crimes are located in relationship to one another.

Strategic crime analysis utilizes large amounts of data that are even more aggregated than tactical and investigative data. For example, information used in tactical crime analysis is primarily made up of crime incidents but includes such information as date, time, location, methods of the crime, and detailed description of the crime. Strategic crime analysis focuses only on those variables that can be easily quantified, such as date, time, location, type of location, type of crime, and priority. Thus, the

type of analysis is more quantitative and the large amount of data calls for statistical operations instead of reading and examining each case individually.

Finally, administrative crime analysis in this figure is literally the "tip" of the triangle in level of aggregation. The focus is presenting the most aggregate or summary information to a variety of audiences.

Overall, these types of analysis fall under the general definition of crime analysis in that each one contains some of the key components of crime analysis. For the purposes of the rest of this report, we will focus on examples of the last three types of analysis, tactical, strategic, and administrative, as they are the types of analysis that are most likely to be conducted on a regular basis by a crime analyst in an average law enforcement agency.

III. Introduction to Crime Analysis Mapping

Historical Overview

The following chart is a brief outline of the history of crime mapping (taken from Weisburd and McEwen, 1997; and Harries, 1999). Mapping itself has a long history, but crime mapping specifically can be traced back to the early 1800s when social theorists began to create maps to illustrate their theories and research about crime. In relation to crime and policing, maps initially were used to examine issues like poverty or demographic characteristics and crime. One of the first police departments to use mapping was New York City in the 1900s. The maps consisted of simple wall maps in which "push pins" were used to indicate crimes that had occurred. During the 1920s and 1930s, sociologists at the University of Chicago used mapping to examine crime and delinquency, specifically juvenile delinquency and related social characteristics. In the 1960s and 1970s, the first computer-generated maps of crime were created. (See Weisburd and McEwen, 1997 for more information).

Early 1800s:	Social Theorists: Single symbol point and graduated area maps
1900s:	New York City Police Department and others: Single symbol point maps, "pin maps"
1920s-30s:	Urban sociologists at the University of Chicago: Graduated area maps of crime and delinquency
1960s-70s:	First computer generated maps of crime
1980s:	Desktop computers available for mapping, but with limited quality; Environmental Criminology theory
1990s:	Desktop GIS and integration with law enforcement systems and data; government funding, etc.

In the 1980s, more advanced technology and desktop computers became available, and more widely used. However, the quality of computerized mapping at that time was limited because of slow processing speeds and poor printing quality. At the same time, environmental criminology theory began to emerge, and academics began to examine the spatial characteristics of crime as well as how location characteristics

might contribute to criminal activity at particular locations over others. In the 1990s, desktop geographic information systems (GIS) became widely available, and in the late 1990s, they began to be generally used by law enforcement agencies and criminologists.

Most recently in the late 1990s, Federal programs such as the Crime Mapping Research Center (National Institute of Justice) and the Crime Mapping and Analysis Program (National Institute of Justice, National Law Enforcement and Corrections Technology Center) were established. As part of its $1 billion Making Officer Redeployment Effective (MORE) program, from fiscal years1995-1998 and in fiscal year 2001, the COPS Office provided funds to law enforcement agencies to acquire crime mapping software and hardware. As with all MORE funded technology, the purpose of this software and hardware was to enhance community policing activities through timesavings and increased officer effectiveness. Since 1995, the Police Foundation's Crime Mapping Laboratory has been funded by COPS to assist police agencies in incorporating crime mapping into their practices. In addition, universities and colleges have begun to offer undergraduate and graduate courses in crime analysis and crime mapping.

Types of Mapping

Manual Pin Mapping

Wall maps have long been a simple and useful way to depict crime incidents or hot spots. Many police departments still have large maps tacked to the wall of the briefing room with the most recent crimes represented by pins. Although useful, manual wall maps, offer limited utility because they are difficult to keep updated, keep accurate, make easy to read, and can only display a limited amount of data. For example, although different colored pins could be used to represent different types of crime, date and time of incidents, the nature of incidents, and other information cannot be displayed easily. In order to update a manual wall map, for example, the pins must be removed each month. Unless a photo or some other mechanism is used to record the previous month's map, the information illustrated on the map is lost. Thus, comparison is difficult, if not impossible, from one month to the next. Finally, the maps become unreadable when they display large amounts of data because of the numerous pins and/or holes.

Computer Mapping

The following is an example of a computer map. It has been taken from MapQuest©, an Internet mapping program, where an address is entered and a map of the surrounding area appears with a pin to locate the address.

Even though it is possible to zoom in and out of this type of map, the geographic features (e.g., locations, streets, parks) are static and cosmetic only. In essence, a computer map is similar to a wall map, in that the computer is used to place a point at a specific location just as a person would put a pin on a wall map. Thus, computer maps have limitations similar to wall maps. For instance, when using MapQuest© to map an address, clicking on a point will not provide information behind that point, such as the specific address. While visually appealing and easy to use, computer mapping does not allow any more effective analysis than manual pin mapping.

Geographic Information System (GIS)

> *A geographic information system (GIS) is a set of computer-based tools that allow a person to modify, visualize, query, and analyze geographic and tabular data.*

A GIS is a powerful software tool that allows the user to create anything from a simple point map to a three-dimensional visualization of spatial or temporal data. A GIS is different from manual pin maps and computer maps in that it allows the analyst to view data behind the geographic features, combine various features, manipulate the data and maps, and perform statistical functions. There are many different types of GIS programs, which include desktop packages (e.g., ArcView®, MapInfo®, GeoMedia®, Atlas GIS®, Maptitude®) as well as professional software (e.g., ArcInfo® and Intergraph®).

Crime Analysis Mapping

"Crime mapping" is a term that has been used for the past few years to refer to research analysis using GIS in a law enforcement setting. In this report, the term crime analysis mapping is used to describe this process because using a GIS to analyze crime is not just the act of placing incidents on a map but also of analysis. Consequently, "crime analysis mapping" is:

> *The process of using a geographic information system in combination with crime analysis techniques to focus on the spatial context of criminal and other law enforcement activity.*

GIS Components

The following is a description of the major components of a GIS, which include data representation, data features, visualization, scale, and querying.

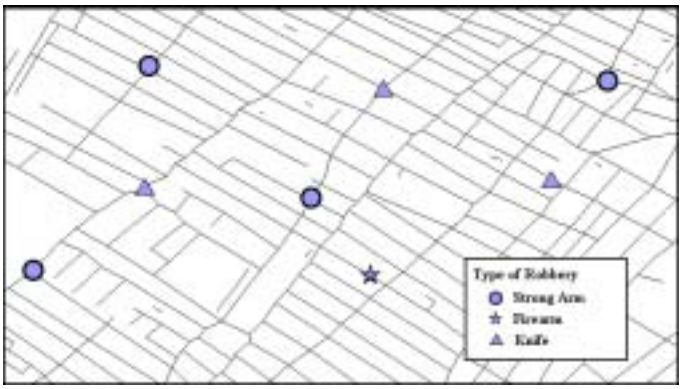
Data representation

Real world data are represented by one of four features in a GIS. They include point, line, polygon, and image features.

Point feature

> *A point feature is a discrete location that is usually depicted by a symbol or label.*

A point feature in the geographic information system is analogous to a pin placed on a paper wall map. Different symbols are used to depict the location of crimes, motor vehicle accidents, traffic signs, buildings, beat stations, and cell phone towers. The following map shows a robbery point map.



Line feature

A line feature is a geographic feature that can be represented by a line or set of lines.

The following map shows how different types of geographic features such as railways, streets, and rivers can be represented by a line in a GIS. Additional examples are streams, streets, power lines, bus routes, student pathways, and lines depicting the distance from a stolen to a recovered vehicle.

Polygon feature

A polygon feature is a multisided figure represented by a closed set of lines.

In the following map, the largest blue polygon represents the city boundary, the green are census tracks, and the black are census block groups. Other examples of polygon features used in law enforcement would be patrol areas, beats, neighborhoods, or jurisdictions. Polygon features can represent areas as large as continents and as small as buildings.

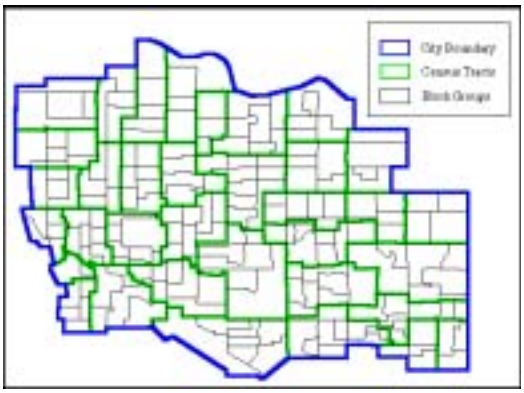


Image feature

> *An image feature is a vertical photo taken from a satellite or a plane that is digitized and placed within the geographic information system coordinate system so that there are -x and -y coordinates associated with it.*

The following image is an example of an aerial photograph. Note that details of the streets, buildings, and environmental features such as landscaping are visible.

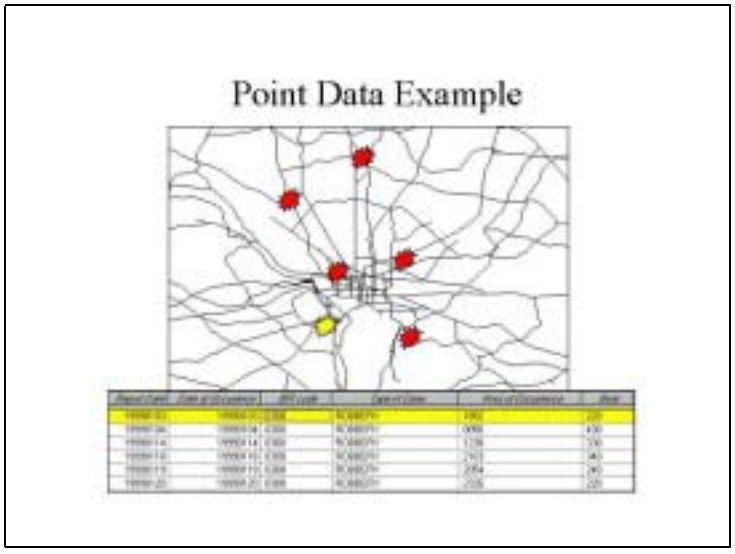
There is a distinction between aerial photography (just the image) and digital orthophotography (the image combined with geometric qualities of the map). Because orthophotographs are located within the geographic information system, they can be viewed with other layers such as street or parcel information. The following image depicts a digital orthophotograph with the corresponding street network and parcel boundaries.

Data of geographic features

Each type of feature has "attributes" or a table of data that describe it. All the attributes for three of the four types of features (point, line, and polygon) are stored in a GIS as a data table (Note that a digital orthophotograph has an –x and –y coordinate but does not have an associated data table worthy of analysis). The ability to view, query, relate, and manipulate data behind these features is the true power of a GIS. A manual pin map and a computer map depict points, lines, and polygons but do not have data associated with the features and are not easily manipulated. In a GIS, simply clicking on a point, line, or polygon can produce the data table associated with that particular feature.

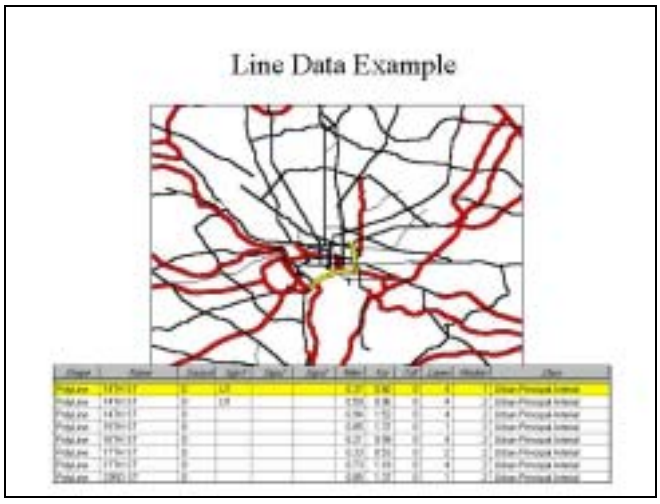
Point data

The following is an example of point data taken from a GIS. The highlighted point has a corresponding data table, which describes the features. For instance, the yellow point is a robbery that occurred at 6:52 pm on January 1st, 1999. In this case, each line of data describes a different point on the map and each variable describes something about that point.



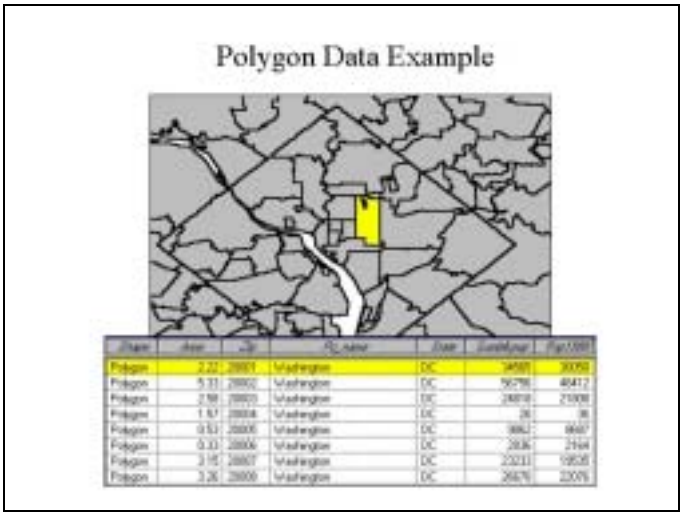
Line data

The following is an example of line data. The table describes the street segments (e.g., the miles, the length of that street segment, and the name of the street). The yellow street segment corresponds to the case highlighted in yellow in the data table. The GIS knows which line corresponds to each case in the table.

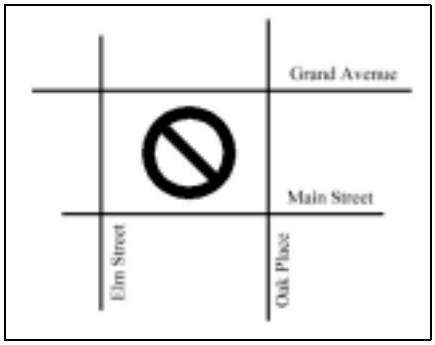


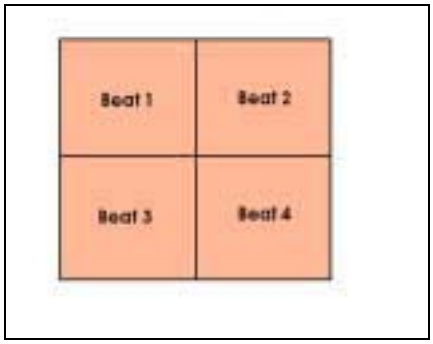
Polygon data

The following image displays the data describing polygons, which are zip codes. The yellow polygon is zip code 20001 in Washington DC with an area of 2.22 square miles and a population of 30,050 in 1990 as is seen in the data table.



Note that the lines themselves only make up the borders of the polygons, rather than being distinct lines with associated data. For example, the image, below left, depicts four intersecting line features that create a square. Each line has associated data; however, the area within the square or polygon that they have formed has no meaning. The image, below right, depicts similar lines; however, these lines are the borders for four separate beats and thus, the lines do not have meaning by themselves, only in relation to the other lines and in the fact that they create a shape.





GIS toolbox

The primary advantage of a GIS is its functionality that allows geographic data to be manipulated. The following are some components that enable data to be manipulated.

Connectivity

> *Connectivity refers to streets and other linear features that are represented by segments that connect at intersections.*

As noted above, data are associated with each line feature. However, each segment connects at an intersection, and connectivity is the ability of the GIS to recognize that the two line segments come together to form an intersection.

Thus, connectivity allows intersections such as Shiawassee and Pine or Chestnut and Ottawa to be located on the map, which is particularly important in law enforcement data since accident information (reports and calls for service) usually list an intersection as the location of an accident.

Contiguity

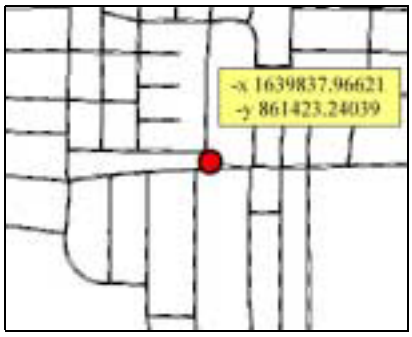
> *Contiguity refers to adjacent areas that are represented by adjacent polygons.*

The following map shows how a GIS includes adjacent polygons representing parcels and buildings. The ability of the GIS to recognize adjacent polygons allows for querying, selection of polygons within others, and visualization of complex land units.

Geometry

> *Geometry refers to the fact that all features in the geographic information system have at least one set of –x and –y coordinates.*

In the example depicted below, the point on the map has a distinct –x and –y coordinate which is listed in the yellow box.



Although these numbers may not make sense at first glance, they are an integral part of the GIS reference system, as every feature in a GIS has at least one –x and –y coordinate. For a point, the –x and –y feature is the center of the point. For a line segment or a polygon, the –x and –y coordinate is at the center of that particular line segment or polygon. Having an –x and –y coordinate for map features, especially points, is important because the location is more precise and there is no need for geocoding (see the explanation of geocoding later in the report).

Visual display/mapping

Thematic approach

> *In a geographic information system, the data are separated by type of feature into what are called "layers" or "themes" as well as by type of data.*

For example, point data of crime and calls for service would not be contained in the same layer or theme because these data come from two different sources. This is a thematic approach to organizing data. This component allows the data to be analyzed and visualized separately or together. Thus, when more than one layer is viewed in the GIS, they are stacked, similar to a stack of pancakes. In the following figure, each layer represents a different type of feature (point, line, polygon, or image) and a different type of data (shopping centers, bus routes, roads, and census tracts).

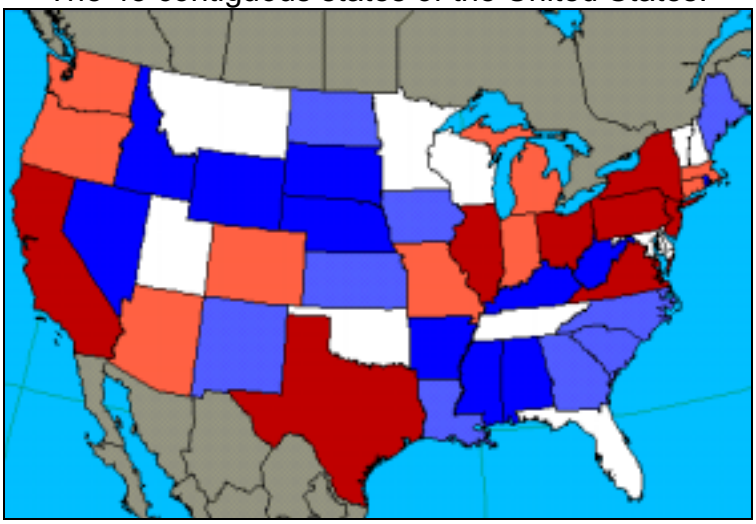
In a GIS, how the layers are stacked is important since some layers are opaque and hide others. For example, orthophotographs are opaque and if placed on top will cover any layers underneath.

Scale

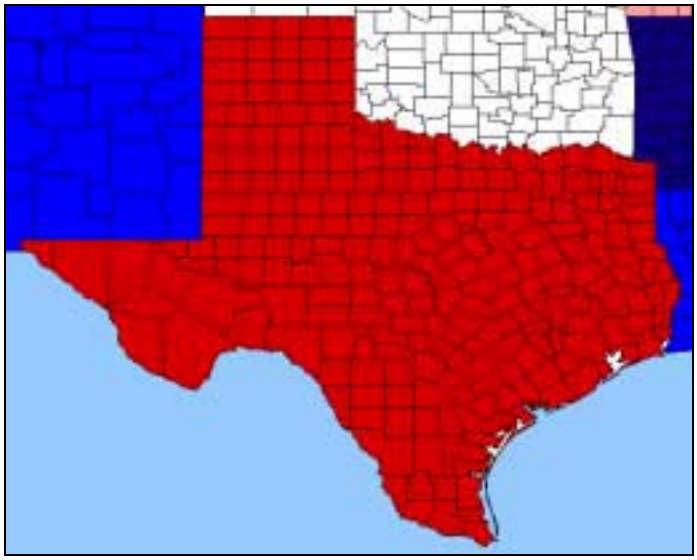
Scale is the relationship between the dimensions of the map and the dimensions of the Earth.

Usually, the scale depends on the purpose of the analysis or map. The following are examples of maps at various scales.

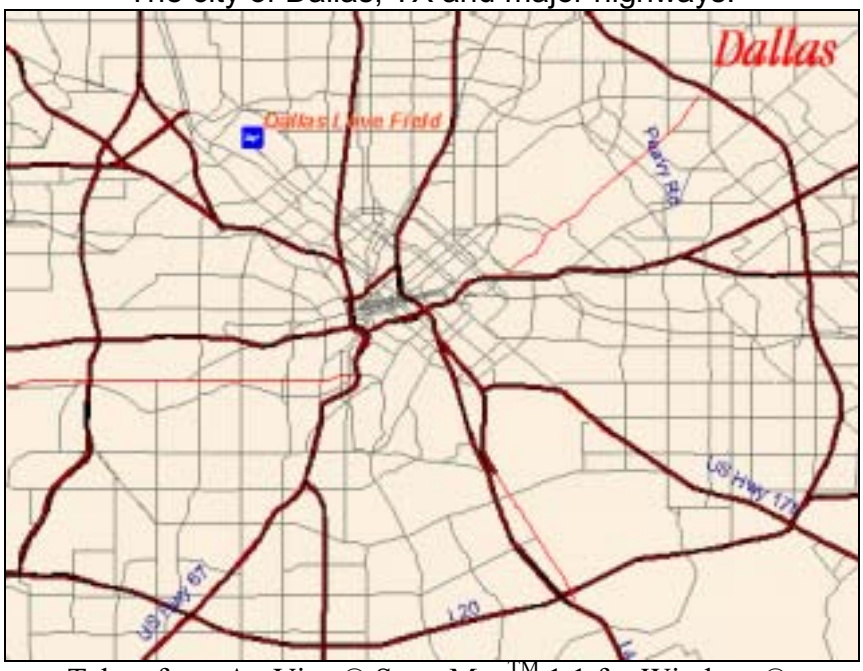
The 48 contiguous states of the United States.



The state of Texas and counties within it.

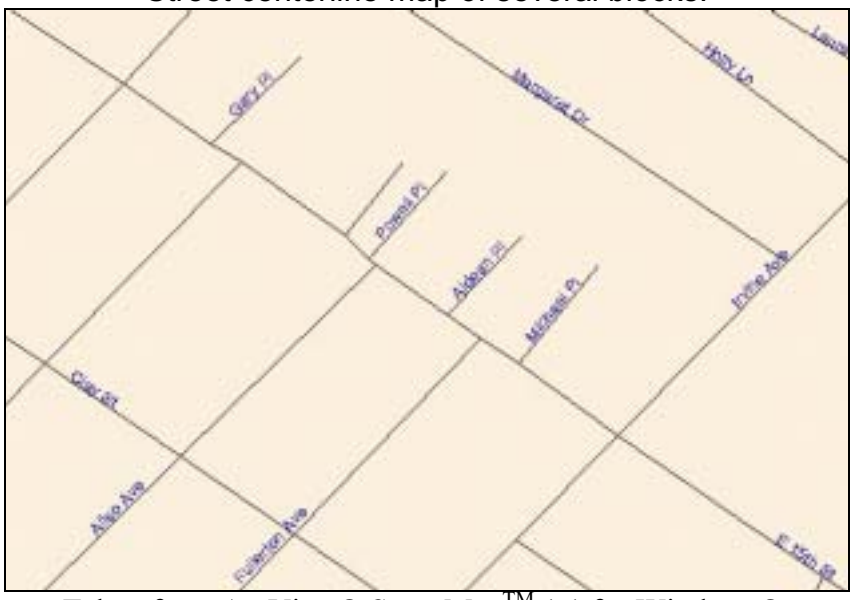


The city of Dallas, TX and major highways.



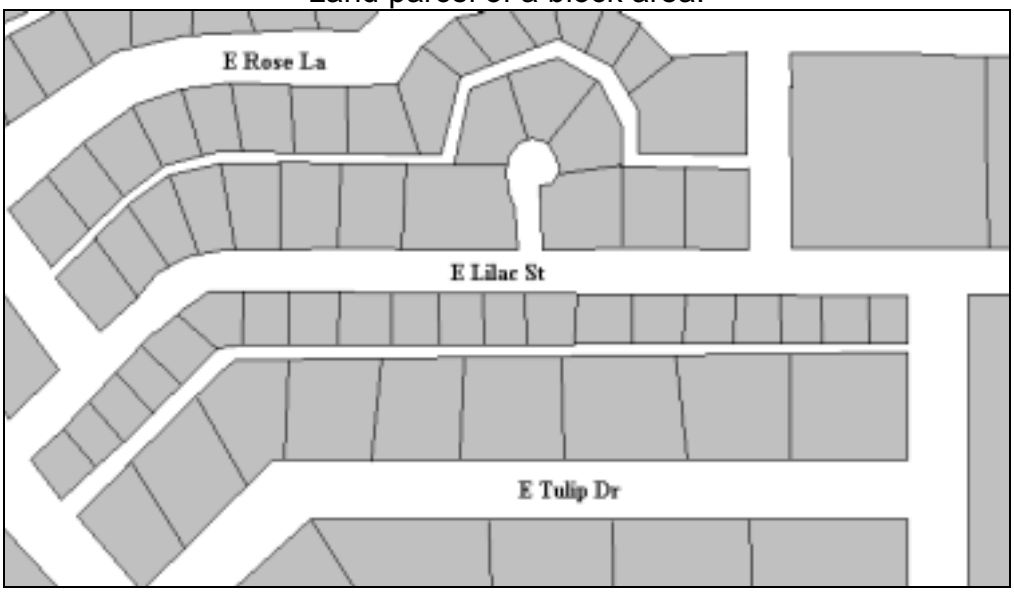
Taken from ArcView® StreetMap™ 1.1 for Windows®.

Street centerline map of several blocks.



Taken from ArcView® StreetMap™ 1.1 for Windows®.

Land parcel of a block area.



Parcel map with buildings.

Orthophotograph of a neighborhood.

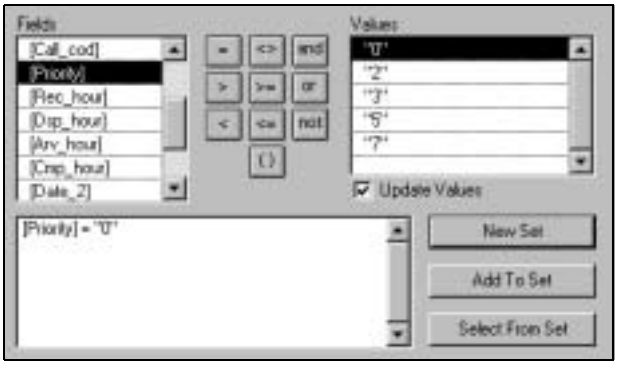
The appropriate scale depends on both the purpose of the map and the type of data that are displayed. For example, it would be impossible to view orthophotographs like the one above for the entire United States at one time. The GIS allows the user to set the scale at which orthophotographs are viewed (e.g., ½ mile or 1 mile). That way, the orthophotographs only become activated when the map is at that scale.

Querying GIS data

Geographic information systems contain the ability to query or select data in various ways.

Tabular queries

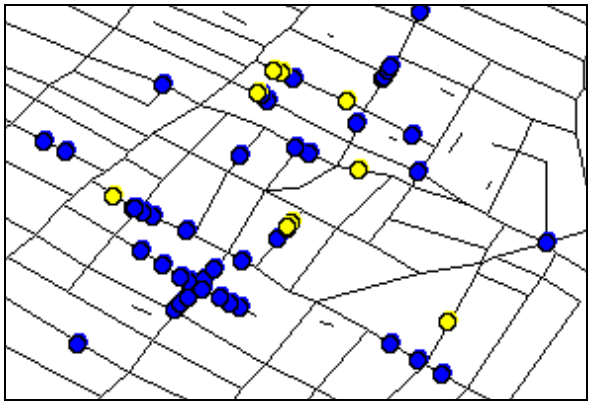
In a GIS software program, query expressions can be created to select features both in the data and on the map. For instance, one can construct a query to select emergency calls for service (priority 0) from tabular calls for service data.



After running this query, the priority 0 calls are selected (highlighted yellow) in the table.

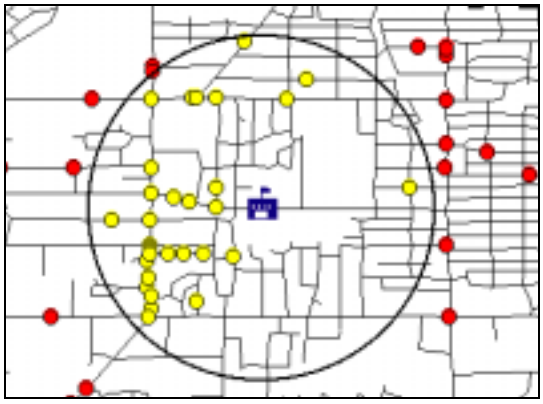
Event_no	Str_name	Str_apt	Date	District	Grid	Call_code	Priority
00203108	9 HECKMAN DR		960628	S	1133	G1300	0
00231068	9 SHERMAN AVE		960720	N	4402	G1300	0
00239616	253 STEGMAN ST		960727	S	1127	G1300	5
00203160	238 CARBON ST		960628	E	3523	G1300	0
00240989	348 WOODWARD ST		960728		3528	G1300	5
00247027	127 RANDOLPH AVE		960802	S	1614	G13	7

Additionally, the priority 0 calls are selected (highlighted yellow) on the map.

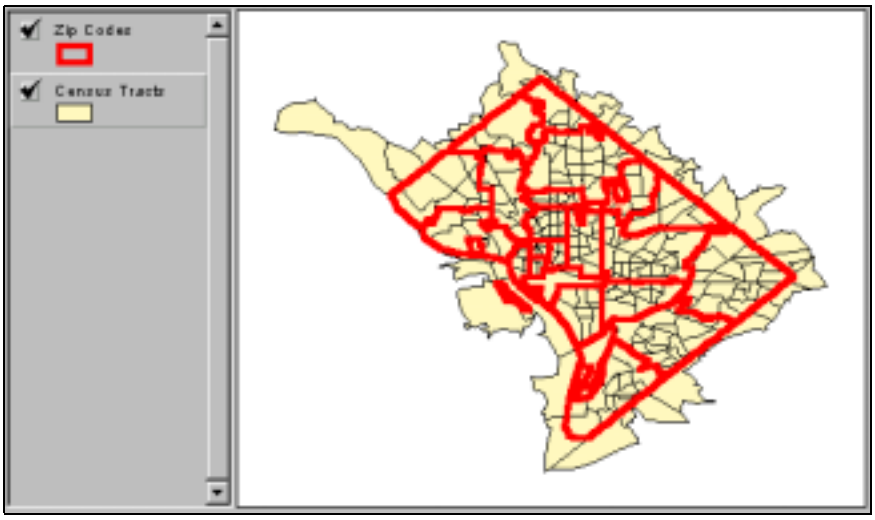


Spatial queries

Spatial queries enable map features to be queried based on their location on the map or their location relative to other features. A very simple example is drawing a one-mile buffer around a school to select the crimes that have occurred within a mile of the school.



In addition, one can select a feature of a map based on its relationship to another feature. The following is an example of selecting zip codes (in yellow) that border any census tract in Washington D.C.



IV. Introduction to Problem Solving

The following is a brief discussion of problem solving. The source of the problem solving and SARA definitions as well as the location of extensive literature on problem solving is the Office of Community Oriented Policing Services (COPS) Web site at www.usdoj.gov/cops/cp_resources/pubs_prod/s5.htm.

Definition of Problem Solving

> *A methodical process for reducing the impact of crime and disorder problems in a community. The problem solving approach is an integral component of the philosophy of community policing*.

SARA Approach to Problem Solving

The SARA approach to problem solving is described as scanning (S), analysis (A), response (R), and assessment (A). That is, once a problem is identified and its characteristics are analyzed, a response is developed and deployed to combat the problem, and after a determined time period, the response is evaluated. The following is a brief discussion of each aspect of the SARA process.

Scanning

> *Scanning is the first step to problem solving and is the identification of a cluster of similar, related, or recurring incidents through a preliminary review of information, and the selection of this crime/disorder problem among competing priorities for future examination.*

One example of using crime analysis information to scan for crime problems is comparison of crime on a monthly basis. Comparison of specific areas over time may indicate a problem area or type of crime. Another example is examining housebreaks over a six-month period to identify small patterns of activity, which could represent a larger housebreak problem.

Analysis

> *Analysis is the use of several sources of information to determine why a problem is occurring, who is responsible, who is affected, where the problem is located, when it occurs, and what form the problem takes.*

Often, individuals think they already know the nature and cause of problems identified in the scanning phase; thus, they do not conduct intensive analysis of the

problem. However, analysis of the problem from several perspectives with several types of data often yields information not previously known. For example, while discussing the auto theft problem, detectives in a jurisdiction in the Southwest US insisted that the auto theft problem centered on cars being taken to Mexico. Yet, when the data were analyzed, it was discovered that nearly 85% of the vehicles were being recovered in or near the jurisdiction. The detectives did not have a good sense of the problem because they only saw a select few of the auto theft and recovery reports.

Response

> *Response is the execution of a tailored set of actions that address the most important findings of the analysis phase.*

A recent report by Mike Scott, entitled *Problem-Oriented Policing: Reflections on the First 20 Years*, offers an evaluation of the last twenty years of problem solving and problem oriented policing and found that police departments are getting very good at responding creatively to the types of problems that they identify (Scott, 2000). Police departments are now working with communities and developing partnerships on a regular basis. Some examples of responses that have been used are working with city engineers to redesign a park that had a high number of assaults, vandalism, and drug dealing incidents (Mankato, MN); convening an advisory board composed of law enforcement, residents, business owners, and charities to address traffic and safety concerns at day-laborer gathering points (Glendale, CA); and establishing a juvenile diversion program whereby police bring together adolescent taggers and the owners of the property they deface to agree on terms for restitution and community service (Santa Ana, CA) (Sampson and Scott, 2000).

Assessment

> *Assessment is the measurement of the impact(s) of the responses on the targeted crime/disorder problem using information collected from multiple sources, both before and after the responses have been implemented.*

For law enforcement agencies, assessment is probably the most challenging part of the SARA process, not only because measures of effectiveness are often difficult to determine and capture, but also because assessment takes time and effort to complete at a time when the problem solving process is winding down. For example, measuring a response such as a crime prevention education campaign is difficult because there may be substantial lag time between intervention and measurable effects of the response.

Crime Analysis and Problem Solving

Crime analysis and mapping play a major role in all phases of the problem solving process. It is important to measure the problem accurately during the scanning, analysis and the assessment phases. Analysts can also assist in the response phase of the SARA process by informing the effective allocation of resources by determining the times when, and areas where the offenses are most frequently or disproportionately occurring. The role of crime analysis in problem solving lies in the fact that members of a law enforcement agency have different experiences and understandings of a problem, and it is necessary for the crime analyst to either support or refute these assumptions by providing a comprehensive analysis of a problem and an evaluation of process and response impact.

V. Data and Geocoding

Types of Data

Data collection and dissemination is a cyclical and on-going process. The term "database" can refer to anything from entire records management systems to simple spreadsheets containing a few variables and a handful of cases. Databases are vital for conducting crime analysis and mapping. It is essential to identify the actual and potential data sources within an agency that can be used for analysis. Below is a description of two distinct categories in which law enforcement information falls.

Tabular Data

> *A list of records contained in a table that, along with information about the record, contain addresses or some other type of geographic variable.*

The unit of analysis in tabular data can be anything that is not inherently geographic. Law enforcement examples of tabular data include crime, calls for service, accidents, field information, sex offender information, and arrests.

Geographic Data

> *Data that are inherently geographic; that is, they describe geographic features.*

The unit of analysis in geographic data is a geographic feature. Examples of quantitative geographic data sources include streets, districts, jurisdictions, census tracks, and bus stop/route data. Law enforcement examples of qualitative geographic data include neighborhood boundaries and pathways children take to and from school. Even though all geographic data have associated attributes (tabular data), the tabular data do not make much sense outside of a GIS. The following table contains the attributes of a geographic street file. Variables such as the length of the street in feet, prefix, street name, suffix, and number of lanes describe each street segment on the map.

Length	Pre	Name	Type	Lanes
373.68484	E	THIRTIETH	ST	2
65.24045	E	FOURTH	ST	2
430.24857	E	THIRD	ST	3
134.70268	E	SECOND	ST	2
309.69322	E	FIFTH	ST	3
234.76184	E	FIRST	ST	4
202.07308	E	TWENTY-EIGHTH	ST	4
240.78427	E	TWELFTH	ST	2
376.39829	E	TWENTY-SEVENTH	ST	2

General Data Integrity Issues

There are various data integrity issues associated with tabular and geographic law enforcement data. This section is not meant to serve as a comprehensive description of the data integrity issues in law enforcement but instead gives a general overview of the major issues.

Data Entry

In a law enforcement setting, oftentimes the individuals, officers, dispatchers and records clerks, who are conducting data entry, do not realize that others are using the data they produce. This lack of awareness can lead to carelessness and result in unreliable data. Data entry errors can be improved by technology (address cleaning software), proper training, and making individuals aware of the uses and importance of the data.

Timeliness

A primary concern in crime analysis, especially in tactical crime analysis, is that data obtained are current and available in a timely manner. Unfortunately, because of human error and technological difficulties, this is not always possible. One method to remedy this problem is to stress the need for and the value of current data for crime analysis. This need should be communicated throughout the department in order to come up with solutions for improving data timeliness.

Data Validity

Validity refers to whether data accurately reflect the concept that they are intended to measure. Although true validity is difficult to measure, law enforcement data, like any other data, are prone to validity issues. For example, many police departments use calls for service information as a proxy for crime. This is problematic, because not all calls that are originally dispatched as a crime are in fact crimes. The best example is a robbery call for service, since there is a common confusion about the difference between a robbery and a burglary. A citizen who has been burglarized may call 911 to report, “they’ve been robbed” when in fact they were not. If the dispatcher enters what the citizen reports and the title of the call is not changed when the actual crime is determined (a common problem), the call for service would not accurately represent the crime that occurred. Even if the call title and crime match, using calls as a proxy for crime is problematic as the date and time variable would indicate when the call was received by the police department, not when the crime actually occurred. Analysis of these variables would yield invalid results in that they would indicate when the citizen called the police and not when the crime actually occurred.

Reliability

Reliability refers to the whether data are measured the same in repeated observations. An example of a reliability issue related to law enforcement data is when there is a policy or law change (e.g., mandatory arrest for domestic violence offenses). Frequently, there will be a sharp increase or decrease that indicates that the data no longer represent the same phenomenon and thus, the numbers are not reliable. Obviously, reliability issues can significantly affect crime analysis results.

Data Transfer Process

The data transfer process can affect data quality and integrity in that data can be inadvertently or unavoidably lost or reformatted. An issue associated with the data transfer process is data compatibility. Police departments are notorious for having data in many different formats, and converting and combining these data is often a time-consuming and frustrating process.

Data Confidentiality/Privacy

Crime analysts are managers of law enforcement data; therefore, crime analysts are responsible for protecting the information and individuals represented within the data. Normally, the data used and created in crime analysis adheres to a jurisdiction's policies on privacy and confidentiality. New situations of providing information have surfaced which require additional and more detailed policies such as the invention of the Internet and the use of mapping. Thus, police departments should include specific crime analysis concerns into their data-protection plan.

On a related issue, the crime analysis unit, itself, should have a written data and analysis request policy that addresses common issues surrounding requests for crime analysis information. A policy, supported by the agency's administration, can provide guidelines for requesting information and expectations of what will and will not be provided. A recent document published by the National Institute of Justice provides a discussion and suggestions specifically for mapping and data confidentiality, see www.ojp.usdoj.gov/cmrc/pubs/welcome.html to download or order a copy of the publication entitled, *Privacy and the Information Age* (Wartell and McEwen, 2001).

Data Management

Metadata

Metadata refers to the data that describes the analyst's work.

Metadata are the data that describe data. Every police department has its own set of procedures that outlines how crime analysis is conducted. Frequently, these procedures are kept only in the analysts' memories, and it is important to have them written down for a variety of reasons. They include consistent data handling and cleaning procedures, guidelines for sharing work with others, keeping track of products and files created, and reducing duplication of effort. These written procedures are also invaluable training tools for new analysts. Some examples of categories of metadata include:

- Location of data files (e.g., on network, mainframe, personal computer)
- Source of the data (e.g., Records Management System, Investigation Bureau)
- Data cleaning procedures
- Geocoding procedures
- Report and map formats
- Methodology for regular reports and studies (e.g., monthly crime report, annual staffing analysis)

Geocoding

The following discussion of geocoding is taken directly from another document produced by the Police Foundation's Crime Mapping Laboratory as a part of the work conducted for COPS. The report is entitled, *Geocoding in Law Enforcement* (2000) and can be found on both the Police Foundation (www.policefoundation.org) and COPS (www.cops.usdoj.gov) Web sites.

Introduction

Geocoding is the process of bringing tabular and geographic data together based on a common geographic unit of analysis. A geographic unit of analysis refers to a spatial characteristic within the data that is necessary to locate it on a map such as address, zip code, beat, or grid. Tabular data are contained in a table and are a list of records that, along with information about the record, contain addresses or some other type of geographic variable. Examples of law enforcement tabular data are calls for service, crime, accidents, citations, sex offenders, and arrests. Along with information about nature of the incident (e.g., type of call or crime, date, time), these data contain the

location of the incident (e.g., address, grid, and/or beat), which will allow it to be geocoded. Geographic data are data that can be displayed on a map such as streets, census tracts, parcels, and buildings. Examples of geographic data specific to law enforcement are police districts, beats, or grid boundaries.

The purpose of geocoding is to assign tabular data to a location on the earth's surface to visualize the spatial characteristics of the data. It is analogous to placing a pin on a map in the appropriate location. Unlike the paper map, when geocoding in a geographic information system, data associated with the pin, or data point, are available. In order to geocode either electronically or manually, there must be a common geographic unit of analysis. In law enforcement, address is primarily used as the geographic unit of analysis to which tabular data are geocoded. However, other types of geographic units are also used such as parcels, zip codes, census tracts, census blocks, or beats. In the case of geocoding, geographic data used for geocoding are called "reference data" since the geographic data are used to reference the tabular data.

The following is a discussion of the geocoding process, regardless of the geographic information system (GIS) software used, and some common problems faced when geocoding law enforcement data.

The geocoding process

In general, there are five basic steps in the geocoding process. They are:

1. Prepare the geographic and tabular files for geocoding.
2. Specify the geocoding parameters.
3. Geocode.
4. Review results.
5. If necessary, respecify parameters and geocode again.

Step 1: Prepare the geographic and tabular files for geocoding

The first step is preparing the tabular and geographic files, which is the most important and can be the most time consuming of the five steps.

Tabular data. Tabular data used in law enforcement primarily consist of calls for service, crime, arrests, and accident data. Other types of tabular law enforcement data can include field information, sex registrant information, or intelligence information. In the past, much of this information was not captured electronically. However, currently, many departments either already have in place or plan to acquire an automated computer aided dispatch (CAD) system and a records management system (RMS) which have the capacity to store digital information as well as standardized

tables of addresses and location names. The most important aspects of these systems as they relate to geocoding are that they reduce the need for manual data entry and provide clear and consistent rules in order to ensure that data are reliable and valid. Because individuals are the data entry mechanism, there is still the possibility of human error and inconsistencies, which is why training should coincide with the technology.

Geographic data. A variety of geographic data types may be used as a reference layer, though street files such as the Census Bureau's TIGER/Line ® files are the most commonly used. Street files are often called centerline files in that they depict the center of the streets by line segments. Details of curbs, alleys, or cul de sacs are not depicted in centerline files. In this context, street files are geographic databases containing records that describe interconnected street segments. More specifically, each street is broken down into sections with address ranges associated with them. These sections usually span between cross streets. The following map is an example of a street centerline file and the darkened line is one street segment. The table below is the data describing the streets.

Street	Fromleft	Toleft	Fromright	Toright
YORK ST	473	479	478	480
YALE AVE	83	173	84	174
YALE AVE	1	81	2	82
WRIGHT AVE	1	91	2	96
WOODWARD ST	283	395	304	380

Street centerline databases generally have fields that describe the physical address along each street segment in the layer. Conventionally, addresses are recorded as

'from' and 'to' ranges for both the left and right sides of each street segment. In the above example, the centerline street segment of Yale Ave that is thicker than the others is represented by the address ranges of 83 to 173 on one side of the street and 84 to 174 on the other side, as highlighted in the table.

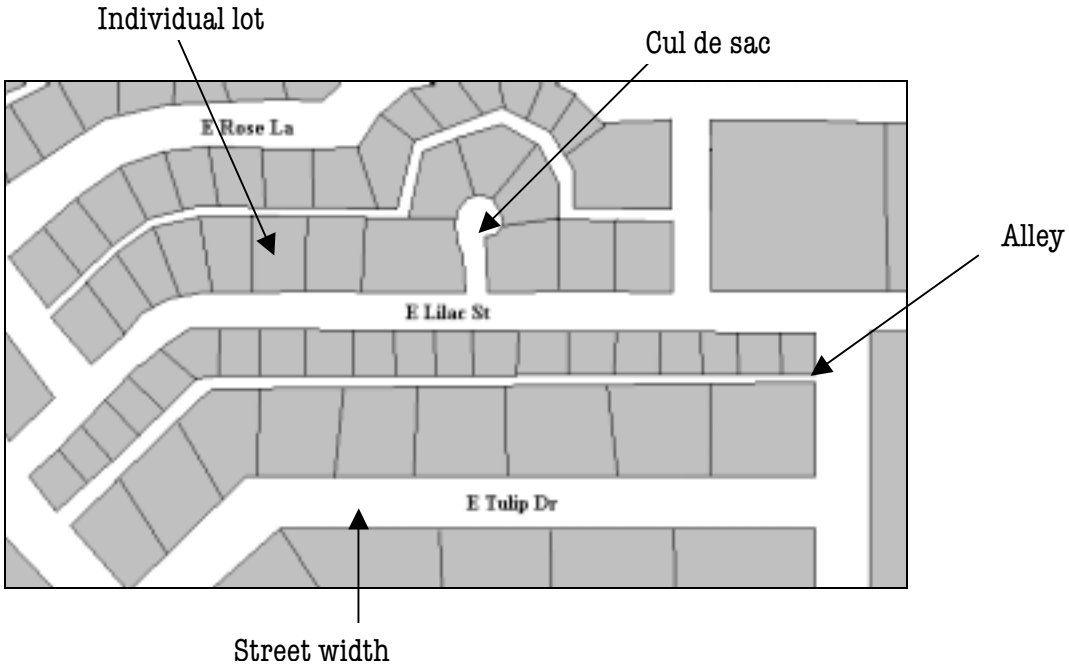
In addition to address ranges, street segments can be depicted by several variables such as street name, type, prefix, and suffix, as noted earlier. Street centerline databases vary in how the addresses are described. In the previous example, address is depicted with a variable called "street" along with the address ranges. The following are tables with highlighted examples of two additional ways in which addresses are found in a geographic database. The prefix and suffix fields are used to store information such as quadrant. The first table highlights a street segment with the prefix W for West Northern Ave. The second table highlights a street segment with the suffix NW for Chesterfield Place Northwest. Type refers to the type of roadway (e.g., street, road, lane, and drive). The highlighted examples in the following tables show Ave for Northern Avenue and Pl for Chesterfield Place.

Shape	L_Lastd	L_Lastd	R_Lastd	R_Lastd	Prefix	Name	Type	Suffix
PolyLine	4901	5099	4900	5098	W	Vista	Ave	
PolyLine	5051	5099	5050	5098	W	Kaler	Cir	
PolyLine	5947	5999	6000	6098	W	Northern	Ave	
PolyLine	5401	5499	5400	5498	W	Orangewood	Ave	
PolyLine	5301	5399	5300	5398	W	Orangewood	Ave	
PolyLine	7451	7301	7452	7300	N	51st	Ave	
PolyLine	7499	7453	7498	7454	N	51st	Ave	
PolyLine	7515	7501	7516	7500	N	51st	Ave	
PolyLine	7605	7517	7604	7518	N	51st	Ave	
PolyLine	7647	7607	7648	7606	N	51st	Ave	

Shape	L_Lastd	L_Lastd	R_Lastd	R_Lastd	Prefix	Name	Type	Suffix
PolyLine	2799	2701	2798	2700		Albemarle	St	NW
PolyLine	3099	2901	3098	2950		Audubon	Ter	NW
PolyLine	2699	2601	2698	2600		Tilden	Pl	NW
PolyLine	2899	2801	2898	2800		Chesterfield	Pl	NW
PolyLine	2899	2801	2898	2800		Allendale	Pl	NW
PolyLine	4201	4249	4200	4298		Lenore	Ln	NW
PolyLine	4799	4601	4798	4600		Broad Branch	Rd	NW
PolyLine	4499	4423	4498	4400		Broad Branch	Rd	NW
PolyLine	4421	4401	0	0		Broad Branch	Rd	NW
PolyLine	4599	4583	4598	4546		Broad Branch	Rd	NW

Because the Census Bureau's mission to count and profile the nation's people and institutions does not require a high level of positional accuracy in its geographic products, its TIGER/Line ® files and centerline maps are designed to show only the relative position of geographic elements.

As previously mentioned, another common layer used as a reference for geocoding is the parcel file. A parcel file is a polygon layer used to keep track of lots, subdivisions, and ownership information primarily for planning and tax purposes. The following is an example of how a parcel map looks in a GIS. Note that it is more specific than a centerline map in that alleys, cul de sacs, lot size, and street widths are discernable.



Parcel files provide a good base layer to examine relationships between land use, zoning, demographic data, and economic data as all of this information is contained in parcel files. Also, parcel reference layers can be very helpful in mapping law enforcement information because they can help to indicate the exact location of an incident (e.g., corner lot), and provide ownership information, which may prove valuable as in the case of rental property.

While parcel files have the ability to be highly accurate, like street files, accuracy is largely dependent on how often and how well the files are maintained. Because of the nature of real estate and other planning mechanisms, keeping parcel files updated and accurate can be a full-time job for several technicians depending on the area.

Successful geocoding depends not only on the quality of the geographic reference layer, but also the tabular data to be mapped. For any crime mapping application to be effective, basic reporting procedures need to be uniform and consistent. While most high-end geocoding software packages incorporate complicated algorithms

making them somewhat forgiving, a well established reporting procedure is often the best way to ensure a high rate of accuracy.

Step 2: Specify geocoding parameters

Step two consists of specifying the parameters of both the reference data and the tabular data to determine how the geographic units from each source will be matched successfully.

Selection of which reference layer would be most effectively used for geocoding must consider the needs of the individual end user. Considerations of accuracy, cost of product, maintenance costs, utility, current reporting procedures, and compatibility with other existing reference layers must be dealt with on a case-by-case basis. In the case of law enforcement, most information is geocoded to the street reference layer. However, sometimes it is necessary to be more specific, in which case a parcel reference layer may be used. For example, one might use the street centerline file to pin map residential burglaries in an entire city since the exact location of the burglary would not be as important as getting a general idea of where the incidents are occurring throughout the city. On the other hand, one might use a parcel file to pin map residential burglaries in a one or two block area to determine exactly which houses were targeted and whether they were along alleys, wooded areas, or on the end of the block.

Parameters set to determine how tabular and geographic data are matched are set within the GIS software and may include spelling sensitivity of the match, address style (e.g., whether to match on address only or address and zip code, or whether to accept partial match scores). A match score denotes the number of address records from the tabular file that were located in the reference layer. Another parameter is offset distance, which is placing a data point a predetermined distance away from the original geocoded location. This may be done to place points on one side of the street segment or another to make the map more readable and/or realistic.

These parameters are choices within the GIS software that will affect the geocode match rate. These preferences should be set and modified only after an examination of the tabular data. One should be completely familiar with the data in order to set these preferences. For example, if the spelling sensitivity parameter is lowered in a city that has two streets named Mill and Miller, inaccurate geocoding may result.

Step 3: Geocode

Once the parameters are set, geocoding is just a push of a button that starts the geocoding process. Often, software packages use a fairly simple method to accomplish the actual placement of the tabular data in relation to the reference layer. The common approach is to place the address point along the street within the range of the street number. For example, this first table highlights one call for service at the address "292 Princeton Ave."

Shape	Bg	Str_name	Str_apt	Date	District	Grid	Call_cod	Priority
Point	37001	292 PRINCETON AVE		960622	S	1112	G1300	5
Point	21002	24 VIRGINIA AVE	F-BSMT	960813	S	1620	G1300	5
Point	09022	133 MARTIN LUTHER KING DR		960801	S	1603	G1300	0
Point	25002	227 MARTIN LUTHER KING DR		960604		1625	G1300	5

The following table depicts the data for the street reference layer, and highlighted is the street segment in which "292 Princeton Ave" falls.

Shape	Street	FromLeft	ToLeft	FromRight	ToRight
PolyLine	PRINCETON AVE	289	315	290	316
PolyLine	E 53RD ST	33	85	34	66
PolyLine	ADLER ST	1	41	2	42
PolyLine	ALBERT PL	1	29	2	30
PolyLine	ARLINGTON AVE	23	71	24	70
PolyLine	ARLINGTON AVE	73	101	72	100

When an incident is geocoded, the point is placed relative to a proportioned length derived from the ratio of the difference between the maximum and minimum address values and the physical length of the line segment.

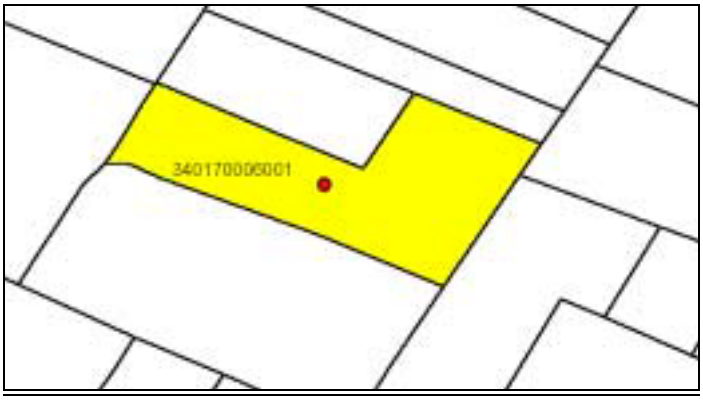
For example, a segment may represent a street with an address range of 101 to 151 for the left side. An address of 125 would be placed approximately halfway down the line on the left side. Although this method usually misses exact real world coordinates, it is often sufficient given the detail of the street file and necessary resolution of the final map. In this example, "292 Princeton Ave" is located near the beginning of the street segment.

As noted earlier, geocoding by street centerline may not be adequate to depict the exact location of an incident. In the case of mapping a few blocks of residential burglaries, one may want to geocode by parcel address. In some cases, such as recording traffic citations along routes that may not have readily discernable addresses, intersection address data can be recorded for later geocoding using street files. Intersection geocoding is often more accurate than street geocoding since there is no mathematical algorithm to define the physical location of the point generated; instead, the point is placed at the center of the intersection of the appropriate line segments. However, even using intersection data to geocode is not completely accurate since, in reality, most incidents occurring at an intersection address do not occur exactly in the middle of where the two streets intersect.

A similar geocoding strategy uses polygons as opposed to previously discussed street centerline files. This method is the same as geocoding specific address data in that a value from the tabular data must match that of a geographic reference layer. For example, calls for service data often have a grid, beat, or district field in addition to an address field. In this case, the incident data has a census block number field.

When geocoding polygons, the grid, beat, or district value is geocoded to the center of the polygon that represents the grid, beat, or district layer. In this example, the census block group layer matches that from the incident data.

Once the incident is geocoded, the point is placed in the exact middle of the polygon, as are all the points geocoded to that polygon.



This type of geocoding is often used to create graduated color thematic maps by aggregating the data by polygon since data geocoded by polygon can no longer be located by address. However, many people geocode by address first and aggregate the data by polygon after the fact to avoid losing address data. Other types of geographic polygon data that can be used as reference layers for geocoding are zip codes, census blocks, census tracts, county, state, and country. Geocoding data at the polygon level is particularly useful when a dataset is very large or when address information is not as reliable as information such as grid or beat information.

Step 4: Review results

Step four, reviewing results, is a matter of determining whether the geocoding process was successful and how successful it was. Most GIS software will have geocoding outcome statistics that indicate how many of the cases were successfully geocoded, how many are a partial match, and how many were not geocoded at all. Obviously, the ideal successful geocoding rate is 100%. Depending on the number of cases and the purpose of the analysis, a rate of 95% can also be acceptable. The important factor in accepting a geocoding rate less than 100% is understanding why some of the incidents are not geocoded. In some cases, missing data or data outside the mappable jurisdiction make up the incidents that are not geocoded. However, many times, there are other reasons that can and should be corrected.

In the case of a street centerline layer, geocoding problems are generally manifested in the form of missing or incorrect address ranges or missing street segments. Street layers often lack address ranges for streets because of recent construction of new roads or errors in the original creation process of the reference layer. The quality of these layers will depend both on those maintaining the layers and the growth rate of the jurisdiction. For example, in a small town that has not added new streets in fifty

years, the street reference layer would be easy to maintain, not only because nothing is being added but also because the town has relatively few streets to maintain. On the other hand, in a large city that is growing rapidly, the street layer would be much more difficult to maintain.

Because street files are generally manually updated, they are also prone to data entry errors. The combination of these problems can be difficult to solve. Many agencies produce and maintain their own street centerline files or rely on their city or town's engineering department to maintain them, and others have opted to purchase street centerline files that have been corrected and are bundled with contracts for regular updates. However, for layers particular to the police department, such as police district boundaries or beat boundaries, someone at the police department will most likely be tasked to maintain these. Fortunately, these layers are typically composed of many less geographic components than a street reference file. In any case, interagency cooperation can prove invaluable as a means for resolving geocoding problems.

Even if the geographic reference layers are complete, there may still be problems with the tabular data used by law enforcement agencies, which stem primarily from having incorrect information or inaccurate data entry. Address errors in calls for service, crime, or accident data are often the source of much of the woes of geocoding in law enforcement and can be categorized into five common types: incorrect street numbers, street name errors, direction errors, incorrect intersections (in the case of intersection geocoding), and discrepancy errors.

- Street number errors can be the result of entry mistakes and are frequently identified as range errors; the address identified is either less than or greater than the address range of the corresponding records in the source file.

- Street name errors can occur for a variety of reasons and are a result of the address record not matching the street name in the source database. These errors are among the most common, with reasons including misspellings, abbreviations, inconsistent street types, or lack of compliance with city addressing standards.

- Direction errors occur when the direction code of the address record does not match the direction code in the source database, either because they are incorrect or missing.

- Unmatched intersections can result from inaccurate intersection addresses or incorrect format. For instance, the intersection of Main Street and Center Avenue is referred to as "Main St & Center Av" and will not be recognized by many GIS software packages if entered as "Main St/Center Av" or "Center Av & Main St."

- Other errors can occur because there is a discrepancy between the common name of a location and the official address. For example, a police agency may have in its computer aided dispatch system a street called "Route 123," but the official name in the street centerline file may be "US HWY 123;" thus, they will not match.

Step 5: If necessary, respecify parameters and geocode again.

Step five is only necessary when there is not a 100% geocoding rate, which seems to happen most of the time with law enforcement data. Once the data have been geocoded and problems have been determined by the geocoding process, there are a few solutions. Some may choose to take care of the problems by changing the preferences (e.g., lowering the spelling sensitivity). However, as noted earlier, this should be done cautiously and with full knowledge of the tabular and geographic datasets, as changing preferences such as spelling sensitivity can lead to incorrect address geocoding.

Another solution is developing alias tables, which allow for multiple names for a single entity. For example, a location such as a park or a mall may be referred to in a computer aided dispatch system as "Central Park" or "Centertown Mall" instead of by address to make them easy for dispatchers to enter. An alias table would replace the common name with the appropriate address in the GIS system so it can be located on the map. However, even though alias tables are helpful, it is still recommended that data be cleaned in the original database to reduce confusion and facilitate consistency in data. Data are not only used for mapping purposes, so cleaning the data only in the GIS would not solve data integrity issues when the data are used elsewhere.

The best way to correct data is to fix it at the source; in other words, bring the errors to the attention of those administering the computer aided dispatch system, to those maintaining the street centerline file, to the officers writing the reports, or to the clerks entering the data. However, this may not always be a realistic or a fast enough solution. In small projects or where a large number of cases share the same few mistakes, manual correction may be possible. Large datasets can often be corrected more efficiently when imported into a database or spreadsheet program which has a "search and replace" utility. In addition, specialized software programs,

referred to as “scrubbers” can be useful for large projects and in instances where data are regularly imported.

Conclusion

These five steps outline the general process of geocoding law enforcement data. Because the types of data, problems, and solutions are common among law enforcement agencies, there is much to learn and share with one another. This overview has not detailed the specific methodology of geocoding in a particular GIS software program since the software used varies from agency to agency. For a specific outline of how to geocode in particular GIS software applications, see the text manual or electronic help files accompanying the software.

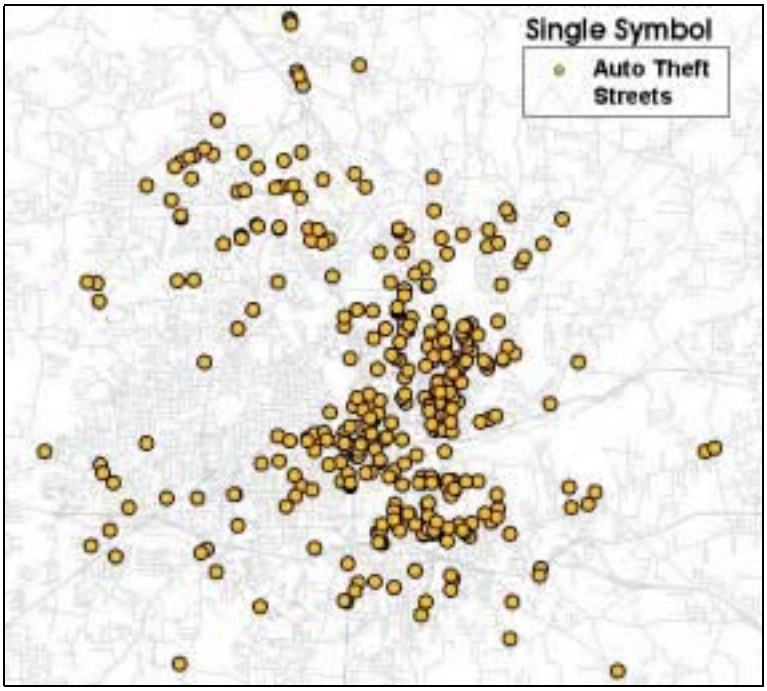
VI. Spatial Analysis Techniques

This section describes and illustrates basic types of mapping that are most commonly used and data classifications that are available in a GIS. This section is meant to serve as a guide and reference for these types of mapping rather than as a "how to" guide for creating crime analysis maps (please note that all of the data used here are fictional, and the maps do not have labels, scales, and North arrows that would be included in a map for presentation, as they are meant to illustrate a point and not represent a map for distribution. For elements of a map and final formatting, see section VII). For assistance in developing thoughtful, appropriate crime analysis maps, see the *Manual of Map Production* (2000) at www.policefoundation.org or www.cops.usdoj.gov produced by the Police Foundation's Crime Mapping Laboratory as a part of the work conducted for COPS.

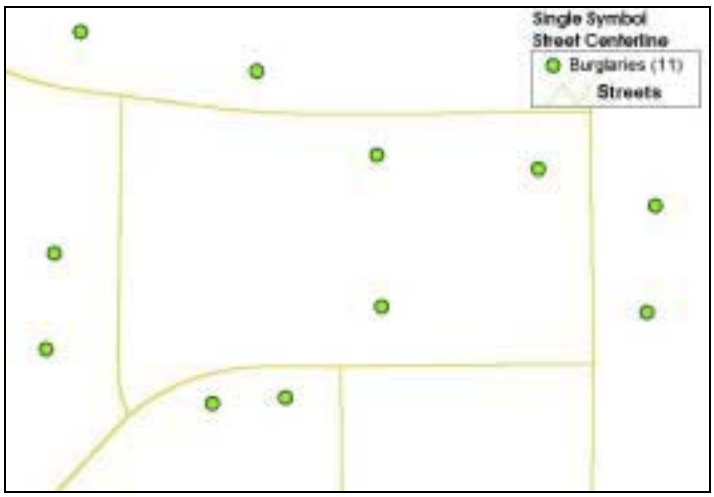
Single Symbol Mapping

Single symbol mapping refers to the use of individual symbols to represent point, line, and polygon features.

The utility of single symbol maps is that they allow for a detailed analysis of small amounts of data. This following is an example of an inadequate single symbol map. This map has too much data for this scale, which is why this method is primarily used for small amounts of data.

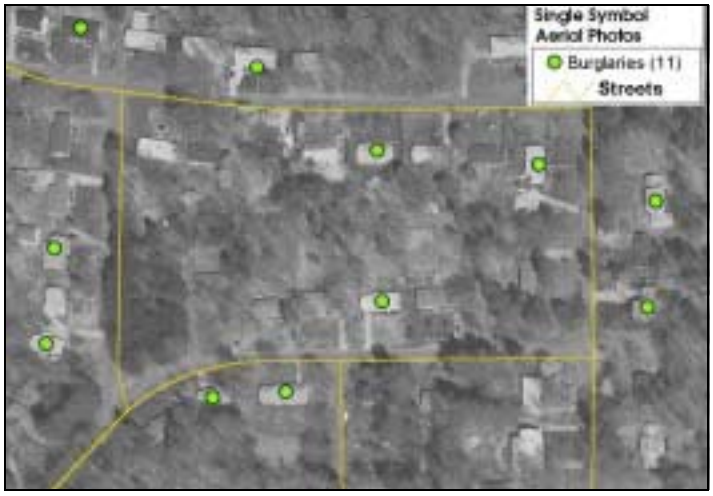


A drawback of single symbol mapping is that if two incidents have the same address, they are placed exactly on top of one another and cannot be differentiated by looking at the map. The following map is a better example of single symbol mapping that uses an appropriate scale. However, to avoid confusion since the points may still be placed on top of one another, one should list the number of incidents in the legend, as is done here or place a number (2) next to a location with more than one incident.

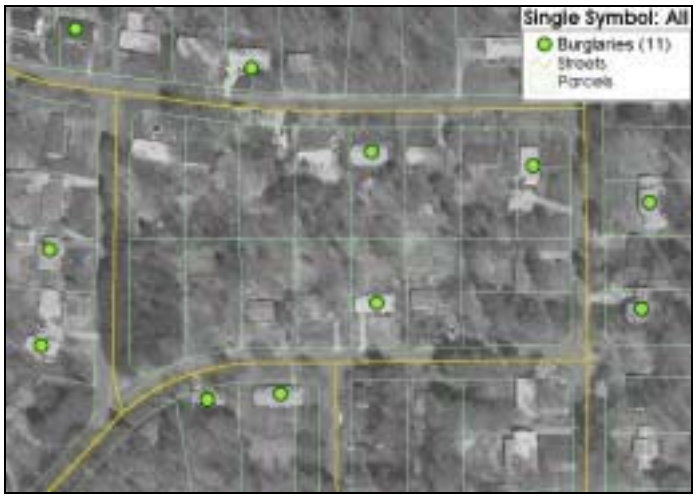


Because single symbol maps are more useful for small amounts of data, they are particularly useful for tactical crime analysis and mapping crime patterns. In addition, they allow a more detailed look at the geography surrounding the incidents. For example, the following map illustrates the same burglary incidents as above with the land parcels drawn that show the number of houses on each block and which were burglarized.

The next map depicts the same data as well as centerline streets with the digitized orthophotograph of the neighborhood that shows the actual houses and surroundings of the burglary locations.



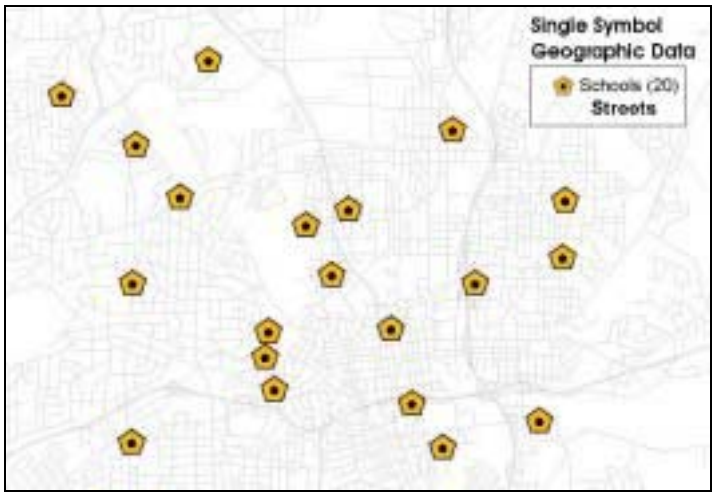
Finally, this map depicts the parcels, orthophotographs, street centerlines, and burglary incident data together. This map could assist in determining additional characteristics of the burglary pattern by examining neighborhood characteristics such as proximity to alleyways or shrubbery, and in responding to the problem by determining potential surveillance locations.



These maps could be used for a neighborhood analysis of accidents or burglary and provide a good example of the use of descriptive geographic data. The key to using a single symbol map effectively is for the analyst to be aware of the number of

incidents on the map and be sure they are all represented and their scale is appropriate.

Single symbol mapping is also helpful in representing geographic data such as schools or churches in that it is known that they are discrete addresses and the risk of two points on top of one another is low. The following is an example of schools in a single symbol map. The user should be aware of the readability of the map in order to determine what is "too much" data.



Graduated Mapping

> *Graduated mapping consists of aggregating data into groupings that are displayed on the map.*

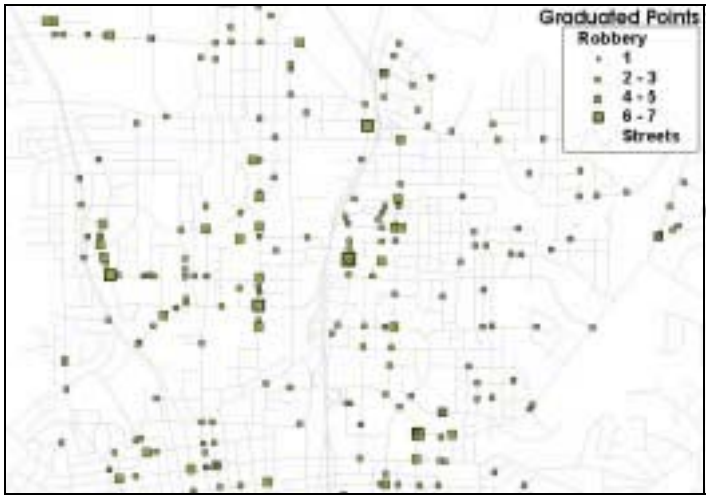
These groupings can be graduated by size or by color and can be classified statistically in various ways. This next section describes the size and color graduations as well as the classifications that are available in most GIS software packages.

Graduation By Size

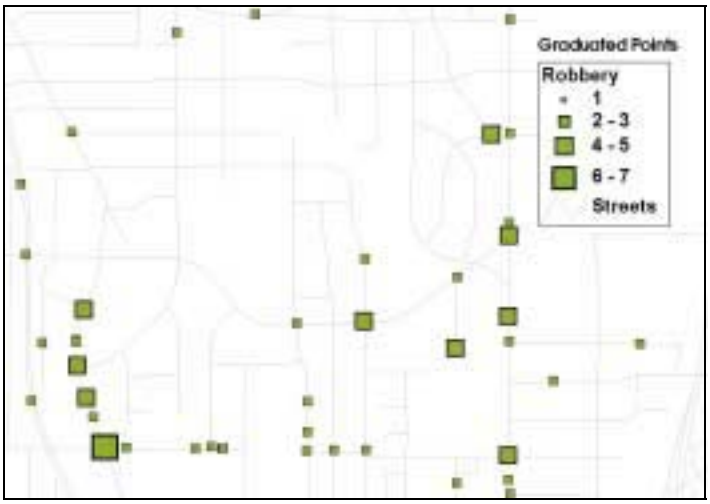
> *Graduated size mapping is the process by which data are summarized so that symbols (point or line features) are altered in size to reflect the frequencies in the data.*

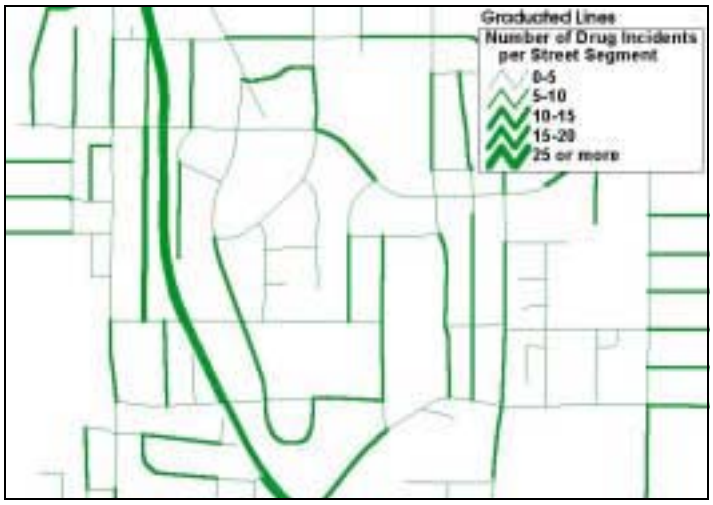
In other words, in this type of map, more than one incident at a given point or line is represented with a larger symbol or a thicker line. One drawback is that oftentimes, the size of the symbol or line is difficult to distinguish and the actual value associated with that symbol is not clearly displayed. In addition, similar to single symbol

mapping, this type of map is most helpful with smaller amounts of data, since too many incidents make the map unclear and difficult to read. The following map is an example where size is difficult to determine and points are overlapping.



This type of map is more useful when mapping law enforcement tabular data when the scale is smaller, see below and at the top of the next page.

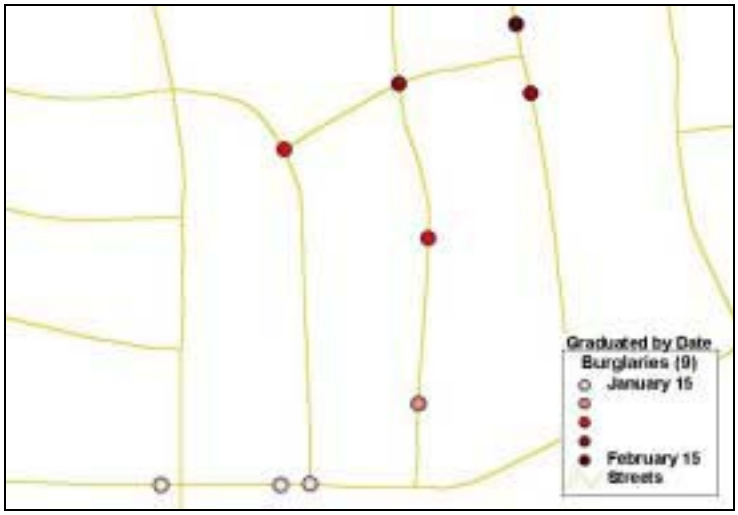




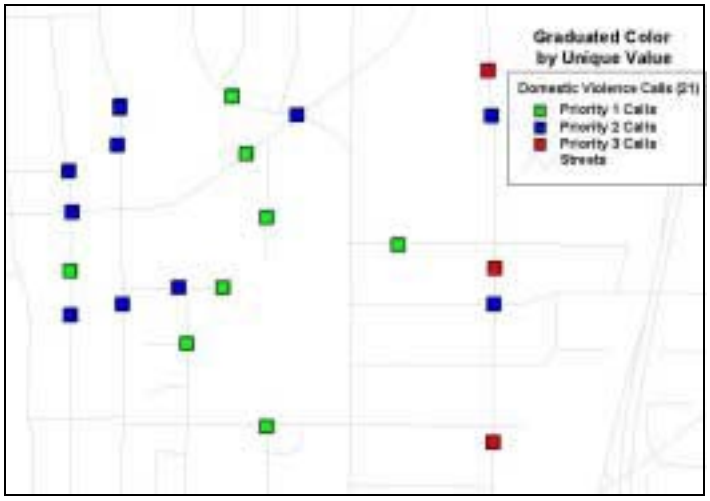
Graduation By Color

In graduated color mapping, symbols (point, line, or polygon features) are altered in color to reflect a particular value of the feature.

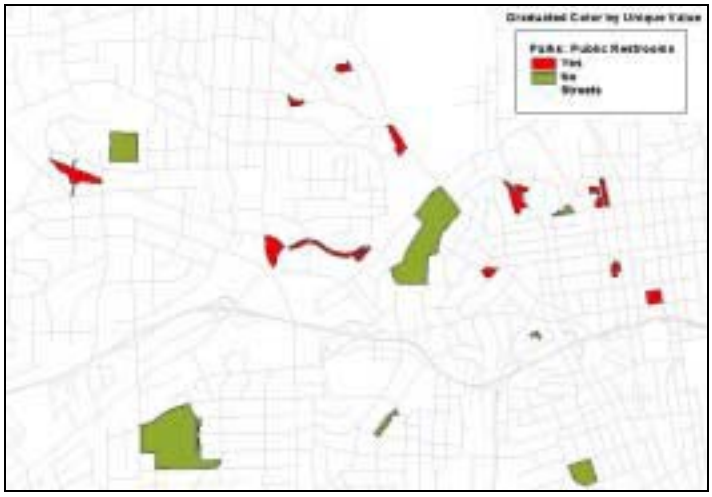
Features can be graduated by any variable. Law enforcement variables include shading by date/time, by priority, by crime type, by number of crimes at a location or in an area, or by crime rate of an area. The next map contains points that are shaded by their date of occurrence and shows the progression from older to the most recent incidents, which are in dark red However, each location must only represent one incident since it would be impossible to shade one point with data from two incidents. As with single symbol mapping, this map is most helpful when examining a small number of cases within crime patterns.



Points can also be shaded by a categorical variable. Each category or unique value is a different color. In the example, the priority of each domestic violence call is a different color.



This method can also be used for line and polygon features. The next map is an example of parks shaded by whether or not they contain public bathroom facilities, which could impact the type of criminal activity in that park.



Classification Methods

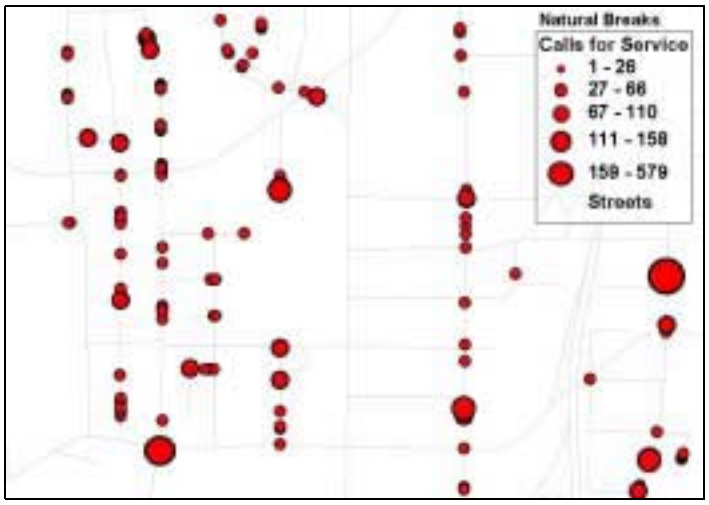
There are several different statistical methods for classifying numeric data in a GIS when creating both graduated size and graduated color maps. The same data are used in the respective point and polygon illustrations to show how different classification methods result in very different maps. Note that in each of the classifications, the user can also change the number of categories, which can also result in different maps of the same data.

Natural breaks

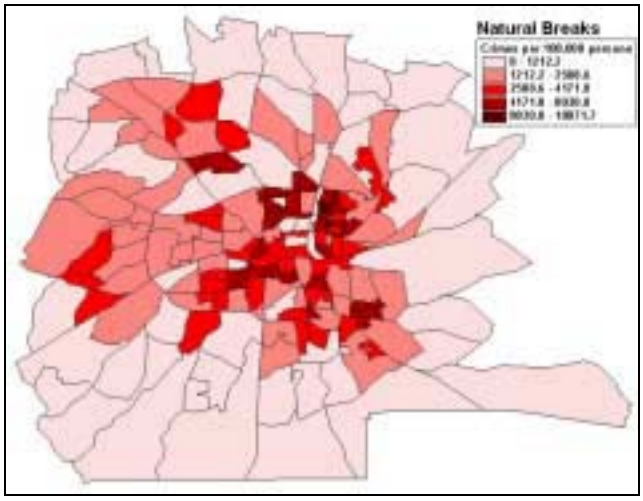
> *This is the default classification in most GIS programs and identifies the natural break points within the data using a statistical formula.*

The software program examines the selected data and their distribution, identifies natural break points, and creates the categories based on the best fit to the data. With each data set, the natural breaks classification would result in different ranges of categories; thus, the classification is "data dependent."

The following is an example of points graduated by size. Note in the legend that the categories do not make much sense, in that they are not evenly distributed or have equal number of values in each. This is because the ranges are determined by the GIS and the nature of the data distribution.



The following is an example of polygons graduated by color.

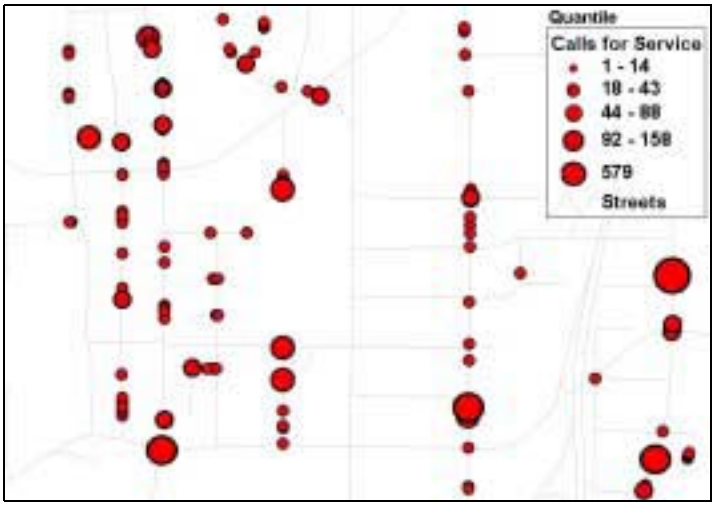


Quantile

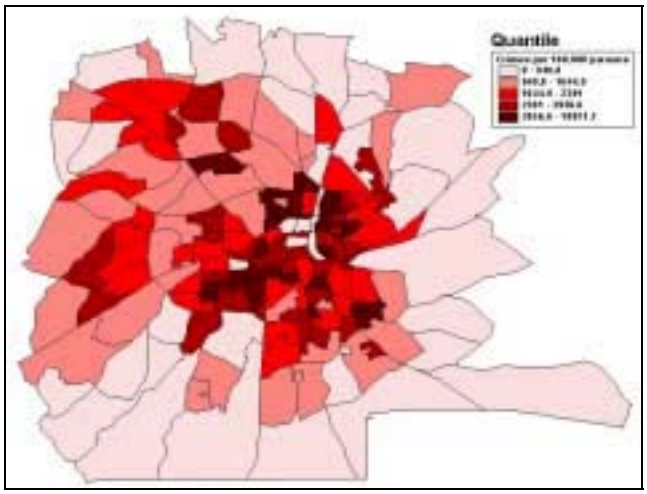
Each class contains the same number of data points.

That is, if there are 100 cases in the data, the GIS sorts them by their values and with five categories, includes the value range for the first 20 cases, the second 20, and so on. Similar to the natural breaks classification, the quantile classification is data dependent.

The following is an example of points graduated by size. Again, the categories do not make much sense, but if we were to look at the data we would see that there are the same number of cases in each category.



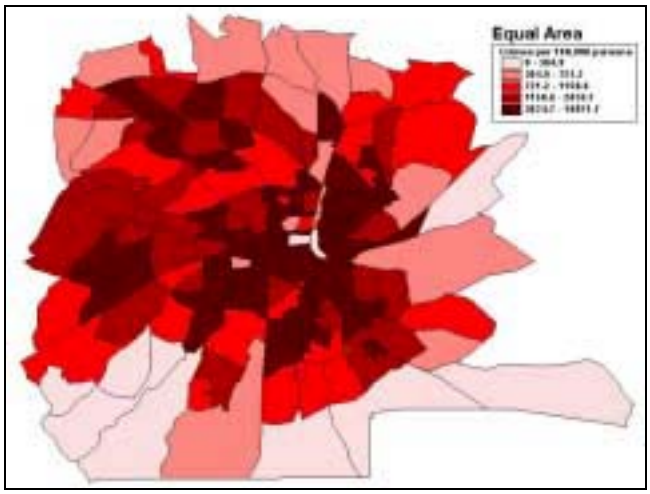
The following is an example of polygons graduated by color.



Equal area

> *This classification applies to polygon features only and determines categories so that the total area of the polygons in each class is approximately the same.*

This method is similar to the quantile classification; however, it looks to the square mileage or other appropriate units of the geographic areas in each class versus the number of data points. Thus, in a legend with five classifications, each category will contain polygons that make up 20% of the total area of the polygons in the analysis. The following is an example of polygons graduated by color.

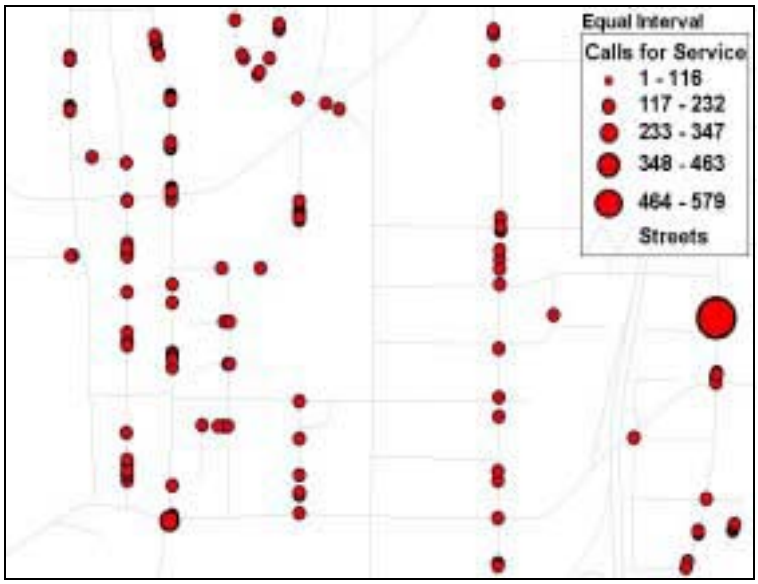


Equal interval

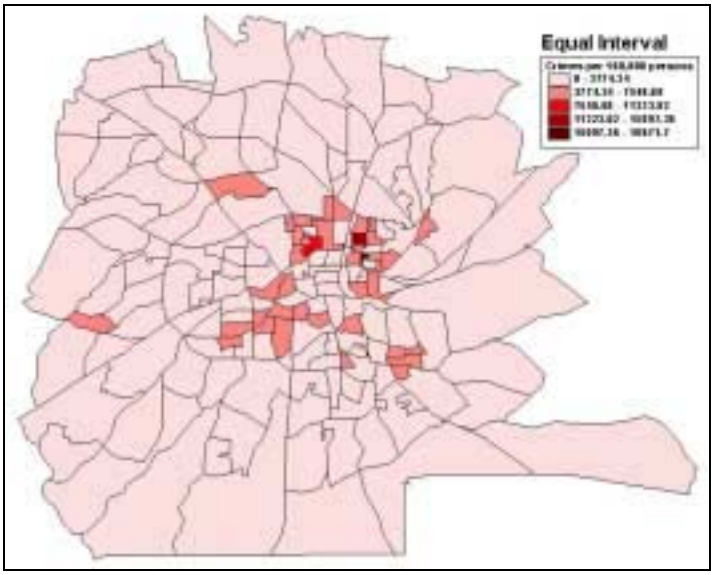
Divides the range of attribute values into equal size sub-ranges.

The GIS determines the range of the values of the distribution and divides by the number of categories to determine the range. For example, if the number of assaults in all the beats of a city ranged from 1 assault to 100 assaults, the categories would be 1-20, 20-40, 40-80, etc. Note that even though the categories seem to overlap, they in fact do not. In this case, all beats with 1 to 20 assaults would be in the first category, but beats with 20.00001 to 40 assaults would be in the second. Even if this is not realistically possible, it is mathematically possible, and it is very important to explain the breakdown system to those individuals using the maps.

The following is an example of points graduated by size. In this case, the categories are even. This classification is still dependent on the data distribution, since as the range of the distribution changes so does the categories. For example, in a data distribution ranging from 1 to 200, the categories would be 1-40, 40-80 and so on, which is different than the categories in the example above.



The following is an example of polygons graduated by color.

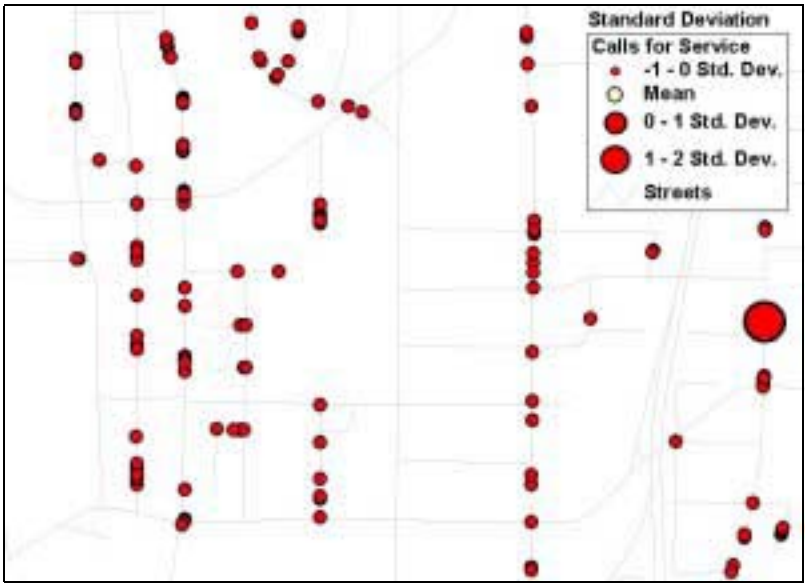


Standard deviation

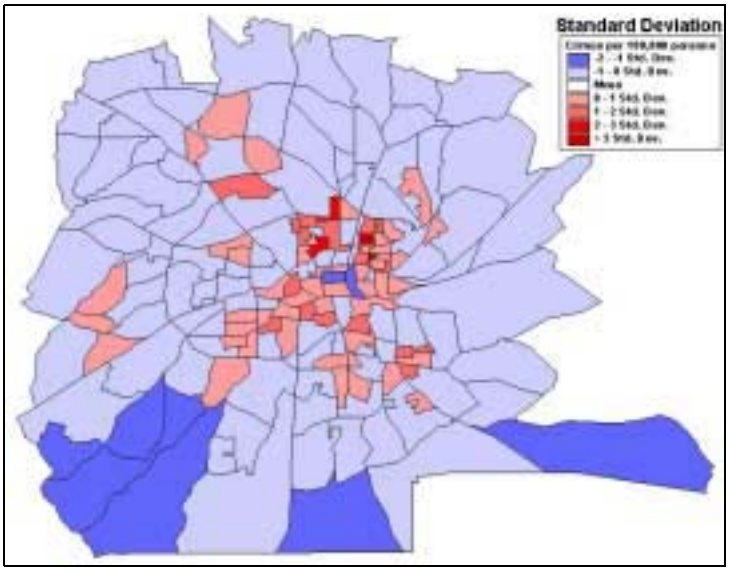
> *The mean value and standard deviations of the geographic features are computed, and the features are shaded according to which category they fall within.*

This classification does not display the actual values of the feature but shows categories of one, two, or three standard deviations above or below the mean. The values behind the classification can be viewed through another function, depending on the GIS software. This classification allows identification of outliers in a distribution and comparison of data with different distributions (would be displayed in two different maps), since the measures of a normal distribution give a common denominator of relative difference.

The following is an example of points graduated by size. Once again, this classification is dependent on the data distribution. Notice that the mean value is not displayed on either one of these maps. Also, in this map there is only one standard deviation below the mean and two above. This indicates that most of the points fall closely around the mean.



The following is an example of polygons graduated by color.



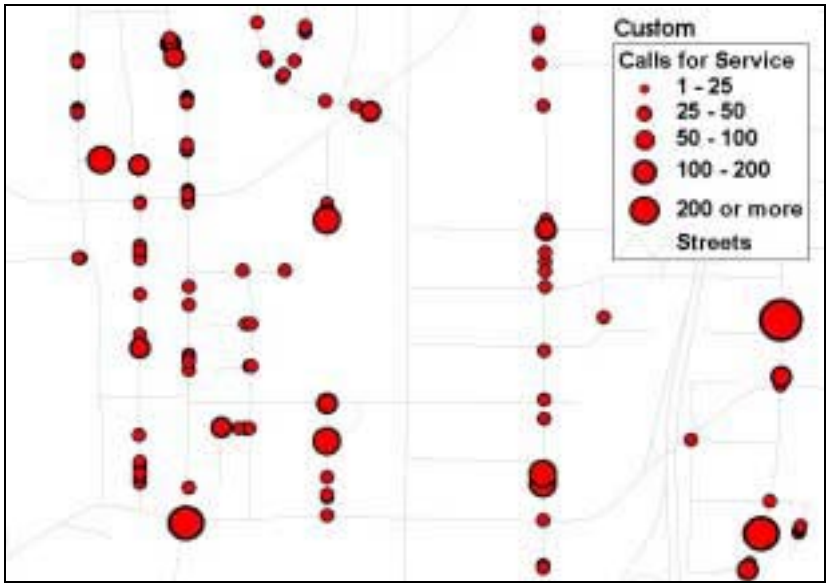
Custom

User determined ranges.

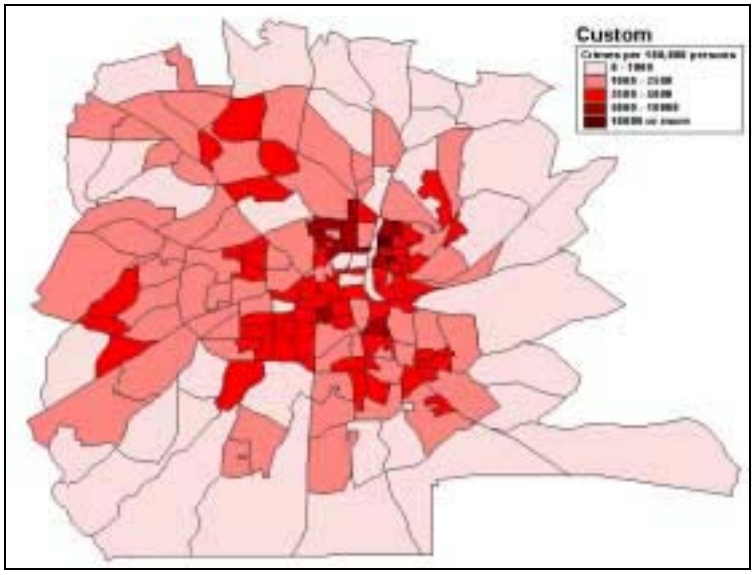
This is the only classification that is not determined by the software and by the characteristics of the data but by the analyst. This method is best for comparing crime or other law enforcement information over time. For instance, calls for service totals and the nature of the distributions tend to be different from month to month. If a classification that is data dependent is used, the colors or size of the symbols will vary in value from map to map. A custom range can be created in which the values for each color or size are the same every month and on every map, which allows comparison.

In order to create custom categories, one might use any of the previous classifications discussed here to get a sense of the data distributions. In addition, it is recommended that when doing a monthly or yearly comparison using custom ranges, that several months or years of data be examined to determine the most appropriate ranges. For this reason, it is best to make the upper limit of the highest range unlimited and use the phrase "or more" as a label (see below) to account for differences. Subjective considerations may also dictate the ranges. For example, in a department that fines properties with more than five false alarm calls for service, the graduation may distinguish between locations with more and less than five calls for service.

The following is an example of points graduated by size.



The following is an example of polygons graduated by color.



VII. Crime Analysis Product Format and Dissemination

The effectiveness of any crime analysis or mapping endeavor has as much to do with the presentation of the results as it does the analysis. If the resulting document of analysis is not legible and understandable to its audience, it is worthless. The following is a discussion of factors to consider when developing a final product, such as methods of dissemination, components of a crime analysis product, and types of crime analysis products. Included also are recommendations for elements of a crime analysis product and elements of a map. These are distinguished from one another since maps include additional elements such as a legend, North arrow, and scale.

Factors to Consider

When developing a crime analysis product, one must consider both the purpose and audience of the product. Crime analysis products can serve many purposes, from informing citizens about recent activity, to assisting the agency in planning, to apprehending a suspected criminal. For example, monthly maps of a town that depict reported crime are useful for providing general information to the public about changes in hotspots of reported crime; however, a detailed map of each hotspot location may be necessary for patrol officers and investigators who need specific information in order to focus their problem solving efforts. In either case, it is important to prepare maps that are appropriate to the purpose.

In addition, there are also many audiences for crime analysis products. They can include police department personnel, the general public, community groups, business groups, school officials, or city council members. By gauging the needs, expectations, and skill level of these individuals, products that are appropriate for each group can be developed. For example, a map of the residences of all known gang members that includes names and case numbers may be useful to gang enforcement officers compiling intelligence information. However, a map with this level of detail would not be disseminated to the public as it may violate an individual's privacy rights or compromise an investigation. It may be appropriate to include a brief notation on the map, such as "law enforcement use only" or "external use" to indicate the intended audience. In general, when producing a crime analysis product, the needs of users of the information need to be balanced with political, legal, and ethical concerns.

Methods of Dissemination

Methods of dissemination of a product inherently rely on the intended purpose and audience. They also rely on the means available, such as the Internet and Intranet capabilities, reverse 911 technology, or the newspaper. For example, a crime analyst

may want to let officers know that there is a sexual assault pattern happening in a certain part of the city and provide them with detailed information about the pattern. The analyst, of course, would not provide this information on the Internet for the public to see, but instead may include selected information on fliers to hand out at a briefing, send a department-wide (internal) e-mail, or attend the briefings of the officers in the affected areas. Thus, the purpose, informing the patrol officers in an area, dictates how that information should be disseminated.

The analyst must also consider what is the most efficient and effective method of dissemination, because frequently, the easiest method is not the most effective. For example, it may be simple to publish a crime pattern bulletin and e-mail it to the department or place fliers on a table in the briefing room for officers to read. But if the officers do not regularly check their e-mail or the table is full of other similar fliers, these methods of dissemination may be ineffective and a more time-consuming method, such as attending briefings, may be warranted. The most effective way to disseminate information depends on the current specific circumstances of the department, and the analyst should continually pay attention to what is appropriate and effective.

Components of Crime Analysis Products

A crime analysis product can include one or more of several types of analytical output, which can include tables, charts, graphs, maps, images, and narratives. In a law enforcement setting, a balance of one or more of these components should be used in any one product, and including all or just one component should be avoided. For example, a two-page essay on the recent burglary activity in Beat 33 will not be as effective as a simple description of the pattern, a table of the relevant information, a chart depicting the time of day and day of week of the activity, and a map that indicates where the activity is occurring. Conversely, a crime analysis product should not contain only a map or a chart. Even though a map or chart should be produced to stand on its own, the crime analyst should also include additional information such as interesting findings, interpretation of the results, and recommendations for future analysis.

Types of Crime Analysis Products

The following are some general types of crime analysis products.

> ***Crime bulletins.*** Short one to two-page documents that describe a tactical short-term trend or pattern.

Memos. A document in letter form that summarizes a request, explains the analysis, highlights the interesting findings, and, in some cases, makes recommendations for response or further analysis. These should be included as cover letters for research and special reports.

Weekly/monthly/quarterly reports and maps. Documents and maps that convey the same information in regular intervals to inform about activity and allow for identifying problems. These products should be consistently formatted to ensure recognizability by customers and allow comparison.

Annual reports. Reports that provide information aggregated by year and are published on a yearly basis. They would include breakdowns by geography, months, and types of activity (e.g., types of crime, types of calls, and accidents) and comparisons among years. They might also include comparisons to other similar jurisdictions as well as to state and national figures.

Research reports. Reports that provide a description of the data, methodology, and analysis of a research project (i.e., problem solving project or evaluation of a program) as well as the results of the analysis, interpretations of the findings, and recommendations for response or future research.

Special reports. These are reports that are requested on an ad hoc basis and address a particular issue such as traffic accidents around schools or efficient allocation of a new squad of officers. The analysis that makes up these reports is less rigorous than the research reports and subsequently takes less time. These special reports make up much of the daily work of the crime analyst.

These general categories can include information about crime, calls for service, arrests, and accidents. They also can be specific to a particular area such as street segment, neighborhood, beat, district, and the entire city. Other more specific types may include lists of incidents, "attempt to locate" bulletins, gang information bulletins, missing persons fliers, and FI card summaries. For template of such reports, see the Police Foundation's product, *Crime Analysis and Mapping Templates* (2001) that are documents that provide guidelines and actual templates (computer files in which the analyst insert his/her own agency and analysis information) for producing these types of reports and maps.

General Crime Analysis Product Elements

The following are the general elements of a crime analysis product.

Title. Includes the nature of the data and geography included as well as the time span included. For example, "Citizen Generated Calls for Service in Precinct 9: January 1, 2001 through June 30, 2001."

File path. This is where the document is located. This is important, so that future requests for the report, an update, or similar report can be easily filled. This assists the analyst in finding the product versus redoing it. An example: F:\Part I Crime 2001\Auto Theft\JanuaryReport.doc.

Credits/date. This includes the name or divisions of the individual(s) who created the report and the date it was created. This allows for the analysts to get credit, for others to direct questions about the product to the appropriate people, and for everyone to know when the product was disseminated. For example, "Prepared by Crime Analysis Unit, December, 2001" or "Prepared by Jane Doe, 01/06/02."

Text, tables, graphics, and/or maps. This is the substantive content of the product and what is included varies from product to product.

Analysis summary. This is an interpretation of the data and interesting findings and is important to ensure appropriate interpretations of the data and results by others. This section is often omitted from crime analysis products.

Disclaimers. This information details what the data and analysis results do not say. For example, conclusions drawn from any report containing crime information can only be made about crimes known to the police, not all crime. Another example is the use of calls for service in lieu of crime data. The difference between the two data sources should be noted as should the limitations of using calls for service (e.g., time and date of call may not be time and date of the criminal incident).

Recommendations. This section would contain suggestions for future analysis or actions based on the results. It is considered optional and may not always be included in a crime analysis product.

Because these elements can be included and combined in an infinite number of ways, a specific example of a crime analysis product is not included here. See below for an example of the map design elements.

Map Design Elements

Maps differ substantively from other components of a crime analysis product, and they contain specific features unique to maps. The following are guidelines for map design elements.

Title. Similar to the title of a general crime analysis product, the title of a map should contain the nature of the data and geography included as well as the time span included.

Legend. This element lists the tabular and geographic data sources displayed in the map and indicates the symbols that are used to represent each data source. In addition, in the case of a map that includes graduation by color or size, the classification used should also be listed. This will allow the reader to understand the divisions of the categories and the analysis that has been conducted. For example, "Classification = Natural Breaks" or "Quantile Classification."

Geocoding rate. As with statistics and tables that are presented in social science, data that are missing from the map should be noted. In the case of a map, this would be displayed as a percentage of the data that have been successfully geocoded. For example, "Geocoding Rate = 99%."

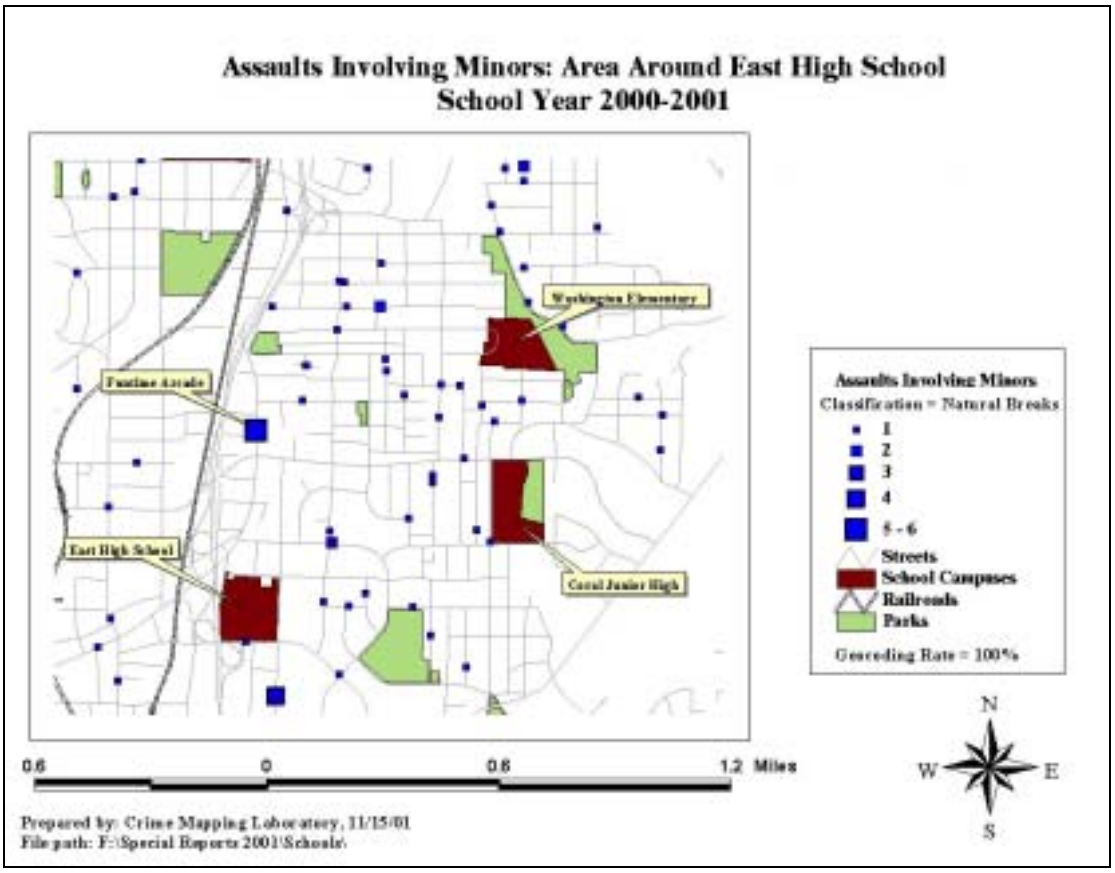
Labels. Should be used in moderation and where appropriate within the map. Labels should orient users to the map as well as highlight analytical results.

Scale Bar. Describes the distance units used in the map.

North Directional. Indicates the geographic orientation of the map.

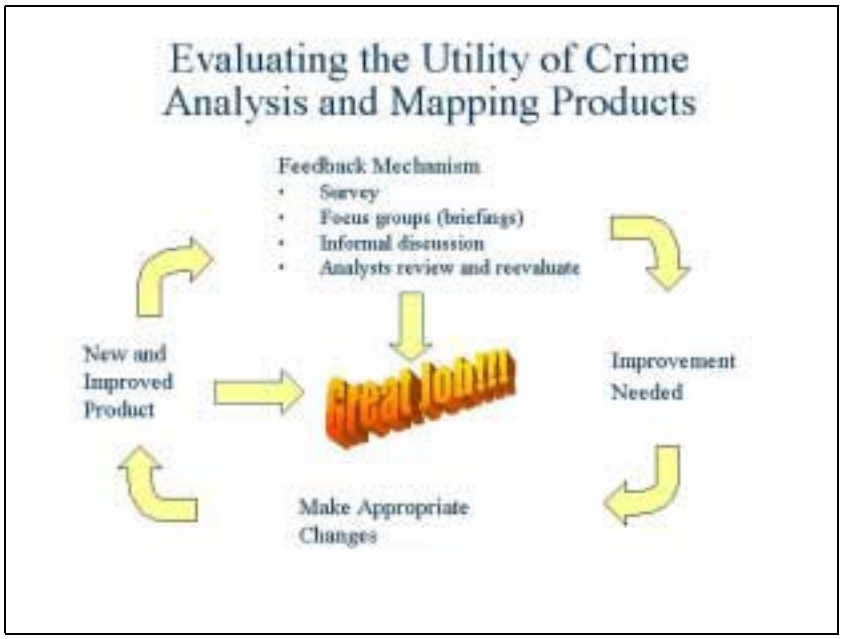
Credits/date. As in the general crime analysis product, this contains the name or division of the individual who produced the map as well as the date it was created.

Remember, these elements are specific to maps and even though maps should basically stand on their own, supplemental description and interpretation of the analysis should be included. The next page shows an example of a map with all of these elements.


Assaults Involving Minors: Area Around East High School
School Year 2000-2001
Washington Elementary
Pastime Arcade
East High School
Coral Junior High
Assaults Involving Minors
Classification = Natural Breaks
1
2
3
4
5 - 6
Streets
School Campuses
Railroads
Parks
Geocoding Rate = 100%
0.6
0
0.6
1.2 Miles
N
W
E
S
Prepared by: Crime Mapping Laboratory, 11/15/01
File path: F:\Special Reports 2001\Schools\

Evaluating the Utility of Crime Analysis and Mapping Products

Finally, a feedback mechanism for crime analysis products is important to determine both their relevance and effectiveness. Customer surveys, informal discussions, and/or focus groups can be used to learn whether a product is serving its intended purpose and is useful to its audience. In addition, it is necessary for the analysts themselves to review and reevaluate current crime analysis products. As noted in the following figure, this process is ongoing. Changes in focus of the department, capabilities of customers, the nature of criminal activity, and information technology are only a few of the factors that could influence needs and purposes of crime analysis products.



VIII. References

Weisburd, D. and McEwen, T. 1998. "Crime Mapping and Crime Prevention." In *Crime Mapping and Crime Prevention: Crime Prevention Studies, Volume 8*. Weisburd, D. and McEwen, T. (eds.) Criminal Justice Press; Monsey, NY. Pp 1-26.

Harries, K. (1999). Mapping Crime: Principle and Practice. US Department of Justice; Washington DC:

Sampson, R. and Scott, M.S. (2000). *Tackling Crime and Other Public Safety Problems: Case Studies in Problem-Solving.* US Department of Justice, Office of Community Oriented Policing Services; Washington DC.

Scott, M. 2000. Problem-Oriented Policing: Reflections on the First 20 Years. US Department of Justice, Office of Community Oriented Policing Services; Washington DC.

Wartell and McEwen, 2001. *Privacy and the Information: Age A Guide for Sharing Crime Maps and Spatial Data.* US Department of Justice; Washington DC

This Page Is Intentionally Left Blank

U. S. Department of Justice
Office of Community Oriented Policing Services

Law Enforcement Intelligence:

A Guide for State, Local, and Tribal Law Enforcement Agencies

Second Edition

David L. Carter, Ph.D.
School of Criminal Justice,
Michigan State University

COPS
COMMUNITY ORIENTED POLICING SERVICES
U.S. DEPARTMENT OF JUSTICE

Law Enforcement Intelligence:

A Guide for State, Local, and Tribal Law Enforcement Agencies

Second Edition

David L. Carter, Ph.D.
School of Criminal Justice,
Michigan State University

This project was supported by Cooperative Agreement #2007-CK-WX-K015 by the U.S. Department of Justice Office of Community Oriented Policing Services. Points of view or opinions contained in this publication are those of the author and do not necessarily represent the official position or policies of the U.S. Department of Justice or Michigan State University. References to specific agencies, companies, products, or services should not be considered an endorsement by the author or the U.S. Department of Justice. Rather, the references are illustrations to supplement discussion of the issues.

Letter from the COPS Office

January 2009

Dear Colleague:

This second edition of *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement* captures the vast changes that have occurred in the 4 years since the first edition of the guide was published in 2004 after the watershed events of September 11, 2001.

At that time, there was no Department of Homeland Security, Office of the Director of National Intelligence, Information-Sharing Environment, or Fusion Centers. Since the advent of these new agencies to help fight the war on terror, emphasis has been placed on cooperation and on sharing information among local, state, tribal, and federal agencies. The successes of community policing are evident, not just within law enforcement, but also through agencies' work with the community to protect civil liberties and civil rights. A strong foundation between the police and the community also yields valuable information for fighting crime and terrorist threats. Through community policing and the wide array of approaches that fall under its umbrella—hot spots, CompStat, problem-oriented policing, and Intelligence-Led Policing—law enforcement can gather and share information that will enhance public safety.

Years of partnership building and problem solving with the community, the private sector, nonprofit organizations, elected officials, social service providers, and other key stakeholders have created an environment in which Intelligence-Led Policing and information sharing is more viable because of the strong relationships established through community policing.

This *Guide* serves as a road map to understanding criminal intelligence and its related methodology, standards, processes, management, and resources. In fact, nearly 85 percent of the material in this second edition is new. I am proud to add this valuable publication to the COPS Office library. My thanks to Dr. David Carter for synthesizing the vast body of law enforcement information and intelligence into one volume that I know will be an indispensable knowledge resource for law enforcement agencies around the country. During these challenging times, community policing is more important than ever.

Sincerely,

Carl Peed
Former Director
Office of Community Oriented Policing Services

Preface

When the first edition of *Law Enforcement Intelligence* was published, it documented unprecedented changes in law enforcement intelligence that occurred largely in response to the September 11, 2001 terrorists' attacks. Indeed, the new initiatives reflected philosophical and operational changes that represented a geometric evolution in law enforcement intelligence in only 3 short years. The first edition of the *Guide* described a broad array of cutting-edge issues and practices. At the time, it seemed implausible that such dramatic changes would occur again. Nevertheless, since the publication of the first edition, a staggering number of significant developments affecting law enforcement intelligence have occurred:

- There were only a few Regional Intelligence Centers across the U.S. that are now evolving into a nationwide network of fusion centers.
- The *Fusion Center Guidelines* had not been written.
- There had been no national fusion center conferences and regional fusion center groups did not exist.
- The Fusion Process Technical Assistance Program, a joint Department of Justice and Department of Homeland Security project, did not exist.
- The Office of the Director of National Intelligence (ODNI) did not exist.
- The Information Sharing Environment did not exist.
- The FBI's Intelligence Directorate did not exist.
- The DEA's National Security Branch of the Office of Intelligence did not exist.
- The National Criminal Intelligence Resource Center did not exist.
- Many intelligence training programs that are now taken for granted did not exist.
- The Joint Regional Information Exchange System—which is now virtually gone— was "the system" for information sharing and analysis.
- "All-hazards" intelligence was not in our lexicon.
- Intelligence-Led Policing was in its infancy.
- What is now the expansive Open Source Center which, as part of the ODNI is aggressively reaching out to state, local, and tribal law enforcement was a narrowly focused program called the Foreign Broadcast Information Service operated by the CIA.
- Relatively few law enforcement agencies had any type of intelligence capacity.
- Suspicious Activity Reporting (SAR) was largely limited to "tips and leads" and there were no unified standards or formal processes to report suspicious activities.

This second edition of *Law Enforcement Intelligence* describes these and many more changes in the philosophy, national standards, and practice of law enforcement intelligence while maintaining the core goal of being a primer on "all things intelligence" for the law enforcement community.

The *Guide* is intended to support policy in law enforcement agencies and seeks to objectively provide the best knowledge and practice of law enforcement intelligence at the time of publication. It is not meant as an academic work nor does it look at theoretical issues or arguments. It is not directed as a guide to the intelligence community except to explain the roles, responsibilities, and restrictions of the intelligence community's state, local, and tribal law enforcement partners.

The Internet references cited in this publication were valid as of June 2009. Given that URLs and web sites are in constant flux, neither the author nor the Office of Community Oriented Policing Services can vouch for their current validity. Please note that some of the sites referenced require a user name and/or password to gain access.

Acknowledgments

In completing this second edition, first and foremost I want to thank Carl Peed, former Director of the Office of Community Oriented Policing Services (the COPS Office). Carl's support for both editions of *Law Enforcement Intelligence* was consistent, strong, and unwavering. Carl, I sincerely appreciate all you have done for this project.

I also thank the membership of the Criminal Intelligence Coordinating Council for taking the time to review the original draft of this *Guide* to ensure that it reflected the information needed by the law enforcement intelligence community. Many people assisted me in the preparation of this *Guide*. Their contributions, large and small, helped in developing the comprehensive contents. While I hope to not leave out anyone, I particularly want to thank: Bill Harris (Delaware Information Analysis Center), Bob Hipple (Indianapolis [Indiana] Metropolitan Police Department), Bruce Parker (Brevard County [Florida] Sheriff's Office, Retired), Ed McGarrell, Steve Chermak, Natalie Hipple, and Jeremy Carter (Michigan State University [MSU]), Hal Wilson (Drug Enforcement Administration), Kathy Suey (Las Vegas Metropolitan Police Department), Kelly Stone (North Central Texas Fusion Center), Lance Ladines (Washington Joint Analysis Center), Mark Johnson (Open Source Center), Merle Manzi (Florida Department of Law Enforcement, Retired), Norm Beasley (Maricopa County [Arizona] Sheriff's Office), Ray Guidetti (New Jersey Regional Intelligence Operations Center), Rick Stephens (FBI), Ritchie Martinez (Arizona High Intensity Drug Trafficking Area), Roger Bragdon (Chief, Spokane [Washington] Police Department, Retired), Sabra Horne and Craig Manly (Office of the Director of National Intelligence), Scott Whitney (Customs and Border Protection), and Tom Martinelli (Wayne State University).

I expressly want to thank those who volunteered to review the *Guide*: Dan Oates (Aurora [Colorado] Police Department), Bob Casey (FBI), Ed McCarroll (Department of Homeland Security [DHS]), Kevin Saupp (DHS), Lisa Palmieri (DHS and International Association of Law Enforcement Intelligence Analysts), Mark Gage (National White Collar Crime Center) and Michael Ronczkowski (Miami-Dade Police Department). I know you were all a little surprised when you discovered the size of the document.

I also had assistance from friends whose work went well beyond "a little help," particularly reading and reviewing drafts. I thank Russ Porter (Iowa Department of Public Safety) for not only his review but also for giving me ideas and perspectives on many issues. Larry Shaw (Florida Department of Law Enforcement) for helping me navigate through the maze of information systems and networks. I sincerely appreciate the extra time and work of Doug Bodrero and Phil Ramer (both of the Institute for Intergovernmental Research) for giving me ideas, reviewing materials, and providing me with comprehensive comments while they were traversing the country on various projects, all for the promise of a meal and a drink.

To Amy Schapiro, COPS Office Social Science Analyst: your constant support and facilitation to make the processes go smoothly are appreciated. To Josh Reinsch of the Michigan State University Intelligence Program, I thank you for your quick

work and willingness to make the extra effort in all that you do for us. And to Robyn Nielsen, also of the MSU Intelligence Program, I truly appreciate your hard work, quick responses, unquestioned dedication, and support for this and other projects. You make my life a lot easier.

To my longtime friend and coconspirator Andi Bannister (Wichita State University): I cannot thank you enough for meticulously reviewing every word of this document and providing suggestions for content, wording, and presentation. As always, you made my work go much smoother (with fewer mistakes!) with all of the time and effort you put into reviewing this *Guide*.

Also important, I thank my wife Karen, children Hilary, Jeremy, and Lauren and son-in-law Joseph O'Donnell who put up with the time I worked on this and other projects—you are always in my thoughts.

Last, I dedicate this *Intelligence Guide* to a beautiful, smart, sweet, bundle of energy who always makes me smile: my granddaughter, Shey Catherine O'Donnell.

David L. Carter, Ph.D.
Michigan State University

Executive Summary

Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies is a policy oriented review of current initiatives, national standards, and best practices.

The first two chapters provide definitions and context for the current state of law enforcement intelligence. Chapter 2 also provides a discussion of homeland security—or "all-hazards"—intelligence. While more law enforcement agencies and fusion centers are embracing the all-hazards approach, its application remains somewhat unclear. This discussion provides a framework for homeland security intelligence policy.

Chapter 3 is a historical perspective that has multiple purposes. First, it provides a discussion of past abuses by law enforcement intelligence because it is important to understand the problems of the past in order to prevent them in the future. Next, the chapter provides a framework for national recommendations and professional standards for the practice of intelligence. Finally, the discussion identifies the various working groups and committees that are framing the current intelligence model and the relationship of those groups to federal agencies and professional law enforcement organizations.

Fundamental to all types of intelligence is a system for managing the flow of information for analysis. This is alternately called the Intelligence Process or the Intelligence Cycle. Chapter 4 is a descriptive discussion of the process as it applies to law enforcement agencies. While there are different models for the Intelligence Process, this discussion relies on the model used in the *National Criminal Intelligence Sharing Plan*.

Recommendations from both the *National Criminal Intelligence Sharing Plan* and the COPS Office-funded International Association of Chiefs of Police intelligence summits urge law enforcement agencies to adopt Intelligence-Led Policing (ILP). The challenge, however, is that there is no universally accepted definition or process for understanding and implementing ILP. Chapters 5 and 6 amalgamate the diverse literature on ILP to provide a holistic view. Chapter 5 focuses on the concept of ILP as it applies to American law enforcement, with a perspective on the British approach from which the concept originated. Chapter 6 focuses on the organizational and administrative processes for implementing ILP.

There is no issue more topical (or controversial) in law enforcement intelligence than the protection of civil rights and privacy. Chapter 7 is a broad examination of the issue identifying the concerns expressed by citizens and illustrating some of the problems faced with intelligence operations through the use of two federal civil rights cases. Integrated into the chapter is a detailed discussion of 28 CFR Part 23 and its application for placing information that identifies individuals or organizations in a criminal intelligence records system. The discussion expands the issues further with a detailed discussion of intelligence records and civil rights liability. The chapter ends with a discussion of how a law enforcement agency can immunize itself against civil rights lawsuits related to the intelligence function.

As a mechanism to enhance widespread information sharing among state, local, and tribal law enforcement agencies, the intelligence fusion concept grew rapidly. This growth was further spurred when fusion centers were embraced by the Information Sharing Environment (ISE) to be the critical information-sharing clearinghouse for terrorism information between law enforcement and other ISE information-sharing partners. Chapter 8 describes the fusion concept and the processes by which a fusion center operates. This chapter also addresses the concerns that critics have expressed about fusion centers.

Every major national standard for intelligence—the *National Criminal Intelligence Sharing Plan*, the *Fusion Center Guidelines*, the *Information Sharing Environment Implementation Plan* and the Department of Homeland Security's *Target Capabilities List*—has recommended establishing a public-private partnership for information sharing to support the intelligence function. Few, however, have established a substantive information-sharing relationship with the private sector. There are difficult hurdles to establishing such a relationship but it certainly is possible. Chapter 9 discusses the recommendations, the issues, and the processes for making public-private partnerships for intelligence a reality.

At the heart of all intelligence activities is the need to manage a wide array of information. A number of critical issues in this process are important to understand. Chapter 10 addresses these issues in a comprehensive manner, relying on best practices and national standards. In a logically organized approach, the key topics discussed are: *Suspicious Activity Reporting* (SAR); defining and using *intelligence requirements;* the *information collection process* including the development of a *collection plan;* the role of *analysis* (from a consumer's perspective); and *intelligence outputs and products*. With the increase of different information-sharing initiatives, one of the challenges has been to ensure that the right information gets in the hands of the right people who can use the information to develop policy and operational responses. This chapter includes a discussion of information-sharing practices to avoid.

A new initiative of the Office of the Director of National Intelligence is the National Open Source Enterprise. The goal of open source information and intelligence is to exploit open sources as "the source of first resort" in any intelligence endeavor. The reasons are that open sources are easier, faster, pose less risk to civil rights, and are less controversial for the agency. Part of this new initiative is to include law enforcement intelligence in open source information sharing. Chapter 11 provides a detailed discussion of open sources, the different types of information that can be obtained, how it can be obtained, and caveats for analysis.

A wide—and confusing—array of federal intelligence resources, including networks, systems, analytic services, applications and products, is available to state, local, and tribal law enforcement. Many have a specialized expertise or a limited area of application, while others are very broad in their application. Chapter 12 discusses federal intelligence resources, starting with a discussion of classified information, including a description of the process for a state, local, or tribal law enforcement officer to obtain a federal security clearance. Most

law enforcement officers, however, will not have a clearance and will be dealing with Sensitive But Unclassified (SBU) information. A discussion is provided of the meaning and rules for SBU information sharing. Important to note: SBU information is going through a government-wide transition to become categorized as Controlled Unclassified Information (CUI) and has some distinct issues for sharing and storing the information. The chapter provides a detailed discussion of CUI and the guidelines imposed for its use. The last part of the chapter is an encyclopedic listing of diverse federal information and intelligence systems and resources.

One of the recommendations of the *National Criminal Intelligence Sharing Plan* is that every law enforcement agency, regardless of size, should develop an intelligence capacity. For some agencies this will be an entire unit, while for other agencies it will be a part-time assignment of one person. In either case, there are management concerns related to the intelligence function. Chapter 13 focuses on management concerns that have relative uniqueness to the intelligence function. It begins with a comprehensive list of factors to consider when developing the intelligence capacity. This is followed by a detailed description of developing a Concept of Operations (ConOps) that serves as the road map for developing and implementing the intelligence function. Finally, a wide range of management issues are discussed, ranging from developing policies to human resources concerns.

The final chapter examines critical issues and challenges for the future and a model for implementing change. The *Guide* also includes comprehensive resources for all aspects of intelligence, a glossary of intelligence terms, and appendixes to support the various discussions. Included in the appendixes are two intelligence audit checklists.

Contents

Letter from the COPS Office v
Preface vii
Acknowledgments ix
Executive Summary xi

Chapter 1: Introduction 1
Perspective 5
Conclusion 6

Chapter 2: Understanding Contemporary Intelligence for Law Enforcement Organizations: Concepts and Definitions 7
Defining Intelligence 10
Law Enforcement Intelligence 11
Homeland Security (All-Hazards) Intelligence 14
National Security Intelligence 15
Emerging Intelligence Initiatives Associated with Homeland Security/All-Hazards Intelligence 19
Fire Service Intelligence Enterprise 19
Medical Intelligence: Protecting the Public Health 20
Gang Intelligence 21
What Is a Gang? 22
National Gang Intelligence Center 23
Conclusion 24
Chapter Annex 2-1: Law Enforcement and Homeland Security Intelligence Case Study 25
Threats Posed by Zebra Mussels 25

Chapter 3: A Brief History of Law Enforcement Intelligence: Past Practice and Recommendations for Change 29
Law Enforcement Intelligence: The Years of Evolution 31
Congressional Inquiries into Intelligence Activities 34
National Crime Commissions and New Initiatives Influencing the Evolution of State, Local, and Tribal Law Enforcement Intelligence 36
The Commissions and their Purpose 36
The National Crime Commissions and Law Enforcement Intelligence 38
Law Enforcement Intelligence Initiatives in the Post-9/11 Environment . 43
Collateral Developments 49
Implications 51
Law Enforcement Intelligence at the State, Local, and Tribal Levels 52
Conclusion 53

Chapter 4: The Intelligence Process (Cycle) for State, Local, and Tribal Law Enforcement 55
Planning and Direction 59
Collection 62
Processing/Collation 64
Analysis 68
Dissemination 69
Reevaluation 73
Conclusion 73
Chapter Annex 4-1: Federal Bureau of Investigation Intelligence Cycle 74
The FBI Intelligence Cycle 74

Chapter 5: The Concept of Intelligence-Led Policing (ILP) 77
Conceptual Foundations 79
Defining ILP 80
Fundamental Perspectives on the History of ILP: The British Experience 82
Perspective 1: The Current State of American Law Enforcement Intelligence 82
Perspective 2: The British National Intelligence Model and Challenges in Adapting It to U.S. Law Enforcement 84
Comparing U.S. and U.K. Law Enforcement Intelligence 86
ILP And Community Policing, Problem Solving, and CompStat 86
Comparing ILP and CompStat 88
Ethical Issues 91
Civil Rights and ILP 91
Public Education 92
Community Members as Law Enforcement Volunteers 93

Chapter 6: Developing and Implementing Intelligence-Led Policing 97
Establishing a Framework for Strategic Priorities and Information Processing: The Information Management Plan 100
The Information Management Plan 102
Establishing Strategic Priorities for Intelligence-Led Policing 102
Intelligence Requirements 107
Collection Plan 107
Analysis 108
Intelligence Products 108
Operational Responses 109
Review of the Process 109
Summary 110
Organizational Infrastructure for ILP 110
Commitment 111

Partnerships 112
Information-Sharing Processes 117
Operational Plan 118
Analytic Capability 118
Tactical and Strategic Response Alternatives 119
Next Steps: Implementation 120
The Implementation Starting Point 122
Conclusion 125
Chapter Annex 6-1:
Community Education Handout 128
Wichita State University
Regional Community Policing Institute 128

Chapter 7: Civil Rights and Privacy in the Law Enforcement Intelligence Process 129

Privacy and Civil Rights: A Foundation 133
Increased Scrutiny of Law Enforcement Intelligence: The Challenge of Balancing Civil Liberties and Community Safety 134
Lawsuits and Decrees Related to Law Enforcement Intelligence Activities 137
Civil Rights Example: First Amendment Free Expression—Two Views 143
The Need for More Controls of Intelligence Inquiries than Criminal Investigations40 145
Maintaining Privacy in the Intelligence Process 146
28 CFR Part 23 – Criminal Intelligence Operating Policies 149
Federal Civil Rights Liability and Intelligence55 155
Providing a Transparent Process 158
Steps to Ensure Protection of Citizens' Civil Rights 160
Conclusion 163
Chapter Annex 7-1:
Protecting Civil Rights and Immunizing an Agency from Liability in the Law Enforcement Intelligence Process 164

Chapter 8: The Intelligence Fusion Process 167
Historical Perspective 169
Refining the Fusion Center Concept 171
Baseline Capabilities for Intelligence Fusion Centers 174
What Is Intelligence Fusion? 175
Why Fusion Centers? 177
Fusion Centers and the Crime Laboratory: An Analogy 179
Fusion Centers and the Information Sharing Environment 180
Operationalizing the Fusion Process 181
Is there a Role for the Private Sector? 183
Concerns About Fusion Centers 184
Fusion Centers and Civil Rights Issues 188
Developing the Fusion Center 190
Outputs of the Fusion Center 193
Conclusion 195
Chapter Annex 8-1: Developing a Memorandum of Understanding 196
Chapter Annex 8-2: Common Terrorism Information-Sharing Standards Program 199
Program Manager/Information-Sharing Environment 199

Chapter 9: Developing Public-Private Partnerships for Law Enforcement Intelligence 201
Background and Perspective 204
U.S. National Standards and Recommendations for Public-Private Partnerships 205
P3I and the Intelligence Process 208
The Information-Sharing Environment and the Private Sector 209
Fundamental Principles of Public-Private Partnerships for Intelligence . . 211
Types of Partnerships 213
Obstacles to Law Enforcement-Private Partnerships 216
Two Critical Issues to Resolve: Sharing Criminal Information and Private Proprietary Information 218
Developing a Successful Public-Private Partnership for Intelligence 220
InfraGard 223
Security/Police Information Network: Nassau County, New York 225
Homeland Security, Information-Sharing, and the Private Sector 227
Critical Infrastructure Sector Partnership 228
Special Note: Terrorism Early Warning Group 230
Conclusion 231
Chapter Annex 9-1: Public-Private Partnership Exercise 232
Sudden Impact: Threat Planning for Infectious Disease in Cattle . . . 232

Chapter 10: Managing Information: A Closer Look at Suspicious Activity Reports, Intelligence Requirements, Collection, Analysis, and Products 235

Suspicious Activity Reporting 237
Suspicious Activity Reporting for a Law Enforcement Agency 238
Suspicious Activity Reporting Processes 240
SARs and Personal Identifying Information 243
Establishing Controls on Suspicious Activity Reports/Information 243
Policy Recommendations for Developing and Managing a Suspicious Activity Reporting System 245
The Nationwide Suspicious Activity Reporting Initiative 246
Summary 248
Intelligence Requirements 251
Filling Gaps/Fulfilling Requirements 252
Applying the Concept to Law Enforcement 254
Comparing Intelligence Requirements and Crime Analysis 254
Requirements and Strategic Priorities 255
Typologies of Requirements 256
Requirements and Criminal Evidence 258
Summary 259
Collection 259
Collecting Information from Corrections Agencies 261
Summary 261
Analysis 262
Analytic Tools 266
Predictive Analysis 270
Critical Variables for the Analysis of a Threat 271
Summary 272
Intelligence Outputs and Products 272
Practices to Avoid with Intelligence Products 276
Summary 277
Conclusion 277

Chapter 11: Open Source Information and Intelligence: A Perspective for State, Local, and Tribal Law Enforcement Agencies 281

Understanding "Open Source" 283
Why Is there Value in Open Source Information? 283
Definitions and Categories 284
Source of First Resort 285
National Initiatives: The National Open Source Enterprise 287
Open Source and Law Enforcement Intelligence (Tradecraft) 289
Law Enforcement Applications of Open Source 290
Open Sources and Civil Rights 291

Attribution and Copyrighted Materials in the Intelligence Process and Reports 294
Metrics for Open Source Use 296
Open Source Content for the Intelligence Process 296
Open Source Information Identifying People and Organizations from Subscription Services and the Media 297
The Social Networking Concept and Issues for Open Source. 298
Newsletters and Blogs 299
Wikis 301
RSS Feeds 301
Gray Literature 302
The Deep Web. 302
The Underground Web 306
A Broadened Perspective of Open Source for Law Enforcement 307
Homeland Security Intelligence and Open Sources 308
Open Source Processes and Protocols 309
Using an Open Source Collection Plan. 309
Techniques and Tools 310
The Need to Determine Accuracy, Reliability, and Validity 311
Avoiding Traffic Analysis: Becoming Anonymous on the Web. 312
The Investment in Critical Thought and Time 314
Conclusion 314
Chapter Annex 11-1: Eclectic Web Sites Sometimes Found Useful for Intelligence 315
Chapter Annex 11-2: The Pre-Search Development Plan 317

Chapter 12: Federal and National Law Enforcement Intelligence Resources, Networks, and Systems 319

What Is Needed to Start?. 322
Federal and National Law Enforcement Intelligence Resources. 322
Classified Information. 323
Security Clearances for SLTLE Personnel 326
Sensitive but Unclassified and Controlled Unclassified Information 328
Sensitive but Unclassified Information. 329
Controlled Unclassified Information 330
Summary. 334
Federal and National Intelligence Resources and Products 335
Department of Justice— Law Enforcement Information Sharing Program 336
Federal Bureau of Investigation Intelligence Initiatives40. 342
Terrorist Screening Center 346
Law Enforcement Online42 347

Guardian and eGuardian 348
Department of Homeland Security Intelligence and Analysis Directorate 348
Homeland Security–State and Local Intelligence Community of Interest (HS SLIC) 351
National Counterterrorism Center (NCTC)50 351
Regional Information Sharing System 353
RISS.NET 354
Drug Enforcement Administration58 356
El Paso Intelligence Center62 357
National Drug Intelligence Center63 358
High Intensity Drug Trafficking Areas65 359
Bureau of Alcohol, Tobacco, Firearms and Explosives68 360
Federal Protective Service Secure Portal70. 361
Financial Crimes Enforcement Network72 361
High-Risk Money Laundering and Related Financial Crimes Areas73 363
Gateway 363
International Justice and Public Safety Network74 364
Accelerated Information Sharing for Law Enforcement 364
Operation Archangel and the Automated Critical Asset Management System 364
Constellation/Automated Critical Asset Management System 366
Law Enforcement Intelligence Unit82 366
Information Sharing 367
International Criminal Police Organization83 367
Summary. 368
A Summary of Selected Intelligence Networks and Applications 369
SBU/CUI Networks 369
SBU/CUI Network Applications 371
Conclusion 371

Chapter 13: Management and Human Resource Issues for the Intelligence Function. 373

A Checklist of Considerations in Developing or Reengineering the Law Enforcement Intelligence Capacity 376
Administration and Management 376
Develop the Intelligence Unit's Infrastructure. 378
Staffing 380
Training 380
Information Management and Information-Sharing 381
Implementation and Assessment 383
Developing the Concept of Operations 383
Contents of a Concept of Operations 385
The ConOps Next Step. 391
Implementing and Managing the Intelligence Structure 391
Establishing an Organizational Framework 391
Chartering an Intelligence Unit. 392
Auditing the Intelligence Function 395
Establishing and Managing Partnerships 396
Sources for Intelligence Management and Resource Trends. 397
Human Resource Issues 398
Staffing 398
Training 400
Categories of Currently Available Intelligence Training Programs. 404
Federal Bureau of Investigation Center for Intelligence Studies29. 404
Drug Enforcement Administration30 404
Federal Law Enforcement Training Center31 405
Other Programs and Training Resources 405
Intelligence Courses in Higher Education 405
Conclusion 406
Chapter Annex 13-1
10 Simple Steps to Help Your Agency Become Part of the National Criminal Intelligence Sharing Plan40 407
Chapter Annex 13-2
Why Law Enforcement Agencies Need an Analytic Function41 409

Chapter 14: Summary, Conclusions, and Next Steps 411
Challenges for the Future 414
Implementing Change: The R-Cubed Approach5 415
Reassessing 416
Refocusing 416
Reallocating 417
Conclusion 417

Figures/Tables 419

Bibliography/Appendixes 425
Bibliography 427
Appendix A: Glossary of Terms for Law Enforcement Intelligence 437
Appendix B: Intelligence Unit Management Audit 453
Audit Criteria for the Law Enforcement Intelligence Function Version 2.0 453
Appendix C:
LEIU Audit Checklist for the Criminal Intelligence Function 465
Appendix D: About the Author 471
David L. Carter, Ph.D. 471

Chapter 1:
Introduction

Introduction

To protect the United States from threats to our security and sovereignty, current initiatives at the federal, state, local, and tribal levels seek to develop a "culture of information sharing."[1] This is a significant challenge that requires the integration of new law, policy, procedure, training, and organizational change.

The National Strategy for Information Sharing focuses on five core principles:

1. Effective information sharing comes through strong partnerships among federal, state, local, and tribal authorities, private-sector organizations, and our foreign partners and allies.
2. Information acquired for one purpose, or under one set of authorities, might provide unique insights when combined, in accordance with applicable law, with seemingly unrelated information from other sources. We, therefore, must foster a culture of awareness in which people at all levels of government remain cognizant of the functions and needs of others and use knowledge and information from all sources to support counterterrorism efforts.
3. Information sharing must be woven into all aspects of counterterrorism activity, including preventive and protective actions, actionable responses, criminal and counterterrorism investigative activities, event preparedness, and response to and recovery from catastrophic events.
4. The procedures, processes, and systems that support information sharing must draw on and integrate existing technical capabilities and must respect established authorities and responsibilities.
5. State and major urban area fusion centers represent a valuable information-sharing resource and should be incorporated into the national information-sharing framework. This will require fusion centers to achieve a baseline level of capability to gather, process, share, and utilize information, and operate in a manner that respects individuals' privacy rights and other legal rights protected by U.S. laws.[2]

To achieve the culture of information sharing, every law enforcement agency in the United States, regardless of size, must have the capacity to understand the implications of information collection, analysis, and intelligence sharing. Each agency must have an organized mechanism to receive and manage intelligence as well as a mechanism to report and share critical information with other law enforcement agencies. In addition, it is essential that law enforcement agencies develop lines of communication and information-sharing protocols with the private sector, particularly those related to the critical infrastructure, as well as with those private entities that are potential targets of terrorists and criminal enterprises.

Not every agency has the staff or resources to create a formal intelligence unit, nor is it necessary in smaller agencies. Even without an intelligence unit, a law enforcement organization must have the ability to effectively consume the information and intelligence products being shared by a wide range of

[1] Program Manager–Information Sharing Environment. *Information Sharing Environment Implementation Plan.* Washington, D.C.: Office of the Director of National Intelligence, 2006.

[2] *National Strategy for Information Sharing.* Washington, D.C.: Executive Office of the President, 2007, pp. 2–3.

organizations at all levels of government. State, local, and tribal law enforcement (SLTLE) will be most effective when a single source in every agency is the conduit of critical information, whether it is the Terrorist Intelligence Unit of the Los Angeles Police Department, the sole intelligence analyst of the Lansing (Michigan) Police Department, or the patrol sergeant who understands the language of intelligence and is the information-sharing contact in the Mercedes (Texas) Police Department. Each law enforcement agency must have an understanding of its intelligence management capabilities, regardless of its size or organizational structure.

This document describes common language and processes for developing and employing an intelligence capacity in SLTLE agencies across the United States as well as articulating a uniform understanding of concepts, issues, and terminology for law enforcement intelligence. While terrorism issues are the most pervasive, the discussion of intelligence in this *Guide* is directed toward "all crimes, all threats, and all hazards." As such, the principles of intelligence discussed in this document apply beyond terrorism and include organized crime and entrepreneurial crime in all forms.

Drug trafficking and the associated crime of money laundering, for example, continue to be a significant challenge for law enforcement. Transnational computer crime, particularly Internet fraud, identity theft cartels, and global black marketeering of stolen and counterfeit goods, are entrepreneurial crime problems that are increasingly relegated to SLTLE agencies to investigate simply because of the volume of criminal incidents. Similarly, local law enforcement is increasingly drawn into human trafficking and illegal immigration enterprises and the often-associated crimes related to counterfeiting of official documents, such as passports, visas, driver's licenses, social security cards, and credit cards. Even the trafficking of art and antiquities has increased, often bringing a new profile of criminal into the realm of entrepreneurial crime. Most recently, the application of intelligence to pervasive violence in America's communities is also an important focus. All require an intelligence capacity for SLTLE, as does the continuation of historical organized crime activities such as auto theft, cargo theft, and virtually any other scheme that can produce profit for an organized criminal entity.

To be effective, the law enforcement community must interpret intelligence-related language in a consistent manner. In addition, common standards, policies, and practices will help expedite intelligence sharing while at the same time protecting the privacy of citizens and preserving hard-won community policing relationships.

Perspective

At the outset, law enforcement officers must understand the concept of law enforcement intelligence, its distinction from national security intelligence, and the potential problems an SLTLE agency can face when the two types of intelligence overlap. A law enforcement executive must understand what is meant by an "intelligence function" and how that function can be fulfilled through the use of different organizational models. Related executive decisions focus on staffing, particularly when there are fiscal limitations. Complicating this mission are two new intelligence responsibilities that have emerged: 1. Information sharing with national security and homeland security partners as part of the Information Sharing Environment and 2. developing a capacity for Homeland Security—or "all-hazards"—Intelligence.

Another important—and pervasive—challenge is to ensure that all new intelligence initiatives fully protect the privacy and civil rights of all persons. Critical issues and new initiatives for this responsibility are discussed throughout the *Guide*, with one chapter devoted specifically to this topic.

These issues pose a wide range of important questions: What kinds of information does the law enforcement agency need (that is, what are its intelligence requirements) from the federal government to most effectively counter terrorism? How are those needs determined? How is the information requested? When and in what form will the information be received? Will a security clearance be needed to review the information that an executive requests? Beyond terrorism, what types of threats exist in a community? How are these threats identified? What kinds of threats are included in "all-hazards" intelligence? What are the best sources and methods (that is, a collection plan) for understanding these threats and developing actionable intelligence? How do we engage the community and private sector in the intelligence process? What are the limitations on collecting and disseminating information between law enforcement and the community and private sector? The answers are not easy, but they are attainable.

From a policy and process perspective, what is meant by information sharing? What information can be collected? What information can be retained in a criminal intelligence records system? How long may the records be retained? When does a person transcend the threshold of exercising his or her rights to posing a threat to community safety? What resources exist to aid an SLTLE agency in accomplishing its intelligence goals? How can the entire law enforcement agency be integrated into the intelligence function? If a law enforcement organization is to be effective, the answers to these questions must be a product of written policy.

The intent of this document is to provide answers—or at least alternatives—to these questions. To begin the process, every law enforcement administrator must recognize that intelligence and information sharing can be effective in preventing terrorism and fighting organized crime. To realize these ends, however, the intelligence process for law enforcement at all levels of government requires the following:

- Reengineering some of the organization's structure and processes so that they are consistent with national initiatives and national standards of good practice in law enforcement intelligence.
- Developing a shared vision of the terrorist or criminal threat.
- Establishing a commitment to participate and follow through with threat information.
- Overcoming the conceptual difficulty of intelligence processes that some personnel find difficult to grasp.
- Committing an agency's resources, time, and energy to the intelligence function.
- Establishing policies and practices that protect individuals' civil rights and privacy.
- Embracing and using contemporary technology, including electronic access to information and an electronic communications capability through a secure connection.
- Having proactive people using creative thought to identify "what we don't know" about terrorism and international organized crime.
- Requiring a law enforcement agency to think globally and act locally.
- Engaging in public-private partnerships for intelligence.
- Engaging the community to participate in the intelligence process.
- Being committed and patient.

Conclusion

The amount of change in the law enforcement intelligence process that has occurred during the past 4 years is unprecedented. The roles and responsibilities for state, local, and tribal law enforcement are challenging from operational, policy, and fiscal perspectives. Despite these challenges, comprehensive plans and new resources have become available to achieve the goal of protecting our communities.

Chapter 2:

Understanding Contemporary Intelligence for Law Enforcement Organizations: Concepts and Definitions

Understanding Contemporary Intelligence for Law Enforcement Organizations: Concepts and Definitions

In the purest sense, intelligence is the end product of an analytic process that evaluates information collected from diverse sources; integrates the relevant information into a logical package; and produces a conclusion, estimate, or forecast about a criminal phenomenon by using the scientific approach to problem solving (that is, analysis). Intelligence, therefore, is a synergistic product intended to provide meaningful and trustworthy actionable knowledge to law enforcement decision makers about complex criminality, criminal enterprises, criminal extremists, and terrorists.

The law enforcement intelligence function has essentially two broad purposes:

1. Prevention involves gaining or developing information related to threats of terrorism or crime and using it to apprehend offenders, harden targets, and use strategies that will eliminate or mitigate the threat. Two generally accepted types of intelligence are specifically oriented toward prevention:
    a. Tactical Intelligence. Actionable intelligence about imminent or near-term threats that is disseminated to the line functions of a law enforcement agency for purposes of developing and implementing preventive, and/or mitigating, response plans and activities.
    b. Operational Intelligence. Actionable intelligence about long-term threats that is used to develop and implement preventive responses. Most commonly, operational intelligence is used for long-term inquiries into suspected criminal enterprises and complex multijurisdictional criminality.
2. Planning and resource allocation provides information to decision-makers about the changing nature of threats, the characteristics and methodologies of threats, and emerging threat idiosyncrasies for the purpose of developing response strategies and reallocating resources, as necessary, to accomplish effective prevention.
    a. This is known as strategic intelligence. It provides an assessment of the changing threat picture to the management of a law enforcement agency for purposes of developing plans and allocating resources to meet the demands of emerging threats.

While investigation[1] is clearly related to the information collection[2] and intelligence processes, the intelligence function is often more exploratory and more broadly focused than a criminal investigation, per se. For example, a law enforcement agency may have a reasonable suspicion to believe that a person or group of people have the intent, capacity, and resolve to commit a crime or terrorist act. Evidence, however, may fall short of the probable cause standard, even for an arrest for criminal attempt or conspiracy. Moreover, there may be a compelling community safety reason to keep an inquiry open to identify other criminal offenders—notably leaders—and weapons that may be used.

[1] "Investigation" is defined as the pursuit of information based on leads and evidence associated with a particularly defined criminal act to identify and apprehend criminal offenders for prosecution in a criminal trial.

[2] "Information collection" in the context of law enforcement intelligence is the capture of information and data to determine if suspicious activities have a criminal nexus and/or to understand the operation of crime phenomena.

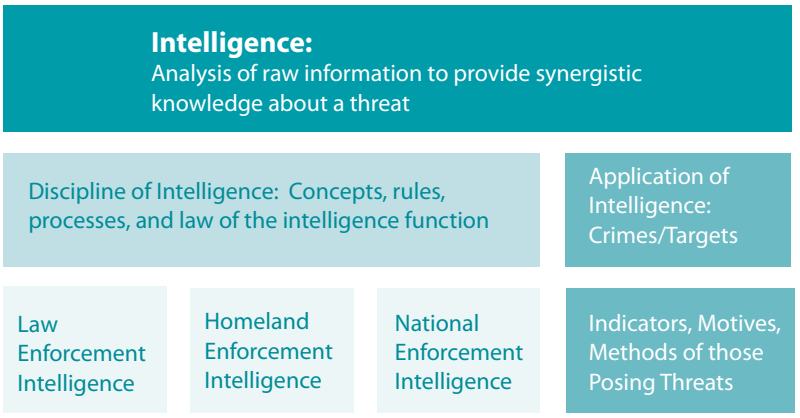
Because of this broader role, the need to keep information secure, and the necessity of keeping records that identify individuals and organizations for whom evidence of criminal involvement is uncertain or tangential,[3] rigid guidelines must be followed. These guidelines are designed to protect the constitutional rights of citizens while at the same time permitting law enforcement agencies to proceed with an inquiry for purposes of community safety. The guidelines are also designed to facilitate accurate and secure information sharing between law enforcement agencies because the nature of terrorism and criminal enterprise threats are inherently multijurisdictional. Further, if law enforcement agencies at all strata of government subscribe to the same guidelines, information sharing can be more widespread because there is certainty that regardless of with whom the information is shared, the security and integrity of the records will remain intact.

Defining Intelligence

There are many misconceptions about the meaning and application of "intelligence;" not only among the lay public but also within law enforcement. Colloquial uses of the term provide an intuitive understanding, such as "Officer Jones collected some good intelligence." These uses, however, lack precision and are unable to account for the diverse applications and rules associated with the intelligence function.

As a primer, there are two broad classes of intelligence, as illustrated in Figure 2-1. The first category is the "discipline" of intelligence, which refers to the set of rules, processes, and lexicon of the intelligence function. This *Intelligence Guide* is solely about the discipline of intelligence. Within the framework of the discipline, there are three types of intelligence of concern for the present discussion:[4] 1. Law enforcement (or criminal[5]) intelligence, 2. Homeland security—also known as "all-hazards"—intelligence, and 3. National security intelligence. While there are important similarities across these three categories, there are also distinct differences. These critical factors are discussed throughout this *Guide* as they specifically relate to state, local, and tribal law enforcement (SLTLE) agencies.

Figure 2-1: Classes of Intelligence



[3] This includes information that would be in the intelligence records system "Temporary File" as well as "Non-Criminal Identifying Information" as defined by 28 CFR Part 23.

[4] This is not an exclusive categorization of intelligence. The discipline of intelligence may be divided into other categories; for example, National Security Intelligence may be divided into "policy intelligence" and "military intelligence." One may also consider "business intelligence," "geospatial intelligence," or "cyber intelligence," among others. The categorization used above is the best model to illustrate critical points for the current discussion.

[5] The author uses the phrase "law enforcement intelligence" because a realm of study in the field of criminal psychology addresses "criminal intelligence" as it relates to the criminal personality and the propensity and processes by which criminals behave.

The second broad class is the "application of intelligence," which deals with knowledge related to a specific crime type. Intelligence analysis that produces information about new methods and indicators in the uses of improvised explosive devices (IED) by jihadists, for example, is the "application of intelligence." Another illustration would be indicators drawn from an analysis of international financial transactions that are characteristic of a money laundering enterprise. An essential ingredient for the application of intelligence is an understanding of the nature and constituent elements of the crime phenomenon of concern. For example, if a community is threatened by multijurisdictional gang activity that operates as a criminal enterprise, an understanding of the gang culture, signs, symbols, hierarchy, and other gang-specific characteristics is essential for analysts and officers to be effective in combating the crime problem. While the two classes of intelligence are inextricably linked for purposes of training and application, it is nonetheless essential to understand the unique aspects of each.

With an understanding of the classes of intelligence, attention will be directed toward the definitions of each.

Law Enforcement Intelligence

This *Guide* uses definitions based on generally accepted practice and standards by the law enforcement intelligence community at the local, state, and tribal levels. This does not mean that other definitions of terms are wrong, but this approach provides a common understanding of words and concepts as most applicable to the targeted audience of this *Guide*.

Before defining intelligence, it is essential to understand the meaning of "information" in the context of this process. Information may defined as "pieces of raw, unanalyzed data that identify persons, organizations, evidence, events or illustrates processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event."[6] As will be seen, information is collected as the currency that produces intelligence.

The phrase "law enforcement intelligence," used synonymously with "criminal intelligence," refers to law enforcement's responsibility to enforce the criminal law. Oftentimes, the phrase is used improperly, and too often, intelligence is erroneously viewed as pieces of information about people, places, or events that can be used to provide insight about criminality or crime threats. It is further complicated by the failure to distinguish among the different types of intelligence.

Figure 2-2: Diverse Information Collected for Intelligence Analysis

[6] Global Intelligence Working Group. *Criminal Intelligence for the Chief Executive. A Training Program for the Chief Executive. Glossary.* Washington, D.C.: Global Justice Information Sharing Initiative, U.S. Department of Justice, 2004.

Pieces of information gathered from diverse sources, such as wiretaps, informants, banking records, or surveillance (see Figure 2-2), are simply raw data that frequently have limited inherent meaning. Intelligence is when a wide array of raw information is assessed for validity and reliability, reviewed for materiality to the issues at question, and given meaning through the application of inductive or deductive logic. Law enforcement intelligence, therefore, is "the product of an analytic process that provides an integrated perspective to disparate information about crime, crime trends, crime and security threats, and conditions associated with criminality."[7] The need for carefully analyzed, reliable information is essential because both policy and operational decisions are made using intelligence; therefore, a vigilant process must be in place to ensure that decisions are made on objective, informed criteria, rather than on presumed criteria.

Often "information sharing" and "intelligence sharing" are used interchangeably by persons who do not understand the subtleties, yet importance, of the distinction. In the strictest sense, care should be taken to use terms appropriately because, as will be seen in later discussions, there are different regulatory and legal implications for "intelligence" than for "information" (See Table 2-1) As such, the subtleties of language can become an important factor should the management of a law enforcement agency's intelligence records come under scrutiny.

Table 2-1: Comparative Illustrations of Information and Intelligence

Information	Intelligence
• Criminal history and driving records • Offense reporting records • Statements by informants, witnesses, and suspects • Registration information for motor vehicles, watercraft, and aircraft • Licensing details about vehicle operators and professional licenses of all forms • Observations of behaviors and incidents by investigators, surveillance teams, or citizens • Details about banking, investments, credit reports, and other financial matters • Descriptions of travel including the traveler(s) names, itinerary, methods of travel, date, time, locations, etc. • Statements of ideologies, beliefs, and practices	• A report by an analyst that draws conclusions about a person's criminal liability based on an integrated analysis of diverse information collected by investigators and/or researchers • An analysis of crime or terrorism trends with conclusions drawn about characteristics of offenders, probable future crime, and optional methods for preventing future crime/terrorism • A forecast drawn about potential victimization of crime or terrorism based on an assessment of limited information when an analysts uses past experience as context for the conclusion • An estimate of a person's income from a criminal enterprise based on a market and trafficking analysis of illegal commodities

[7] Carter, David L. *Law Enforcement Intelligence Operations.* 8th ed. Tallahassee, Florida: SMC Sciences, Inc. 2002.

Definitions and Context

State and local law enforcement have consistently defined law enforcement intelligence as containing the critical element of "analysis" before any information can be characterized as "intelligence." For example, the International Association of Chiefs of Police *Criminal Intelligence Sharing* plan funded by the Office of Community Oriented Policing Services observes that:

> …intelligence is the combination of credible information with quality analysis—information that has been evaluated and from which conclusions have been drawn.[8]

Similarly, the Global Intelligence Working Group, a project that is funded by the Office of Justice Programs and is part of the Global Justice Information Sharing Initiative, discusses law enforcement intelligence by observing:

> …the collection and analysis of information to produce an intelligence end product designed to inform law enforcement decision-making at both the tactical and strategic levels.[9]

Following a consistent vision, the International Association of Law Enforcement Intelligence Analysts states that intelligence is an analytic process:

> …deriving meaning from fact. It is taking information collected in the course of an investigation, or from internal or external files, and arriving at something more than was evident before. This could be leads in a case, a more accurate view of a crime problem, a forecast of future crime levels, or a hypothesis of who may have committed a crime or a strategy to prevent crime.[10]

In creating standards for state, local, and tribal law enforcement, the Commission on Accreditation for Law Enforcement Agencies (CALEA) seeks to provide specific guidance on policies and practices that ensures efficacy and protection from liability on all aspects of law enforcement duties. With respect to intelligence, CALEA's standards note:

> Certain essential activities should be accomplished by an intelligence function, to include a procedure that permits the continuous flow of raw data into a central point from all sources; a secure records system in which evaluated data are properly cross-referenced to reflect relationships and to ensure complete and rapid retrieval; a system of analysis capable of developing intelligence from both the records system and other data sources; and a system for dissemination of information to appropriate components.[11]

It is clear not only from these discussions, but also from the legacy of law enforcement intelligence from various national crime commissions examining intelligence-related activities at the state and local level, that a common thread is that information must be analyzed before it is classified as intelligence. Chapter 3 will show that there is a fundamental reason for this: regulations applying to state, local, and tribal intelligence records must[12] meet standards of assessment that do not apply to federal agencies.[13] As a consequence, the analytic component is essential for the definition.

[8] International Association of Chiefs of Police. *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Federal, State, and Local Levels.* A Summit Report. Alexandria, Virginia: IACP, 2002, p. v.

[9] Global Intelligence Working Group. *National Criminal Intelligence Sharing Plan*. Washington, D.C.: Office of Justice Programs, 2003, p. 6.

[10] International Association of Law Enforcement Intelligence Analysts. *Successful Law Enforcement Using Analytic Methods.* Internet-published document, undated, p. 2.

[11] Commission on Accreditation of Law Enforcement Agencies. *Standards for Law Enforcement Accreditation.* "Standard 51.1.1 – Criminal Intelligence." Washington, D.C.: CALEA, 2002.

[12] Most notably, 28 CFR Part 23 as well as various court decisions.

[13] These issues are described in detail, in both Chapter 3 and Chapter 7.

It is often stated that for every rule there is an exception. The definition of law enforcement intelligence fits this axiom. As a matter of functional practicality, the FBI Directorate of Intelligence (DI) categorizes intelligence somewhat differently. As observed by one FBI DI official in a confidential interview:

> In the law enforcement/national security business, [intelligence] is information about those who would do us harm in the form of terrorist acts or other crimes, be they property crimes or violent crimes. … [The FBI DI] produces both "raw" (or unevaluated intelligence) and "finished" intelligence products (those that report intelligence that has had some degree of analysis).

Given the nature of the FBI DI's responsibilities and the need to get the critical threat information into the hands of the law enforcement community quickly, this definition is more appropriate for its role. Law enforcement executives need to be aware of the different roles and the different context when interpreting information. These differences are not in conflict; rather, they coexist to support the different missions and responsibilities of agencies at all levels of government. Similarly, the need for a different approach to the "Intelligence Cycle" exists for the FBI compared to SLTLE because of different intelligence demands.

The remedy is simple: Those responsible for the intelligence function need to understand these differences and apply policies and practices (described later) that are most appropriate for the types of intelligence being produced and consumed.

Homeland Security (All-Hazards) Intelligence

While the phrase "homeland security intelligence" is relatively new, it integrates well-established law enforcement responsibilities, most notably the "order maintenance" function of law enforcement.[14] These new intelligence responsibilities have emerged within the homeland security framework requiring that intelligence activities at the state, local, and tribal levels must assess threats posed by "all hazards." While there certainly are gray areas within this framework, the key factor for law enforcement agencies is to focus on threats posed by hazards that have implications for responsibilities for public safety and order maintenance. Within this context, the author defines homeland security intelligence as the collection and analysis of information concerned with noncriminal domestic threats to critical infrastructure, community health, and public safety for the purpose of preventing the threat or mitigating the effects of the threat.

A public health emergency or natural disaster, for example, will necessarily involve a law enforcement agency to assist in maintaining order and executing operations to maintain public order until the crisis is resolved. Homeland security intelligence may identify community safety vulnerabilities emerging from the emergency or disaster and give this information to law enforcement agencies so that appropriate precautions can be put into place. In yet other cases, information may begin as homeland security intelligence and become law enforcement intelligence, such as a general threat to critical infrastructure that evolves into a

[14] For a discussion of "order maintenance" responsibilities see Carter, David L. *Police and the Community.* 7th ed. Upper Saddle River, New Jersey: Prentice Hall, 2000.

threat where an individual is identified. If an individual is identified as related to a critical infrastructure threat, in all likelihood a criminal nexus has emerged and a law enforcement intelligence inquiry may proceed jointly with homeland security intelligence.

This form of intelligence presents many challenges because it is not purely criminal, yet addresses responsibilities that law enforcement agencies have to manage within their communities. Homeland security intelligence is not clearly delineated either as a matter of law or of policy, yet it is increasingly prevalent because of the impact of Department of Homeland Security (DHS) responsibilities, particularly in the arena of critical infrastructure.

As noted above, in some cases law enforcement intelligence and homeland security intelligence may overlap. This is illustrated by an actual case study appended at the end of this chapter related to a threat associated with zebra mussels that has both homeland security and criminal implications. The value of the case study is to illustrate not only homeland security intelligence but also law enforcement intelligence as applied to a nontraditional threat.

National Security Intelligence

In understanding the broad arena of intelligence, some perspective of national security intelligence (NSI) is useful for SLTLE agencies. This primer is meant to familiarize the law enforcement reader with basic terms, concepts, and issues, and is not intended as an exhaustive description.

NSI may be defined as "the collection and analysis of information concerned with the relationship and homeostasis of the United States with foreign powers, organizations, and persons with regard to political and economic factors as well as the maintenance of the United States' sovereign principles."[15] NSI seeks to maintain the United States as a free, capitalist republic with its laws and constitutional foundation intact, and identify and neutralize threats or actions that undermine United States sovereign principles.

NSI embodies both policy intelligence and military intelligence. Policy intelligence is concerned with threatening actions and activities of entities hostile to the U.S., while military intelligence focuses on hostile entities, weapons systems, warfare capabilities, and order of battle. Since the fall of the Soviet Union and the rise of threats from terrorist groups, both policy and military intelligence have evolved to grapple with the character of new threats. The organizations responsible for NSI are collectively known as the Intelligence Community (IC).

The IC is a federation of 16 executive branch agencies and organizations that work within their own specific mission as well as in an integrated fashion to conduct threat assessment and intelligence activities necessary for effective foreign relations and the protection of United States national security. These activities include the following:

- Collection of information needed by the President, the National Security Council, the Secretaries of State and Defense, and other Executive Branch officials for the performance of their duties and responsibilities

[15] Carter, David L. *Law Enforcement Intelligence Operations*. 8th ed. Tallahassee, Florida: SMC Sciences, Inc., 2002.

- Production and dissemination of intelligence related to national security and the protection of U.S. sovereign principles from interference by foreign entities
- Collection of information concerning, and the conduct of activities to protect against, intelligence activities directed against the U.S., international terrorist and international narcotics activities, and other hostile activities directed against the U.S. by foreign powers, organizations, persons, and their agents
- Administrative and support activities within the U.S. and abroad that are necessary for the performance of authorized activities such as foreign relations, diplomacy, trade, and the protection of interests of our allies
- Such other intelligence and activities as the President may direct as related to national security and the U.S. relationship with foreign entities.

The 16-member IC consists of the following organizations:[16]

1. Air Force Intelligence.
2. Army Intelligence.
3. Central Intelligence Agency.
4. Coast Guard Intelligence.
5. Defense Intelligence Agency.
6. Department of Energy.
7. Department of Homeland Security.
8. Department of State.
9. Department of the Treasury.
10. Drug Enforcement Administration.
11. Federal Bureau of Investigation.
12. Marine Corps Intelligence.
13. National Geospatial-Intelligence Agency.
14. National Reconnaissance Office.
15. National Security Agency.
16. Navy Intelligence.

As seen in the definition and descriptions of NSI, there is no jurisdictional concern for crime. As a result, constitutional restrictions that attach to criminal cases that law enforcement faces on information collection, records retention, and use of information in a raw capacity do not apply to IC responsibilities where there is no criminal investigation.

SLTLE agencies have no direct jurisdiction as related to NSI; however, this does not mean that they will not encounter NSI or receive collection tasks to support NSI. Indeed, given that the Federal Bureau of Investigation (FBI) is a member of the IC, there is a strong likelihood that SLTLE officers serving on a Joint Terrorism Task Force will encounter or be exposed to NSI. Similarly, since the Drug Enforcement

[16] www.intelligence.gov/1-members.shtml

Administration (DEA) is also a member of the IC, officers working on an Organized Crime Drug Enforcement Task Force may also encounter this intelligence. In both instances the officers typically will have Top Secret or Secret security clearances that provide access to classified documents which may provide additional insights about the information, including the source of the information and the method of collection. Nonetheless, it is a slippery slope for SLTLE officers to rely on this information for a criminal investigation because there is a strong likelihood that the methods of collecting the NSI would not meet constitutional muster in a criminal trial.

Even if it appeared that constitutional standards may be met, there are other potential problems when using the information in a criminal enquiry. Since the accused in a criminal proceeding has the right to be confronted by his or her accusers, the exercise of this right could compromise sensitive sources and methods. While the Classified Information Procedures Act (CIPA) provides a mechanism to deal with the process, some find that it is cumbersome and may result in greater complications than would otherwise be necessary.[17]

The next issue deals with constitutional law. If the information was collected from NSI sources in a manner inconsistent with the Constitution, it is likely, based on the "Fruits of the Poisonous Tree Doctrine," that any subsequent evidence developed during the course of that investigation would be subject to the Exclusionary Rule. Consequently, the evidence would be inadmissible.

Liability is a final issue concerning state, local, and tribal officers' access to NSI. Specifically, in a criminal investigation, if SLTLE officers used NSI that was collected in a manner inconsistent with constitutional standards or if that information (including personal records) was kept as intelligence records that were under the custodianship of a state, local, or tribal law enforcement officer, it is possible that the officer(s) and the chain of command (through vicarious liability) of that officer's agency could be liable under 42 USC 1983, Civil Action for Deprivation of Civil Rights. Under this provision, as most officers are well aware, if a state or local officer, acting under the color of state law, violates the civil rights of a person, the officer and his or her chain of command may be sued in federal court. Even though that officer may be working on a federal task force under the supervision of a federal officer, such as an FBI Supervisory Special Agent, the applicable test is whether the officer is paid by and bound by the employment rules of his or her state or local employing jurisdiction.[18]

Based on authorities from the National Security Act of 1947; Executive Order 12333; various executive directives, and the U.S. Attorney General Guidelines, the FBI is the lead agency in domestic intelligence collection. It is important that SLTLE understand the distinction between the authority of IC agencies to collect and retain information and that of SLTLE agencies.

A new challenge emerges with the Information Sharing Environment (ISE) created by the Intelligence Reform and Terrorism Prevention Act of 2004. As will be discussed in the next chapter, the ISE seeks to share all information related to

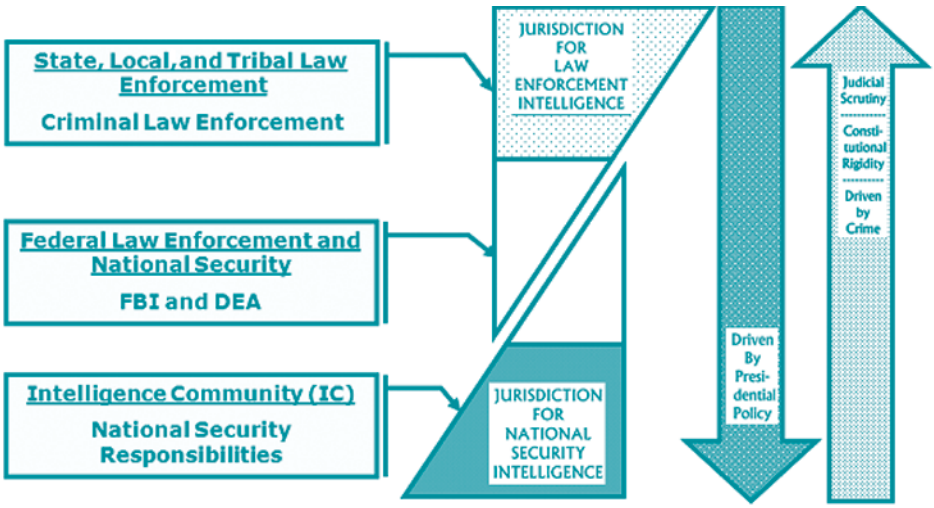
[17] The author has elected not to discuss CIPA in any detail because it deals with federal investigations rather than state, local, and tribal criminal investigations. For the person interested in further exploring CIPA, see www.usdoj.gov/usao/eousa/foia_reading_room/usam/title9/crm02054.htm.

[18] The FBI and DEA may keep such records in their custody on the basis of their national security responsibilities. While it is possible to hold a federal officer liable based on what is known as a "Bivens Suit"—derived from the case of *Bivens* v. *Six Unknown Agents* 403 US 388 (1971)—it would be difficult, particularly under the conditions of counterterrorism.

threats to the homeland. The challenge arises particularly if SLTLE agencies collect or retain information related to a national security threat rather than to a crime. SLTLE agencies sole jurisdiction as related to intelligence is based in their statutory authority to enforce the criminal law. As such, there is extensive constitutional rigidity and judicial scrutiny of their processes as well as the information that is collected and retained in a criminal intelligence records system (See Figure 2-3). Conversely, constitutional protections do not attach in the same way to the collection and retention of information by the IC. As a result, these agencies have greater latitude in the types of information they possess.

The processes are complicated further regarding the collection of information domestically (within the territory of the United States) that is related to national security threats. The primary responsibility for collecting domestic information for national security falls within the authority of the DHS, the FBI, and the DEA, which can produce intelligence for dissemination to SLTLE. U.S. foreign intelligence agencies, however, are prohibited from working with state and local law enforcement in a manner that could be interpreted as "tasking intelligence collection." As a result, SLTLE agencies should rely on their relationship with the DHS, the FBI, and the DEA on matters of domestic intelligence, including when those matters involve international terrorism activity. (See Figure 2-3)

Figure 2-3: Law Enforcement and National Security Intelligence Authority Comparison



Effective policy and processes must be implemented and enforced to ensure that SLTLE agencies do not maintain improper information about individuals and organizations in their records system as a product of the ISE. These issues will be discussed in greater detail in the chapter on civil rights.

The lessons learned from this brief review of national security intelligence are threefold:

1. State, local, and tribal law enforcement officers have no jurisdiction to collect or manage NSI.
2. Use of NSI in a criminal investigation by a state, local, or tribal law enforcement officer could derail the prosecution of a case because of civil rights protections.
3. Use of NSI in a criminal investigation by an SLTLE officer and/or retention of NSI in a records system or in the personal records of an SLTLE officer could open the possibility of civil liability from a Section 1983 lawsuit.

Emerging Intelligence Initiatives Associated with Homeland Security/All-Hazards Intelligence

While the range of activities that could be encompassed by homeland security intelligence is broad, two initiatives are moving forward with greater rapidity: the Fire Service Intelligence Enterprise and Public Health/Medical Intelligence.

Fire Service Intelligence Enterprise

The Fire Service Intelligence Enterprise (FSIE), a new initiative that is in its infancy, is epitomized by this observation from *Fire Chief* magazine:

> Does the fire service, or emergency services in general, have a role in the world of intelligence? This question probably would never have been asked prior to Sept. 11, 2001, but it is being asked now. Given that firefighters are among the country's first responders to terrorist incidents, natural disasters, industrial accidents, and everyday emergencies, the answer is a resounding yes.[19]

Asking law enforcement about the fire service role in intelligence operations does not evoke a response with the same vigor. The reason, for the most part, is uncertainty: Law enforcement is uncertain about the types of information they can share with the fire service and whether the fire service holds a unique role beyond the private sector.

Exploration has resulted in the FSIE experimental initiative. Based on a test program from the Fire Department of New York (FDNY) along with joint efforts from within DHS—the Intelligence & Analysis Directorate (I&A) and the Federal Emergency Management Agency (FEMA)—the concept is being further explored.[20]

> Though not a federally sanctioned establishment or organization, its establishment by state and local fire service officials and industry groups was a result of advice and support provided by the State and Local Program Office to the FDNY and FEMA's United States Fire Administration. This relationship contributed to a draft approach for state and local fire services to share threat and related information among the country's nearly 1.2 million firefighters

[19] Pitts, Diane, "Getting the 411," *Fire Chief,* January 1, 2008. firechief.com/leadership/incident-command/intelligence-community-information-sharing-0101/index.html

[20] For a list of the intelligence and information requirements of the FSIE, see: Office of Intelligence and Analysis. *National Strategy for the Fire Service Intelligence* Enterprise. Washington, D.C.: U.S. Department of Homeland Security, 2008, pp.14–21.

and EMS customers. I&A continues working with the United States Fire Administration and the National Fire Academy in Emmitsburg, Maryland, to incorporate intelligence training into their course curriculum and ensure that our first responders better understand the events surrounding or leading up to their involvement in an incident.[21]

FSIE's objective is to establish a direct information conduit between the fire service and both DHS and local law enforcement, largely through a fusion center. The law enforcement agency would pursue a direct information-sharing relationship with the fire service per a directive of the National Response Plan. The National Response Plan mandates the alignment of federal coordinating structures, capabilities, and resources into a unified, all-discipline, and all-hazards approach to domestic incident management.[22]

Through sharing pre-incident information and intelligence and real-time incident updates, situational awareness will be enhanced to support the preparedness efforts of both local fire departments and the DHS. Rapid and comprehensive information sharing also is imperative to establishing a common operational picture on the local and national levels during a major incident.[23]

The difficulty for the FSIE concept is that it predominantly exists within the "all-hazards" framework of intelligence about which law enforcement is still attempting to identify and resolve its intelligence role. Further, the issues of information sharing and civil rights remain difficult to resolve unequivocally. Similarly, some members of the fire service are not overly enthusiastic about being associated with the law enforcement intelligence function.

Amalgamating the fusion concept with the all-hazards approach to intelligence requires a critical review of operating processes, responsibilities, and roles. The jury is out on whether the FSIE will be a fruitful initiative. Nonetheless, law enforcement executives and intelligence commanders should be aware of the FSIE concept and explore the role, if any, it holds in the local law enforcement intelligence structure.

Medical Intelligence: Protecting the Public Health

A growing component of the all-hazards responsibility in homeland security intelligence deals with public health threats. Medical intelligence assesses public health trends, organizations, and related events that can affect the health of a community. There has been significant growth in the military on medical intelligence where the focus is broader, notably looking at foreign medical trends. Comprehensive resources on medical intelligence can be found at these resources:

- The Armed Forces Medical Intelligence Center[24]
- The WWW Virtual Library collection on Epidemiology[25]
- The Biodefense and Public Health Database[26]
- The Centers for Disease Control and Prevention (CDC) WONDER Database of Health and Risks.[27]

[21] Tomarchio, Jack. " Focus on Fusion Centers: A Progress Report." Prepared statement before the Ad Hoc Subcommittee on State, Local and Private Sector Preparedness and Integration, Committee on Homeland Security and Government Affairs, United States Senate, April 17, 2008, p. 7.

[22] Ibid

[23] Pitts, Op. Cit.

[24] mic.afmic.detrick.army.mil (restricted access site).

[25] www.epibiostat.ucsf.edu/epidem/epidem.html

[26] www.biohealthbase.org

[27] wonder.cdc.gov

The significant points to note are these:

1. There is a distinct trend toward medical intelligence as a tool to assist in the protection of our communities.
2. Medical intelligence will become an increasingly important intelligence responsibility as a result of the all-hazards mandate.
3. There are resources to assist in identifying public health threats.

Gang Intelligence

Gang intelligence provides challenges to fully understanding the application of current law, regulation, policy, and practice for law enforcement intelligence. As noted previously, intelligence is the output of the analytic process; however, with those persons specializing in gang investigations, the term "intelligence" is commonly used more broadly. Typically, gang specialists include "indicators" under the rubric of intelligence; for example, information about gang behaviors, signs and symbols of different gangs ("colors" and "tagging"), the modus operandi of different gangs, and trends in the different gang activities. Frequently, much of this information is not analyzed, or at least not analyzed in the same sophisticated manner as the intelligence process. As a practical element of the discussion in this section, the recognition of this fact is functional; thus, when discussing gang intelligence, this common application of the term by gang investigators will be used.

Certainly there is an important role for analysis when dealing with gangs; however, gang data and information are not subject to analysis as frequently as they should be. This should change not only with the expansion of analytic expertise in law enforcement agencies, notably through fusion centers, but also as a result of approval of the *Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces*[28] by the Global Intelligence Working Group.

The following is information from the FBI:

- "Today, gangs are more violent, more organized, and more widespread than ever before."
- "There are approximately 30,000 gangs, with 800,000 members, impacting 2,500 communities across the U.S."
- Latino gangs are sowing violence and crime in big cities like Los Angeles, Chicago, and New York, but are also spreading to rural and suburban areas.
- The violent gang MS-13—composed mainly of Central American immigrants from El Salvador, Honduras, and Guatemala—"has a significant presence in Northern Virginia, New York, California, Texas, as well as places as disparate and widespread as Oregon City, Oregon; and Omaha, Nebraska." MS-13 is estimated to have some 8,000 to 10,000 hard-core members—and is growing increasingly sophisticated, widespread, and violent.[29]

With many criminal gangs taking on the characteristics of transjurisdictional criminal enterprises, the need for information sharing and analysis of threats is essential. The tools and resources of intelligence can be important factors in effectively dealing with gang problems.

[28] Global Intelligence Working Group. *Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces.* Washington, D.C.: Bureau of Justice Assistance, U.S. Department of Justice, 2008.

[29] www.fbi.gov/page2/april05/swecker042005.htm

Gang intelligence provides challenges in the application of current law, regulation, policy, and practice for law enforcement intelligence. As noted previously, intelligence is the output of the analytic process. For those specializing in gang investigations, however, "intelligence" is commonly viewed more broadly, typically including information about gang behavior, indicators, modus operandi, and trends that are largely derived from raw information learned from investigations rather than analysis. As a practical element of this discussion, the subtle distinction between what is meant by "intelligence" by gang investigators as compared to the meaning of "intelligence" by those working in the law enforcement intelligence community should be recognized.

What Is a Gang?

The initial vision when hearing the word "gang" is a group of young males, typically in the inner city involved in "turf battles" and who spray paint gang symbols on property and is involved in violent, often deadly, confrontations with other collectives of young men. Typically, a vision of the well-known Los Angeles-based "Crips" and "Bloods" gangs is part of that picture. While these kinds of gangs certainly exist, gangs encompass a much larger population.

The National Gang Threat Assessment[30] divided gangs into six broad categories:

1. National and Regional Street Gangs.
2. Gangs and Organized Crime.
   - Asian Organized Crime
   - Russian Organized Crime
3. Gangs and Terrorist Organizations.
   - Domestic Terrorist Groups
   - International Terrorist Groups
4. Prison Gangs.
5. Hispanic Gangs.
6. Outlaw Motorcycle Gangs.

As can be seen from these categories, the line between gangs and organized crime may be blurred. Similarly, the line between gangs and terrorist organizations can also be difficult to discern because often both use the tactics of intimidation and fear to accomplish their goals.

While each state has its own statutory definitions of a gang, most use a model similar to that of the Violent Gang and Terrorist Organization File (VGTOF) of the National Crime Information Center (NCIC). According to VGTOF guidelines, a gang member must be characterized as, and have at least two of, the following criteria:

- Has been identified as a gang member by an individual of proven reliability.
- Has been identified as a gang member by an individual of unknown reliability, and that information has been corroborated in significant respects.

[30] National Alliance of Gang Investigators Associations. *National Gang Threat Assessment.* Washington, D.C.: Bureau of Justice Assistance, U.S. Department of Justice, 2005.

- Has been observed by law enforcement members to frequent a known gang's area, associate with known gang members, and/or affect that gang's style of dress, tattoos, hand signals, or symbols.
- Has been arrested on more than one occasion with known gang members consistent with gang activity.
- Has admitted membership in a gang at any time other than at the time of current arrest/incarceration.[31]

As can be seen, the value of intelligence and information sharing for both identifying and classifying a person as a gang member can be an important tool. This is particularly true because gangs are often transjurisdictional. Both tactical and strategic intelligence can provide important information to law enforcement agencies about gang threats and trends.

Two initiatives have been developed that serve to enhance the use of intelligence when dealing with the gang threat: The National Gang Intelligence Center and the *Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces.*

National Gang Intelligence Center

The National Gang Intelligence Center (NGIC) integrates the gang intelligence assets of all Department of Justice agencies and has established partnerships with other federal, state, and local agencies that possess gang-related information, thereby serving as a centralized intelligence resource for gang information and analytical support. This enables gang investigators and analysts to identify links between gangs and gang investigations, further identify gangs and gang members, learn the full scope of their criminal activities and enterprises, determine which gangs pose the greatest threat to the United States, identify trends in gang activity and migration, and guide the appropriate officials in coordinating their investigations and prosecutions to disrupt and dismantle gangs. The NGIC's mission is to support law enforcement agencies through timely and accurate information sharing and strategic and tactical analysis of federal, state, and local law enforcement intelligence focusing on the growth, migration, criminal activity, and association of gangs that pose a significant threat to communities throughout the United States.[32]

The NGIC focuses on gangs operating on a national level that demonstrate criminal connectivity between sets of common identifiers. In addition, because many violent gangs do not operate on a national level, the NGIC will also focus on selected regional-level gangs. To maximize effectiveness, the NGIC produces intelligence assessments, intelligence bulletins, joint agency intelligence products, and other nonstandard intelligence products for its customers.[33]

Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces

Developed by the Gang Intelligence Strategy Committee (GISC) of the Global Justice Information Sharing Initiative, the *Gang Guidelines* seek to develop an integrated strategy to deal with gangs by cohesively linking both intelligence and operational responses to gang threats through task forces. On the issue

[31] National Gang Center. *Brief Review of Federal and State Definitions of the Terms "Gang," "Gang Crime," and "Gang Member."* Undated and unpublished web document. www.nationalgangcenter.gov/documents/definitions.pdf.

[32] "Attorney General's Report to Congress on the Growth of Violent Street Gangs in Suburban Areas," Washington, D.C.: U.S. Department of Justice, 2008, p. 14. www.usdoj.gov/ndic/pubs27/27612/27612p.pdf.

[33] www.usdoj.gov/criminal/ngic

of intelligence, the *Gang Guidelines* stress the importance of analysis and recommend the use of the intelligence process to manage and assess raw information. Similarly, the Gang Guidelines embrace the *National Criminal Intelligence Sharing Plan* as the intelligence model that should be used in all gang intelligence initiatives. Finally, the *Gang Guidelines* recognize the important role that intelligence can fulfill by more efficiently and effectively directing task forces responses to gang threats.

The *Gang Guidelines* are new, having been approved in late 2008; however, with their endorsement by the Criminal Intelligence Coordinating Council there will likely be widespread adoption by law enforcement agencies, fusion centers, and gang task forces.

Conclusion

The intent of this chapter was to provide the reader with insight into the meaning of intelligence, the diverse types of intelligence, its role, and some of the complications that emerge from using the term. Law enforcement intelligence, for example, is defined somewhat differently by the FBI and the DEA than it is by SLTLE agencies. The reason for the difference is based on the sources of information used by the FBI and the DEA as well as the responsibilities these federal law enforcement agencies hold for disseminating unique critical information in a timely fashion. The important point is that the consumer simply needs to know the different definitions and the different context. With this knowledge, information can be interpreted and used most effectively.

Also introduced in this chapter was the concept of homeland security intelligence and the unique role it fulfills for law enforcement agencies. While not a traditional activity for law enforcement, homeland security intelligence seeks to enhance public safety and order while protecting the community from nontraditional threats.

Finally, Chapter 2 addressed the meaning of NSI and the complications it conceivably can pose for SLTLE agencies. Once again, it is important to understand the issues and parameters of each type of intelligence. The proverbial bottom line is that understanding the definitions and their application is an essential foundation for the remaining topics discussed throughout this *Intelligence Guide*.

Chapter Annex 2-1: Law Enforcement and Homeland Security Intelligence Case Study

This illustration is based on an actual case. It demonstrates the interrelationship between the two types of intelligence.

Threats Posed by Zebra Mussels

A congressman from a Midwestern state was a vocal supporter of legislation to ban Internet gaming in the U.S. An individual who opposed this legislation made a threat to the congressman's office that if the congressman voted for the legislation, the individual would introduce zebra mussels into some of his state's lakes.

Zebra mussels (*Dreissena polymorpha*) are an invasive species native to the Black Sea and Caspian Sea regions of Eurasia. In 1988 they were introduced to U.S. fresh water in Lake St. Clair— between Lake Erie and Lake Huron on the Michigan, U.S.—Ontario, Canada, border— through ballast water discharged from transoceanic vessels. The zebra mussel competes with native species of mussels and is particularly prone to clogging pipes, valves, and drains that affect drinking water, hydroelectric plants, and a wide variety of manufacturing firms. According to the Nonindigenous Aquatic Species Program of the U.S. Geological Survey, "Zebra mussels can have profound effects on the ecosystems they invade…and represent one of the most important biological invasions into North America".[33] Zebra mussels are small and easily transported in a plastic bag, jar, or bucket. They can stay alive out of the water for several days in cool, humid conditions by simply closing their shell tight. Under the right environmental conditions, it would take as few as three zebra mussels to begin an "invasion" in a body of water.[34]

The congressman voted for the ban on Internet gaming. Recently, zebra mussels have been appearing in local lakes in the congressman's state. The immediate issue: Is the presence of the newly discovered zebra mussels in the congressman's state a product of the threat?

[33] See nas.er.usgs.gov/queries/FactSheet.asp?speciesID=5.

[34] Personal Correspondence, Nonindigenous Aquatic Species Program biologist, U.S. Geological Survey, Gainesville, Florida.

Criminal Intelligence

Zebra mussels are explicitly included in the United States Code (42 USC §42 and §43–the Lacey Act). Mere transportation of zebra mussels is a federal misdemeanor. If an individual intentionally causes damage or loss of property as a result of the introduction of zebra mussels, or conspires to do so, this can be the federal crime "Animal Enterprise Terrorism," punishable as a felony, depending on the value of property loss.

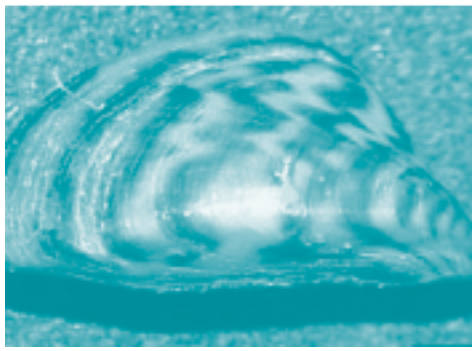
Other possible federal and state crimes include extortion, terroristic threat, and criminal environmental law violations.

Homeland Security Intelligence

A determination should be made of hazards posed to the community and economy by this threat. Are threats posed to other bodies of water as a result of this act? What preventive/protection measures should local critical infrastructure or key resources vulnerable from this threat take? Intelligence requirements need to identify persons with zebra mussels in their possession and determine the reason. Businesses and government entities whose operations could be affected by the zebra mussels must be identified and notified.

Case Intelligence Requirements

- What information is available about the individual who made the threat?
  - Has the congressman received threats in the past? If so, collect all related information.
  - Are there vocal activists against the ban on Internet gaming who could be reasonably tied to the congressman and/or the state?
  - Are there any links between these individuals and environmental issues?
- How can zebra mussels be introduced into a new environment?
  - What do zebra mussels look like?
  - What are the different methods/processes that might be used for introduction?
  - What are the indicators of zebra mussels being introduced?
- What evidence is needed to prove:
  - The zebra mussels were intentionally introduced?
  - There was intent to cause damage or a loss of property?
- What damage was caused by the zebra mussels?
  - What is the evidence that supports this?



Standing Intelligence Requirements

- If someone is identified with zebra mussels in his or her possession:
  - Identify the individuals and the reasons for their possession of the zebra mussels.
  - Document precautions taken to avoid introduction of the zebra mussels to the local environment?
  - Document any evidence to support the elements of applicable state and/or federal laws?
    - What additional evidence may be needed?

Homeland Security Intelligence Requirements

- Is there a need for the fusion center to forecast their spread and impact or can this be handled more effectively by another agency?
  - If so, which agency?
  - Is there a memorandum of understanding in place to work with this agency?
- What are the characteristics of the new host environment that would help target places where the zebra mussels may be introduced and flourish?
- Do any of the identified host environments have characteristics that increase the seriousness of the invasion (for example, public water supply, hydroelectric plant, manufacturing, commercial, or recreational body of water)?

Chapter 3:

A Brief History of Law Enforcement Intelligence: Past Practice and Recommendations for Change

A Brief History of Law Enforcement Intelligence: Past Practice and Recommendations for Change

Controversies have surrounded law enforcement intelligence because of past instances where the police maintained records of citizens' activities that were viewed as controversial, not traditional, suspicious, or perceived as anti-American, even though no crimes were being committed. This, of course, violates fundamental constitutional guarantees and offends the American sense of fairness concerning government intrusiveness. Unfortunately, the boundary is not precise about the types of information the police can collect and retain. Some legal guidelines lack clarity and the application of law to factual situations is often difficult. Beyond the legal ramifications, law enforcement's early intelligence initiatives often lacked explicit focus and typically maintained a shroud of secrecy. We can learn important lessons from these historical experiences that provide context and guidance for law enforcement intelligence today.

Aggravating these factors was an unclear relationship between law enforcement intelligence and national security intelligence that has changed continuously since the mid-20th century. The changes have been both politically and legally controversial as these initiatives sought to respond to changing sociopolitical events in American history, most recently through post-9/11 counterterrorism efforts. As a result, there is value in understanding selected portions of history from both types of intelligence to gain context and understand the lessons learned.

Law Enforcement Intelligence: The Years of Evolution

Early law enforcement intelligence units going back to the 1920s used a records process known as the "dossier system." Essentially, intelligence files were nothing more than dossiers—files containing a collection of diverse raw information—about people who were thought to be criminals, thought to be involved with criminals, or persons who were thought to be a threat to the safety and order of a community. Bootleggers during prohibition and many of the high-profile criminals of the early twentieth century—for example, Bonnie and Clyde, the Barker Gang, Machine Gun Kelly, Al Capone—were the typical kinds of persons about whom police agencies kept dossiers.

During the depression of the 1930s, little was done in the law enforcement intelligence arena. Other priorities were higher: the pervasive threat to the country was the economy, not criminality. Circumstances began to change in the latter part of the decade as communism —or the "Red Scare"—became predominant. The police relied on the only system they knew: the dossier.

In 1937, U.S. Representative Martin Dies (D-Texas) became the first chairman of the House Committee on Un-American Activities. Dies, a supporter of the Ku Klux Klan, fueled the fire of concern about communism in the United States, including labeling people as Communists who appeared "un-American," which often resulted in their loss of jobs and functional displacement from society. Concern

about communism was pervasive, but was of secondary interest in the 1940s because of World War II. After the war, when the Soviet Union was formed and built its nuclear arsenal, the Red Scare reemerged with even greater vigor.

The fires were fanned significantly in 1950 by Senator Joseph McCarthy (R-Wisconsin) who was using this national concern as the foundation for his floundering reelection bid to the Senate. McCarthy railed against the American Communist Party and called for expulsion from government, education, and the entertainment industry anyone who was an avowed Communist or Communist sympathizer. Because of fear about the Soviet Union among the American public, the war on communism resonated well.

Responding to expressions of public and government concern, local law enforcement agencies began creating intelligence dossiers, known as "Red Files," on persons who were suspected Communists and Communist sympathizers. Law enforcement agencies, therefore, were keeping records about people who were expressing their political beliefs and people who were known to sympathize with these individuals. The fact that these people were exercising their constitutional rights and had not committed crimes was not considered an issue because it was felt that the presence of, and support for, communism within the nation was a threat to the national security of the United States.[1]

The dossier system had become an accepted tool for law enforcement intelligence; therefore, when new overarching challenges emerged, it was natural for law enforcement to rely on this well-established mechanism for collecting and keeping information. In the 1960s, law enforcement met two challenges where intelligence dossiers appeared to be an important tool: the Civil Rights movement and the anti-Vietnam War movement. In both cases, participants appeared to be on the fringe of mainstream society. They were vocal in their views and both their exhortations and actions appeared to many as being "un-American." This was aggravated by other social trends: World War II baby boomers were in their teens and 20s, exploring their own newly defined world of "sex, drugs, and rock n' roll" and contributing to the stereotype of the "long-haired, dope-smoking, commie-hippie spies"—a sure target for a law enforcement traffic stop.

An overlap among these social movements was viewed by many as conspiratorial. Moreover, rapidly changing values, stratified in large part along generational and racial lines, created a sense of instability that appeared threatening to the mainstream. Rather than being culturally unstable, as we have learned in hindsight, it was simply social evolution. Because of the dissonance in the 1960s and the largely unsupported assumption that many of the activists and protestors "might" commit crimes or "might" be threats to our national security, law enforcement agencies began developing dossiers on these individuals "just in case." Typically, dossier information was not related to specific crimes, rather, it was kept as a contingency should the information be needed in some future investigation. There is little doubt that law enforcement was creating and keeping these dossiers with good faith to protect the community from activities then viewed as threats; however, that faith does not mitigate unconstitutional practices.

[1] It was rationalized that such activities were warranted on the grounds of a "compelling state interest." This argument, however, did not meet political or constitutional scrutiny.

There was additional concern during this time because of the activist nature of the U.S. Supreme Court during the era of Chief Justice Earl Warren (1953–1969). Many of the "liberal decisions" of the Warren Court were met with disfavor and the often-expressed belief that the Court's decisions[2] were "handcuffing the police." With regard to the current discussion, perhaps most important was that the Warren Court led a generation of judicial activism and expanded interpretations of the Constitution. Moreover, it symbolically motivated activist attorneys from the 1960s to try new strategies for the protection of constitutional rights. Among the most successful was reliance on a little-used provision of the Civil Rights Act of 1871, codified as Title 42 of the U.S. Code, Section 1983–Civil Action for Deprivation of Rights.

Commonly referred to as "1983 suits," this provision essentially provides that anyone who, acting under color of state or local law, causes a person to be deprived of rights guaranteed by the U.S. Constitution or federal law may be civilly liable. The initial lawsuits focused on whether a city, police department, and officers could be sued for depriving a person of his or her constitutional rights. The Supreme Court held that they could. A significant aspect of the case was that the police could be sued if there was "misuse of power possessed by virtue of state law and made possible only because the wrongdoer is clothed with the authority of state law."[3] This opened the floodgates for lawsuits against law enforcement (and correctional institutions).

Initial lawsuits focused on various patterns of police misconduct such as excessive force and due process violations. The reach of lawsuits against law enforcement grew more broadly with decisions holding that the police chain of command could be held vicariously liable for the actions of those under their command, as well as their parent jurisdiction. Moving into the late 1960s and early 1970s, such lawsuits moved toward law enforcement intelligence units. It was increasingly discovered that law enforcement agencies were keeping intelligence files on people for whom there was no evidence of criminality. The practice of keeping intelligence dossiers on a contingency basis was found to be improper, serving no compelling state interest and depriving those citizens of their constitutional rights. As a result, the courts repeatedly ordered intelligence files to be purged from police records and in many cases police agencies had to pay damage awards to plaintiffs. The decisions also permitted citizens to gain access to their own records. Many activists publicized their intelligence files as a badge of honor, often to the embarrassment of the police.[4] Law enforcement intelligence operations were cut back significantly or eliminated as a result of the embarrassment and costs associated with these lost lawsuits. The lessons learned from this era suggest caution in the development of intelligence records—information must be collected, retained, reviewed, and disseminated in a manner that is consistent with legal and ethical standards.

This lesson is reinforced by the findings of the United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities[5] —the Church Committee, named after its chairman, Frank Church (D–Idaho)[6]—which held extensive hearings on domestic intelligence, most notably

[2] Among the most often cited are *Miranda* v. *Arizona* (police must advise arrestees of their Fifth and Sixth Amendment rights prior to a custodial interrogation); *Mapp* v. *Ohio* (applying the Exclusionary Rule to the states); *Gideon* v. *Wainwright* (right to appointed counsel); and *Escobedo* v. *Illinois* (right to counsel when the process shifts from investigatory to accusatory).

[3] *Monroe* v. *Pape* 365 U.S. 167 (1961).

[4] For example, it was not uncommon to find notations and even photographs of an "intelligence target" having dinner or attending a public event such as a movie or the theater. The citizen would then pose a rhetorical question, "Is this how you want your tax dollars spent?"

[5] United States Senate, Select Committee to Study Governmental Operations with Respect to Intelligence Activities. *Intelligence Activities and the Rights of Americans, Book II, Final Report*. Washington, D.C.: Library of Congress, 1976.

[6] Alternately known as the Church Commission.

the Federal Bureau of Investigation's (FBI) Counter Intelligence Program, which spanned the years 1959 to 1971. The committee's conclusion:

> Domestic intelligence activity has threatened and undermined the Constitutional rights of Americans to free speech, association and privacy. It has done so primarily because the Constitutional system for checking abuse of power has not been applied.

Concern was widespread about all aspects of intelligence. The combined effect of these diverse factors prompted the U.S. Department of Justice (DOJ) to develop guidelines for the management of criminal intelligence records that were maintained by state and local law enforcement agencies.

Codified as 28 CFR Part 23[7]—Criminal Intelligence Systems Operating Policies,[8] the regulation governs interjurisdictional and multijurisdictional criminal intelligence systems that are operated by or on behalf of state and local law enforcement agencies and that are funded with federal funds. The regulation, created in 1979, stemmed from an amendment to the Omnibus Crime Control and Safe Streets Act of 1968.

The Justice System Improvement Act of 1979 created significant changes in DOJ organizations and stimulated regulatory changes, including creation of this regulation by the DOJ Office of Legal Policy. The regulation arose out of concern about aggressive information collection and intelligence activities by state and local law enforcement agencies that frequently involved collecting and retaining information about citizens who were expressing unpopular beliefs but whose actions were not criminal.

Since the federal government cannot mandate policy to state and local governments, the only method by which such policy could be leveraged was to make the policy implementation a condition for the acceptance of federal funds. The regulation provides guidelines on the collection, retention, review, dissemination, and purging of criminal intelligence records. Essentially, the regulation requires that, before information that identifies an individual or an organization may be retained in the criminal intelligence records system of a state or local law enforcement agency, there must be sufficient evidence to establish a reasonable suspicion that the individual [or organization] is involved in criminal behavior. When the regulation was created, many viewed this as a significant barrier to effective intelligence operations. Hindsight, however, has proven that the regulation is an important tool for maintaining citizens' civil rights without placing an undue burden on intelligence activities.

Congressional Inquiries into Intelligence Activities

During this era, inquiries into the Intelligence Community (IC) moved away from assessing the efficiency of intelligence operations and toward assessing the legality and propriety of the actual operations conducted. As will be seen, the recommendations made by three congressional committees would result in major changes in both the jurisdiction and roles of IC members with respect to law enforcement and national security intelligence. This would lead to the separation

[7] Code of Federal Regulations.

[8] www.iir.com/28cfr

of the two types of intelligence activities—the so-called "wall between domestic and international intelligence."

In 1975, the Rockefeller Commission (Commission on CIA Activities within the United States) recommended limiting the Central Intelligence Agency's (CIA) authority to conduct domestic intelligence operations. Furthermore, the commission also recommended that the director of central intelligence and the director of the FBI set jurisdictional guidelines for their respective agencies. In 1976, the House Select Committee on Intelligence (the Pike Committee, chaired by Otis Pike, D–New York) also made recommendations to further limit the jurisdictional overlap between agencies responsible for national security intelligence and agencies primarily responsible for law enforcement intelligence. It was the recommendations of the Church Committee, however, that were the most profound in developing the wall of separation.

The Church Committee, an inquiry formed by the U.S. Senate in 1976, examined the conduct of the IC in a broader fashion than did the Rockefeller Commission.[9] The recommendations made by this inquiry led to jurisdictional reformations of the IC. Most of the recommendations were directed at developing new operational boundaries for the FBI and the CIA. Out of the committee's 183 recommendations, the following illustrate how law enforcement intelligence was separated from national security intelligence:[10]

- The committee recommended that agencies such as the National Security Agency, the CIA, and military branches not have the power to conduct domestic intelligence operations (that is, law enforcement intelligence functions). Specific attention was given to the role of the CIA, noting that "the CIA should be prohibited from conducting domestic security activities within the United States."[11]
- The committee recommended that the FBI have "sole responsibility" for conducting domestic intelligence investigations of Americans.
- The FBI should "look to the CIA as the overseas operational arm of the intelligence community."[12]
- All agencies should ensure against improper intelligence activities.

The recommendations of the Church Committee have been widely recognized as a primary reason for the separation of law enforcement intelligence from national security intelligence. The call for this separation, however, did not mean that the agencies should stop working with each other. In fact, the Church Committee also recommended that the FBI and the CIA continue sharing information and make a better effort to coordinate their initiatives. This was operationally complicated: How do the two agencies work together and coordinate initiatives when there are substantial limitations on the kinds of information that can be collected and shared? Moreover, what, if any, role did state, local, and tribal law enforcement (SLTLE) intelligence have in this arrangement? The result was increased compartmentalization both between the agencies and within each agency.[13] Recommendations to improve law enforcement intelligence, however, have not been limited to the federal level. Such recommendations have also been made for state and local law enforcement agencies.

[9] Johnson, L. *A Season of Inquiry: The Senate Intelligence Investigation.* Lexington, Kentucky: The University Press of Kentucky, 1985.

[10] For a complete review of the recommendations made by the Church Committee visit the Public Library tab on www.aarclibrary.org and click on "Church Committee Reports". For a more complete review of the formation of the Church Committee, see note 14.

[11] United States Senate Select Committee to Study Governmental Operations with Respect to Intelligence Activities. *Intelligence Activities and the Rights of Americans, Book II, Final Report.* April 26, 1976. Washington, D.C.: U.S. Government Printing Office, 1976.

[12] Ibid

[13] For example, because of the regulations—or at least the interpretation of the regulations—FBI agents working within the former Foreign Counter Intelligence Division were often barred from sharing information with agents working on criminal investigations.

National Crime Commissions and New Initiatives Influencing the Evolution of State, Local, and Tribal Law Enforcement Intelligence

Since 1931, 15 national crime commissions have examined a wide array of crime issues in the United States, ranging from street crime and drug trafficking to organized crime and terrorism. Most have included assessments and recommendations related to some aspect of law enforcement intelligence. Understanding the broad intent of the commissions, followed by those with specific intelligence recommendations, demonstrates a well-established legacy for establishing law enforcement intelligence operations that are objective, analytic, and respectful of privacy and civil rights. While the recommendations reflect forward thinking, not all recommendations were embraced immediately—largely because they represented a change in the police occupational culture of the era. Nonetheless, important concepts were established that served as the foundation for today's law enforcement intelligence practices.

The Commissions and their Purpose

The National Commission on Law Observance and Enforcement (known as the Wickersham Commission) issued a series of reports and memoranda from 1928 to 1931 examining all aspects of serious crime in the United States. The intent was to address the growth of organized crime (particularly that arising from Prohibition) and increases in violent crime that appeared to correlate with growing industrialization and urbanization. The Commission also sought to understand the failure of law enforcement, the courts, and corrections to manage America's crime problem effectively. For the next 3 decades there were no major national commissions examining crime, in large part, no doubt, because of Americans' preoccupation with the Great Depression, followed by World War II, and post-World War II concerns about the growing nuclear threat from the Soviet Union. Indeed, these global events were largely responsible for virtually none of the Wickersham Commission's recommendations being implemented.

In November 1963, the assassination of President John F. Kennedy prompted President Lyndon B. Johnson to create what came to be known as the Warren Commission (U.S. Supreme Court Chief Justice Earl Warren). While the Commission's goal was to determine the circumstances leading to the assassination, the less controversial results of the Commission examined the relationships among federal, state, and local law enforcement, their communications, and generally their ability to work together for a common purpose: protecting the President of the United States. Unbeknownst at the time, the assassination was a harbinger of a violent and paradigm-changing decade to come.

As the 1960s progressed, increased concern about crime was emerging because of the growth of violence, the increase in drug use, the greater awareness of organized crime, and concerns about inequities in the administration of justice, particularly as related to minorities. To address these concerns, in 1965 President Johnson created the President's Commission on Law Enforcement and

Administration of Justice, an inquiry that complemented President Johnson's domestic social agenda known as "The Great Society." The President's Commission investigated all aspects of the criminal justice system, as well as specific inquiries into narcotics and organized crime, in a series of task force reports that were released 1967.

Recognizing that the 1960s was the "decade of social revolution" on many fronts, there were concerns about problems ranging from violence, riots in our cities, increases in the use of narcotics, a growth of illegal dangerous drugs, to concerns about moral decay, often illustrated by the increasing presence of pornographic materials. In 1967, a series of violent demonstrations in cities throughout the U.S. spurred by the Civil Rights Movement led to the creation of the National Advisory Commission on Civil Disorders (known as the Kerner Commission, chaired by Governor Otto Kerner of Illinois) as an attempt to understand the dynamics of civil disobedience and civil disorders as well as to evaluate the government's response. The following year, 1968, saw the creation of two additional commissions: The National Commission on the Causes and Prevention of Violence and the U.S. Commission on Obscenity and Pornography.

The social upheaval of the 1960s was characterized by many factors, including a significant rise in the abuse of illegal drugs, as learned in earlier commission reports. As a result, a new inquiry was created specifically to examine this issue more closely; the U.S. Commission on Marihuana and Drug Abuse (1970).

One of the signature components of the 1967 President's Commission was the attempt to professionalize all aspects of the criminal justice system. Following this lead was the Justice Department's National Advisory Commission on Criminal Justice Standards and Goals (1973) as well as a series of reports from working groups of that commission known as the *National Advisory Committee on Criminal Justice Standards and Goals* (1976).

National inquiries, seeking to identify causes of various crimes as well as providing blue-ribbon advice on the best tactics, recommended strategies and programs to deal with crime. These included the Justice Department's National Advisory Committee for Juvenile Justice and Delinquency Prevention (1980); the Attorney General's Task Force on Violent Crime (1981); the President's Commission on Organized Crime (1983); and the Attorney General's Commission on Pornography (1986).

Throughout the 1990s there were no national commissions on crime issues as had been so prevalent in the previous 3 decades. There was, however, a significant increase in government-sponsored research and program development on a wide array of crime-related issues from the National Institute of Justice, the Bureau of Justice Assistance, the Bureau of Justice Statistics, the Office of Juvenile Justice and Delinquency Prevention; and the newest Justice Department agency, created in 1994, the Office of Community Oriented Policing Services (the COPS Office). In many ways, the products of these agencies were a surrogate for the national commissions.

Table 3-1: National Crime Commissions in the U.S., 1931–2004

- National Commission on Law Observance and Enforcement (Wickersham Commission), 1931.
- President's Commission on the Assassination of President Kennedy (Warren Commission), 1964
- President's Commission on Law Enforcement and Administration of Justice, 1967
- National Advisory Commission on Civil Disorders (Kerner Commission), 1967
- National Commission on the Causes and Prevention of Violence, 1968
- U.S. Commission on Obscenity and Pornography, 1968
- U.S. Commission on Marihuana and Drug Abuse, 1970
- National Advisory Commission on Criminal Justice Standards and Goals, 1973
- National Advisory Committee on Criminal Justice Standards and Goals, 1976
- National Advisory Committee for Juvenile Justice and Delinquency Prevention, 1980
- Attorney General's Task Force on Violent Crime, 1981
- President's Commission on Organized Crime, 1983
- Attorney General's Commission on Pornography, 1986
- Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission), 1999
- National Commission on Terrorist Attacks Upon the United States (9/11 Commission), 2004

In the late 1990s, there was a growing concern about terrorism, particularly after attacks on the U.S. military and the U.S. embassy bombings in Africa, as well as a general increase in terrorist attacks throughout the Middle East. As a result, the U.S. Congress mandated a 5-year annual inquiry into the susceptibility of the U.S. to attacks using weapons of mass destruction (WMD). The Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (known as the Gilmore Commission, chaired by former Virginia Governor James Gilmore) issued its first report in 1999.

In 2004, the latest significant commission, the National Commission on Terrorist Attacks Upon the United States (9/11 Commission), issued its report. It had implications for the criminal justice system but addressed much wider issues. They are discussed later in this chapter.

The National Crime Commissions and Law Enforcement Intelligence

Not all of these commissions addressed the issue of intelligence directly; however, all called for increased use of diverse analytic techniques to not only understand crime and criminal justice but also to aid in forecasting crime for purposes of prevention—a fundamental construct of the intelligence process.

The Wickersham Commission observed there was a need to study and understand the crime environment (that is, analysis) as an important tool for capturing criminal offenders. Thirty-three years later, one of the earliest explicit recommendations for intelligence and information sharing between federal

agencies and state and local law enforcement came from the 1964 President's Commission on the Assassination of President Kennedy (the Warren Commission). While the majority of the Commission's recommendations were directed at federal agencies, notably the Secret Service and the FBI, it also recommended that these agencies work more closely with local law enforcement. Specifically, the Commission called for increased information sharing and stronger liaison between local and federal agencies.[14]

The 1967 reports of the President's Commission on Law Enforcement and Administration of Justice emphasized many of the same factors, but provided significantly more research, more detail, and explicit recommendations. Moreover, the year following the release of the President's Commission reports, Congress passed landmark legislation—the Omnibus Crime Control and Safe Streets Act of 1968—which, among other things, provided funding for implementing many of the Commission's recommendations. Within the intelligence arena, the President's Commission recommended:

> Police departments in every major city should have a special intelligence unit solely to ferret out organized criminal activity and to collect information regarding the possible entry of criminal cartels into the area's criminal operations.[15]

Interestingly, the President's Commission noted that "criteria for evaluating the effectiveness of the [intelligence] units, other than mere numbers of arrests, must be developed".[16] That debate remains. The President's Commission went on to recommend that the "…Department of Justice should give financial assistance to encourage the development of efficient systems for regional intelligence gathering, collection, and dissemination."[17] This would become a reality roughly a decade later when the Regional Information Sharing System (RISS) and its six regional intelligence centers were created by the Justice Department.[18]

While the intelligence focus of the President's Commission was largely on organized crime and to a lesser extent on narcotics control, the Kerner Commission's focus was on civil disobedience and violent civil disorders. With respect to the riots and civil disorders experienced by America's cities, the Kerner Commission made this observation:

> No particular control tactic was successful in every situation. The varied effectiveness of control techniques emphasizes the need for advance training, planning, adequate intelligence systems, and knowledge of the [inner city].[19]

Further, the Kerner Commission recommended that law enforcement agencies should do the following:

> Establish an intelligence system to provide police and other public officials with reliable information that may help to prevent the outbreak of a disorder and to institute effective control measures in the event a riot erupts.[20]

The National Commission on the Causes and Prevention of Violence made similar observations:

[14] The Warren Commission Report. *Report of the President's Commission on the Assassination of President John F.* Kennedy. New York: Barnes and Noble, Inc., 2003. [Originally published in 1964].

[15] President's Commission on Law Enforcement and Administration of Justice. *Task Force Report: Organized Crime.* Washington, D.C.: U.S. Government Printing Office, 1967, p. 20.

[16] Ibid.

[17] Ibid., p. 22.

[18] See www.riss.net.

[19] National Advisory Commission on Civil Disorders. *Summary Report.* Washington, D.C.: U.S. Government Printing Office, 1968, p. 6

[20] Ibid., p. 16.

> A major weakness of many police departments is the absence of a reliable intelligence system. The absence has gravely handicapped police and public officials in anticipating and preventing trouble, and in minimizing and controlling a disorder that has broken out. In large part, this happens because of a failure to learn about and to understand neighborhood problems and grievances and to develop reliable information concerning community organizations and leaders. Related to this problem is the need for a reliable mechanism to monitor, to collect, and to evaluate rumors and also the need for an effective program to counter false and provocative rumors which can aggravate tension and incite violence.[21]

The recognition that intelligence could be a valuable tool for forecasting threats and dealing with complex criminality was growing slowly as a wide range of systemic crime-related social problems were examined by these national inquiries. Intelligence was being viewed more broadly as evidenced by the most comprehensive recommendation yet from the National Advisory Commission on Criminal Justice Standards and Goals. The National Advisory Commission developed a standard expressly for intelligence operations—ironically, it is Standard 9.11—that states, in part:

> Every police agency and every state immediately should establish and maintain the capability to gather and evaluate information and to disseminate intelligence in a manner which protects every individual's right to privacy while it curtails organized crime and public disorder.[22]

The standard is remarkably similar to a recommendation from the *National Criminal Intelligence Sharing Plan* that was released 31 years later. Interestingly, the standard notes that "information" is collected and "intelligence" is disseminated. This reference to analysis had not been articulated clearly in the previous commission reports. Moreover, the attention to individual privacy that was included in the standard is also an important ingredient that is critical to all law enforcement intelligence activities today.

Furthermore, included in the National Advisory Commission's report were recommendations directed at the structure and operations of the intelligence functions for state and local law enforcement agencies. These recommendations included the following:

Establishing Intelligence Functions

- Each state should develop a centralized law enforcement intelligence function with the participation of each police agency within the state.[23]
- States should consider establishing regional intelligence networks across contiguous states to enhance criminal information-sharing processes.[24]
- Every local law enforcement agency should establish its own intelligence function in accordance with its respective state's intelligence function.[25]

Intelligence Function Operations

- Each state and local intelligence function should provide support to federal agencies.

[21] National Commission on the Causes and Prevention of Violence. *Law and Order Reconsidered.* Washington, D.C.: U.S. Government Printing Office, 1968, p. 312

[22] National Advisory Commission on Criminal Justice Standards and Goals. *Police.* Washington, D.C.: U.S. Government Printing Office, 1973, p. 250.

[23] Ibid

[24] National Advisory Committee on Criminal Justice Standards and Goals. *Organized Crime–Report of the Task Force on Organized Crime.* Washington D.C.: U.S. Department of Justice, Law Enforcement Assistance Administration, 1976.

[25] Ibid

- Operational policies and procedures should be developed for each local, state, and regional intelligence function to ensure efficiency and effectiveness.[26]
- Each agency should have a designated official who reports directly to the chief and oversees all intelligence operations.
- Each agency should develop procedures to ensure the proper screening, securing, and disseminating of intelligence-related information.[27]

In 1976, the concept and operating policies for intelligence were expanded even further by the National Advisory Committee on Criminal Justice Standards and Goals. The Committee's publication, *Organized Crime–Task Force Report on Organized Crime* has a chapter on intelligence that provides more detail than that provided by any previous commission or inquiry. Beyond recommendations for the creation of an intelligence unit, the standards include recommendations for maintaining privacy, the use of the "need-to-know" and "right-to-know" standards for dissemination, standards for purging intelligence records, and the need to maintain individual and organizational accountability in the intelligence function.[28] While the recommendations focus on organized crime, including drug trafficking, compared to the "all crimes, all hazards" approach used by law enforcement in the post-9/11 environment, many of the 1976 standards and discussions of intelligence are consistent with today's vision of good practice in law enforcement intelligence.

Created in 1983, the President's Commission on Organized Crime was a comprehensive examination of all aspects of organized crime, ranging from "traditional" organization crime (that is, the Mafia, La Cosa Nostra) to drug trafficking cartels, sophisticated money laundering operations, and entrepreneurial crime of all types and commodities. The intent was to provide a comprehensive insight into organized crime, its structure, its effects, and how best to control it. It recognized that effective intelligence analysis was a critical tool to enable law enforcement to deal successfully with multijurisdictional complex criminality.[29]

By the mid-1980s, criminal enterprises had grown dramatically and encompassed a diverse array of illegal activities, from drug trafficking to counterfeiting consumer commodities. Investigators and intelligence units had neither the expertise nor the personnel to contain the problem effectively. This was aggravated by a failure of law enforcement to generally understand the nature of organized crime and by poor information sharing among law enforcement agencies at all strata of government.[30] Organized crime was characterized as a "rapidly changing subculture" that was outpacing the capability of law enforcement to control it. Increasingly, organized crime was viewed largely as a federal responsibility that would be supported by state and local law enforcement through information sharing and participation on task forces.

Similar to the issues of organized crime, the Attorney General's Commission on Pornography (1986) recognized that intelligence operations would be a useful tool for stopping interstate traffic in obscene and pornographic materials. However, state and local law enforcement tended to view this as a low priority and not a good investment of time and resources.

[26] Ibid

[27] National Advisory Committee on Criminal Justice Standards and Goals. *Disorders and Terrorism: Report of the Task Force on Disorders and Terrorism.* Washington, D.C.: U.S. Department of Justice, Law Enforcement Assistance Administration, 1976.

[28] National Advisory Committee on Criminal Justice Standards and Goals. *Organized Crime–Report of the Task Force on Organized Crime.* Washington, D.C.: U.S. Government Printing Office, 1976, pp. 121–135.

[29] President's Commission on Organized Crime. *Organized Crime and Money Laundering.* Washington, D.C.: U.S. Government Printing Office, 1984.

[30] President's Commission on Organized Crime. *Final Report.* Washington, D.C.: U.S. Government Printing Office, 1987.

In the 1990s, following an increased number of terrorist attacks in the Middle East and particularly after the bombings of U.S. embassies in Dar es Salaam, Tanzania, and Nairobi, Kenya, questions began to emerge about the United States mainland as a terrorist target and the ability of the U.S. to effectively forecast, manage, and respond to an attack "at home"—particularly an attack involving WMD. As a result, in 1999 the U.S. Congress mandated the creation of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (the Gilmore Commission). The annual reports, issued between 1999 and 2003, went beyond WMD and explored terrorism more broadly—particularly after 9/11—and what the U.S. Government needed to do to effectively protect the homeland. In addition to recommending more robust intelligence and information sharing, the Gilmore Commission urged policymakers to move beyond simply reacting to the September 11 terrorist attacks and develop forward-thinking efforts by government at the federal, state, and local levels, and by the private sector as well. In its 2002 report, the Gilmore Commission stated the following:

> Intelligence—its timely collection, thoughtful analysis, and appropriate dissemination—is the key to effective prevention of terrorist attacks. From the inception of our deliberations, we have said that "more can and must be done to provide timely information—up, down, and laterally, at all levels of government—to those who need the information to provide effective deterrence, interdiction, protection, or response to potential threats."

While improvements have been made, that statement is still true today.[31]

That message was reinforced, particularly with regard to information sharing, in a staff report from the National Commission on Terrorist Attacks Upon the United States (the 9/11 Commission). One issue of concern was the effectiveness of information sharing by the FBI with state and local law enforcement. The commission's staff report stated, in part, the following:

> We heard complaints that the FBI still needs to share much more operational, case-related information. The NYPD's Deputy Commissioner for Counterterrorism, Michael Sheehan, speculated that one of the reasons for deficiencies in this information sharing may be that the FBI does not always recognize what information might be important to others. … Los Angeles Police Department officials complained to us that they receive watered-down reports from the FBI. … We have been told that the FBI plans to move toward a "write to release" approach that would allow for more immediate and broader dissemination of intelligence on an unclassified basis.[32]

These issues are being addressed through the *National Criminal Intelligence Sharing Plan* (NCISP) and, more specifically through the development of law enforcement intelligence "requirements" by the FBI. Moreover, former FBI Executive Assistant Director for Intelligence Maureen Baginski specifically stated in remarks at the 2004 COPS Office National Community Policing Conference that the initiatives of the FBI Office of Intelligence included a revised report-writing style that would facilitate information sharing immediately, including sharing with intelligence customers who did not have security clearances.[33]

[31] Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction. *Implementing the National Strategy.* Washington, D.C.: RAND Corporation, 2002, p.30.

[32] National Commission on Terrorist Attacks Upon the United States (2004). *Staff Statement No. 12: Reforming Law Enforcement, Counterterrorism, and Intelligence Collection in the United States, 2004,* p. 8. www.9-11commission.gov/staff_statements/staff_statement_12.pdf.

[33] Baginski, Maureen. Remarks in a keynote address at "Community Policing for America's Future: National Community Policing Conference," Office of Community Oriented Policing Services, Washington, D.C.: June 22, 2004.

Interestingly, the 9/11 Commission's staff report on reformation of the intelligence function included many of the issues and observations identified in previous commission reports during the previous 40 years. The difference, however, is that substantive change is actually occurring, largely spawned by the tragedy of September 11, 2001.

The 9/11 Commission Report issued a wide range of recommendations related to intelligence. Cooperative relationships, the integration of intelligence functions, and a general reengineering of the intelligence community were at the heart of their recommendations. In commentary, the Commission noted the role of state, local, and tribal law enforcement agencies:

> There is a growing role for state and local law enforcement agencies. They need more training and work with federal agencies so that they can cooperate more effectively with those authorities in identifying terrorist suspects.[34]

The 9/11 Commission went on to recognize the following:

> The FBI is just a small fraction of the national law enforcement community in the United States, a community comprised mainly of state and local agencies. The network designed for sharing information, and the work of the FBI through local Joint Terrorism Task Forces, should build a reciprocal relationship in which state and local agents understand what information they are looking for and, in return, receive some of the information being developed about what is happening, or may happen, in their communities.[35]

The 9/11 Commission also recommended creation of a new domestic intelligence entity that would need to establish "…relationships with state and local law enforcement…"[36] In proposing a new National Counterterrorism Center (NCTC), the Commission stated that the Center should "… [reach] out to knowledgeable officials in state and local agencies throughout the United States."[37] Implicit in the Commission's recommendations is that terrorism is a local event that requires critical involvement of state and local government in prevention and response.[38]

The inquiries into crime and justice from the Wickersham Commission through the 9/11 Commission have the same themes: Attack the root causes of crime; understand all aspects of the crime dynamic; attack crime from a holistic approach; work with and share information between agencies; move beyond traditional approaches; and protect the privacy and civil rights of individuals. Whether the crime is strong-armed robberies or terrorism, these principles run true. Certainly, the practice of law enforcement intelligence has listened to and learned from these lessons in a frenzy of change during the post-9/11 era.

Law Enforcement Intelligence Initiatives in the Post-9/11 Environment

Several important initiatives have been spurred by the terrorist attacks of September 11, 2001 that have had a significant and fast effect on the evolution of law enforcement intelligence. The more significant developments occurring during this time are listed in Table 3-2.

[34] National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report.* Washington, D.C.: U.S. Government Printing Office, 2004, p. 390. www.9-11commission.gov/report/911Report.pdf.

[35] Ibid., p. 427.

[36] Ibid., p. 424.

[37] Ibid., p. 404.

[38] Ibid.

In October 2001, about 6 weeks after the 9/11 attacks, the International Association of Chiefs of Police (IACP) held its annual meeting in Toronto, Ontario, Canada. There, the Police Investigative Operations Committee discussed the need for SLTLE agencies to reengineer their intelligence function as well as the need for national leadership to establish standards and direction for SLTLE agencies. From this meeting, the IACP, with funding support from the COPS Office, held the Intelligence Summit in March 2002. The summit developed a series of recommendations, a criminal intelligence sharing plan, and adopted *Intelligence-Led Policing*.[39]

The Global Justice Information Sharing Initiative (Global), a group funded by the U.S. Office of Justice Programs, was already in existence with the charge of developing processes and standards to efficaciously share information across the criminal justice system. In response to the IACP Intelligence Summit of 2002, Global created a new subgroup, the Global Intelligence Working Group (GIWG). The purpose of the GIWG was to move forward with the summit's recommendations. The first GIWG product was the *National Criminal Intelligence Sharing Plan*.

Table 3-2: Significant Post-9/11 Law Enforcement Intelligence Initiatives

- COPS/IACP Intelligence Summit, 2002
- Global Intelligence Working Group (GIWG)
- Counter-Terrorism Training Coordination Working Group (CTTWG)
- *National Criminal Intelligence Sharing Plan* (NCISP)
- Criminal Intelligence Coordinating Council (CICC)
- Minimum Criminal Intelligence Training Standards
- Fusion Center Guidelines
- Department of Homeland Security (DHS) Target Capabilities List (TCL)
- Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA)
  - Creation of the Office of the Director of National Intelligence (ODNI) and appointment of the Assistant Deputy Director of National Intelligence (ADDNI) for Homeland Security and Law Enforcement
  - Creation of the Directorate of Intelligence (DI) at the FBI
  - Creation of the National Counterterrorism Center (NCTC)
  - Creation of the Information Sharing Environment (ISE)
- Creation of the Interagency Threat Assessment and Coordination Group (ITACG)
- National Strategy for Information Sharing (NSIS)
- Second COPS/IACP Intelligence Summit

Formally announced at a national signing event in the Great Hall of the U.S. Department of Justice on May 14, 2004, the *National Criminal Intelligence Sharing Plan* (NCISP) signified an element of intelligence dissemination that is important for all law enforcement officials. With formal endorsements from the DOJ, DHS, and the FBI, the NCISP provided an important foundation on which state, local,

[39] International Association of Chiefs of Police. *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels.* Alexandria, Virginia: International Association of Chiefs of Police, 2002.

and tribal law enforcement agencies could create their intelligence initiatives. The intent of the plan was to provide SLTLE agencies (particularly those that do not have established intelligence functions) with the necessary tools and resources to develop, gather, access, receive, and share intelligence.

The NCISP[40] established a series of national standards that have been formally recognized by the professional law enforcement community as the role and processes for law enforcement intelligence today. The plan is having a significant effect on organizational realignment, information-sharing philosophy, and training in America's law enforcement agencies.

The NCISP also recognized the importance of local, state, and tribal law enforcement agencies as a key ingredient in the nation's intelligence process and called for the creation of the Criminal Intelligence Coordinating Council (CICC) to establish the linkage needed to improve intelligence and information sharing among all levels of government. Composed of members from law enforcement agencies at all levels of government, the CICC was formally established in May 2004 to provide advice in connection with the implementation and refinement of the NCISP. Members of the CICC serve as advocates for local law enforcement and support their efforts to develop and share criminal intelligence for the purpose of promoting public safety and securing our nation. Because of the critical role that SLTLE play in homeland security, they must have a voice in the development of policies and systems that facilitate information and intelligence sharing. The CICC serves as the voice for all levels of law enforcement agencies by advising the U.S. Attorney General and the Secretary of Homeland Security on the best use of criminal intelligence as well as the capabilities and limitations of SLTLE agencies related to information sharing.[41]

During the same period that these initiatives were occurring, many states and regions somewhat independently were developing multijurisdictional intelligence capabilities intended to maximize the diverse raw information input for analysis and examine potential acts of terrorism that may occur within regions. The units, called "fusion centers," were embraced by the DHS, which began providing funding to enable some of the centers to operate. The concept of "intelligence fusion" caught on rapidly as an efficient and effective mechanism for developing intelligence products. With recognition that other crimes, such as financial crime and weapons offenses, may have a nexus with terrorism, the centers' foci broadened to "all crimes." Moreover, with the broad mission of the DHS, which was increasingly providing substantial amounts of funding, the fusion centers' focus broadened further to encompass "all crimes, all hazards, all threats."

Recognizing the benefits of standardization to enhance the quality of work being done by the fusion centers, the GIWG created the *Fusion Center Guidelines*[42] for developing a series of recommendations and good practices for law enforcement agencies that are participating in the intelligence fusion process. While primarily focusing on criminal intelligence, the *Guidelines* also give attention to the law enforcement information-sharing relationship with the private sector, as well as public safety issues related to homeland security intelligence. The fusion process

[40] it.ojp.gov/documents/NCISP_Plan.pdf

[41] www.iir.com/global/council.htm

[42] it.ojp.gov/topic.jsp?topic_id=209

seeks to have as many law enforcement agencies as possible as information-sharing partners. Analytic outputs will be more robust as law enforcement participation increases because there will be a wider array of diverse information being entered into the analytic process. The recommendation from the NCISP and the second COPS/IACP Intelligence Summit that all agencies, regardless of size, should develop an intelligence capacity is clearly an important ingredient for increased agency participation with fusion centers.

At virtually the same time, the DHS was developing plans to meet its mission, mandated in Homeland Security Presidential Directive-8 "…to prevent, respond to, and recover from threatened and actual domestic terrorist attacks, major disasters, and other emergencies…".[43] A critical part of this initiative was to define critical knowledge, skills, abilities, and processes (that is, "capabilities") that were necessary for law enforcement and emergency services personnel to perform these tasks. These capabilities have been articulated in detail in the *Target Capabilities List*[44] (TCL). Intended to protect the nation from all hazards, "…the TCL is a national-level, generic model of operationally ready capabilities defining all-hazards preparedness."[45] The list is broken down into different "areas" associated with prevention and response. The "Prevent Mission Area" has two specific intelligence-related target capabilities: "Information Gathering and Recognition of Indicators and Warnings" and "Intelligence Analysis and Production." The "information gathering" capability is focused on "…the continual gathering of only pure, unexamined data…" that can be used in the intelligence process to identify threats and indicators of threats. This is the type of information that is essential for effective analysis and is the currency that fusion centers rely on law enforcement agencies to submit to the fusion process, typically through tips, leads, suspicious activity reports, and observation of terrorism or criminal indicators.

> The "intelligence analysis" target capability involves "…the merging of data and information for the purpose of analyzing, linking, and disseminating timely and actionable intelligence with an emphasis on the larger public safety and homeland security threat picture. This process focuses on the consolidation of analytical products among the intelligence analysis units at the Federal, State, local, and tribal levels for tactical, operational, and strategic use. This capability also includes the examination of raw data to identify threat pictures, recognize potentially harmful patterns, or connect suspicious links to discern potential indications or warnings."[46]

The discussion of both of these target capabilities in the *Target Capabilities List* refers to both the *NCISP* and *Fusion Center Guidelines* as standards and processes to accomplish the capabilities. The integration of these initiatives strives to create a culture of information sharing that inextricably includes state, local, and tribal law enforcement.

Building on these initiatives—and on other new programs and activities in the Intelligence Community as well as recommendations from the 9/11 Commission—Congress passed the Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). Among the many important aspects of this legislation are four particularly

[43] For more information on the National Preparedness Goal, Homeland Security Presidential Directive-8 and the *Target Capabilities List*, see the Fact Sheet at www.llis.dhs.gov/docdetails/details.do?contentID=14468. (must register to access)

[44] Available online at www.llis.dhs.gov/docdetails/details.do?contentID=26724.

[45] U.S. Department of Homeland Security. *Target Capabilities List. A Companion to the National Preparedness Guidelines.* Washington, D.C.: U.S. Department of Homeland Security, 2007, p. 1.

[46] Ibid., p. 91.

important factors that are significant for the current discussion: creation of the Office of the Director of National Intelligence (ODNI), creation of a Directorate of Intelligence (DI) in the FBI, creation of the National Counterterrorism Center (NCTC), and mandating the creation of the Information Sharing Environment.

The first factor of the IRTPA provisions related to SLTLE was creation of the ODNI. The Director of National Intelligence (DNI) serves as the head of the Intelligence Community and as a principal advisor to the President on issues related to national security. One of the unprecedented aspects of this office is the formal recognition that SLTLE has a role in both national security and homeland security. The staff of the ODNI includes an Assistant Deputy Director of National Intelligence (ADDNI) for Homeland Security and Law Enforcement. While the role and functions of this position are still evolving, essentially the ADDNI is responsible for policy issues related to information sharing between the Intelligence Community and SLTLE. Moreover, the ADDNI advises the Intelligence Community on law enforcement capabilities, operations, and restrictions related to national security.

The second factor was creation of the FBI Directorate of Intelligence (DI) to manage all FBI intelligence activities.[47] The DI is organized as part of the FBI's National Security Branch and is embedded in all investigative domains—counterterrorism, counterintelligence, WMD, cyber, and criminal inquiries.[48] A key responsibility of the DI is identifying threats and sharing threat information with SLTLE agencies and the Intelligence Community. The DI's goal is to be a "full and trusted partner who can be relied on to proactively bring FBI resources to the table to help resolve threats."[49] The IRTPA mandate firmly established and expanded the DI's authority over the management of the FBI's intelligence functions, including oversight of field intelligence operations and coordination of human source development and management.

The third factor was the creation of the National Counterterrorism Center (NCTC). The NCTC serves as the primary organization for integrating and analyzing all intelligence pertaining to terrorism with the exception of purely domestic terrorism. The NCTC also serves as the central knowledge bank on terrorism information and provides all-source intelligence support to government-wide counterterrorism activities. Its mission is essentially to "get the right counterterrorism information into the right hands of the right people" in DHS, the FBI, the Intelligence Community and, indirectly, SLTLE. The NCTC seeks to bring intelligence from across the federal government into one place to integrate and analyze it then disseminate the integrated intelligence to customers.[50]

The final IRTPA factor of concern to SLTLE is creation of the Information Sharing Environment (ISE). The IRTPA required the President to establish an ISE "for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties." It also required designation of a program manager for the ISE who is charged with planning and overseeing the ISE's implementation and management.

[47] Rather than create a new domestic intelligence agency, as recommended by the 9/11 Commission, the legislation increased the intelligence authority and responsibilities of the FBI.

[48] www.fbi.gov/intelligence/intell.htm

[49] Statement by FBI Assistant Director Wayne Murphy, Directorate of Intelligence, at the 2007 IACP Intelligence Summit, Washington, D.C., November 27, 2007.

[50] www.nctc.gov/nic

The Information Sharing Environment Implementation Plan[51] is designed to increase the sharing of terrorism information among and between the 16-member Intelligence Community, law enforcement agencies at all levels of government, and the private sector as well as foreign partners. The ISE seeks to "…implement an effective, widespread culture of information sharing, balanced with a need for security and the protection of privacy and civil liberties…"[52] The Implementation Plan provides a detailed process and action steps that indicate significant expectations for state, local, and tribal law enforcement to be participants in the ISE. *The Implementation Plan* further stipulates that each state must identify a primary state fusion center that will be the information-sharing nexus between the federal ISE and SLTLE agencies.[53]

As is evident from the above initiatives, information sharing has become the fundamental principle for intelligence processes to protect the United States. Despite new programs, legislation, and regulations, information sharing across governmental levels was still problematic. In an attempt to remedy this, key decision-makers and representatives of all levels of the ISE were to meet on a consistent basis and resolve information-sharing problems as members of the new Interagency Threat Assessment and Coordination Group[54] (ITACG) within the NCTC. ITACG members include the DHS, the FBI, members of the Intelligence Community, and state and local law enforcement representatives. A key role of the ITACG is to support the efforts of NCTC to produce "federally coordinated" terrorism-related information products intended for dissemination to state, local, and tribal officials and private-sector partners.

ITACG members, particularly at the state and local levels, help define the intelligence products needed by each type of consumer. Because each level of government has different priorities, ITACG members provide advice, counsel, and subject matter expertise to the Intelligence Community regarding the operations of SLTLE agencies, including how such entities use terrorism-related information to fulfill both their counterterrorism responsibilities and their core mission of protecting their communities.

Beyond these responsibilities, a key role of the ITACG is to coordinate the production and timely dissemination of specific intelligence products to SLTLE officials. The intelligence products include the following:

- Alerts, warnings, and notifications of time-sensitive terrorism threats to locations within the United States
- Situational awareness reporting regarding significant events or activities occurring at the international, national, state, or local levels
- Strategic assessments of terrorist risks and threats to the United States.[55]

The ISE was evolving beyond a plan and moving into actual policy and processes. Taking the next step, in October 2007 the White House released the *National Strategy for Information Sharing* (NSIS).

> The Strategy will assist the Administration in ensuring that Federal, State, local, and tribal government employees responsible for protecting our Nation from future attacks or responding should an attack occur understand the

[51] www.ise.gov/docs/ise-impplan-200611.pdf

[52] Ibid. Program Manager's Office, p. 83.

[53] In November 2007 a letter, jointly signed by the U.S. Attorney General and Secretary of Homeland Security, was sent to each state governor concerning the designation of a primary fusion center. The letter stated, in part, "…Guideline 2 states that DOJ and DHS will work with governors or other senior state and local leaders to designate a single fusion center to serve as the statewide or regional hub to interface with the federal government and through which to coordinate the gathering, processing, analysis, and dissemination of terrorism, law enforcement, and homeland security information in an all-crimes approach. … it is imperative for your office to designate one fusion center to serve as the statewide hub. … In designating a single fusion center, please give consideration to developing an inclusive strategy that is consistent with the federal efforts to constitute the ISE."

[54] www.whitehouse.gov/nsc/infosharing/sectionIV.html

[55] Ibid.

> Administration's expectations and plans for achieving improvements in the gathering and sharing of information related to terrorism. [56]

The strategy goes on to note:

> The President's guidelines recognized that State, local, and tribal authorities are critical to our Nation's efforts to prevent future terrorist attacks … The informational needs of State, local, and tribal entities continue to grow as they incorporate counterterrorism and homeland security activities into their day-to-day missions. Specifically, they require access to timely, credible, and actionable information and intelligence about individuals and groups intending to carry out attacks within the United States, their organizations and their financing, potential targets, pre-attack indicators, and major events or circumstances that might influence State, local, and tribal preventive and protective postures.[57]

The role of state, local, and tribal law enforcement intelligence is undeniable.

In many ways, post-9/11 intelligence developments came full circle with the second IACP/COPS Intelligence Summit. While many important and substantive changes have been made in law enforcement intelligence, the *2008 Summit Report* observed the following:

> The participants in the follow-up IACP Criminal Intelligence Sharing Summit nevertheless made it clear that many of the nation's law enforcement agencies do not participate in the criminal intelligence sharing plan. Too many state, local, and tribal agencies, it would seem, underestimate their importance to the criminal intelligence sharing process, overestimate the burdens of full participation, and/or remain unaware of how to contribute to the vital work of the plan.[58]

Clearly, challenges remain.

Collateral Developments

A number of other activities were either already in place or were in development concurrently with the above initiatives. The distinction of these activities is that they have helped facilitate the goals and processes of the strategies described above.

Counter-Terrorism Training Coordination Working Group (CTTWG)[59]

The CTTWG was formed in 2002 to facilitate interagency coordination, information exchange, and sharing of innovative training initiatives among federal agencies involved in terrorism and antiterrorism training. The group was later expanded to include representation from the major law enforcement and law enforcement training organizations. Further expansion of the CTTWG included policy-level agency representatives from a broad range of federal agencies; law enforcement organizations involved in federal, state, local, and tribal law enforcement training; and academe. The CTTWG recognized that, increasingly, training issues and programs being brought before them were focusing on the discipline of

[56] *National Strategy for Information Sharing.* Washington, D.C.: Executive Office of the President, 2007, p. 1.

[57] Ibid., p. 17.

[58] International Association of Chiefs of Police. *National Summit of Intelligence.* Washington, D.C.: Office of Community Oriented Policing Services, U.S. Department of Justice, 2008, p. 2.

[59] www.counterterrorismtraining.gov.

intelligence. As a result, greater attention was focused on intelligence training and how to maximize the use of limited resources by ensuring that the intelligence training conveys a consistent, quality message; is not duplicative; is consistent with national standards; and meets the needs of law enforcement. Among the new intelligence initiatives was the creation of an online Law Enforcement Intelligence Master Training Calendar.[60] The group also assumed responsibility for preparing Version 2.0 of the Minimum Criminal Intelligence Training Standards.

Minimum Criminal Intelligence Training Standards[61]

Recognizing that the intelligence capacity of America's law enforcement community could not be realized without effective training, the CTTWG developed the *Minimum Criminal Intelligence Training Standards*. The standards identify six law enforcement focal areas— Chief Executive, Intelligence Commander/Manager, Intelligence Analyst, Criminal Intelligence Officer, General Law Enforcement Officer, and Train-the-Trainer— critical to successful intelligence activities. For each area, a group of experienced law enforcement intelligence professionals articulated learning objectives and identified key knowledge, skills, and abilities that are needed to execute intelligence responsibilities. With position-specific knowledge of the intelligence process increased within the law enforcement community, the willingness and ability to proactively contribute to the ISE increases significantly. Version 2.0 of the standards was approved in October 2007.

Global Justice Extensible Markup Language Data Model (GJXDM)

Because of the administrative independence among and between each component of the criminal justice system, many criminal justice information systems evolved in a manner that would not easily permit electronic information sharing. Frequently relying on proprietary data models from vendors, information often had to be exchanged in hard copy or be reentered. The Global Justice Information Sharing Initiative took on the task of developing a common data model that could serve as a standard used by all system components. The GJXDM is an Extensible Markup Language (XML) standard designed specifically for criminal justice information exchanges, providing law enforcement, public safety agencies, prosecutors, public defenders, and the judicial branch with a tool to share data and information effectively and in a timely manner.[62] There are three primary parts to GJXDM: the Data Dictionary (identifying content and meaning), the Data Model (defining structure and organization), and the Component Reuse Repository (a database). While the intent of the data model was to enhance criminal justice information sharing, the model has been embraced as a means of enhancing electronic sharing of criminal intelligence data. As a result, the GJXDM serves as an important technological component to support the ISE.

National Information Exchange Model[63] (NIEM)

A joint initiative of the DOJ and the DHS, NIEM embraced the GJXDM data model and built an information-sharing policy framework that met the mandates of the Homeland Security Act of 2002, the Intelligence Reform and Terrorism Prevention Act of 2004, and Homeland Security Presidential Directive 5 (HSPD-5).

[60] The Intelligence Master Training Calendar is available on the public side of the National Criminal Intelligence Resource Center web site: mastercalendar.ncirc.gov.

[61] The standards are available at: www.it.ojp.gov/documents/min_crim_intel_stand.pdf.

[62] it.ojp.gov/topic.jsp?topic_id=228

[63] See www.niem.gov.

> Rather than nationwide integration of all local, state, tribal, and federal databases, NIEM focuses on cross-domain information exchanges between key domains and communities of interest across all levels of government—whether between individual local law enforcement agencies, law enforcement and emergency service agencies, and other domains, or between local, state, tribal, regional, and federal agencies.[64]

The development of a common data standard and data-sharing model is clearly an important thread that permeates the culture of information sharing.

Grants for Training, Technical Assistance, and Technology

Various agencies and bureaus within both the DOJ and the DHS have been committed to providing grant support to further the intelligence mission. A wide variety of intelligence training programs have been supported, special activities to provide technical assistance, and assistance in purchasing technology and information systems— consistent with GJXDM and NIEM—have been critical to the development of the information-sharing culture. A factor that is particularly important to note is that many of the intelligence-related initiatives have been collaborative partnerships between the DOJ and the DHS. Beyond the support these initiatives have provided, this collaboration demonstrates information sharing in practice.[65]

Implications

The ISE *Implementation Plan* states that there is a need to "promote a culture of information sharing across the Information Sharing Environment." While a great deal of work and resocialization remains, a review of the initiatives discussed above demonstrates that significant strides have been made. While the ISE will face challenges to meet its ultimate goal, the changes that have been made in a comparatively short amount of time represent important milestones and are a significant leap forward.

Collectively, these initiatives have changed the philosophy of law enforcement intelligence that reflects the following:

- A commitment to information sharing both within and between law enforcement agencies
- The need to establish an objective, thoughtful intelligence function that has consistent national professional standards
- The recognition that state, local, and tribal law enforcement agencies have an important role in both homeland security and national security
- A process committed to preventing terrorism and multijurisdictional criminality
- A commitment to pursuing the intelligence function in a manner that is consistent with privacy and civil rights protection.

[64] *Introduction to the National Information Exchange Model.* Washington, D.C.: NIEM Program Management Office, February 12, 2007, p. 3.

[65] Sources to gather information about grants, training, and technical assistance from both the DOJ and the DHS include: www.counterterrorismtraining.gov, www.ncirc.gov, www.llis.dhs.gov, www.iir.com, and www.fema.gov/emergency/nims/compliance/grants.shtm.

Law Enforcement Intelligence at the State, Local, and Tribal Levels

Although the recommendations provided by the various national crime commissions were designed to strengthen law enforcement's capabilities to fight organized crime, by the mid-1980s, criminal enterprises had grown dramatically and encompassed such a diverse array of illegal activities, that the ability of SLTLE agencies to deal with these problems was limited. Investigators and intelligence units had neither the expertise nor the personnel to contain the problem effectively. This was aggravated by a failure of law enforcement to generally understand the nature of the problem and by poor information sharing among law enforcement agencies at all strata of government.[66] Organized crime was characterized as a "rapidly changing subculture" that was outpacing the capability of law enforcement to control it. As a result, law enforcement intelligence units were often relegated to being little more than an information clearinghouse or, in some cases, viewed as a failed initiative.[67]

Despite the lack of success, many within the law enforcement community still viewed the intelligence function as important to law enforcement agencies. A primary limitation of state and local intelligence units, however, was their inability to move beyond the collection of information to a systematic method of analyzing the collected data. The solution, then, was to have "the analytical function… guides the data collection [procedure]" rather than vice versa.[68]

Another limitation of law enforcement intelligence was that many law enforcement executives either did not recognize the value of intelligence and/or did not have the skills necessary to use intelligence products effectively. Furthermore, intelligence personnel did not possess the analytic (and often reporting) skills needed to produce meaningful intelligence products. The need for training was considered an important solution to this problem, and still is.

A historical issue was that intelligence units tended to be reactive in nature, often viewed as a repository of sensitive information rather than a proactive resource that could produce information critical for preventing crime and apprehending offenders. Similarly, intelligence units tended not to produce consistent, specifically defined products. Instead, intelligence reports tended to be written on an ad hoc basis to address critical matters.

A final limitation was that intelligence products were not disseminated in a timely or comprehensive manner. This, perhaps, was the greatest setback because the character of organized crime was constantly changing: different commodities were being trafficked, methods of operations tended to change, and participants in the operation of the enterprise changed. The need for timely and relevant information was seen as a necessary component for improving law enforcement intelligence operations.

While the majority of the past recommendations focused on the development and operations of intelligence units, recommendations have also been made regarding the ethical issues associated with state and local intelligence operations.

[66] President's Commission on Organized Crime. *Final Report.* Washington, D.C.: U.S. Government Printing Office, 1987.

[67] Martens, F., "The Intelligence Function," in *Major Issues in Organized Crime Control: Symposium Procedings, Washington, D.C.,* September 25–26, 1986. ed. Herbert Edelhertz, Washington, D.C.: U.S. Department of Justice, National Institute of Justice, Government Printing Office, 1987.

[68] Ibid.

Similar to the concerns that led to the formation of the Church Committee at the federal level, potential abuses of power was also a concern at the state and local levels. Accordingly, recommendations were made to ensure that citizens' civil rights remain intact.

For example, the *Law Enforcement Intelligence Unit File Guidelines*[69] were created to provide a practical policy and procedures that were intended to facilitate an effective intelligence process that was compliant with 28 CFR Part 23 and protected citizens' rights. Similarly, the Commission on Accreditation for Law Enforcement Agencies (CALEA) has recommended that every agency with an intelligence function establish procedures to ensure that data collection on intelligence information is "limited to criminal conduct that relates to activities that present a threat to the community" and to develop methods "for purging out-of-date or incorrect information."[70] In other words, the CALEA standard identified the need for law enforcement agencies to be held accountable for abuses of power associated with their intelligence activities. The latest revision of the CALEA intelligence standard embraces the *National Criminal Intelligence Sharing Plan* and its recommendations.

As will be seen later, the development of the Intelligence-Led Policing concept and the creation of the *National Criminal Intelligence Sharing Plan* have been important milestones in the evolution of law enforcement intelligence. By creating both an overarching intelligence philosophy and a standard for operations, state, local, and tribal law enforcement intelligence is becoming more professional. It is embracing more sophisticated tools, developing greater collaboration as one voice from the law enforcement intelligence community, and moving with a greater sense of urgency because of 9/11.

Conclusion

While we have evolved in our expertise and professionalism, many of the same issues remain. What are the lessons learned from history?

- Building dossiers full of raw, diverse information provides little insight—analysis is needed to give meaning to the information.
    - The improper collection of information can have a negative impact on our communities, including a chilling effect on the constitutional right of freedom of speech.
- To be effective, intelligence units must be proactive by developing unique products and disseminating the products to appropriate personnel on a consistent and comprehensive basis.
- A clear distinction is needed between law enforcement intelligence and national security intelligence. While some information can support the goals of both forms of intelligence, the competing methodologies and types of information that may be maintained in records mandates that the distinction remain clear and that overlap occurs only for clear purposes of public safety, including the apprehension of offenders and prevention of criminal and/or terrorists' acts.

[69] it.ojp.gov/process_links.jsp?link_id=3773

[70] Commission on Accreditation for Law Enforcement Agencies. *Standards for Law Enforcement Agencies*. 4th ed., 1998.

- Targeting people is unlawful without some evidence of a criminal predicate.
  - If the reason for the target is their support of an unpopular cause.
  - If they are being targeted because of their political beliefs, religion, race, ethnicity, or other attribute or characteristic (such as people who are perceived to be Muslim).
  - Targeting without lawful justification can result in civil rights suits and vicarious liability lawsuits, which can be both costly and embarrassing to the police department.
- The need to institute a privacy policy and civil rights protections are essential professional objectives.
- Monitoring an individual's behavior is proper if reasons can be articulated that reasonably support the notion that…
  - The person may be involved in criminality now or in the future.
  - There is a reasonable threat to public safety.
- Retaining information in intelligence files about an individual or an organization is improper if there is no reasonable suspicion of his or her criminal involvement, unless that information is used only as noncriminal identifying information and is labeled as such.
- A full-time law enforcement intelligence function should be organized professionally and staffed with personnel who are specifically trained in analysis and intelligence product preparation.
- There must be clear lines of communication between the intelligence unit and decision-makers.
- Law enforcement intelligence units must be evaluated regularly to ensure functional utility and operational propriety.
- Information sharing remains an important priority.

While past abuses of the intelligence function were no doubt done in a good faith effort to protect the community, nonetheless they were abuses. The changes that have occurred, particularly in the post-9/11 environment, and the professional development of the law enforcement intelligence function have demonstrated a respect for civil rights, a reliance on the scientific approach to problem solving, and a commitment to keeping America's communities safe.

Chapter 4:

The Intelligence Process (Cycle) for State, Local, and Tribal Law Enforcement

The Intelligence Process (Cycle) for State, Local, and Tribal Law Enforcement

Regardless of the type of intelligence, the single function that permeates all activities is the Intelligence Process (also known as the Intelligence Cycle). This process provides mechanisms to ensure the consistent management of information that will be used to create intelligence. This chapter is an overview of the Intelligence Process. Many of the issues introduced here will be discussed in detail in the remaining chapters of this *Guide*.

The Intelligence Process has been depicted in a variety of ways throughout the intelligence literature. The number of phases in the process may differ, depending on the model used, but the intent of each model of the Intelligence Process is the same:

> To have a systemic, scientific, and logical methodology to comprehensively process information to ensure that the most accurate, actionable intelligence is produced and disseminated to the people who provide an operational response to prevent a criminal threat from reaching fruition.

The process applies to all crimes, whether terrorism, drug trafficking, gangs, or any other criminal enterprise. Indeed, the process also helps identify circumstances where there is a nexus among these different types of crimes.

National Criminal Intelligence Sharing Plan: Training Recommendation for the Intelligence Process

Recommendation 18: Training should be provided to all levels of law enforcement personnel involved in the criminal Intelligence Process. The training standards, as contained within the *National Criminal Intelligence Sharing Plan*, shall be considered the minimum training standards for all affected personnel. Additionally, recipients of criminal intelligence training, as recommended in the *National Criminal Intelligence Sharing Plan*, should be recognized and awarded certificates for successful completion of training.

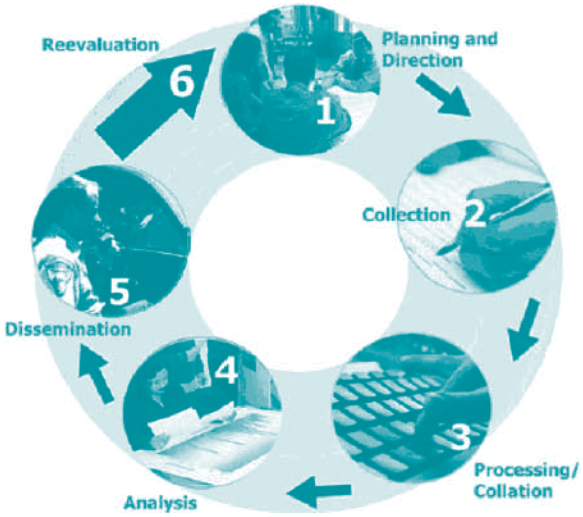
To be consistent with established national standards, the model used in this discussion is the one prescribed in the *National Criminal Intelligence Sharing Plan* (NCISP). While often depicted as "steps," in practice the different components of the process are phases, and there is a constant ebb and flow of information between phases as information is processed and shared. The Intelligence Process, therefore, is not a series of independent steps that are mechanically processed in an unbending sequential order; rather, they represent a recipe for intelligence and information sharing that will frequently change according to the availability of "ingredients" and the "nutritional needs" of the consumer.

The model of the Intelligence Process used in the NCISP (Figure 4-1) has six phases:

1. Planning and Direction.
2. Collection.
3. Processing/Collation.
4. Analysis.
5. Dissemination.
6. Reevaluation.

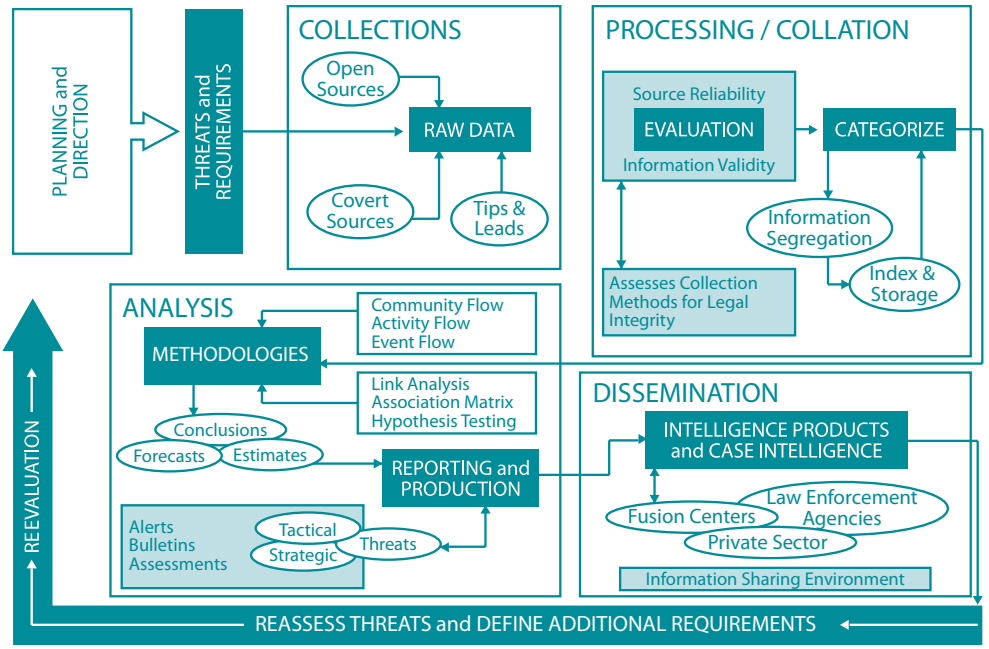
Each phase may be broken down into subprocesses (Figure 4-2) that collectively contribute to an effective information management and analysis system.

Figure 4-1: Intelligence Process, NCISP



In many ways, the Intelligence Process acts like a radar sweep across a community. The process seeks to identify potential threats, determine the status of suspicious activity, and provide indicators of criminality so that operational units can develop responses. An illustration of the ebb and flow of the Intelligence Process: An intelligence bulletin may describe certain indicators. An officer observes behaviors that are consistent with these indicators, collects further information that is processed through the cycle, thereby providing an analyst with more raw data to help refine the analysis. When a more refined analysis is once again disseminated back to operational units, the likelihood increases of providing more explicit intelligence that operational units may use to prevent a crime or a terrorist attack.

Figure 4-2: Intelligence Process and Subprocesses



As an illustration, an intelligence bulletin describes an emerging threat of Eastern European organized crime operating protection rackets in a major midwestern city. A police officer working neighborhoods with large populations of Russian immigrants has noticed an increase in thefts and property damage to small businesses largely operated by immigrants. In light of the intelligence bulletin, the officer provides information to the intelligence unit that crimes reported as simple thefts and property destruction within this area of the city may, in reality, be symptoms of "enforcer" activities of Eastern European organized crime protection schemes. The analyst corroborates the information with practices of the organized crime group in other cities and provides the additional information to officers in a revised bulletin. To be most effective, the Intelligence Process requires this ongoing two-way flow of information.

Planning and Direction

The intelligence function involves the coordination of many activities. Similar to intermeshed gears, there must be a plan for how each moving part will operate in concert with other elements and how the gears will collectively manage a change in the environment. The gears of the Intelligence Process are prioritized and synchronized in the first phase of the cycle: Planning and Direction.

Former FBI Executive Assistant Director for Intelligence Maureen Baginski often stated, "The absence of evidence is not the absence of a threat." As part of the Planning and Direction process, it is important to recognize not only the threats that have been identified, but also dynamic threats where evidence indicating their presence may appear serendipitously. A threat may emerge within a jurisdiction or region for a wide variety of reasons; therefore, personnel must be trained to be vigilant in looking for evidence of threats (that is, indicators). This, however, must be a pragmatic process.

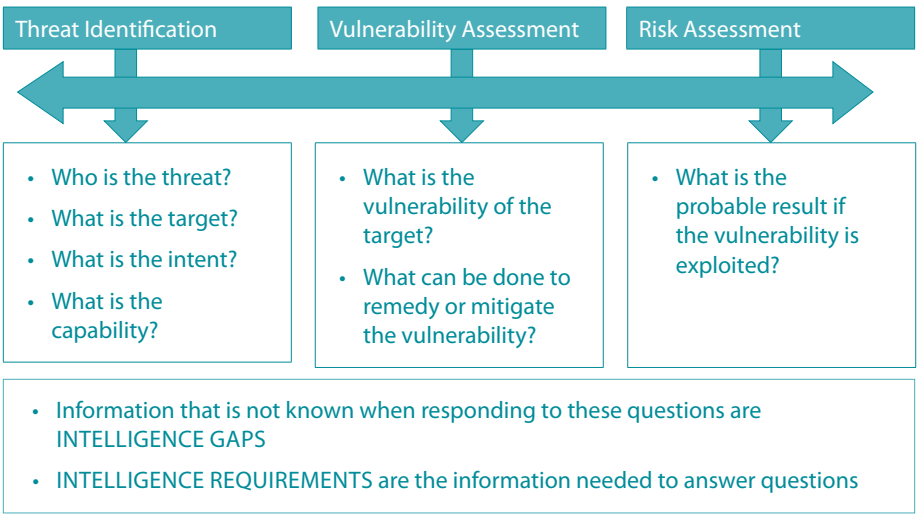
While a common perspective is that the Intelligence Process should take an "all-crimes/all-threats approach," pragmatically, these threats are not "equal" and must be prioritized considering the probability of their presence and the nature of the harm they pose to a community. This process is described in detail in Chapter 6. Threat prioritization is part of the "Direction" component of the first phase. This is done through ongoing threat assessments that are constantly refined by information that is processed through the Intelligence Cycle. A threat must be assessed on multiple criteria as illustrated in Figure 4-3.

The first threat component is threat identification. When evidence of a threat is identified, the Intelligence Process must assess where the threat lies on a multivariate continuum of probability. While quantifying a threat would add an element of precision, typically the variables related to a threat can be measured only on an ordinal scale:[1] for example, based on qualitative data a judgment can be made on the relative value of a threat variable on a scale of 1 to 10. As illustrated in Figure 4-4, the first two variables (A and B) measure the quality of the information. The second two variables (C and D) measure the probable outcome of the threat. Combined, they provide guidance for decision-making. A moderate assessment of the quality of information may produce a different operational

[1] An "ordinal scale" is a scale of measurement whereby data are put in a rank order, but where there is no fixed amount of difference between the points on the scale. For example, college sports rankings will rate the top 20 teams. The ranking, however, does not mean that the team ranked first is 20 times better than the 20th-ranked team.

response as the severity of the threat increases. As severity decreases, a higher quality of information may be desired before an operational response is made. This is basically a method to weigh risk/outcome tradeoffs.

Figure 4-3: Threat Assessment Components for Planning and Direction



The next step is a vulnerability assessment of probable targets. When a threat is identified, the universe of targets is typically narrowed. Regardless if the probable number of targets is large or small, some judgments can be made on how vulnerable the targets are. As vulnerability increases, so does the seriousness of the threat. As an example, assume that a small group of eco-terrorists plans on fire-bombing the sales inventory of various automobile dealers who sell large trucks. Most dealership sales lots are easily accessible 24 hours a day. As such, their vulnerability increases and so does the threat. In a different scenario, assume that the same group of eco-terrorists plans to fire-bomb tanks at a military installation to protest fuel consumption and damage done to the environment by the tanks traversing their training range. In this case, target vulnerability is low because of the inaccessibility to the tanks on the military base and the ability of the tanks to withstand Molotov cocktails should the intruders get near them. As should be apparent, target vulnerability is an important variable in any threat assessment.

Figure 4-4: Simplified Threat Assessment Illustration[2]

Making Threats										Posing Threats
	Low	----------								High
	1	2	3	4	5	6	7	8	9	10
Variable A	Reliability and Validity of Information on Threat									
	Low	----------								High
	1	2	3	4	5	6	7	8	9	10
Variable B	Weight of Evidence of Threat									
	Low	----------								High
	1	2	3	4	5	6	7	8	9	10
Variable C	Severity of Threat									
	Low	----------								High
	1	2	3	4	5	6	7	8	9	10
Variable D	Probability of Occurrence									

Once threats and target vulnerability have been identified, a risk assessment is made. Risk is epitomized by the question: "What is the probable result if the vulnerability is exploited?" In the above illustration, the risk to the automobile dealers may be high and the risk to the military installation may be low; however, before a conclusion may be drawn on risk, more information is needed to corroborate judgments and determine if there are other, previously undiscovered, compounding factors. This process helps define further intelligence requirements—information that needs to be collected to better understand the threat.

Essentially, the threat assessment process seeks to make a distinction on whether an intelligence target is "making a threat" or "posing a threat." This is obviously subjective; hence, as much information as practicable should be collected and analyzed on these three factors. In most instances, there will be insufficient information to make a meaningful assessment of each component of the threat assessment model. As a result, answers to the "requirements" questions will help clarify the threat picture. Obtaining additional information will increase the quality of intelligence by identifying and eliminating error.

It should also be recognized that previously undefined threats may also emerge. Changes in the character of a community may stimulate new threats, the presence of a particular target may draw a threat, or the threat simply may appear as a result of the combined effect of many factors. The point to note is that law enforcement personnel must be trained to identify behaviors that are more than merely suspicious, record the behaviors with as much detail as possible, and forward this information to the intelligence analysts.

The importance of the threat assessment model in Planning and Direction lies within the ability to maximize resources and operational initiatives for those crimes and circumstances which pose the greatest risk to public safety and

[2] This scale is not intended to be a threat assessment tool, but an illustration of the threat assessment concept in the discussion.

security. In many ways, the Intelligence Process looks for images through a lens that is out of focus. The two-way exchange of information helps focus the lens to understand if a threat is present and the degree of risk it poses. The Planning and Direction process constantly monitors changes in the environment and helps define changing priorities as well as new two-way information sharing needs.

Beyond resource issues, Planning and Direction requires the identification of threat priorities to focus awareness training for officers on how to recognize all threats. It also requires policy and procedural mechanisms to make the organization sufficiently nimble to respond effectively to the changing threat environment. Just like the Intelligence Process itself, the Planning and Direction phase is characterized by an ebb and flow of information that provides insight so that the evolving threat environment can be managed efficaciously.

Collection

Collection is the gathering of raw information that will be used by analysts to prepare intelligence reports and products. As a way to better envision the Collection phase of the process, law enforcement personnel typically will gather information in five basic forms:

1. A response to *intelligence requirements.*
2. A response to terrorism or criminal *indicators.*
3. *Suspicious Activity Reports* (SAR) of activities observed by or reported to officers.
4. *Leads* that officers develop during the investigation of unrelated cases.
5. *Tips* that may come from citizens, informants, or the private sector.

The response to *intelligence requirements* is information that is intentionally and specifically sought to answer certain questions. That information may be sought from open sources or may be a product of law enforcement methods, such as interviews, surveillance, undercover operations, or other law enforcement processes. A response to *indicators* would be law enforcement officers collecting information based on their observation of circumstances or behaviors they recognize because of information they gained from training and/or intelligence bulletins that describe such indicators. Typically, indicators will include the signs and symbols of criminal activity such as graffiti, the symbol of an extremist group on a wall or a car, or unusual activity at a location that is consistent with threat activity described in an intelligence report.

Typically, information collected from *SARs* is based on behavior observed by law enforcement officers who, relying on their training and experience, believe the individual may be involved in criminal activity, in the past or the future, although a specific criminal nexus is not identified. The term *leads* refers to information that officers develop about a probable emerging threat that is largely unrelated to the current investigation but comes to light during the inquiry. *Tips* reflect information that has been observed by citizens and submitted to a law enforcement agency for further inquiry.

Information Collection Disciplines Used by the Intelligence Community

In light of the Information Sharing Environment (ISE), there is a benefit to understanding some of the terminology used in the Intelligence Community (IC) even though it is generally not used by law enforcement intelligence. With regard to information collection, five general "collection platforms" or "collection disciplines" are used by the IC:

1. Human Intelligence (HUMINT) is the use of human beings to collect or confirm information through overt, covert, or clandestine methodologies.
2. Signals Intelligence (SIGINT) is an umbrella term for different methods of intercepting and exploiting electronic signals, whether intercepted on the ground, via aircraft, or by satellite. There are three forms of SIGINT:
   - Communications Intelligence (COMINT), which is the collection and exploitation of communications signals including any form of electronic voice communications, fax, wireless devices, and voice over Internet protocol (VOIP).
   - Electronic Intelligence (ELINT) is the interception of noncommunications transmissions such as radar, transponder, motion detectors, and so forth.
   - Foreign Instrumentation Signals (FISINT) is the interception and exploitation of performance and tracking data (usually telemetry) during tests of weapons systems and space vehicles.
3. Imagery Intelligence (IMINT) is derived from visual photography, infrared image capture, lasers, electro-optics, visual radar, and satellite imagery.
4. Measurement and Signatures Intelligence (MASINT) is the analysis of electronic emanations from equipment and seeks to detect information patterns in a different part of the electronic spectrum not previously captured by other methods.
5. Open Source Intelligence (OSINT) is the analysis of information available to the public without legal process or covert methods.

The collection process must seek to establish a criminal nexus with any person or organization that is identified in criminal intelligence records. This nexus is referred to as a *criminal predicate*. The standard for that criminal predicate is reasonable suspicion that is more than mere suspicion that the identified person is committing or is about to commit a crime. In practice, law enforcement agencies collect information on individuals where no criminal predicate exists. Examples are SARs, tips, and leads. This may appear to be a contradiction, but it is an inherent part of the Intelligence Process that has a remedy. The law enforcement agency has an obligation to determine if there is veracity to the criminal allegations found in SARs, leads, or tips. This is the purpose of the two-tiered "Temporary File" and "Permanent File" records system used for intelligence records. In practice, *retention* of collected information becomes the critical issue for demonstrating the criminal predicate.

The reader should note that care was taken to specify that the criminal predicate must be established when collecting and retaining information that *identifies people or organizations*. The critical point to note is that constitutional rights attach when identity is established.

The Intelligence Process will also seek to collect information about crime trends, methods of criminal operations, ideologies of extremists groups, and other nonidentifying information that helps describe and understand criminal

phenomena. The criminal predicate rule does not apply to these types of information because individuals are not identified.

A final issue of Collection—and the entire Intelligence Process—is operations security (OPSEC). OPSEC focuses on identifying and protecting information that might provide an intelligence target with clues to an inquiry, and thereby enable the target to thwart the inquiry.[3] To protect the integrity of the intelligence inquiry, it is essential to maintain the security of collection sources, methods, and content.

Processing/Collation

This phase of the Intelligence Process, Processing/Collation, has four distinct activities, as illustrated in Figure 4-5. The first is to evaluate raw data from the collection phase to determine its utility for analysis. An assessment should first examine the *reliability* of the source of the information. Ideally, the individual who was the primary collector should record a statement of reliability. The importance of this assessment relates to the confidence level an analyst will give the information when making judgments during the analysis. The conclusion drawn by an analyst when using information derived from a completely reliable source will be different from a source deemed unreliable.

The next assessment during evaluation examines the *validity* of the raw information. Validity is epitomized by the question: "Does the information actually portray what it seems to portray?" Validity assessment may be done by the collector and/or the analyst. The collector may believe that if information comes from a reliable source and it is logical, then validity is high. Conversely, the analyst may have competing information that questions the validity. In such cases, the analyst should define intelligence requirements to collect additional information in order to gain the most accurate raw information for a robust analysis. The Intelligence Cycle, therefore, starts over, even though this is only the third phase.

Source reliability and information validity are often initially assessed using the ordinal scales similar to those depicted in Figure 4-6. These rudimentary scales nonetheless provide important fundamental guidelines for intelligence assessments. As such, law enforcement personnel should be trained to provide these assessments when collecting information for the Intelligence Cycle.

A next form of evaluation is to assess the *method* by which the information was collected to ensure that it meets constitutional standards. Recommendation 6 of the NCISP states:

> All parties involved with implementing and promoting the *National Criminal Intelligence Sharing Plan* should take steps to ensure that the law enforcement community protects individuals' privacy and constitutional rights within the Intelligence Process.[4]

[3] See www.belvoir.army.mil/dptms/opsec.asp

[4] Global Intelligence Working Group. *National Criminal Intelligence Sharing Plan*. Washington, D.C.: Global Intelligence Working Group, 2003, p. 21.

Figure 4-5: Processing and Collation Activities

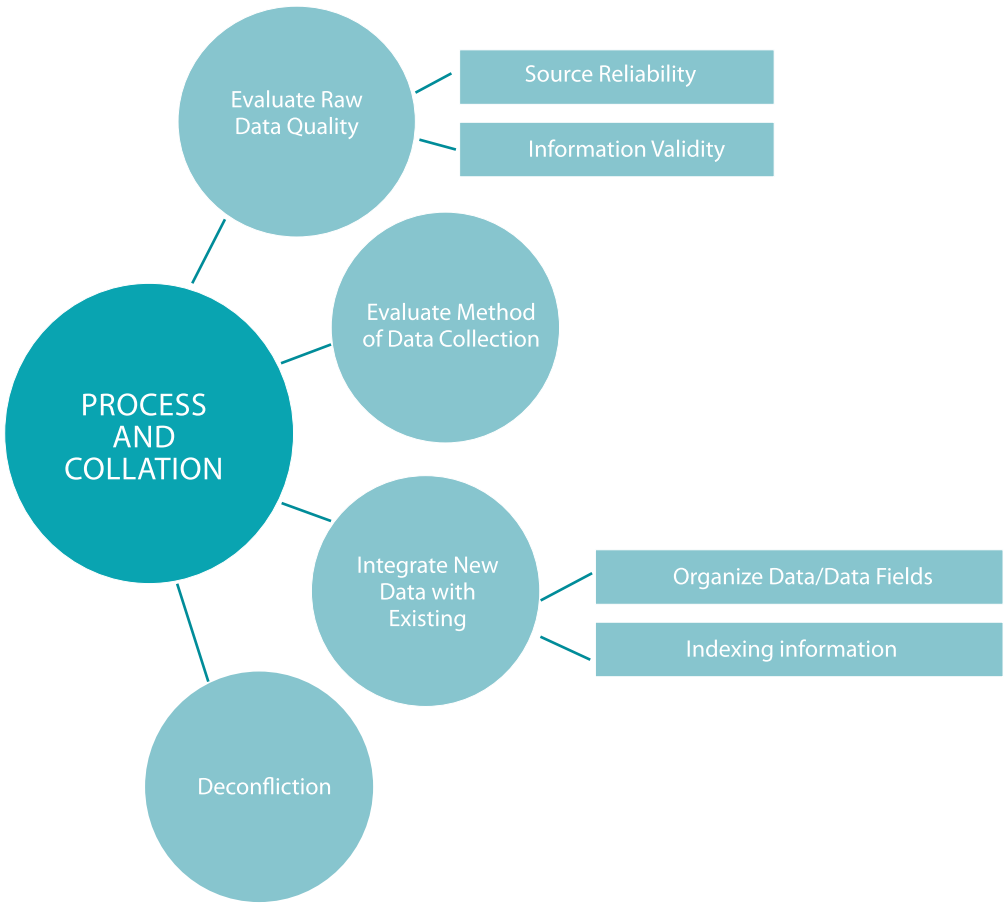
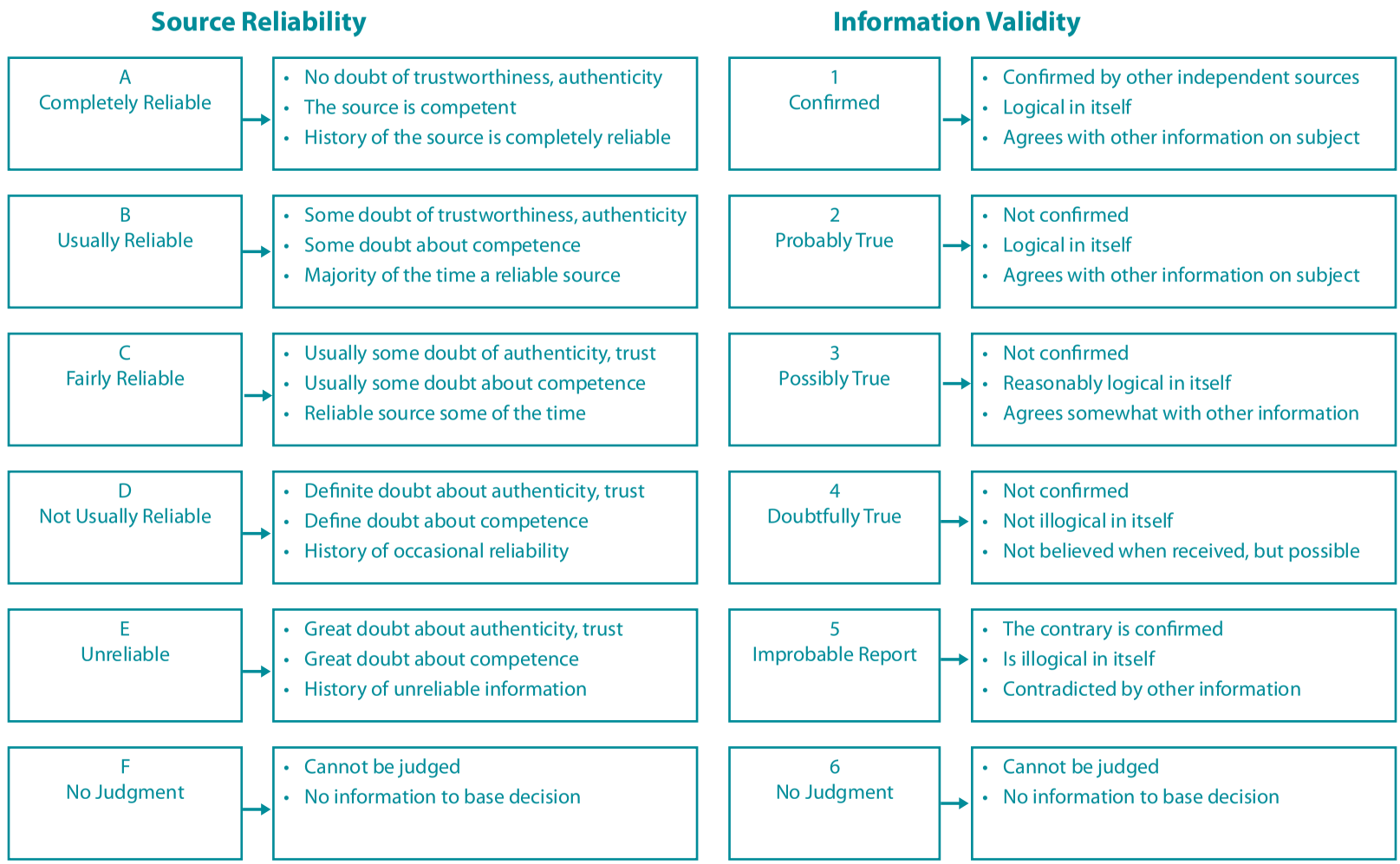


Figure 4-6: Example of Reliability and Validity Rating Scales



One of the first issues of information collection is the assessment of the *method* used to collect the data. When a law enforcement agency is collecting information, it must follow lawful processes; for example, information collected about a person should be consistent with constitutional standards (including the four exceptions[5] to the Fourth Amendment search warrant requirement). The issue of lawful collection methods is important for three reasons: First, it is a constitutional guarantee that law enforcement officers have sworn to uphold. Second, if there is a criminal prosecution of the intelligence target, critical evidence could be excluded from trial if the evidence was not collected in a lawful manner. Third, if a pattern emerges that information about individuals was collected on a consistent basis that does not meet constitutional standards, this may open the agency to civil liability for civil rights violations.

Not only is this assessment a professional obligation, it also is particularly important should the intelligence target be prosecuted. Once again, training should seek to ensure that the information was lawfully collected and the facts of the collection are carefully documented.

The third activity in the collation/processing phase is to integrate the new information with existing data. During this process, in consideration of all other information that has been collected, the following questions may be asked:

- Does it meet the criminal predicate test?
- Is the information relevant and material (as opposed to being just "interesting")?
- Does the information add new questions to the analysis?
- Does the information need corroboration?
- Does the information support the working hypotheses of the inquiry or does it suggest a new or alternative hypothesis?

The answers to these questions will help define requirements and directions for the inquiry. This process also includes organizing and indexing the data to standardize the data fields and enhance the ability to make accurate data comparisons.

A final activity during this phase is "deconfliction," the process or system used to determine whether multiple law enforcement agencies are conducting inquiries into the same person or crime. This is accomplished in several ways, including using deconfliction information systems such as the National Drug Pointer Index (NDPIX) managed by the Drug Enforcement Administration (DEA). The deconfliction process not only identifies if multiple inquiries exist, but a system like NDPIX also notifies each agency involved of the shared interest in the case and provides contact information. This is an information- and intelligence-sharing process that seeks to minimize conflicts between agencies and maximize the effectiveness of the inquiry.

In sum, the Processing/Collation phase of the Intelligence Cycle is important for two reasons: 1. It seeks to provide quality control of information through the process and 2. It provides important insights into defining intelligence requirements.

[5] These are: 1. Consent; 2. the Plain View Doctrine; 3. A search incidental to a lawful arrest; and 4. Exigent circumstance.

Analysis

Analysis is the heart of the Intelligence Process. Entire books have been written on analytic methodologies and the critical thinking process. The intent of the current discussion is not to repeat this information, but provide some insights into analytic responsibilities that will be of benefit to the intelligence consumer.

The analytic process is essentially the scientific approach to problem solving. It is the use of established research methodologies—both quantitative and qualitative—that seek to objectively integrate correlated variables in a body of raw data in order to derive an understanding of the phenomena under study. It is synergistic in nature; the completed analysis provides knowledge rather than a simple recitation of facts. The outcome, however, is only as good as 1. The quality of the raw information submitted for analysis and 2. The quality of the analysis. Effective training, policy direction, supervision, and an operational plan for the intelligence function are essential for the analytic process to produce robust and actionable intelligence.

The phrase "actionable intelligence" has two fundamental applications for law enforcement. The first is tactical, wherein the output of analysis must provide sufficient explicit information that operational units can develop some type of response. In some cases that response is minimal, such as providing indicators of terrorism or criminal activity for patrol officers to observe. In other cases, it may involve a complex operational activity to make arrests. The second application of actionable intelligence is strategic, describing changes in the threat picture of a jurisdiction or region; that is, the intelligence may describe changes in crime types, crime methodologies, or both.

The output of the analytic process is reports, referred to as *intelligence products*. During the course of the analysis, the intelligence analyst will prepare explicit inferences about the criminal enterprise in order to understand its effects. These are typically expressed in the form of *conclusions, forecasts,* and *estimates* that are explained in the products.

A *conclusion,* as the term infers, is a definitive statement about how a criminal enterprise operates, its key participants, and the criminal liability of each. A forecast[6] describes the expected implications of the criminal enterprise, the future of the enterprise, changes in the enterprise or its participants, and threats that are likely to emerge from the enterprise. An *estimate* focuses on monetary effects, changes in commodity transactions, and/or likely future effects of the criminal enterprise; for example, profits from a new criminal enterprise, economic losses associated with a terrorist attack, or the increase of contraband if new smuggling methods are used.

There are different consumers of intelligence, each of whom has somewhat different needs. Line officers need to have information that concisely identifies criminal indicators, suspects, addresses, crime methodologies, and vehicles thought to be associated with a criminal enterprise. Administrators and managers need information about the changing threat environment that has implications

[6] Sometimes the word "prediction" is used instead of forecast. Prediction is a definitive statement of the future that in reality is virtually impossible to determine. Intelligence analysis is probabilistic in nature; hence the term "forecast" is used to describe what is likely to occur in light of the currently known facts.

for the deployment of personnel and expenditure of resources. Analysts need a comprehensive package of information that includes raw data sources, methods, and intelligence requirements. Intelligence reports that contain little more than suppositions, assumptions, rumors, or alternative criminal scenarios are not "actionable."

Dissemination

An intelligence product has virtually no value unless the system is able to get the right information to the right people in a time frame that provides value to the report's content. Dissemination—or information sharing—seeks to accomplish this goal. Many issues could be discussed related to dissemination, including the various intelligence and information records systems, privacy issues, information system security issues, operations security of shared information, the means of dissemination, interoperability issues, and the *Global Justice Data Standards*.[7] However, the intent of the current discussion is to describe the general philosophy and rules of intelligence dissemination.

Pre-9/11, the general philosophy of intelligence dissemination tended to focus on "operations security;" that is, intelligence records were not widely disseminated out of the concern that critical information would fall into the wrong hands, thereby jeopardizing the inquiry as well as possibly jeopardizing undercover officers, informants, and collection methods. While these issues still remain important, the post-9/11 philosophy is radically different. Indeed, law enforcement seeks to place as much information in the hands of as many authorized people who need it to prevent threats from reaching fruition. Basically, the idea is that the more people who receive the information the greater the probability of identifying and interrupting a threat. Perhaps the critical question is, "Who is considered an authorized person?"

Right to know and need to know

Even with this changed philosophy, important rules of dissemination seek: 1. to protect individuals' civil rights and 2. maintain operations security as needed. To accomplish these goals, the first rules of dissemination provide criteria to determine who should receive the intelligence. The accepted standard has a two-pronged test:

1. Does the individual to which the information is to be disseminated have the *right to know* the information? This is determined by the recipient's official capacity and/or statutory authority to receive the information being sought.
2. Does the recipient have a bona fide *need to know* the information? The information to be disseminated is pertinent and necessary to the recipient in order to prevent or mitigate a threat or assist and support a criminal investigation.[8]

Intelligence products that provide information about criminal indicators and methodologies are intended to receive wide distribution so that officers are aware of these factors during the course of their daily activities. As a general rule, it can be assumed that anyone working in law enforcement meets the right-to-know and need-to-know tests for these types of intelligence. However,

[7] As a comprehensive resource, see it.ojp.gov.

[8] Adapted from: Law Enforcement Intelligence Unit. *Criminal Intelligence File Guidelines, Section IX: File Dissemination.* Sacramento, California: Law Enforcement Intelligence Unit, revised 2002.

intelligence reports related to a specific criminal inquiry that identifies individuals or organizations would have a significantly more limited dissemination. While all law enforcement officers would have the right to know this information, only those officers working on some aspect of the inquiry have the need to know the information.

With the changing intelligence philosophy and the recognized need to involve the private sector and nonlaw enforcement government personnel in the ISE, the application of *right to know* and *need to know* has changed somewhat from the pre-9/11 era.[9] For example, anyone in law enforcement has the *right to know* intelligence (by virtue of his or her employment). Similarly, a member of the National Guard or a Department of Homeland Security (DHS) intelligence analyst working in a state fusion center would also have the *right to know* intelligence by virtue of his or her assignment, even though he or she is not a law enforcement employee. In yet a different application, the corporate security director of a nuclear power plant would have the right to know intelligence that is related only specifically to the security director's responsibilities of protecting the plant.

Once again, because of the new intelligence philosophy a significantly broader range of law enforcement officers have the *need to know* intelligence. The rationale, as stated previously, is that all officers need to be aware of threats to increase the probability of stopping the threat. The need to know certain intelligence by nonlaw enforcement personnel should be determined on a case-by-case basis. For example, in all likelihood there is no need for a DHS analyst to know intelligence related to auto thefts; however, the DHS analyst would need to know the information related to a criminal enterprise smuggling cocaine from Colombia because of the value of communications between the DHS analyst and other federal agencies such as the DEA or Immigration and Customs Enforcement.

Third Agency Rule

Another information-sharing restriction is found in what is commonly called the Third Agency Rule. Essentially, if an officer receives intelligence from an intelligence source (such as a fusion center), that officer cannot disseminate the intelligence to a third party without permission from the original source. As an example, Officer Adam receives intelligence from the Central Fusion Center. Officer Adam cannot give the intelligence directly to Officer Baker without first gaining permission from the Central Fusion Center. This is a general rule—with some exceptions that will be discussed later—and it will be stated or applied differently between agencies. Consumers of intelligence need to be aware of the local applications of the Third Agency Rule.

There are two types of intelligence: case intelligence and intelligence products. Case intelligence identifies people; intelligence products provide general information about threats and indicators. For case intelligence, it should be assumed that the Third Agency Rule is intact, while for intelligence products, it may be assumed that the Third Agency Rule is waived. Fundamentally, the reason is that when individuals or organizations are not identified in intelligence products, civil rights do not attach. Again, a review of agency policy will determine the exact applications of the rule locally.

[9] A review of the goals and action steps in the *Information Sharing Environment Implementation Plan* clearly demonstrates the mandate for these additional intelligence consumers. See www.ise.gov/docs/ise-impplan-200611.pdf.

It should be reinforced that in law enforcement intelligence, both the right-to-know and need-to-know provisions as well as the Third Agency Rule, serve two purposes: 1. To protect individuals' civil rights and 2. To maintain operations security of intelligence inquiries.

Classified Information[10]

A great deal of detailed information has been written about classified information. For the most part, these regulations apply to the intelligence community and federal law enforcement. As a rule, unless working in a fusion center or assigned to a Joint Terrorism Task Force, most state, local, and tribal law enforcement (SLTLE) officers will not have security clearances or access to classified information; however, having a basic understanding of information classification provides perspective for the following discussion. Essentially, classified information is a designation of information that is critical to the security of the United States. Explicit processes and procedures for classifying, storing, providing access, and generally handling this information have sanctions, including federal criminal violations, if the processes are violated.

There has been a great deal of debate about the need for security clearances for SLTLE personnel. Law enforcement executives and managers argue that they need a security clearance to have access to information about threats within their jurisdiction. On this same theme, a report from the Congressional Research Service stated the following:

> … these officials might need some access to classified information, for example, "real time" intelligence information concerning terrorism threats, to adequately plan, coordinate, and execute homeland security activities.[11]

Federal authorities respond that they will provide all information needed to SLTLE personnel about threats within a community—a response met with some skepticism.[12]

Another issue to be aware of is that federal security clearances are not universal; for example, if a law enforcement executive has a security clearance from the Department of Defense as a result of his or her military reserve status or if an officer has a DEA clearance that was investigated by the U.S. Office of Personnel Management as part of a Organized Crime Drug Enforcement Task Force, those clearances often are not recognized by the FBI for having access to classified information for which the FBI is the custodian. These are issues about which the reader should be aware—they remain to be resolved.

Chapter 10 discusses a range of issues related to classified information and security clearances. Suffice it to note at this point that classified information may be disseminated only to an individual who has the appropriate type of security clearance, which establishes the right to know. The need to know still must be determined before dissemination, even if the individual has the appropriate level of clearance.

[10] For detailed information on classified information see the Information Security Oversight Office at www.archives.gov/isoo/policy-documents/eo-12958-amendment.html#1.2.

[11] Reese, Shawn. *State and Local Homeland Security: Unresolved Issues for the 109th Congress.* Washington, D.C.: Congressional Research Service, Library of Congress, 2005, p. 11.

[12] In a joint publication by the Major Cities Chiefs Association and the Major County Sheriffs' Association, a resolution to handle the backlog of security clearances applications for SLTLE personnel was offered as follows:

> Chiefs and sheriffs will join with DHS to implement a comprehensive plan to eliminate the backlog of pending applications and expedite the security clearance process. Features of the plan include:
>
> 1. Reduction in requests for TOP SECRET/Sensitive Compartmented Information (TS/SCI) clearances and accesses.
> 2. Focus primarily on faster and more useful SECRET-level clearances.
> 3. Law enforcement agencies propose to conduct background investigations and expedite adjudication of SECRET level clearances.
> 4. DHS agrees to provide training on clearance process.
> 5. DHS agrees to assist major law enforcement agencies in expediting priority security clearances.
> 6. Per federal statutes/regulations, DHS commits to accept clearance granted by other agencies.
>
> Source: *Intelligence and Information Sharing: DHS and Law Enforcement.* Major Cities Chiefs Association and Major County Sheriffs' Association, 2007, p. 3. (Unpublished report.)

Sensitive But Unclassified Information (SBU)/Controlled Unclassified Information (CUI)

SBU—or "tear line"[13]—Information does not have any formal restrictions, clearances, or sanctions as found with classified information. Rather, the SBU designation is more akin to a professional responsibility that is expected to be honored in light of one's professional obligations. While most SLTLE officers will not have a security clearance, virtually all will have access to SBU information. SBU information may have been previously classified but typically "sources" and "methods of collection" have been removed, thereby declassifying the information and rendering it SBU. In other cases, the inherent sensitivity of the information based on its character, such as an analysis of terrorists' tactics that produces indicators of terrorist activity, may warrant the SBU label.

Among the many forms of SBU labels, particularly at the federal level, the two most commonly used in law enforcement are *Law Enforcement Sensitive (*LES*)* and *For Official Use Only* (FOUO). As a general rule, LES information may be shared with anyone in the law enforcement community (sworn or nonsworn) who has the right to know and a need to know the information. FOUO means that the information may be shared with anyone who has the right to know and the need to know. For example, information about a threat to a nuclear power plant would be shared with the corporate security director and manager of the plant. These are general rules which, in practice, have no enforceable sanctions should they be violated. Rather, they provide guidance on disseminating sensitive information and rely on the professional decisions of those who receive the information to maintain security.

Because of the lack of explicit guidance and the wide range of SBU dissemination labels, there is both uncertainty and inconsistency in dissemination processes. As a result, one of the mandates of the Intelligence Reform and Terrorism Prevention Act of 2004 was to develop the ISE which included, as one of the ISE program manager's responsibilities, the creation of a labeling protocol for SBU information that had a consistent meaning and application across the entire ISE. This is particularly true given the important role of sharing unclassified terrorist information with state, local, and tribal law enforcement. There is a need to disseminate information; that is, share important information with others, but that information sharing must be controlled—protecting information and ensuring that it is not disseminated inadvertently.

As a result, the federal government is in the process of changing SBU label markings with a new information control model called *Controlled Unclassified Information* (CUI). A number of new factors with CUI provide more specific and universal direction than has existed with SBU labels. Although Chapter 10 contains a discussion of these details, it should be noted for purposes of dissemination in the Intelligence Process that there are controls for establishing the right to know for unclassified information that need to be safeguarded.

[13] The "tear line" refers to a classified report where there is a summary of the report at the bottom that excludes information about the sources of information and/or methods of information collection. This summary may be torn off the report; hence, it is referred to as tear line information and it is SBU.

Reevaluation

The classic definition of a "system" is a series of interconnected component processes that have an interrelated purpose of which a change in one component will affect the other components. The Intelligence Process is indeed a system. As each component—or phase—processes information, it will affect the body of knowledge in the other components as related to the intelligence inquiry. Just like any system, homeostasis—that is, a "steady state" of the system—must be maintained. This is the purpose of reevaluation: To ensure that all information is being processed in a comprehensive manner, the Intelligence Process must be ongoing with each new piece of information in the process being added to the full body of new knowledge to aid in developing the most precise intelligence possible. Reevaluation also serves as a measurement to determine if the intelligence products created by this process have value. Are threats accurately identified? Are all components of the Intelligence Process functioning as intended? Are effective operational interventions able to be developed based on the intelligence?

Conclusion

This chapter described the Intelligence Process (or cycle) as depicted in the *National Criminal Intelligence Sharing Plan*. The introduction of key terminology and concepts provides perspective on how they relate to the Intelligence Process and, as will be seen, the role of the Intelligence Process in other intelligence initiatives, including Intelligence-Led Policing.

Chapter Annex 4-1: Federal Bureau of Investigation Intelligence Cycle

This illustration is based on an actual case. It demonstrates the interrelationship between the two types of intelligence.

The FBI Intelligence Cycle

The Federal Bureau of Investigation (FBI) Directorate of Intelligence (DI) has significantly different intelligence responsibilities than state, local, or tribal law enforcement agencies. This difference is a result of its national criminal intelligence responsibilities and the FBI's national security responsibilities. One model of the Intelligence Cycle is not "better" than the other; rather, they are just slightly different approaches based on different operational responsibilities. The following brief description of the FBI DI Intelligence Cycle will provide an understanding of the FBI's approach and terminology that can be valuable for SLTLE personnel when they are communicating with the FBI's intelligence personnel.

The Intelligence Cycle is the process of developing unrefined data into polished intelligence for use by policymakers. It consists of the six steps described in the following paragraphs. The graphic below shows the circular nature of this process, although movement between the steps is fluid. Intelligence uncovered at one step may require going back to an earlier step before moving forward

Requirements are identified information needs—what we must know to safeguard the nation. Intelligence requirements are established by the Director of National Intelligence according to guidance received from the President and the National and Homeland Security Advisors. Requirements are developed based on critical information required to protect the United States from national security and criminal threats. The Attorney General and the Director of the FBI participate in the formulation of national intelligence requirements.

Planning and Direction is management of the entire effort, from identifying the need for information to delivering an intelligence product to a consumer. It involves implementation plans to satisfy requirements levied on the FBI, as well as identifying specific collection requirements based on FBI needs. Planning and direction also is responsive to the end of the cycle, because current and finished intelligence, which supports decision-making, generates new requirements. The Executive Assistant Director for the National Security Branch leads intelligence planning and direction for the FBI.

Collection is the gathering of raw information based on requirements. Activities such as interviews, technical and physical surveillances, human source operation, searches, and liaison relationships collect intelligence.

Processing and Exploitation involves converting the vast amount of collected information into a form usable by analysts. This is done through a variety of methods including decryption, language translations, and data reduction. Processing includes entering raw data into databases where the data can be used in the analysis process.

Analysis and Production is the conversion of raw information into intelligence. It includes integrating, evaluating, and analyzing available data, and preparing intelligence products. The information's reliability, validity, and relevance are evaluated and weighed. The information is logically integrated, put into context, and used to produce intelligence. This includes both "raw" and finished intelligence. Raw intelligence is often referred to as "the dots"—individual pieces of information disseminated individually. Finished intelligence reports "connect the dots" by putting information into context and drawing conclusions about its implications.

Dissemination—the last step—is the distribution of raw or finished intelligence to the consumers whose needs initiated the intelligence requirements. The FBI disseminates information in three standard formats: *Intelligence Information Reports*, *FBI Intelligence Bulletins*, and *FBI Intelligence Assessments*. FBI intelligence products are provided daily to the Attorney General, the President, and to customers throughout the FBI and in other agencies. These FBI intelligence customers use the information to make operational, strategic, and policy decisions that may lead to the levying of more requirements, thereby continuing the FBI Intelligence Cycle.

Chapter 5:

The Concept of Intelligence-Led Policing (ILP)

The Concept of Intelligence-Led Policing (ILP)

Participants in the International Association of Chiefs of Police (IACP)/Office of Community Oriented Policing Services (the COPS Office) 2002 intelligence summit recommended the adoption of Intelligence-Led Policing (ILP) by America's state, local, and tribal law enforcement (SLTLE) agencies in the post-9/11 era. ILP was envisioned as a tool for sharing information that would aid law enforcement agencies in identifying threats and developing responses to prevent those threats from reaching fruition in America's communities.[1] This was reinforced by a recommendation in the *National Criminal Intelligence Sharing Plan*[2] (NCISP) to adopt ILP and has been echoed broadly by law enforcement leaders and reflected in new programming by the U.S. Department of Justice and the U. S. Department of Homeland Security.

The challenge, however, is that there are differing views of the ILP concept and its application. Indeed, there is a movement toward the adoption of ILP without a universally accepted definition or a manual of practice. The intent of the discussion in this chapter is to provide a perspective of ILP in the context of contemporary developments in law enforcement intelligence, integrating the more commonly accepted applications of ILP, and particularly focusing on the processes required to implement the concept.

Implementation of ILP requires a realistic understanding of the current intelligence capacity across the spectrum of American law enforcement and a flexible approach to meet the capabilities and needs of major cities and counties as well as small departments and rural communities.

Conceptual Foundations

The NCISP states, "The primary purpose of *Intelligence-Led Policing* is to provide public safety decision-makers [with] the information they need to protect the lives of our citizens."[3] How is this accomplished? There is no manual of practice for ILP because, like community policing, it must be tailored to the characteristics of the individual agency. ILP may be characterized as follows:

> …an underlying philosophy of how intelligence fits into the operations of a law enforcement organization. Rather than being simply an information clearinghouse that has been appended to the organization, ILP provides strategic integration of intelligence into the overall mission of the organization.[4]

The concept of ILP must be created through an inclusive development process to ensure that it is integrated with an agency's goals and functions, its capabilities, and the characteristics of both the agency and the jurisdiction it serves. It is not an add-on responsibility of the agency but an adaptation to more efficiently and effectively deal with multijurisdictional threats and serious crime that touch communities. There are no shortcuts in the process—it requires creativity, organizational introspection, and a willingness to adapt the organization. The following discussions provide a framework for understanding the diverse aspects

[1] www.theiacp.org/Portals/0/pdfs/Publications/intelsharingreport.pdf

[2] Global Intelligence Working Group. *National Criminal Intelligence Sharing Plan.* Washington, D.C.: U. S. Office of Justice Programs, 2003.

[3] Ibid. p. v.

[4] Carter, David L. *Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement Agencies.* Washington, D.C.: Office of Community Oriented Policing Services, U.S. Department of Justice, 2004, page 41.

of the ILP concept. Building on this understanding, the next chapter (Chapter 6) discusses the policy and organizational dynamics necessary to effectively implement ILP.

Defining ILP

There is no universally accepted definition of ILP, although the components of most definitions are the same, or at least similar. In 2009, the Bureau of Justice Assistance (BJA), in partnership with the Global Justice Information Sharing Institute, produced two definitions of ILP in which the conceptual foundation was articulated as building on the lessons of Problem-Oriented Policing and CompStat and applying these principles to a threat-based environment of multijurisdictional complex criminality. The conceptual foundation embraces recent initiatives in law enforcement intelligence, ranging from the operation of the Regional Information Sharing System (RISS), to the products of the Global Justice Information Sharing Initiative, to the development of the National Information Exchange Model.

In the document, the BJA states that ILP is:

> ILP can be defined as a collaborative law enforcement approach combining problem-solving policing, information sharing and police accountability, with enhanced intelligence operations.

However, for the purposes of their document, BJA narrowed the definition to the following:

> ILP is executive implementation of the intelligence cycle to support proactive decision making for resource allocation and crime prevention.[5] In order to successfully implement this business process, police executives must have clearly defined priorities as part of their policing strategies.

Building on these foundations, this author proposes an operational definition of ILP as follows:

> The collection and analysis of information related to crime and conditions that contribute to crime, resulting in an actionable intelligence product intended to aid law enforcement in developing tactical responses to threats and/or strategic planning related to emerging or changing threats.

Breaking the definition down to its critical components will provide a better understanding.

Collection

An essential part of the intelligence process is the collection of raw information that may be used in the analysis. Collection should be focused to identify and understand threats that emerge in a jurisdiction. This focus, often determined by an analyst who will define intelligence requirements, is based on information received from officers, confidential sources, and citizens in the form of tips, leads, and Suspicious Activity Reports. The key point is that collection seeks raw information within defined parameters that is essential for effective analysis.

Analysis

Analysis is the scientific approach to problem solving. It relies on deductive and inductive reasoning to define requirements and forecast threats. Analysis may be

[5] Global Justice Information Sharing Initiative. Navigating Your Agency's Path to Intelligence-Led Policing. Washington, DC: U.S. Department of Justice, Office of Justice Programs, Bureau of Justice Assistance, 2009, p. 2.

quantitative, notably for strategic analysis, but frequently it is qualitative, for both tactical and strategic analysis. The Office of the Director of National Intelligence (ODNI) has stated that analysis is "a process in the production of intelligence in which intelligence information is subjected to systematic examination in order to identify significant facts and derive conclusions."[6] The ODNI goes on to make the following distinctions between raw information and analyzed information (that is, intelligence):

- Raw information:
  - Provides input
  - Builds awareness
- Analyzed information (intelligence):
  - Provides understanding
  - Reduces uncertainty
  - Enables better decisions

The analytic process is synergistic, providing integrated meaning and deriving knowledge from diverse raw facts. Moreover, analysis is used to define "intelligence gaps" and articulate "requirements."

Crime and Conditions that Contribute to Crime

ILP focuses on threats and it becomes essential to identify variables within a community and the surrounding region that support the generation and maturation of crime. These variables can be wide-ranging: The emergence of organized criminal elements within the region who traffic in drugs or guns; the emergence of an extremist group that articulates hate or violence; conflict within a region that may be a breeding ground for violence between racial, ethnic, or religious groups; and a variety of unique characteristics that are idiosyncratic to a given community, such as proximity to an international border. It is important that the information collected provide insight into the existence of the conditions, factors that will exacerbate the conditions and individuals who may be instrumental in exploiting the conditions to commit terrorism or crime.

Actionable Intelligence

Paraphrasing former FBI Executive Assistant Director for Intelligence Maureen Baginski, intelligence helps law enforcement officers make decisions. Essentially, for intelligence to be useful it must provide direction for developing and executing plans. A law enforcement agency must be able to take an intelligence report and implement some type of activity that will prevent or mitigate crime. This means that the intelligence produced by an analyst will drive operational responses to, and strategic planning for, threats.

With actionable intelligence, a law enforcement agency has sufficient information to develop preventive interventions to threats. The report may describe either imminent threats to a community or region, wanted persons who may pose threats, or threat methodologies about which law enforcement officers should be aware. The basic premise is that the agency must be able to use the information in some manner. Moreover, actionable intelligence should ensure that the right information is placed into the hands of the people who can do something about the threat.

[6] Ramsey, Theresa. *Global Maritime Intelligence Integration (GMII) Enterprise.* PowerPoint Presentation. Washington, D.C.: Office of the Director of National Intelligence, May 9, 2007.

Tactical Responses to Threats

Both tactical and strategic intelligence are extensions of actionable intelligence. Depending on the nature of the threat, a wide array of tactical responses may be deemed appropriate, ranging from increasing mass transit security procedures to being aware of suspicious activities at a potential intelligence target. Tactical intelligence is all about prevention: Using information related to terrorism and crime threats for strategies that will eliminate or mitigate short-term and immediate threats. Tactical intelligence is epitomized by the question, "What type of operational response can be developed using this intelligence?"

Strategic Planning Related to Emerging or Changing Threats

Threats within a community typically change over time. Strategic analysis is used primarily for planning and resource allocation to understand the changing nature of the threat picture. Information is provided to decision-makers about the changing nature, characteristics, and methodologies of threats and emerging threat idiosyncrasies so that they can develop response strategies and reallocate resources. If, for example, a community has never had a problem with right-to-life extremists and a new clinic opens that offers abortion procedures, a strategic analysis may provide insight into whether the clinic and its personnel will be subject to any type of threat by extremist groups.

By using strategic analysis, plans may be developed to either prevent a threat from maturing or mitigate the threat should it emerge. It is epitomized by the question, "What future plans and resources must be configured, and how must they be configured, to meet threats defined in the strategic analysis?"

Fundamental Perspectives on the History of ILP: The British Experience

To refine our vision of ILP, context is needed. Specifically, one needs to understand the dynamics within the American law enforcement environment that will influence the implementation of ILP as well as limitations to adopting the British National Intelligence Model for U.S. law enforcement.

Perspective 1: The Current State of American Law Enforcement Intelligence

Some evidence suggests that ILP can provide an important element to community security to prevent (or at least mitigate) terrorism, violence, criminal extremism, and complex criminality. This author agrees. The concern, however, is how ILP is implemented. At one meeting, a strong ILP advocate urged law enforcement leaders to take the Nike® approach and "just do it." The problem is that American law enforcement is neither structurally nor substantively ready to support the ILP infrastructure. Just like a building, the foundation must first be in place—most American law enforcement agencies have gathered some bricks, but they are a long way from completing the foundation.

During the past 20 years, this author has provided intelligence training to literally thousands of law enforcement personnel representing hundreds of agencies at all levels of government from every state and most territories.[7] Yet this is a

[7] Also, as a means of comparison, this author has provided intelligence training to law enforcement agencies in Europe, Asia, and Australia.

small proportion of American law enforcement. What has been learned is that agencies that have an intelligence capacity are the exception, rather than the rule. Moreover, what is commonly called an intelligence unit or capacity in most agencies is, in practice, more of a hybrid organizational entity that may be doing crime analysis and/or investigative support. In many cases, there is also the integration of crime analysis and intelligence analysis despite the fact that these are different.[8] In other cases, there may be multiple intelligence capacities that are function-specific, such as gang intelligence, drug intelligence, and/or organized crime intelligence. Once again, many of these activities are more akin to investigative support than to intelligence.

Historically, the vast majority of American law enforcement agencies have had no intelligence capacity or training on the intelligence function and processes—typically, they were viewed as something needed only by the largest agencies. Of the agencies that had an intelligence capacity, the legacy has been somewhat problematic. Early law enforcement initiatives typically did not conduct analyses. Instead, they kept dossiers on individuals who were "suspicious" or were deemed to be threats of some sort, often based on intuitive, rather than empirical, threat criteria. In the 1960s and 1970s, many agencies were sued under federal civil rights legislation[9] for maintaining intelligence records on people who had not committed crimes but were engaged in behaviors and ideologies that were deemed to be unconventional or un-American. While these practices generally no longer exist, the legacy lives on, with many members of the public remaining suspicious of current law enforcement intelligence activities.

Beyond the civil rights issues, the intelligence function was often ill-defined, typically remaining out of the mainstream of state and local law enforcement activities. There were few analysts and many were poorly trained, often inheriting the title of "analyst" as a result of longevity, not expertise. It was often difficult to distinguish what the intelligence unit, as an organizational unit, contributed to the total law enforcement mission. While there were certainly exceptions to such a characterization, it was the status quo for most American law enforcement intelligence initiatives. Although this has changed dramatically, the history remains a difficult obstacle to overcome.

This change began in the post-9/11 era, leading to an increased awareness of intelligence and growing intelligence capacities, In particular, this was the result of the IACP/COPS Office intelligence summit; the efforts of the Global Intelligence Working Group (GIWG); the release of the NCISP; the creation of the Criminal Intelligence Coordinating Council (CICC); the growth of intelligence fusion centers; and the wide array of new law enforcement intelligence training programs typically available at no charge to SLTLE agencies. Nonetheless, this is a long way from being comprehensive. The next step of being active participants in the Information Sharing Environment (ISE) is, in reality, barely on the horizon for most SLTLE agencies.

Increasing numbers of agencies have some form of intelligence capacity, yet comparatively, the numbers are still small. Moreover, many agencies—even

[8] Crime analysis assesses the interactive effects and covariance of explicit variables of crimes that have occurred in order to determine a perpetrator's methodologies with the intent to clear the crimes and prevent future incidents by apprehending the perpetrator. Intelligence analysis deals with threats, whether from terrorism, criminal extremism, or organized crime, through the analysis of information that suggests a threat, the identification of intelligence requirements, and the use of both target and vulnerability assessments, with the intent of preventing the threat from reaching fruition.

[9] Specifically, 42 United States Code, Section 1983—Civil Action for Deprivation of Civil Rights.

moderate-sized departments—either do not see the need for an intelligence capacity or feel they cannot justify devoting resources to develop an intelligence capacity because of competing demands, notably, increasing violent crime rates and managing calls for service. For the vast majority of these agencies, the chief executive—as well as others in the chain of command—typically relies on historically based assumptions about intelligence and does not understand the rapid evolution and value of the modern law enforcement intelligence function. In light of these factors, there is limited motivation for such agencies to adopt ILP. The issue is not that agencies do not want to participate in fusion centers and the ISE; they often do not see the value in light of other responsibilities.

Based on these issues, an earlier point warrants repeating: Most American law enforcement agencies do not have the foundation to implement ILP. An intelligence foundation must first be constructed.

Perspective 2: The British National Intelligence Model and Challenges in Adapting It to U.S. Law Enforcement

When seeking to make use of a new concept, we often look to other models in an attempt to learn what works and adopt (or adapt) that practice. The British have a longer and more sophisticated legacy in law enforcement intelligence than U.S. law enforcement. All provincial British constabularies have had some form of a fairly long-standing intelligence unit to deal with organized crime, drugs, and other complex crimes unique to their jurisdictions. As an example, many of the British constabularies have a Football Intelligence Unit to deal with hooliganism at soccer matches. At a national level, the National Drugs Intelligence Unit was created in the 1980s to deal with the significant increase in transnational drug trafficking and associated crime, such as money laundering. The service relied on personnel assigned (that is, "seconded") from police forces throughout England and Wales. In 1992, the unit was expanded and renamed the National Criminal Intelligence Service (NCIS) to deal with all forms of organized crime. In particular, the NCIS evolved in response to the changing political environment associated with the European Union (EU), where, among other factors, immigration and customs checkpoints were eliminated for persons traveling between the EU member countries. In 2006, a new agency was created, the Serious Organised Crime Agency (SOCA), that integrated the NCIS along with a national investigative body, the National Crime Squad, and the drug enforcement functions of Her Majesty's Revenue and Customs Service.[10]

In the 1990s, the British government began implementing a business plan philosophy for all elements of government service. It had two fundamental initiatives: either "privatise" portions of government service, or apply a business model to the remaining government services. The move had wide-ranging effects: for example, the British National Rail Service—BritRail— was sold in pieces to various private companies. Similarly, local governments "privatised" such functions as vehicle maintenance and the janitorial service. The national police training function in England and Wales was also changed to a quasiprivate organization called CENTREX, which in April 2007 evolved to be part of the

[10] SOCA is an intelligence-led agency responsible for dealing with major organized crime. The United Kingdom (U.K.) Security Service (MI5) is responsible for dealing with threats to U.K. national security with the greatest emphasis on terrorism, but also espionage, including domestic intelligence. The Secret Intelligence Service (MI6) is responsible for collecting intelligence outside of the U.K.

National Police Improvement Agency (NPIA). The point is that the mandate to use business processes permeated virtually every aspect of British government, including the police.

As part of this movement, in the late 1990s, NCIS, with advice from Her Majesty's Inspectorate of Constabulary[11] (HMIC), developed the British National Intelligence Model[12] (NIM), which was initially released in 2000 and formally adopted in 2002 as accepted policy by the British Association of Chief Police Officers (ACPO), which is a national police policymaking body. The NIM followed the government policy of using a business process model to deal with crime control.

The adoption of the NIM by ACPO meant that the chief constables of the 43 provincial police forces in England and Wales agreed to adopt the NIM and adapt it to meet the needs of their policing area.[13] The intelligence function within the constabularies largely deals with violent crime, football hooliganism, nonserious (local) organized crime, and unique local recurring crime problems.

The British police movement to ILP in accordance with the NIM has not been easy. Many did not understand the concept because it required a reallocation of resources and added a significant analytic component to each police force. The NIM was criticized by many as being an esoteric model that created a great deal of data and new processes that were not providing good value for money. Its full implementation has been much slower than anticipated, and as one might assume, some of the police forces have embraced the concept much more openly than others, who, in some cases, are using the NIM largely in name only.

Despite these problems, there have also been important successes as a result of the NIM. Many lessons learned from the NIM can be adopted in the United States, and a unique body of model practices, including analytic models, are available from the HMIC[14] (of course, needing adaption to the United States). American law enforcement agencies, however, have a significantly different experience in law enforcement intelligence that prohibits wide-scale adoption of British ILP, with some notable exceptions in the predominantly larger U.S. major cities and counties. Some perspective will provide greater understanding.

As mentioned previously, England and Wales have 43 police forces, the result of the amalgamation of many smaller police agencies in the 1960s. The smallest of these constabularies has around 900 sworn constables who are policing sizeable geographic areas that have both urban and rural characteristics. Most of the agencies have 1,200 to 1,600 sworn personnel. While not a national police force, national standards apply to all agencies for training, promotion, operations, and salary. Indeed, personnel may transfer laterally between the constabularies.

Given the size of these police forces and their reasonable operating budgets,[15] all have the resources to hire analysts and the flexibility to reassign personnel to meet the needs of a comprehensive new initiative such as ILP. This is not meant to infer that the constabularies are flush with money and people; rather, one finds significantly more flexibility, resources, and diverse expertise in large agencies than in the small departments typically found in the United States. Moreover,

[11] The HMIC is an organization in the British Home Office responsible for inspecting the British police forces to ensure that they are efficient organizations using "good practice" and providing "good value for money" in their service.

[12] More detail on the National Intelligence Model can be found in the ACPO document at www.acpo.police.uk/asp/policies/Data/nim2005.pdf.

[13] England and Wales have 43 provincial constabularies, whose chief constables are responsible to the local police authority (somewhat akin to a board of police commissions). The commissioner of the London Metropolitan Police reports to the British Home Secretary and has much broader authority and flexibility. While ACPO policy is not binding on the London Metropolitan Police, it has also adopted the NIM. An additional police service, the City of London Police, which is the smallest police agency in the U.K., is responsible for a small geographic area known as "the square mile" that largely encompasses the London financial district.

[14] Go to the HMIC web site at inspectorates.homeoffice.gov.uk/hmic and search for "intelligence."

[15] The national budget, through the Home Office, provides 51 percent of the funding for each provincial police force; 49 percent comes from local funds. This permits the Home Office to exert greater influence for national standards and priorities, although in practice, each chief constable retains significant autonomy.

having a solid history of sophisticated law enforcement intelligence analysis, the British police service was able to adopt the NIM and ILP with greater ease.

Comparing U.S. and U.K. Law Enforcement Intelligence

Compared with the British police structure, America's roughly 18,000 law enforcement agencies, most of which have 10 or fewer sworn officers, have diverse policing standards both between and within states. They often have limited budgets, all of which typically come from local funds, with some exceptions in the form of short-term federal grants. Federal standards and recommendations are largely unenforceable unless tied explicitly to special conditions in a grant.

In light of these radical differences and the significantly different history of law enforcement intelligence, when one compares U.S. and U.K. policing, it is unreasonable to assume that the basic practices of the NIM, as found in the United Kingdom, and, by extension, ILP, can be implemented effectively in the United States on a short-term wholesale basis. In America, we need to start at a far more basic level. A functional model of ILP must be developed that has both the flexibility and applicability to the American law enforcement landscape.

At the outset, ILP should be viewed as a philosophy, not a process. Indeed, American law enforcement agencies should rely on this philosophy to develop new intelligence-based processes that functionally balance each agency's jurisdictions, characteristics, and resources. The lessons learned from community policing can be a valuable guide.

Developing ILP in a law enforcement agency requires two developmental activities: 1. Devising the information collection framework to manage threats within a jurisdiction and 2. Developing the organizational infrastructure to support the ILP initiative. These will be discussed in detail in Chapter 6.

ILP And Community Policing, Problem Solving, and CompStat

A common concern expressed by police executives is that the shift toward ILP—largely the result of increased counterterrorism responsibilities—may require a shift of resources away from community policing. It becomes a question of how community policing and ILP are integrated. As will be seen, there are more commonalities between the two than one may intuitively expect. Indeed, new dimensions of ILP depend on strong community relationships. Crime will continue to be a critical responsibility for the police as will the need for community support. Moreover, with increased social tension resulting from the homeland security environment, the need is even greater to maintain a close, interactive dialog between law enforcement and the community.

Community policing has developed skills in many law enforcement officers that directly support new ILP responsibilities: The scientific approach to problem solving, environmental scanning, effective communications with the public, fear reduction, and community mobilization to deal with problems are among the

important attributes community policing brings to this challenge. The NCISP observed these factors, noting the following:

> Over the past decade, simultaneous to federally led initiatives to improve intelligence gathering, thousands of community-policing officers have been building close and productive relationships with the citizens they serve. The benefits of these relationships are directly related to information and intelligence sharing: COP officers have immediate and unfettered access to local, neighborhood information as it develops. Citizens are aware of, and seek out COP officers to provide them with new information that may be useful to criminal interdiction or long-term problem solving. The positive nature of COP/citizen relationships promotes a continuous and reliable transfer of information from one to the other. It is time to maximize the potential for community-policing efforts to serve as a gateway of locally based information to prevent terrorism, and all other crimes.[16]

Furthermore, the Office of Domestic Preparedness Guidelines for Homeland Security describe the roles community policing has in the intelligence process. These include the following:

- Providing examples and materials that may aid in the recognition of terrorism to community policing contacts to make members of the community aware of those actions, behaviors, and events that constitute "suspicious."
- Organizing community meetings to emphasize prevention strategies, vigilance, and public awareness.
- Ensuring that members of the community are aware of the means of, and processes for, relaying observed data to police officers and police organizations, just as they are, or should be, aware of methods to relay information to community policing officers.
- Encouraging prevention, proactive policing, and close working relationships between the police and the community.[17]

These factors precipitated the development of ILP as an underlying philosophy of how intelligence fits into the operations of a law enforcement organization. Rather than being simply an information clearinghouse that has been appended to the organization, ILP provides strategic integration of intelligence into the overall mission of the organization. In many ways, ILP is a new dimension of community policing, building on tactics and methodologies developed during years of community policing experimentation. Some comparisons illustrate this point. Both community policing and ILP rely on these activities:

- Information Management
  - Community policing—Information gained from citizens helps define the parameters of community problems.
  - ILP—Information input is the essential ingredient for intelligence analysis.
- Two-way Communications with the Public
  - Community policing—Information is sought from the public about offenders. Communicating critical information to the public aids in preventing crime and reducing fear.

[16] it.ojp.gov/ncisp

[17] www.ojp.usdoj.gov/odp/docs/ODPPrev1.pdf

- ILP—Communications from the public can provide valuable information for the intelligence cycle. When threats are defined with specific information, communicating critical information to citizens may help prevent a terrorist attack and, like community policing, will reduce fear.

- Scientific Data Analysis
  - Community policing—Crime analysis is a critical ingredient in the CompStat[18] process.
  - ILP—Intelligence analysis is the critical ingredient for threat management.
- Problem Solving
  - Community policing—Problem solving is used to reconcile community conditions that are precursors to crime and disorder.
  - ILP—The same process is used for intelligence to reconcile factors related to vulnerable targets and trafficking of illegal commodities.

The importance of these factors is illustrated in the comments of FBI Director Robert Mueller in announcing an increased concern for terrorism at major national events during the summer of 2004. When referring to the photographs of seven terror suspects believed to be in the United States, Director Mueller stated:

> We need the support of the American people … to cooperate when called upon, as agents will be reaching out to many across the nation to help gather information and intelligence … to be aware of your surroundings and report anything suspicious … to "BOLO" [Be On the Lookout] for those pictured above. … Have you seen them in your communities? Have you heard that someone might be helping them to hide? Do you have any idea where they might be? If so, we need you to come forward.[19]

These words reflect the operational essence of the interrelationship of law enforcement intelligence and community policing. Like community policing, ILP requires an investment of effort by all components of the organization as well as the community. Gone are the days when intelligence units operated in relative anonymity. Based on the precepts of the ILP philosophy and the standards of the NCISP, law enforcement intelligence is an organization-wide responsibility that relies on a symbiotic relationship with residents.

Comparing ILP and CompStat

The CompStat process, with its origins in the New York Police Department, has been an important tool for law enforcement agencies to effectively deal with crime trends on a timely basis. The process has been adopted in varying forms and with consistent success by many midsized and large law enforcement agencies across the United States and in several foreign countries. A solid foundation of research supports CompStat as a crime-management tool that demonstrates the value of innovative approaches to law enforcement problems.[20]

As law enforcement personnel grapple with understanding ILP, many have suggested that it is the same as CompStat. Certainly, there are important similarities that will help in the adoption of ILP; however, there are also important substantive differences that must be recognized. At the heart of the matter is

[18] For a good contemporary discussion of CompStat, see: Shane, Jon, "CompStat Process." *FBI Law Enforcement Bulletin* 73 (2) (April 2004): 12–23.

[19] www.fbi.gov

[20] A great deal of research and literature can be found at www.ncjrs.org. Use the search utility for "CompStat."

the fact that CompStat and ILP are different because of a number of functional variables that are illustrated in Figure 5-1.

As can be seen, ILP is concerned with "all crimes and all threats," not just terrorism; however, the nature of crime that ILP focuses on typically is multijurisdictional and often complex criminality, such as criminal enterprises.

The value of CompStat is its identification of emerging, significant crime series or serious crime within a jurisdiction (that is, hot spots), based on a timely analysis of incident reports. The analysis of data captured by crime reporting can provide important information—such as geographical parameters and modus operandi—that can be used to forecast continued criminal incidents in the immediate future, aid in problem solving, and provide descriptive information, such as behaviors, targets, and criminal instruments that operational units may use to apprehend perpetrators, disrupt criminal activity, or alter crime-generating environments.

Conversely, ILP focuses on threats rather than crimes that have occurred (although a threat may also include a threat emerging from a crime series, such as a serial murder). The threat information may be derived from Suspicious Activity Reports filed by an officer, tips and leads submitted by community members, significant changes in sociodemographics within a region or other indicators (some of which may be collateral crimes) that reasonably suggest the presence or emergence of a serious multijurisdictional crime problem. Rather than analyze information and evidence derived from incident reports, the intelligence analyst must define intelligence requirements consisting of information that the analyst needs to more definitively identify the threat and factors that are contributing to the threat's evolution.

Similarly, to be effective, both community policing and ILP require feedback on information analysis—whether it is crime analysis or intelligence analysis—to be consistently informed of potential problems or threats that may be encountered during the course of a shift.

In this regard, what kind of information do street officers need from the intelligence unit? Ideally, intelligence analysis should address four broad questions:[21]

1. Who poses threats? This response identifies and describes people in movements or ideologies who pose threats to community safety.
2. Who's doing what with whom? This includes the identities, descriptions, and characteristics of conspirators or people who provide logistics in support of terrorism and criminal enterprises.
3. What is the modus operandi of the threat? How does the criminal enterprise operate? What does the terrorist or extremist group typically target and what are the common methods of attacking? How do members of the extremist group typically integrate with the community to minimize the chance of being discovered?
4. What is needed to catch offenders and prevent crime incidents or trends? What specific types of information are being sought by the intelligence unit to aid in the broader threat analysis?

[21] On a related note, following the terrorists' attacks of September 11, 2001, the FBI developed a series of interview questions for persons who may have knowledge about terrorism. State and local law enforcement were asked to participate in the questioning of some persons who were in the U.S. on visas. There was a mixed response, largely based on the perspective of local government leaders. Despite this, the questions were also intended to provide insight and information for officers. More information, as well as the protocol questions, can be found in: General Accounting Office. Homeland Security. *Justice Department's Project to Interview Aliens After September 11, 2001*. Report to Congressional Committees. Report Number GAO-03-459, April 2003. www.gao.gov.

Both CompStat and ILP are prevention-oriented and are driven by an information flow coming from the line level upward. Intelligence awareness training for street officers recognizes that officers on patrol have a strong likelihood of observing circumstances and people that may signify a threat or suggest the presence of a criminal enterprise. The patrol officer must be trained[22] to regularly channel that information to the intelligence unit for input into the Intelligence Cycle for analysis. Like community policing, this requires new responsibilities for patrol officers and organizational flexibility to permit officers to explore new dimensions of crimes and community problems that traditionally have not been part of their responsibilities.

While there are fundamental similarities, the methodology and focus of ILP is notably different from, and more difficult than, CompStat because of the differences in the raw data. Understanding these differences and, more important, the role ILP fulfills is an important foundation for the following discussions.

Figure 5-1: Comparison of CompStat and Intelligence-Led Policing

Similarities of CompStat and Intelligence-Led Policing: Important Lessons Learned from CompStat Can Be Applied to ILP

- ✓ Both have a goal of prevention
- ✓ Commitment to the concept by the chief executive is essential
- ✓ Analysis serves as the basis for operational responses
- ✓ Processes for constant raw information flow for analysis must be in place
- ✓ Community engagement is critical for reporting suspicious activities
- ✓ Intervention activities are driven by definable evidence of crime and threats
- ✓ Administrative and organizational flexibility are required
- ✓ Research and lessons learned serve as the basis for creative intervention
- ✓ Managers and supervisors are held demonstrably accountable

While principles and processes are similar, there are also substantive differences

CompStat	Intelligence-Led Policing
• Intrajurisdiction	• Multijurisdiction
• Incident-driven	• Threat-driven
• Analysis based on known facts from reported crime data and investigations	• Analysis-based tips, leads, suspicious activity reports, and information collection
• Focuses on crime sprees and incident trends with intent to apprehend specific offenders	• Focuses on root causes and conditions that contribute to serious crime and terrorism
• Relies on crime mapping, incident analysis, modus operandi analysis	• Relies on link analysis, commodity flow, transaction analysis, association analysis
• Time-sensitive (24 hour feedback/ response)	• Strategic (inherently long-term)
• Predominant focus on street crime (burglary, robbery, homicide, assault, theft, etc.)	• Predominant focus on criminal enterprises (terrorism, organized crime, violence, etc.)
• Reported criminal incidents drive collection and analytic parameters	• Intelligence requirements drive collection and analytic parameters

[22] Training—including line officer training—is discussed in detail, including line officer training, in a later chapter.

Ethical Issues

Another important characteristic similar to both community policing and ILP is the emphasis on ethical decision-making. In community policing, the need for ethical decision-making was based on the need to develop trust between the police and community, among other reasons. Without this trust, the public would not provide the critical information needed for crime control. The need for ethical decision-making in ILP is similar, but goes a step further. Because of concerns about the types of information being collected by law enforcement and how that information is retained in records, concerns have been expressed that law enforcement may violate citizens' rights in the quest for terrorists. As a result of these concerns, the aura of ethical decision-making and propriety of actions must be unquestioned in the law enforcement intelligence function.

Civil Rights and ILP

A unique challenge in dealing with ILP is maintaining privacy and protecting individuals' civil rights. CompStat and crime analysis each have an entirely different set of legal rules. Typically, CompStat deals with aggregate data of criminal incidents and the attributes of those incidents. In those types of analysis, individuals are not identified; therefore, civil rights do not attach to the data. If the crime analysis focuses on the identification of individuals, the identification is a result of evidence obtained during the criminal investigation leading to probable cause for arrest. The law of criminal evidence and procedure applies to the further collection of evidence, and the information is retained in the law enforcement agency's records management system (RMS), which has rules of wide latitude for keeping information about criminal suspects, witnesses, and victims.

Conversely, as noted previously, ILP deals with threats and conditions that may facilitate the threats. At this point, there are no civil rights issues of consequence. However, as the intelligence process identifies individuals and organizations for which there is only a reasonable suspicion that they may take advantage of the conditions to commit criminal acts in the future, the information is classified as "criminal intelligence information." As such, this information may only be entered into a separate "criminal intelligence records system," not the RMS. Consequently, there must be adherence to the guidelines of 28 CFR Part 23.[23] Failure to do so could open the law enforcement agency to civil liability.

For the current discussion of ILP, the point to note is simply this: There are significantly different rules for the collection, retention, and dissemination of "criminal intelligence information" compared to "criminal investigation information." Beyond the information management differences, there are conceivable differences in the method of analysis that is performed when individuals are identified as either intelligence targets or witnesses. As such, there must be a separate records system and supporting policies developed for ILP as well as training on the proper method of processing information used in ILP.

[23] Technically, 28 CFR Part 23 applies only to federally funded multijurisdictional criminal intelligence records systems operated by state, local, and tribal law enforcement agencies. In practice, however, it must be assumed that 28 CFR Part 23 applies to all state, local, and tribal agencies for two reasons: 1. The NCISP recommends that all agencies adopt these guidelines as a national standard of good practice and 2. Precedent in federal civil rights cases suggests that adherence to the federal guidelines can be an affirmative defense should a civil rights case be brought against an agency for the types of information being retained in a criminal intelligence records system.

Public Education

As noted previously, public education is critical for effective ILP. The lessons learned from community policing provide important insights. The public encompasses many different groups and different public education initiatives need to be provided to each constituent group. For example, what does the agency want to accomplish with a public education program: Reducing fear? Developing volunteers for the police department? Resolving community tensions, such as demonstrated resentment toward the Muslim community? Is the goal simply to give citizens information about terrorism indicators to aid in prevention? The important point to note is that a specific goal should be related to the public education initiative.

Such a program may also stratify the community in order to give specific types of information to different targeted audiences. Who in the community should be targeted for an education program: The business community? Civic and church groups? Graduates of the Citizens' Police Academy (CPA)? Nonlaw enforcement government employees? Teachers and students? The general community? Demographically defined segments of the community?

Different segments of the community may have different needs. For example, since approximately 85 percent of America's critical infrastructure is owned by the private sector, a special public education program may focus on threat-related issues for this narrowly defined community. Conversely, a completely different kind of public education may be directed toward graduates of the CPA who may be trained to work as volunteers during crises or a heightened alert status. Yet a different public education agenda would be directed toward a particular ethnic or religious community within a city. Each segment of the community has a different goal. In this case, the business sector to harden potential targets, the CPA graduates to aid the police in response to increased service demands, and the ethnic community to gain information about suspicious persons and their actions.

These segments may be further divided, particularly if there are unique targets within the community. The business community, for example, may be broken down into different segments: Different threats may target a nuclear plant or telecommunications switching station (both are critical infrastructure) or a meat processing plant or university genetic research laboratory (both of which may be a target of domestic environmental extremists).[24] The law enforcement agency will have to conduct a threat assessment to fully understand the character of the threat within the community as well as to understand the agency's intelligence requirements.[25] Collectively, these elements have a symbiotic relationship to aid in the development of a public education program.

[24] At times, targets may not be readily apparent in a community. Does East Lansing, Michigan, appear to be a terrorist target? In 1992, the Animal Liberation Front started a fire in the Michigan State University (MSU) mink research facility and caused more than $2 million in damages. On December 31, 1999, a fire in MSU's Agricultural Hall caused $700,000 in damages and destroyed years of research. Earth Liberation Front claimed responsibility, targeting genetic research.

[25] The threat assessment and intelligence requirements will be discussed in a later chapter.

Community education programs should also intend to have a specific outcome. Whether it is to reduce fear or to enlist support for volunteer efforts, all public education initiatives should incorporate five factors related to the intelligence function:

1. Know how to observe.
2. Know what is suspicious.
3. Know how to report.
4. Know what to report.
5. Know what happens next.

To maximize the quality and quantity of information provided by the community, law enforcement must provide a framework of knowledge. The more that law enforcement can educate the community, the more robust the feedback from the community.[26] In this regard, Tables 5-1 and 5-2 illustrate a range of items that may be incorporated into a public education program from both a topical and an outcome perspective.

Community Members as Law Enforcement Volunteers

Oftentimes, community members ask what they may do to aid in counterterrorism. One important element is serving as a volunteer for the law enforcement agency. Experience has shown that community volunteers can save the agency money as well as often provide unique expertise. Money can be saved when citizens are able to perform tasks that would otherwise have to be performed by a law enforcement employee; for example, the Austin (Texas) Police Department uses volunteers as part of its Civil Defense Battalion to accomplish these goals.

Obviously, an agency needs to develop some means of screening volunteers as well as provide structure for their work agreement and for administrative controls when they are performing activities on behalf of the law enforcement agency. In this regard, an important resource is Volunteers in Police Service (VIPS).[27] The VIPS web site provides a wide array of resources, documents, policies, and tips that can make a law enforcement volunteer program functional and easy to manage.

Volunteers with unique occupational experience may be particularly valuable to the intelligence function. An attorney, accountant, people with experience in researching land titles, and academic researchers and scholars are illustrations of professional volunteers who could provide important assistance to the intelligence function. Of course, background checks and nondisclosure agreements must be required of all such volunteers.

[26] www.policevolunteers.org

[27] Ideally, the law enforcement agency would be able to provide feedback to the citizen about information that was reported. Many times this is not feasible in the intelligence environment; however, it serves as positive reinforcement to the citizen when feedback is provided.

Table 5-1: Examples of Topics in a Public Education Program

- Understanding terrorism
- What is terrorism (defined/explained)
- Why people commit terrorist acts
- Perspectives of terrorism
- Asymmetric warfare
- An act of terror is defined by the victim
- How terrorism can touch a community…
  - » As a target
  - » Logistics and support provided to terrorists
  - » Activities that fund terrorist organizations
- New preparedness resources for local emergency services
- What is being done at the national level
  - » National strategies developed
  - » National threat assessment by FBI
  - » FBI reprioritized and reorganized to aid state and local law enforcement
- What is being done at state and local levels
  - » Participation in Joint Terrorism Task Forces
  - » Officers receiving antiterrorism training
  - » New communications and information sharing (Automated Trusted Information Exchange, RISS, Law Enforcement Online) that give local law enforcement more access

Table 5-2: Examples of Actions the Public Can Take

- Keep informed to know what to look for and report to the police
  - » Law enforcement must be prepared to share information with public
- Be aware, yet be fair
- Be cognizant of threats, but avoid stereotyping and hyperbole
- Information on how to talk/deal with children regarding terrorism
  - » www.ed.gov/admins/lead/safety/emergencyplan/index.html
  - » www.fema.gov/kids/
  - » www.atf.gov/kids/index.htm
- Information on how to protect family www.ready.gov
- Safety checklist
- Communications information
- What "awareness" means
- Explain the Alert System
- How to help children cope with fear
- Safety issues
- Equipment and resource checklist
- Understand the Homeland Security Advisory System and its effect

Conclusion

As noted in a recent publication from the Office of Community Oriented Policing Services:

> For the past 20 years, community policing has encouraged law enforcement to partner with the community to proactively identify potential threats and create a climate of safety. Its emphasis on problem-solving has led to more effective means of addressing crime and social disorder problems. In the 21st century the community policing philosophy is well-positioned to take a central role in preventing and responding to terrorism and in efforts to reduce citizen fear.[28]

The prudent executive will explore these avenues as part of a comprehensive, community wide homeland security strategy. Because of the concern for terrorism and Islamic extremism, the need to embrace all elements of the community becomes an even higher priority. As noted by the Muslim Public Affairs Council: "Ultimately, U.S. counterterrorism efforts will require a partnership between policymakers and the American Muslim community…".[29]

[28] Scheider, Matthew, Robert Chapman, and Michael Seelman, "Connecting the Dots for a Proactive Approach." *Border and Transportation Security.* Washington, D.C.: Office of Community Oriented Policing Services, 2004. www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=245.

[29] Muslim Public Affairs Council. *A Review of U.S. Counterterrorism Policy: American Muslim Critique and Recommendations.* Washington, D.C.: Muslim Public Affairs Council, 2003, p. 8.

Chapter 6:

Developing and Implementing Intelligence-Led Policing

Developing and Implementing Intelligence-Led Policing

Chapter 5 established the concept and issues associated with Intelligence-Led Policing (ILP). Building on those concepts, this chapter will identify the processes and elements required to implement ILP in a state, local, and tribal law enforcement (SLTLE) agency. Because of the conceptual nature of ILP, it must be designed to meet the explicit needs of a given agency. This is complicated by the fact that there are a wide range of resource and environmental variables that will also influence implementation.

The important point to note is that there is not a single model of ILP that can be plugged into an agency. Rather, as will be seen, there are tools that can be used to identify the intelligence needs of an agency and then craft the policies and processes to make ILP functional for each department.

Essentially, intelligence is about managing information; specifically, the information that is needed to identify threats of concern to a community, and having sufficient information about the threat to develop operational responses to prevent or mitigate the threat. As depicted in Figure 6-1, this is a three phase-process as related to the integration of ILP into a law enforcement organization. The first phase examines the elements necessary for the information management process to be effective and it begins with developing the information management plan. The second phase is creating the organizational infrastructure to make the information management plan functional. The third phase is implementation. The following discussions address these three phases.

Figure 6-1:
Three Phases of ILP Development in an SLTLE Organization

Establishing a Framework for Strategic Priorities and Information Processing: The Information Management Plan

The information management framework is a business plan that guides a focused series of processes for the intelligence function. This plan identifies priority problems and institutionalizes a process for monitoring the problems through the application of seven critical components. A rudimentary approach is used in Table 6-1 to explain each component by indicating the kinds of questions each component is intended to answer and the organizational positions most likely to be responsible for answering the questions.

Table 6-1: Seven Components of the Information Management Plan

The Concept...	Asks the question…	Responsibility…
Strategic Priority	What problems are important to me?	Executive
Intelligence Requirements	What additional information do I need to better understand each problem, its causes, and its effects?	Executive, Commander, and Analyst
Collection Plan	Where (sources) and how (methods) will I get the additional information that I need to better understand the problem?	Commander and Analyst
Analysis	Collectively, what does the new information mean and what new insights does it provide about the problem?	Analyst with review by Supervisor
Intelligence Products	What actionable information do I need to tell other people in order to prevent or control the problem?	Analyst with Commander's Advice
Operational Responses	What explicit operational activities may be implemented to prevent or mitigate the priority problems? What resources are needed?	Intelligence and Operations Commanders
Process Review	From this process: • Was the information accurate and useful? • Could the problem be altered as a result of the information? • What will make the process better?	Intelligence and Operations Commanders with Feedback to Executive

Integrated within the information management plan is the Intelligence Process (discussed in Chapter 4). The six phases of the Intelligence Cycle operationalize the acquisition and processing of information needed for the intelligence function. The information management components collectively create the information management plan; the Intelligence Cycle is the mechanism for ensuring that information is collected, assessed, and processed in a manner that is scientific and consistent with accepted practice.

As illustrated in Figure 6-2, the Intelligence Process is a critically important subsystem of the information management plan. The current discussion, however, focuses on the essential components necessary develop and implement the plan. It lays the foundation for operationally responding to threats as well as providing a quality control mechanism for both information management and information processing.

Figure 6-2: Structure of the Information Management Plan

The Information Management Plan

The seven core components of the management plan integrate the intelligence function with all other agency responsibilities. It should be emphasized that these are management components, not functional components, per se. For example, the "analysis" component of the management plan focuses on the role analysis plays in information management. Conversely, the analysis phase of the Intelligence Process is focused on developing intelligence from raw data. The following discussions provide a brief description of each of the plan's components.

Establishing Strategic Priorities for Intelligence-Led Policing

Intelligence strategic priorities are the articulated criminal and terrorist threats that must be monitored and managed by a law enforcement agency in light of the impact these threats have on public safety and security. A strategic priority must be specified in the context of the local community and the law enforcement agency's intent to manage that priority.

Defining intelligence priorities can become a complex process because law enforcement organizations have a wide range of potential responsibilities ranging from traffic control to counterterrorism. Pragmatically, because of resource limitations, these different responsibilities cannot be treated equally. Each responsibility must be given a priority that will guide the allocation of resources and the amount of organizational effort that will be devoted to addressing it.

Even within each responsibility there will be additional prioritization. To use a familiar example, it is inescapable that virtually every SLTLE agency will have a strategic priority related to traffic control. Within the traffic control strategic priority there will be subpriorities such as these:

- Traffic accident investigation
- Driving under the influence enforcement
- Speed enforcement
- Vehicle registration and regulatory enforcement
- Parking enforcement.

This does not mean there will be no parking enforcement, but under normal circumstances parking enforcement may occur only when there is a complaint. Priorities can also change with circumstances. As an example, parking enforcement may be given a high priority when vehicles have to be moved from an emergency snow route or a hurricane evacuation route when warranted by the weather conditions. It is essential, therefore, that a law enforcement agency identify priorities within a dynamic framework that prescribes the conditions under which priorities will change and how the priority will be addressed (for example, parking enforcement only on the emergency routes but no attention to parking enforcement in commercial loading zones).

Strategic priorities are influenced by the systemic influence of several environmental factors. These include the following:

- Known public safety threats
- The seriousness of each threat
- Political priorities within a community
- Resources of the law enforcement agency
- Expertise of the law enforcement agency
- Special funding obligations (such as the conditions of a grant award or legislative mandates)
- Obligations in partnership agreements with other law enforcement agencies, public safety agencies, or the private sector
- Personal/professional priorities of the law enforcement executive.

These are legitimate factors because their effects on organizational prioritization are a product of an interactive balance among the factors. This process applies throughout the law enforcement organization, including intelligence.

Obviously, there are many different foci that ILP may address, particularly in light of the "all-crimes, all-threats, all-hazards" approach to intelligence. Important information must be gained by executives, both empirically and ideologically, that will help focus the prioritization process. In setting strategic priorities for ILP, the law enforcement executive may seek answers to a variety of questions, such as the following:

- ILP and the Overall Agency Mission
  - What is the priority of ILP in relation to the mission, responsibilities, and other strategic priorities of the law enforcement agency?
    - What proportion of the agency's work force will be exclusively dedicated to ILP?
    - What facility, equipment, supply, and service needs are required to support the various ILP full-time assignments?
    - What are the time and resource requirements to support personnel who devote a portion of their time to ILP (including training)?
- Threat-Related Assessment Factors
  - What known threats to public safety exist within the jurisdiction?
  - What threats may emerge?
  - What critical infrastructure is in the jurisdiction?
  - What key resources are in the jurisdiction?
  - What unique characteristics exist within the community that may heighten or aggravate either a criminal or homeland security threat? (For example, proximity to an international border, ports, refineries, geographic area that is disproportionately susceptible to natural disasters.)
  - What unique crime problems in the community need to be addressed? (For example, firearms violence, gangs, drug trafficking.)

- Administrative and Environmental Factors
  - What political mandates exist that are related to real or perceived threats that must be addressed?
  - What resources and expertise does the agency have or have access to that will support ILP? (For example, analysts, analytic software, fee-based information systems.)
  - What intelligence-related agreements has the agency entered into that obligates the agency and its resources? (For example, fusion center, Joint Terrorism Task Force, regional task forces.)
  - What obligations does the agency have to focus on specific intelligence-related initiatives, processes, and/or outcomes as a result of grants or special funding (such as a crime-control tax)?
- Executive Prerogatives
  - What personal and/or professional commitments and/or philosophies of the chief executive must be addressed in establishing strategic priorities?

The answers to these and other questions unique to the jurisdiction will provide the framework within which strategic priorities for ILP may be articulated and prioritized. The next phase is to operationalize the priorities. For example, assume that a law enforcement agency identified four ILP strategic priorities, in no particular order of importance, as the following:

1. Terrorism.
2. Homeland security.
3. Violence by firearms.
4. Gangs.

Within each of these priorities there will be a subset of priorities that must be operationally defined as they apply to the agency. For example, the FBI's definitions of international and domestic terrorism are as follows:

> International terrorism involves violent acts or acts dangerous to human life that are a violation of the criminal laws of the United States or any state, or that would be a criminal violation if committed within the jurisdiction of the United States or any state.
>
> Domestic terrorism is the unlawful use, or threatened use, of force or violence by a group or individual based and operating entirely within the United States or Puerto Rico without foreign direction committed against persons or property to intimidate or coerce a government, the civilian population, or any segment thereof in furtherance of political or social objectives.[1]

[1] Federal Bureau of Investigation. Counterterrorism Division. *Terrorism: 2002–2005*. Washington, D.C.: Federal Bureau of Investigation, undated, p. v.

While suiting the FBI's needs, these definitions are not likely to be as useful for a state, local, or tribal law enforcement agency that is defining its strategic priorities. Rather, an agency may use a more simplified definition to meet its needs; for example, the strategic priority of terrorism may be articulated simply as this:

- Terrorism[2]
  - Internationally affiliated terrorist groups
  - Individual radicals who support the ideology of internationally based terrorist groups
  - Right-wing criminal extremist
  - Environmental criminal extremists
  - Right-to-life criminal extremists.

With respect to the strategic priority of homeland security,[3] a state, local, or tribal law enforcement agency should define the priority within the context of unique characteristics of a jurisdiction. For example, the homeland security priority of an agency located near the U.S.-Mexico border may include strategic awareness of tuberculoses; a community where there is a high density of cattle raised for beef processing may include mad cow or hoof-and-mouth disease; an agricultural community that raises crops may focus on the accidental or intentional introduction of a communicable crop disease such as soybean rust. The significant point to note is that with the current all-hazards approach to homeland security intelligence, factors beyond the traditional expertise of law enforcement need to be explored when identifying threats (hazards) and defining strategic priorities for homeland security.

In light of the "all-crimes, all-threats, all-hazards" approach used in contemporary intelligence activities, the strategic priorities for intelligence will tend to be broader than was historically the case. Strategic priorities for the law enforcement agency will be defined throughout the organization and take many different forms (see Chapter Annex 6-1 for selected, and diverse, statements of strategic priorities from three law enforcement agencies). Specifically for ILP, an example of strategic priorities may be simply listed as illustrated in Table 6-2.

Within the framework of strategic priorities, an assessment must be made of what information is already known about the nature of each priority. Gaps in the information are then articulated as intelligence requirements.

[2] Note that each subcategory specifically includes the conditional modifier of "terrorist" or "criminal." This is an important factor because state, local, and tribal law enforcement agencies may collect and retain only information that identifies individuals and organizations where there is a criminal nexus, not just an extreme ideology.

[3] The reader should recall that homeland security intelligence deals with all hazards that have implications for law enforcement public safety and order maintenance functions.

Table 6-2: Examples of ILP Strategic Priorities

The Anytown Police Department's strategic priorities for Intelligence-Led Policing are:

- Terrorism
  - » Internationally affiliated terrorist groups
  - » Individual radicals who support the ideology of internationally based terrorist groups
  - » Right-wing criminal extremists
  - » Environmental criminal extremists
  - » Right-to-life criminal extremists
- Homeland Security
  - » Critical Infrastructure
    - ▪ Anytown water treatment plant
    - ▪ Anytown Naval Air Station
    - ▪ Anytown electrical substation
  - » Key Resources
    - ▪ FastCar Assembly Plant of Anytown
    - ▪ Anytown Grain Elevator Complex
    - ▪ GoodBeef Stockyards and Auction Barn
- Violence by Firearms
  - » Homicide by firearm
  - » Robbery by firearm
  - » Assault by firearm
- Gangs
  - » All criminal gang activity
- Organized crime activity
  - » Loan sharking
  - » Credit card fraud

Intelligence Requirements

While the use of intelligence requirements has been a long-standing practice of the Intelligence Community, it is a relatively new practice for law enforcement. Again, because of jurisdictional differences, requirements have slightly different applications for the law enforcement community.

Information that is missing but needed to understand a threat, target, or suspect is an "intelligence gap." Information that is identified to fill this gap is an "intelligence requirement." Requirements help administrators make decisions, and those decisions vary widely, such as these examples:

- Determining if a reasonable suspicion exists
- What resources to deploy
- Whether to prepare for a new threat
- Determining if a new target exists within a community
- Alternatives for preparing for a new threat or hazard
- Determining if new partnerships need to be developed to manage a change in the threat picture
- Determining if a new expertise needs to be developed to manage a threat
- Identifying new training personnel that an agency will need to deal with the changing threat picture.

The significant point to note is that requirements define the types of information that has to be collected to address the strategic priorities. Collecting information to fill the intelligence requirement requires a proactive deployment of resources. This may include open sources, law enforcement and intelligence information systems, human sources, undercover officers, patrol officers, informants, community partnerships, public-private partnerships, or the use of technical surveillance resources. These are articulated in the collection plan.

Collection Plan

The collection plan is a systematic procedure for gathering relevant information from all lawful sources that responds to intelligence requirements to produce an intelligence product. Usually the collection plan includes a specified time frame; although in the case of a standing intelligence requirement that time frame may be ongoing. The collection plan is related to the strategic priorities via the intelligence requirements by collecting targeted information about threats from both strategic and tactical perspectives. Some factors to be considered in the collection plan include the following:

- Is the requirement sufficiently clear to locate and identify the specific information that is needed?
- Have open sources been used as the "source of first resort"?
- Has any portion of the information already been collected in the form of tips, leads or Suspicious Activity Reports (SAR)?
- Do partnerships exist that can assist in responding to the intelligence requirement? (For example, private sector partnerships, the fusion center, community partnerships, and so forth.)

- If not available from open sources or previously collected information, what method(s) will be used to collect the information?
- What sources will be used to collect the information?
- What unique technological methods, if any, are needed to collect the information?
- Are there legal and/or administrative restrictions on collecting the information?
- Are there explicit notifications or approvals required for the collection of specific types of information?
- Can source validity and information reliability be accurately assessed? If not, other collection sources and methods should be explored.

Collected information is processed using the constructs of the Intelligence Cycle. As sufficient valid and reliable information is collected and analyzed, intelligence products are developed to monitor the strategic priorities and determine what, if any, operational responses are needed to address threats in each priority area.

Analysis

Raw data collected in accordance with the collection plan has little value until it has been analyzed. Relying on the scientific approach to problem solving, logical reasoning, and objective interpretation of data, the analytic process gives an integrated meaning to diverse individual pieces of information. Analysis establishes connections between the different data, cause and effect, and correlations of activities and behaviors. The new knowledge derived from analysis can provide insights into imminent and emerging threats, as well as potential intervention methods.

Certainly a goal of effective analysis is to ensure that the conclusions drawn from the process are "actionable"; that is, when the information from the analysis is given to operational units in the law enforcement agency, there is sufficient detail that enables the operational units to develop specific plans to prevent and/or mitigate threat. This actionable information is presented in a written form known as the intelligence products.

Intelligence Products

Intelligence products are the reports and delivery mechanisms that convey the findings of the analytic process. Ideally, an intelligence unit or fusion center will establish a menu of products that meet the specific needs of its various consumers. The products should have a consistent format and appearance (that is, a "brand") that will aid consumers in selecting the products most applicable to their responsibilities. For example, when a threat is identified and reported, managers will need different types of information than line officers will need. Situational awareness, a strategic assessment, and tactical indicators represent intelligence products that have a different focus on the same threat.

Each intelligence unit and fusion center will determine the types of intelligence products it will produce. Important, the products are the primary methods that the intelligence function will communicate with their customers. The overall

utility of the intelligence unit will be judged by the intelligence products it disseminates. The products must be of sufficient quality, substance, and utility that operational units of the agency are able to develop tactics and strategies to prevent threats from reaching fruition.

Ensuring that these characteristics are embodied in each intelligence product will maximize the utility of the product which, in turn, contributes to public safety and security.

Operational Responses

Identifying threats through the Intelligence Process is an important ingredient for public safety. Intelligence, however, is only part of the security equation: the critical next element is for operational commanders to develop intervention activities that will stop or mitigate the threat. Some of the operational responses will be fairly simple, such as providing indicators of the threat so that officers will be aware of them while carrying out their daily responsibilities. Other interventions may be more sophisticated such as using suppression tactics (saturation patrol, for example), proactive intervention (such as consistent car stops and field interviews of persons and their associates reasonably believed to part of the threat), target hardening, community education, development of a task force, and aggressive use of traditional investigative tactics that may serve to identify and apprehend offenders. It is important to note that operational units should rely on the intelligence function as a resource when developing intervention strategies. The analyst has the most comprehensive insight into the threat and may provide valuable feedback to operational planning.

Implementing operational responses inevitably requires the expenditure of resources. While resource allocation is part of the operational commander's responsibility when developing intervention methods, the intelligence function can assist in prioritizing and focusing strategies. This can translate to a more efficient use of resources.

Review of the Process

A final step of the information management plan is to review the process to establish what intelligence was developed and if any new gaps have emerged. It should ask such questions as these:

- Was the information or intelligence accurate?
  - Was the threat accurately identified?
  - Was the nature of the threat and its characteristics accurately identified?
- Was the target accurately identified?
  - Were the vulnerabilities of the target accurately identified?
- What was learned from victims, witnesses, offenders, and locations?
- Was there useable intelligence from any technical or surveillance activity?
- What was learned about intelligence gaps and is there information that can be collected on a standing basis to prevent future intelligence gaps?

- Did the threat change after the operational response? If so, why?
- Did the operational activity cause displacement which, in turn, will cause new threats to emerge in a different geographic area?
- What operational responses were used and are the threats vulnerable to the same approach in the future?
- Have new threats been identified or have new threats emerged?
- Were partner agencies (include private sector) involved in any aspect of collection or response?
    - What were the benefits?
    - What feedback have they provided?
    - What feedback have they received?
- What measures have been put in place to minimize the possibility of the threats arising again?[4]

The review is an important tool for evaluating the information management plan, Intelligence Process, operational responses, and the status of strategic priorities. Indeed, the review can also be critical for defining new intelligence requirements and reordering the priorities.

Summary

The information management plan is like a skeletal structure linking the components together. It serves as the framework to make the organizational components functional for ILP.

Organizational Infrastructure for ILP

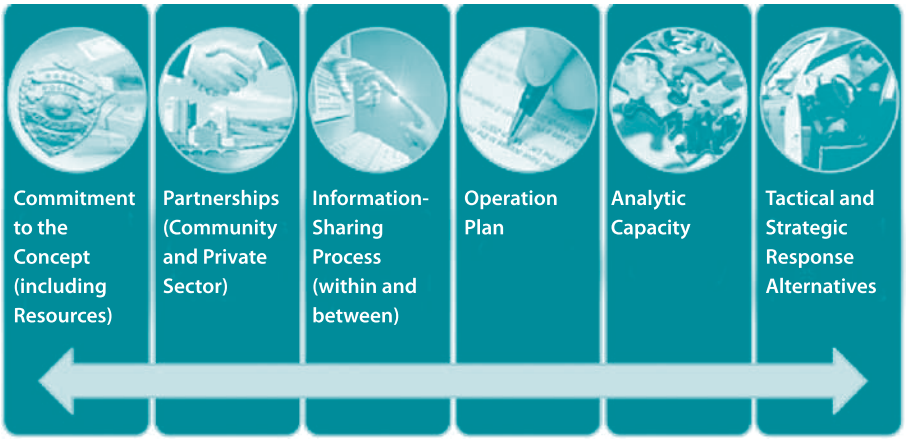
Before the ILP concept can be introduced into a law enforcement agency, a number of components (see Figure 6-3) must be developed, each of which complements the definition of ILP provided in Chapter 5. The complexity and detail of these ingredients vary widely between agencies, depending on such factors as these:

- Size of the agency
- Resources
- Demographics of the jurisdiction
- Location of the jurisdiction
- Character of the jurisdiction (industrial, commuter population, central city, suburb)
- Relationship with the community (supportive, conflictive, large undocumented population)
- Perspective on intelligence by elected officials and community leaders.

An assessment of these variables—many of which will be intuitive to the agency—will help guide the development of each ILP component.

[4] Based on: National Centre for Policing Excellence. *Guidance on the National Intelligence Model.* London, U.K.: Association of Chief Police Officers, 2005, p. 94.

Figure 6-3: Components of ILP



Commitment

The change to ILP must start with the chief executive because if the leadership of a law enforcement agency does not understand and buy in to the concept, it will never be functionally adopted. The law enforcement executive's commitment must be demonstrated through allocation of personnel and resources to develop and implement the concept. If agency personnel do not believe the leader is committed to the new program, implementation efforts will not be effective.

An excellent example of a leader's demonstration of commitment is seen in the following experience:

> When Dr. Gerry Williams was chief of police in Aurora, Colorado, in the late 1980s, he decided to implement community policing. There was a great deal of resistance, and he recognized the need to educate Aurora police personnel on the concept. He asked that a team from the National Center for Community Policing at Michigan State University prepare a 4-hour awareness program that would be mandatory for all Aurora police employees to attend on the change in policing philosophy. He also asked the team to offer the training at 12 different times throughout the day (over a 2-week period) that would cover every shift so all personnel would have the opportunity to attend the mandatory training on their regularly scheduled duty time. At each of the 12 sessions—whether offered in the middle of the night or the middle of the day—Chief Williams opened the training by making a firm statement that the movement to community policing was going to be the unquestioned policing philosophy to be used by the Aurora Police Department and that resources would be committed to ensure the change would take place. Chief Williams then sat down in the middle of the front row where everyone was certain to see him and sat through every one of the 12 sessions. It did not take long for the word to spread through the department that "the chief is serious about this" because he set other duties aside to attend the entirety of all the sessions. This was an important sign of commitment. Moreover, the chief answered questions during the sessions and interacted with officers on the breaks to reinforce his commitment.

Commitment begins with the chief executive's true understanding of the concept. In some cases, this has occurred after the chief executive has attended a training program developed exclusively from the executive's perspective (such as the BJA program, "Criminal Intelligence for the Chief Executive"). A program such as this provides fundamental concepts that show the value of intelligence, demonstrates how intelligence integrates with the department's overall mission, and permits the chief to interact with others who may not only provide reciprocal support but also may permit an exchange of ideas on how ILP may be used.

The chief executive should also formally articulate his or her support of the concept in a policy statement. The policy statement provides the organizational parameters of ILP and gives all members of the agency a tangible reference point for understanding how ILP is to be implemented and used.

Perhaps the best symbol of commitment is the dedication of resources to ILP. Training agency personnel, assigning them to the intelligence function, and dedicating funding to the development and execution of ILP sends a strong message to agency personnel about the executive's commitment.

It is also critically important to gain commitment to the concept from commanders and managers because they are responsible for the actual execution of ILP. If commanders and managers have neither a clear understanding of how ILP can benefit the agency nor of their ILP responsibilities for directing personnel under their command, full implementation will not occur, regardless of the chief executive's support. In all types of organizations, there have been instances in the management process in which middle managers have defeated a new initiative simply by not thoroughly ensuring that personnel under their command perform the duties necessary to make the initiative work. This reflects an old adage in management: "Managers may not be able to turn the water on, but they can easily turn it off."

Component 1—Key Takeaways

- The chief executive must understand and support the concept of ILP:
  - How ILP fits into the department's mission
  - Articulated commitment to the concept
- Commitment of people and resources:
  - Training
  - Infrastructure development
- Commitment must extend throughout the chain of command

Partnerships

Effective ILP requires the development of a range of partnerships. There are good examples of this in the counterterrorism area (such as the Terrorism Early Warning Groups) as well as the precedent established in community policing. The range of partnerships includes the private sector, nonlaw enforcement government service, and the community. Each can be an important source of information for the intelligence process. The fundamental rationale for public-private partnerships

is based on the fact that when more people know what to observe and how to report it to law enforcement, the greater the probability of collecting information that may be used to stop a terrorist attack or criminal enterprise.

There is a precedent of success for including community members as part of the information-collection process, as seen in programs used by the Turkish National Police, Israeli Police, and the London Metropolitan Police. Each has developed programs aimed at the community to report specific types of information—essentially, "intelligence requirements"—to the police to aid in preventing terrorism. Certainly, if community partnerships are effective in these diverse cultures, they can be effective in the United States. Moreover, public-private partnerships are a simple extension of many current programs used throughout the United States that deal with crime, ranging from Neighborhood Watch to Volunteers in Police Service.

One question that emerges is whether the average community member is interested in participating in ILP programs. A pilot program offered by the Regional Community Policing Institute at Wichita State University extended an open invitation to local residents in Wichita, Manhattan, and Topeka, Kansas, to attend a public awareness session on citizen reporting of suspicious activities possibly related to terrorism. More than 600 people attended the sessions in the heartland because of their concern about the threat and their desire to contribute to counterterrorism initiatives.

Engaging the community can significantly increase the information-collection parameters for the intelligence process. Several key factors make these partnerships work effectively for ILP.

- The law enforcement agency must establish trusted relationships with people through local law enforcement officers. Typically, a "meet and greet" alone will not suffice. Information that may be sensitive, confidential, or even fearful may need to be exchanged. As a lesson learned from community policing, the bond of trust established through an ongoing dialog becomes a critical element.
- Once trust is established, an effective means of two-way communication must be established with each individual. In some cases, this may be technological, such as e-mail or telephone. In other cases, individuals may feel comfortable sharing the information only on a one-to-one basis with their trusted law enforcement partner.
- Just as with officers, training—or public awareness—about the signs and symbols of terrorism and organized crime is important for enabling the partner to identify substantive information that should be reported. For example, a community partner may see a symbol, tattoo, or foreign word that is symbolic of a terrorist or criminal entity, but if he or she has not been trained to recognize these symbols, the information will not be reported. Similarly, community and private partners should receive information about behaviors that are unusual and which suggest criminality in order to enhance their specific awareness.[5]

[5] A good example of behaviors is found in the Michigan State Police video, *Seven Signs of Terrorism,* which is available for public distribution. www.michigan.gov/msp/0,1607,7-123-1564-155763--,00.html.

- Partner training should also include instruction on the type of information that should be documented for reporting to law enforcement. While documentation of behaviors, evidence, vehicles, and personal descriptions are second nature to law enforcement officers, it is not a customary practice for nonlaw enforcement personnel. Explaining what kinds of information should be reported—along with date, time, and location—is an important element in partner training.
- The agency should develop a policy and process to protect the privacy and safety of community partners. As will be discussed in detail in a subsequent chapter, there should be a privacy policy to protect business partners' proprietary information that may need to be disclosed during the information-sharing process. Partners need to be informed of these policies in order to reinforce the trusted relationship.

Illustrations of Partnerships in Other Countries

Israel. During the height of the Al-Aqsa Intifada, the Israeli Police sought alternative methods for gaining information about planned terrorist attacks. One technique was to establish community partnership patrols that worked with the residential Palestinian population is such cities as Tel Aviv and Jerusalem. The Israeli community partnership officers developed trusted, often confidential, relationships with many Palestinian citizens in these cities with the expressed intent to gain information or indicators about possible terrorist attacks. The motives of the Palestinians were quite simple: Many of the Palestinians who worked and resided in Israeli cities had been victims of terrorists' attacks alongside the Israeli victims.

Turkey. After a series of terrorists attacks in Istanbul in November 2003, the Turkish National Police (TNP) interviewed captured terrorists to learn how they were recruited into the PKK (Kurdistan Workers' Party) and the Turkish al-Qaida. It was learned many were recruited in high school and often initially participated with the group out of social pressure rather than commitment to the group's cause. As a result, the TNP began outreach and education programs in the high schools both to dissuade young people from joining these groups and to gain information that could be used in the intelligence process.

A number of good partnerships have emerged, notably in larger law enforcement agencies. The New York (City) Police Department's SHIELD[6] is a comprehensive information-sharing and public information program. The Delaware Information Analysis Center[7] has established formal relationships with nonlaw enforcement government organizations and targeted private-sector entities for information sharing over the secure Automated Trusted Information Exchange network. The Nassau County (New York) Police Department created the Security/Police Information Network as a comprehensive public-private information-sharing network that is stratified by sectors and divided between vetted and nonvetted information-sharing partners using e-mail and periodic meetings. There are certainly other examples, but the point is clear: Partnerships are critical, there are models to provide guidance, and partnerships must be established throughout America's communities, not just in major metropolitan areas.

[6] See www.nypdshield.org.

[7] See dsp.delaware.gov/Intelligence.shtml.

As may be expected, the development process and expected outputs differ somewhat between community partners and private sector partners

Community Partnerships

Just as with any other crime or community problem, it is important to enlist the support of the community. In the intelligence arena, two factors make community partnerships more challenging. First, the agency is concerned about threats, and second, many community members are uncomfortable with the intelligence role in law enforcement. On the issue of threats, it is insufficient to simply tell citizens to be aware of suspicious activities. More guidance is needed. In many instances, citizens have reported something to this effect: "A man who looks like he's from a Middle-Eastern country is taking a picture of a bridge." In such cases, whether intentional or not, citizens are often falling prey to a stereotype. Beyond this factor, there is virtually no value to such information alone. Citizens need to be given guidance about looking at behaviors that are suspicious and instruction on how to document those behaviors when reporting the information to a law enforcement agency. This reduces the possibility of stereotyping people and provides more valuable information to the law enforcement agency.

With respect to the intelligence role, many people have expressed concern that forming community partnerships for intelligence is akin to turning citizens into informants on their neighbors. This belief goes hand in hand with the belief that many people hold that law enforcement agencies are collecting as much information as possible on all citizens—or at least on citizens who do not share "law enforcement beliefs." Many individuals assume that intelligence activities routinely violate citizens' privacy and civil rights. The challenge is to educate skeptics about the process and the importance of citizen involvement in ILP simply because citizens are often in a place to observe suspicious behaviors more often than are law enforcement officers. The notion of citizen participation goes back to one of the most fundamental principles of modern law enforcement articulated by Sir Robert Peel in developing the London Metropolitan Police in 1829: "The police are the public and the public are the police."

As noted previously, training sessions for citizens can be quite helpful in this process. In a number of communities, both in the United States and abroad, citizen training programs have resulted in reasonable degrees of success. The programs should tell citizens 1. What to look for, 2. What kind of information they should document, and 3. How to report the information to a law enforcement officer or agency.[8] Providing such information increases efficiency and decreases the possibility of stereotyping.

Component 2a—Key Takeaways

- Enlist community support
- Establish trusted lines of communication with community members
- Provide community training so community members will recognize the signs and symbols of terrorism, crime, and other threats facing the community
- Tell the community what kinds of information are needed by the agency
- Tell the community how to report information

[8] Chapter Annex 6-1 is a community handout used by the Wichita State University Regional Community Policing Institute to emphasize these points.

Public-Private Partnerships

Public-private partnerships are more structured than community partnerships. While all businesses are subject to partnerships, those that are prone to threats (in light of specific threats that are identified in a region) should be given the highest priority. The private sector has a great deal to offer in information sharing—many have global contacts and communications systems that can also be of value to a law enforcement agency. Whether it is the use of delivery persons who can be alert to suspicious behaviors, security personnel at corporate facilities, or salespersons who can be aware of unusual or suspicious purchases, the value of raw information exchanged with the private sector can be robust.

In some cases, a law enforcement agency may develop an intelligence liaison contact with a company to serve as the primary two-way point of contact between the company and the law enforcement agency. Such a partnership will increase the efficiency and effectiveness of the information-sharing process. As with community partnerships, the law enforcement agency will need to train appropriate company personnel and in some cases, special training may be provided that is unique to a given corporate sector. This is conceptually similar to the terrorism early warning (TEW) group concept that has been instituted in many communities throughout the United States.[9] Given that law enforcement intelligence focuses on all crimes and all threats, the intelligence liaison contact will be concerned with threats broader than terrorism.

When law enforcement agencies work more closely and have more detailed information exchanges with the private sector, two issues of particular importance must be addressed. The first is protection of citizens' privacy. Instances occur in which a citizen's or lawful U.S. resident's identity may be provided to the private sector, for example, between law enforcement agencies and the airline industry. While there are bona fide reasons for providing information about individuals, care must be taken to ensure accuracy of the information provided and protect the individuals' privacy. The second issue is protecting the proprietary information of companies. In some instances, a company may provide information about its products or business processes to a law enforcement agency as a means of identifying and mitigating threats. It is incumbent on the law enforcement agency to ensure that any such proprietary information is protected.

Component 2b—Key Takeaways

- Enlist support of the private sector:
    - Give priority to threat-prone sectors, particularly in light of regional threats
- Create an intelligence liaison contact
- Provide training to recognize the signs and symbols of terrorism, crime, and other threats that may be encountered
- Tell the partners the types of information the agency needs
- Protect citizens' privacy
- Protect proprietary information

[9] A wide range of information on TEW groups may be found by using the search utility on www.llis.gov.

Information-Sharing Processes

The heart of effective intelligence is the capture and sharing of critical raw information. It is logical that each law enforcement agency must develop an effective mechanism to record and manage this array of information that is distinct from or segregated from other records in the agency's records management system. This mechanism will have a significantly different structure between law enforcement agencies, depending on the agency's size and resources. Despite these differences, a number of questions must be answered when developing an intelligence or sensitive information records capability in a U.S. law enforcement agency. Among these are the following:

- Where and how will this information be stored? It should be noted there are still agencies in American law enforcement that, because of their small size and rural—sometimes remote—locations, do not have networking capabilities. Some still operate with paper records, photocopies, and faxes.
- How will SARs, tips, and leads be assessed, managed, and stored?
- How will source reliability and information validity be evaluated?
- How will overall accuracy of information (including the documentation trail) be ensured?
- Who has the authority to enter information into the system, and how will entries be audited?
- How will the information be secured?
- Who will have access to the information, and under what circumstances is access permitted?
- Is the records system meant for raw information storage or for criminal intelligence records? If the latter, a 28 CFR Part 23-compliant policy should be developed.
- What are the information-sharing rules, and who makes the dissemination decisions?
- Have adequate measures been taken for security of information?
- For electronic systems, are data compatibility standards in place? Are data standards consistent with the Global Justice Extensible Markup Language Data Model[10] and the National Information Exchange Model?[11]

While each question could be discussed at length, for the current discussion it must be recognized that all of these issues must be addressed as part of building an ILP structure. For large agencies, these issues typically have been resolved, but for the majority of law enforcement agencies, many of which have only a few police officers, this is new ground. Yet if they are expected to collect raw information for the fusion centers and the Information Sharing Environment (ISE), the questions must be addressed.

Finally, as a result of articulated national standards and precedence in civil law, every agency that develops a criminal intelligence records system should ensure that it meets accepted regulatory and legal standards.[12]

Component 3—Key Takeaways

- Explicit processes and policies must be developed to ensure that the right information is disseminated to the personnel who need it
- Ensure that information-sharing mechanisms are two-way
- Policies must address both intra- and extradepartmental processes

[10] See it.ojp.gov.

[11] See www.niem.gov.

[12] In particular, the records system should be 28 CFR Part 23-compliant and a privacy policy should be in place. See it.ojp.gov/privacy/206/28CFR_Part_23.PDF and it.ojp.gov/default.aspx?area=privacy&page=1260, respectively.

Operational Plan

Most law enforcement agencies have an operational plan in place that includes a mission statement, goals, objectives, and a system of directives. Many of these elements apply directly to ILP without any change; for example, standards of personnel conduct or officer safety guidelines apply uniformly. Elements of a departmental operational plan, however, typically are directed toward criminal investigation and apprehension. Consequently, the ILP operational plan must deal with the operational components of managing threats. The goals and objectives of ILP should be clearly articulated. Operational differences between intelligence and investigations should be spelled out, as should the relationship of ILP to the agency's criminal apprehension mission. Even such issues as personnel evaluation will differ in ILP compared with traditional performance measures.

The operational plan is the road map to executing ILP as an agency strategy.

Component 4—Key Takeaways

- The *National Criminal Intelligence Sharing Plan* states, "For *Intelligence-Led Policing* to be effective, the process must be an integral part of an agency's philosophy, policies, and strategies and must also be integral in the organization's mission and goals" (p. 7)
- Each element of the agency's operational plan should be coordinated to include the ILP mission
- An ILP operational plan should be developed to guide the agency's intelligence activities

Analytic Capability

Without analysis, there is no intelligence; however, most American law enforcement agencies do not have an analyst because they simply do not have the budget. In addition, political and collective bargaining implications often need to be addressed if a chief executive explores the hiring of an analyst. On the political side, it is often difficult for lay citizens—including city council members—to understand why funding should be allocated in a small law enforcement agency for an analyst when there is an increase in crime. Unfortunately, in many communities, it would be more difficult to add a police employee who was a nonsworn analyst than to add another sworn officer. Furthermore, in states where there is mandatory collective bargaining, such as Michigan, it is difficult to add positions that are law enforcement-related without either obtaining concessions from the collective bargaining unit or a renegotiated collective bargaining agreement.[13] As a result, many agencies need to explore options for developing an analytic capability. An agreement with the fusion center, a shared analyst between agencies, the use of volunteer analysts, or the use of college interns as analysts are among the alternatives that an agency may use to develop an analysis capability.

While not perfect, creative options may be the only recourse; for example, a fundamental analysis performed by officers may be the only alternative. There is precedent for this with officers using problem analysis as part of problem-oriented policing. The Center for Problem-Oriented Policing[14] offers a downloadable model

[13] The strength of collective bargaining units and contents of collective bargaining agreements vary widely, even in states with binding arbitration. As a result, each collective bargaining agreement must be examined separately.

[14] www.popcenter.org

problem-oriented policing curriculum that provides instruction on analysis. While not designed for ILP, it can assist in developing the analytic skills that officers need for threat analysis.

The point to note is that rather than relying on intuition, agencies should use an objective assessment of facts to provide a stronger foundation for ILP.

Component 5—Key Takeaways

- Analysis is the key to effective intelligence:
  - Of necessity, the analytic capability of agencies varies widely, ranging from sophisticated to simple
- Sometimes the analytic process is similar to the basic analysis individual officers do in problem-oriented policing
- An important element is to develop the analytic mindset

Tactical and Strategic Response Alternatives

The distinction between tactical and strategic analysis was discussed earlier. Developing response alternatives to criminal threats represents a different way of thinking about crime. The FBI Counterterrorism Division, for example, historically worked cases with the intent of making an arrest as soon as probable cause was developed. The intelligence-led approach now used in FBI counterterrorism is to gain as much information as possible about all investigative targets rather than making immediate arrests. One approach may be to "turn" a target to become an informant, permitting the informant to continue to operate. In other cases, a target may remain under constant surveillance, despite the presence of probable cause, so that the agency can identify as many associates as possible, as well as understand the way the targets communicate, finance, and generally operate their enterprise, with the goal of disrupting the criminal organization. While many of these targets will eventually be arrested—as is often the case in ILP—arrest is not the only goal. Rather, an important goal is to dismantle the criminal organization to eliminate the threat. As noted by Ratcliffe and Guidetti,

> Intelligence-led policing is a conceptual framework for conducting the business of policing. It is not a tactic in the way saturation patrolling is, nor is it a crime-reduction strategy in the way situational crime prevention is. Rather, it is a business model (John and Maguire, 2003) and an information-organizing process that allows police agencies to better understand their crime problems and take a measure of the resources available to be able to decide on an enforcement tactic or prevention strategy best designed to control crime.[15]

Component 6—Key Takeaways

- Unlike operational activities used to suppress crime or apprehend offenders, new tactics must be used to deal with threats
- Instead of immediately arresting criminal suspects, the agency may monitor the suspects' behavior for further intelligence value
- Depending on the nature of threats, creative new initiatives need to be developed to prevent threats; often this may not involve arrests

[15] Ratcliffe, J.H. and R. Guidetti. "State Police Investigative Structure and the Adoption of Intelligence-Led Policing." *Policing: An International Journal of Police Strategies and Management,* 2007. www.jratcliffe.net, under research publications, "State Police Investigative Structure and the Adoption of Intelligence-Led Policing"

Next Steps: Implementation

Often, agencies will ask for a template on how to implement ILP. The fact is that there is no universal template. Rather, each agency must examine the ILP philosophy and critical components, design an implementation scheme in light of the needs, resources, and articulated goals, and tailor the practice of ILP to those requirements. The implementation process is an exercise in organizational change to place the components "in action."

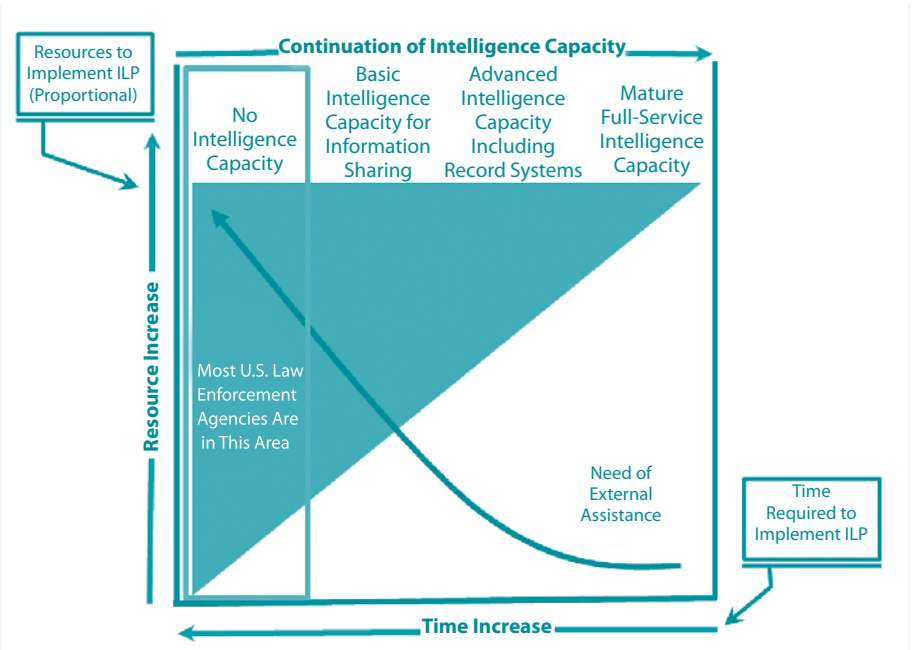
Self-Assessment of the Agency's Intelligence Capacity

In examining the intelligence capabilities of American law enforcement agencies, the author developed a four-point qualitative scale to describe the intelligence capacity based on policies, expertise, and information sharing capabilities.[16] As illustrated in Figure 6-4, the categories are as follows:

- No Intelligence Capacity
- Basic Intelligence Capacity for Information Sharing
- Advanced Intelligence Capacity Including Records Systems
- Mature Full-Service Intelligence Capacity.

While information sharing and connectivity have increased in recent years, most American law enforcement agencies have a minimal intelligence capacity. Time and resources—including specialized expertise—are needed to develop the infrastructure and knowledge within the agency to enable the agency to have a functional intelligence operation. Resources and external assistance include assistance with policy development, training, access to critical information systems, and other infrastructure components.

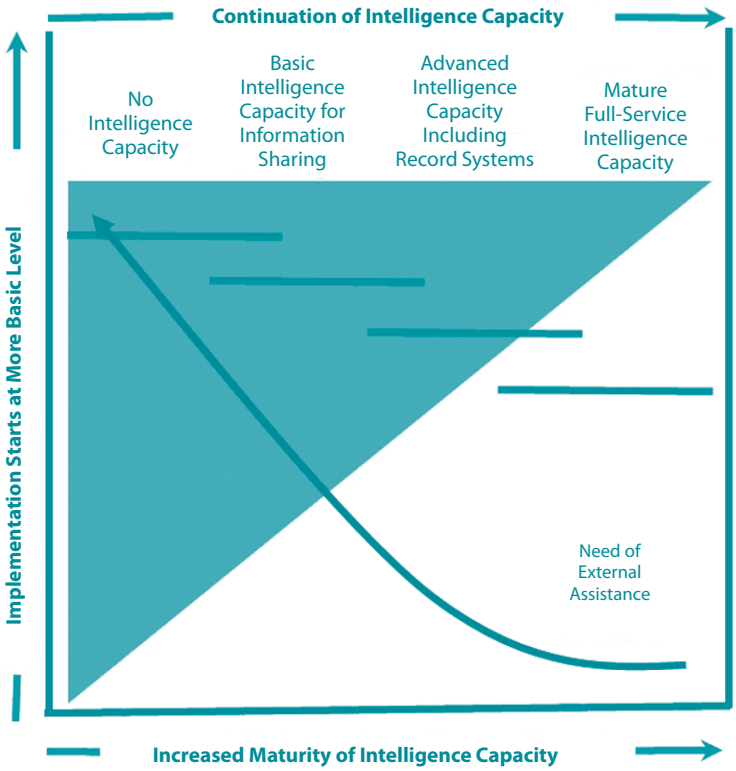
Figure 6-4: ILP Continuum of Variables



[16] As part of Department of Homeland Security-funded intelligence training programs, the author and his colleagues developed a comprehensive self-assessment tool that measures organizational variables across seven dimensions, providing a refined measurement of a law enforcement agency's ILP capacity. Agencies can access this self-assessment at no cost by enrolling in the training. For more details about the training, see intellprogram.msu.edu.

The categories describing the intelligence capacity are not dichotomous, but exist on a continuum. That is, depending on the operational characteristics of the agency's intelligence function, the intelligence capacity will be somewhere on a continuum within that category (see Figure 6-5). As might be expected, the lower on the continuum, the greater the need for external assistance and resources to develop the capacity to a level that is needed for the agency

Figure 6-5: ILP Subcontinuums of Variables



In determining the level of the intelligence capacity, and the place to start for developing or reengineering the intelligence function, a law enforcement agency must conduct a self-assessment of critical variables. Table 6-3 illustrates the operational characteristics that describe the four levels. Below each operational characteristic are action steps that should be taken to at least maintain the current level or move forward.

Certainly the "operational characteristics" and the "action steps" are not absolutes for determining a law enforcement agency's intelligence capability. Rather, they represent important milestones that can be identified and assessed in the implementation process.

The Implementation Starting Point

Any new initiative must have a starting point that provides an accurate picture of the organization's current state of knowledge and capabilities. In the United Kingdom, when the National Intelligence Model was introduced to the provincial constabularies, the starting point was fairly unified across all police forces with a strong foundation, given their history. In the United States, the starting point is at a significantly more fundamental level. To determine this starting point, several questions must be answered in each law enforcement organization:

- What is the knowledge level of the chief executive and command staff regarding the current philosophy and practice of law enforcement intelligence, including ILP?
- Is there an intelligence unit or intelligence capacity in the law enforcement agency?
  - Does the current intelligence capacity operate in a manner consistent with current practice, including the NCISP and the Minimum Standards set by the Counterterrorism Training Coordination Working Group?[17]
  - Has the current intelligence capacity developed a privacy policy?
  - What processes have been addressed and considered in extending the current intelligence capacity to ILP?
  - Is the law enforcement agency accredited by the Commission on Accreditation for Law Enforcement Agencies (CALEA)? If so, what compliance commitments and policies have been put in place to meet the CALEA standard for intelligence?
- What is the level of general awareness and knowledge of all law enforcement personnel concerning law enforcement intelligence?
- What internal resources are available to assist in developing and implementing ILP?
- What external resources are available to assist in developing and implementing ILP?
- Has the law enforcement agency established a particular relationship and/or processes related to the state or regional fusion centers?
  - Does the agency have someone assigned full- or part-time to a fusion center?
- Are there particular obstacles or challenges that must be resolved before implementing ILP?[18]

The intent of these questions is to collectively establish a profile of the agency's intelligence capacity, if any, so that the law enforcement agency has a clear picture of its starting point. This assessment will help guide the agency toward the next step in the implementation process.

As noted previously, a critical tool for socialization is providing fundamental knowledge to personnel. The need for training cannot be overemphasized, particularly awareness training for line personnel. New policies and procedures will have little meaning if personnel do not understand the concepts. Once again, the vast majority of America's uniformed law enforcement officers simply are unaware of the intelligence process and their role in it because our pre-9/11

[17] www.it.ojp.gov/documents/criminal_intel_training_standards.pdf

[18] These can be wide-ranging. For example, some agencies that operate under binding collective bargaining may have to resolve duty changes and training in a new collective bargaining agreement. Another example is that in some localities, the city council has forbidden a law enforcement agency from developing an intelligence capacity because of privacy and civil rights concerns. In yet other agencies that are operating under an intelligence-related court order or consent decree, changes may need to be made in the order prior to developing and implementing ILP.

Table 6-3: Organizational Self-Assessment Factors of an Intelligence-Led Policing Capacity

No Intelligence Capacity	Basic Intelligence Capacity for Information Sharing	Advanced Intelligence Capacity Including Intelligence Records Systems	Mature Full-Service Intelligence Capacity
Operational Characteristics: • No systematic intelligence training has been provided to personnel. • No intelligence policy or procedures. • No connectivity to intelligence records systems. • No systematic intelligence initiatives in the agency beyond sharing some intelligence products received from FBI, Department of Homeland Security, fusion center, etc.	**Operational Characteristics:** • Limited intelligence training, typically an investigator. • Generic intelligence policy. • No criminal intelligence records system. • No or minimal connectivity to intelligence records systems. • Intelligence activity limited to an individual or two identifying and sharing intelligence products and some BOLOs (be on the lookout).	**Operational Characteristics:** • One or two criminal intelligence analysts. • A formal criminal intelligence records system. • Connectivity to RISS.net (Regional Information Sharing System), LEO and/or LEIU (Law Enforcement Intelligence Unit).	**Operational Characteristics:** • Multiple analysts • Multisource connectivity • Advanced analyst training • Comprehensive records system
Action Steps: • Develop intelligence capacity as per *National Criminal Intelligence Sharing Plan* (NCISP) standards • Awareness training for all agency personnel as per the Minimum Criminal Intelligence Training Standards for United States Law Enforcement and Other Criminal Justice Agencies (Minimum Standards) • Develop operational plan • Establish logistics to receive and store Controlled Unclassified Information (CUI) • Develop privacy policy • Designate intelligence liaison officer (ILO) for fusion center • Establish community partnerships • Establish connectivity with RISS.net and/or Law Enforcement Online (LEO)	**Action Steps:** • Review policies related to intelligence operational plan • Awareness training for all agency personnel as per the Minimum Standards • Establish public-private partnerships • Establish community partnerships • Ensure that CUI meets security standards • Ensure that privacy policy is in place or create one • Establish an ILO	**Action Steps:** • Ensure that intelligence records are 28 CFR Part 23-compliant • Write/review privacy policy for consistency with ISE guidelines • Ensure that all officers have received intelligence awareness training • Review operational plan as per the NCISP • Ensure that analyst training is compliant with the Minimum Standards • Identify a fusion center liaison • RISS, LEO, and LEIU memberships • Community partnerships established • Public-private partnerships established	**Action Steps:** • Ensure that all processes are NCISP-compliant • Advanced analyst training • ILO training program • Fusion center liaison • RISS, LEO and LEIU Memberships • Community partnerships established • Public-private partnerships established • Review privacy policy with ISE guideline
Assumption for all four categories: The Global Intelligence Working Group and ISE standards and guidelines are sufficiently new that most agencies have not fully addressed the standards, if at all.			

philosophy that intelligence was to have very limited information sharing for operational security purposes. The paradigm has shifted dramatically, and local American law enforcement has a significant learning curve ahead of it.

When a commitment has been made to implement ILP, one of the top priorities is to provide training at two cognitive levels.[19] The first is awareness, which in reality, is more like education than training because the intent is to understand the concept of intelligence, how it works, and how it will contribute to the law enforcement mission. The second level is the development of skills and applications of intelligence, such as information collection, reporting processes, and proper use of intelligence reports. Beyond the cognitive-level training, there must be training that is explicitly directed to the different organizational levels and assignments within an agency that need the knowledge and skills to effectively perform in the ISE. The Minimum Standards provide the critical foundation content that is needed in any of these training initiatives. Moreover, the flexibility inherent in the Minimum Standards permits each agency to tailor the training program to its particular needs.

Change is a difficult process that most people initially resist; therefore, an early step in the process to introduce ILP is to overcome this resistance or dogmatism. The most effective way to accomplish this is by developing an understanding of ILP and demonstrating the benefits the change will produce for the individual and the organization. In a nutshell, people at all levels of the organization must be sold on the new concept—in this case, ILP. Changing attitudes, values, and beliefs—that is, resocializing people—is a difficult process requiring proactive initiatives, vigilance, patience, and the recognition that some people will never accept the change.

One of the key methods to help the socialization process is to demonstrate commitment and allocate resources to ILP.

With the resocialization process under way in a law enforcement agency, an operational plan must be developed that articulates the mission and processes of the agency's intelligence capacity. Indeed, the first recommendation of the *National Criminal Intelligence Sharing Plan* addresses the need for an intelligence infrastructure for all American law enforcement agencies regardless of size.[20] Once again, the operational plan will be unique to each agency. While there are certain components that can be modeled, the vast differences between agencies minimize the ability to use a true model operational plan. Instead, assistance should be provided in the process of developing an operational plan that meets the needs and capabilities of each SLTLE agency.

After training has been provided and the operational plan developed and disseminated throughout the agency, the plan should be implemented through a formal notification to all personnel. Regardless of the level of planning, some aspects of the plan simply will not work. The need to obtain feedback from personnel to determine what works and what does not is essential. Plans that do not work should not be viewed as failures but as part of the fine-tuning process to make the plan work as effectively as possible.

[19] Government-sponsored or -endorsed intelligence training can be found on the Intelligence Master Training Calendar at www.ncirc.gov.

[20] Global Intelligence Working Group. *National Criminal Intelligence Sharing Plan. Recommendation 1.* Washington, D.C.: Office of Justice Programs, 2003, page v.

Finally, an important, yet often overlooked tool for effective ILP is a performance evaluation system that recognizes and rewards those individuals who are practicing ILP, as well as a performance assessment of the entire ILP initiative.

If a traditional evaluation system for assessing individual performance is in place that is based purely on quantitative variables—number of citations issued, number of reports written, number of arrests made, number of calls answered, and so forth—then the largely qualitative character of an officer's activities will not be considered in the performance evaluation system. Employees know that organizational success is inextricably tied to the evaluation process; therefore, if success in ILP is going to be achieved, there must be a personnel assessment system that values the practice.

Similarly, the agency's overall success in effectively implementing ILP must be measured, as well. Goals from the operational plan should be stated in a measurable form so that ongoing assessments may adjust the components and modify implementation as necessary to ensure efficient and effective practice of ILP.[21]

Conclusion

A theme that has permeated this discussion is that the introduction of ILP is an exercise in organizational change—a process that is always difficult. While important lessons can be learned from the British National Intelligence Model as well as from other countries that have experimented with ILP, such as Australia, American law enforcement agencies have a significantly different experiential and structural demography that prevents a comprehensive adoption of the model at this point. Most law enforcement agencies in the United States are just beginning to enter the intelligence arena and, therefore, the introduction of ILP must start at a basic level.

In summary, as agencies begin to introduce ILP, a number of important lessons from the organizational change process can help guide this transformation:[22]

- There must be a stimulus for change. There must be a leader with a vision willing to take the first step in challenging the status quo—a change agent. Important, this stimulus must be ongoing and widespread. Given this, a change agent must address two significant elements: 1. vigilance in effort and 2. diversity in focus.
- There must be administrative commitment. The effective administrator must provide ongoing support for a new initiative or program; that is, provide consistency between what is said and what is done. If administrators are not willing to try such things as reallocation of resources, amending policies and procedures, or experimenting with new ideas, then there is little reason to believe the sincerity of their pronouncements. If commitment is not shown to either employees or politicians, the probability for success will be reduced significantly.

[21] One method for monitoring implementation status and success is to use the ILP Self-Assessment Tool prepared as part of the Michigan State University (MSU) "Sustaining Intelligence" training program funded by the U.S. Department of Homeland Security. More information on this tool may be obtained by contacting the MSU School of Criminal Justice Intelligence Program – intellprogram.msu.edu.

[22] Modified from: Carter, David L. *The Police and Community. 7th ed.* Upper Saddle River, New Jersey: Prentice Hall, 2002, chapter 9.

- Any change must be grounded in logical and defensible criteria. While it is somewhat of a cliché, it is worth noting that changing to simply shake up the organization would be dysfunctional rather than productive. If politicians and employees are going to tie their professional fortunes to change, they must be given good evidence to support the change. Moreover, since change consumes resources, it is wasteful to pursue it unless this change is well-grounded in logic and evidence.
- People at all levels must be able to provide input. For a new endeavor, the importance of team-building cannot be understated. Any initiative must have participation from as many people as possible. Not only will this diverse input provide new insights, but team-building provides ownership and, hence, a sense of investment and responsibility by members of the team.
- There must be sufficient time for experimentation, evaluation, and fine-tuning of any new program or idea. When a new initiative is started, it will inherently contain bugs because not every malady or problem can be anticipated, and some ideas will not work as originally conceived. Just because operational problems arise, it does not mean the idea was bad. Administrators, politicians, and employees must be flexible, adjusting their activities until there has been sufficient time to actually evaluate the initiative's true effects.
- Before change is introduced, the plan must be communicated to all persons and their support must be enlisted. Politicians, citizens, and employees alike must understand clearly what is being done and why. There is a tendency to assume that everyone knows and understands the issues of a new endeavor to the same extent as those who are immersed in the planning. Lack of communication is something that can destroy a new activity but, fortunately, is fairly easy to avoid. Remember that communication is more than sending messages; it also involves gaining feedback from the messages. Be cognizant of the issue, recalling the admonishment, "Don't leave people in the dark."
- Change takes time in order to have an effect; major change may take a generation. Americans are generally a short-term and impatient culture. When implementing major organizational and behavioral change such as ILP, a key ingredient is resocialization of employees, citizens, and political leaders. This is inherently a long-term endeavor that requires patience and stamina before positive results can be seen. This sense of time must be instilled in all involved in order to minimize frustration and impatience.
- Recognize that not everyone will buy in to new ideas. For virtually any endeavor that is proposed, we must recognize that complete support is improbable; it is the nature of the human psyche. One must take care, however, to not discount people who oppose new initiatives as being "lost causes" or who are obstructionists. Listen to their concerns—they may raise some valid issues that need to be addressed. If their ideas are used positively, people who oppose a new initiative may become part of the team. Realism dictates, however, that there will still be those who oppose the new system (frequently for personal reasons). In these cases, an administrator's options are: 1. continue to try to convince them to change; 2. Ignore or avoid them; 3. Place employees in an assignment where they can do little damage; 4.

Increase the quality of the relationship with those political leaders and employees who support the initiative; or 5. Tolerate employees or politicians until they resign, retire, or lose their influence.

- Be flexible and open in your view of organizational, philosophical, and programmatic change. No matter how much thought is given to a new initiative and how much effort is invested in planning, we still must recognize that many ideas are losers. We often will not know this until the idea has been tried and evaluated. Even in failure, we can learn something. Unfortunately, given the culture of our political environment, there is a tendency to mandate success—a practice that is tantamount to a search for mediocrity. Both within the police organization and the broader political system, we must maintain the freedom to fail. Without this, creative new ideas will be few and far between.
- The chance always exists that one may be placed on the hot seat from a political perspective. It cannot be denied that any attempt at change carries risks—the more massive the change, the greater the risk. Questioning traditional orthodoxy is not easily accepted by organizations, particularly bureaucratic organizations typically found in government. Proponents of new initiatives must understand that when they are on the forefront of change, their political necks are on the line. In light of this, administrators must be supportive and empathic with the politicians and employees supporting the change.
- Change requires challenging conventional wisdom or, at least, traditions. Debating the value of traditions has not been a politically popular avenue for people to follow, yet it is a necessary one for new ventures to be undertaken. When conventional wisdom is challenged, it will be met with resistance, criticism, and, perhaps, ridicule from doubters, dogmatists, and traditionalists. The astute leader must be prepared to deal with these reactions both personally and professionally. Important, when those who support the leader's ideas of change are attacked, the leader has the obligation to reassert that person's value and contributions to the organization.
- The organization's personnel evaluation system must measure and reward effective involvement in change. Since change requires a personal commitment or investment, there must be some individual benefits that can be accrued from one's participation. Benefits do not have to be monetary, but they can include such things as positive reinforcement, job perquisites, creative freedom, recognition, and awards or commendations. Similarly, awards and expressions of appreciation must also be afforded to those who substantially help usher change. In essence, without rewards, failure is ensured.

ILP holds great potential for American law enforcement. For success, however, the change process to implement ILP must begin at the most fundamental level; it must be deliberate and be tailored to the needs and resources of the agency.

Chapter Annex 6-1: Community Education Handout

Wichita State University Regional Community Policing Institute

The Citizens' Role in Counterterrorism

OBSERVE

- **Be aware of potential attackers who may be conducting surveillance of a target**
  - Behaviors include unusually long observation of a target, including taking notes, photographs, drawing schematics, and similar documentation, recording or monitoring activities, drawing diagrams, making notes on maps, using vision enhancing devices, possessing floor plans or blueprints
- **Be aware when a stranger attempts to gain information about an important place or potential target**
  - Questions may include the schedule and types of deliveries, security, and operations that go "beyond curiosity"
- **Potential attackers may "test security"**
  - These include walking or driving into prohibited areas as an "accident" to determine the type of security or police response
- **Be aware of strangers acquiring unusual quantities and kinds of supplies that could facilitate an attack**
  - This could include law enforcement, military or security supplies, uniforms, identification badges, explosives, weapons, chemicals; false identities, etc.
- **Be suspicious of people who "don't belong" and/or whose behavior is unusual**
  - For example, furtive conduct, the appearance of a "dry run" of an attack, the deployment of assets or supplies to commit the attack.

DOCUMENT

- Jot down descriptions of people and vehicles
  - People – race/ethnicity, sex, age, complexion, height, weight, clothing
  - Vehicles – "CYMBAL" – Color, Year, Make, Body and License
- Make a note of both:
  - The behaviors that drew your attention to the individuals
  - The types of behavior you observed

REPORT

- Call the local police
- Remember…
  - What may seem to be inconsequential may be an important piece of information in a larger puzzle
  - Follow your intuition

RESOURCES

Office of Community Oriented Policing Services
www.cops.usdoj.gov

Terrorism Answers
www.terrorismanswers.com

United For a Stronger America
www.weprevent.org

U.S. State Department, Counterterrorism Office
www.state.gov/s/ct/

National Center for Disaster Preparedness
www.ncdp.mailman.columbia.edu

National Academies Press, Terrorism and National Security Collection
stills.nap.edu/collections/terror/index.html

Department of Homeland Security Preparedness Web Site
www.ready.gov/

FirstGov for Citizens
www.firstgov.gov/Topics/Usgresponse.shtml

Citizens Corps
www.citizencorps.gov

Federal Bureau of Investigation
www.fbi.gov

Regional Community Policing Training Institute
at Wichita State University

Intelligence Program
School of Criminal Justice
Michigan State University

Regional Community Policing Institute
Wichita State University
www.wsurcpi.org

Intelligence Program/School of Criminal Justice
Michigan State University
intellprogram.msu.edu

Chapter 7:

Civil Rights and Privacy in the Law Enforcement Intelligence Process

Civil Rights and Privacy in the Law Enforcement Intelligence Process

In the process of providing public safety, an inherent responsibility of all law enforcement agencies is the protection of citizens' civil rights—intelligence activities are no exception. One of the most important and fundamental aspects of American life is the freedoms afforded to every citizen through civil rights protections. Despite the perceptions of some, law enforcement officials accept this responsibility. They understand that the protection of civil liberties is just as important as protecting the community from crime and terrorism. While this is a fundamental truth, there is debate on where the line should be drawn with respect to the degree of intrusion allowed to the government on privacy and personal liberty in order to protect America's citizens and the country's sovereignty from external threats, such as terrorism.

One question that has been debated is whether some civil liberties should be reduced to protect America from terrorism. This issue is embodied in the philosophical question of which is more important—protecting Americans from a terrorist attack that may kill thousands of people or protecting individual civil liberties which are the lifeblood of America's most sacred principles? In truth, when examined objectively, there is no unequivocal right or wrong answer to this question because it is philosophical in nature and depends on each individual's personal philosophy and life's experiences.

Fortunately, the working law enforcement officer does not have to deal with this philosophical debate. Rather, the officer must focus on fairly explicit rules that ensure that constitutional protections for citizens remain intact. These include the following:

- Law enforcement cannot collect information on individuals for intelligence activities unless there is a criminal predicate. The law enforcement officer must have reliable, fact-based information that reasonably infers that a particularly described intelligence subject has committed, is committing, or is about to commit a crime.
- All information collected about an individual for intelligence purposes must be done in a manner that is consistent with the law of criminal procedure.
- Collected information cannot be retained indefinitely. Instead, it may be retained only if there is reliable information that provides sustained evidence of a criminal predicate.
- The law enforcement agency has the responsibility of protecting the privacy of information they collect about individuals in the course of intelligence operations. This protection of privacy extends to the dissemination of information only to officials who have the right to know and a need to know the information to further a criminal inquiry.
- When there is no evidence of a sustained criminal predicate, all intelligence records about an individual must be purged (destroyed).

Each issue will be discussed in the coming pages. Because of the importance and emotions on both sides of the debate, there has been a significant increase in the scrutiny of law enforcement intelligence activities to ensure that information is being collected, used, retained, and disseminated in a proper manner. Indeed, many law enforcement agencies have been criticized for their intelligence function, not only because of perceived abuses, but even for the potential for abuse. This last point deserves special attention.

The "potential for abuse" does not mean abuse will occur, rather it means that the opportunity for abuse exists if there are no control factors in place to prevent abuse. The three most salient factors are these:

1. Policy.
2. Training.
3. Supervision and accountability.

Policy establishes the agency philosophy, standards, expectations, and decision-making boundaries of any organizational task and responsibility.

Training provides the knowledge, skills, and abilities to perform any particular occupational task. It specifies the method of performing, what must be done, how it should be done, and what should not be done. It demonstrates the application of policy and typically informs personnel of implications and sanctions if the task is not performed correctly.

Supervision and accountability are organizational mechanisms to ensure that policy is followed and performed in the manner specified by the training. Subordinates' activities and behaviors are monitored by a supervisor to hold the individuals accountable for performing their responsibilities only in a manner that is sanctioned by the agency.

With clearly defined policy, effective training, and responsible supervision, the potential for abuse is dramatically reduced. Two additional factors that can also affect the potential for abuse are systemic to the organization. First is the type of people the agency employs. What are the requirements? What characteristics are sought in new employees? What factors in the selection process shape the type of person who is hired? The clay used to mold the law enforcement officer will significantly influence the effectiveness of policy, training, and supervision.

The second factor is agency leadership. The tone that the leader establishes for the department, as well as expectations of the leader, will be reflected in the behaviors of the employees. A leader who establishes clear expectations of personnel performance and supports those expectations with both rewards and sanctions, as appropriate, will also significantly lower the probability of abuse from occurring.

The potential for abuse exists with all types of law enforcement assignments, not just intelligence. Modern law enforcement seeks to perform all law enforcement responsibilities in a lawful, professional manner. To conclude that the law enforcement intelligence unit or an intelligence fusion center is inherently flawed simply because of the potential for abuse is a fallacious argument.

Privacy and Civil Rights: A Foundation

To begin, some basic definitions are in order. The term privacy refers to individuals' interests in preventing the inappropriate collection, use, and release of personally identifiable information. Privacy interests include privacy of personal behavior, privacy of personal communications, and privacy of personal data.[1] The U.S. Constitution does not explicitly use the word privacy, but several of its provisions protect different aspects of this fundamental right. Although an explicit federal constitutional right to an individual's privacy does not exist, privacy rights have been articulated in different contexts by the U.S. Supreme Court.[2] Privacy protections are numerous and include protection from unnecessary or unauthorized collection of personal information (e.g., eavesdropping), public disclosure of private facts, and shame or humiliation caused by release of personal information."[3]

Recommendations from the National Criminal Intelligence Sharing Plan (NCISP)

Recommendation 6: All parties involved with implementing and promoting the National Criminal Intelligence Sharing Plan should take steps to ensure that the law enforcement community protects individuals' privacy and constitutional rights within the intelligence process.

Recommendation 9: In order to ensure that the collection or submission, access, storage, and dissemination of criminal intelligence information conforms to the privacy and constitutional rights of individuals, groups, and organizations, law enforcement agencies shall adopt, at a minimum, the standards required by the Criminal Intelligence Systems Operating Policies federal regulation (28 CFR Part 23), regardless of whether or not an intelligence system is federally funded.

The term civil rights is used to imply that the state has a role in ensuring that all citizens have equal protection under the law and equal opportunity to exercise the privileges of citizenship regardless of race, religion, sex, or other characteristics unrelated to the worth of the individual. Civil rights, therefore, are obligations imposed on government to promote equality. More specifically, they are the rights to personal liberty guaranteed to all United States citizens by the Thirteenth and Fourteenth Amendments and by acts of Congress. Generally, the term civil rights involves positive (or affirmative) government action, while the term civil liberties involves restrictions on government.[4] As such, civil liberties refers to fundamental individual rights derived from the Bill of Rights, such as freedom of speech, press, or religion; due process of law; and other limitations on the power of the government to restrain or dictate the actions of individuals. Civil liberties offer protection to individuals from improper government action and arbitrary governmental interference.

Privacy, civil rights, and civil liberties have important implications for the law enforcement intelligence process, particularly in light of past abuses. Critics claim that law enforcement has not changed its intelligence practices and that post-9/11 counterterrorism initiatives have made law enforcement agencies even more intrusive. Understanding this concern and the consequent scrutiny of law enforcement intelligence activities by those concerned about civil rights abuses provides an important perspective.

[1] For a comprehensive review of privacy issues, particularly related to various types of electronic information collection, including the Internet and e-mail, see: Lilly, Jacob R. "National Security at What Price?: A Look Into Civil Liberty Concerns in the Information Age Under the USA PATRIOT Act Of 2001 and a Proposed Constitutional Test For Future Legislation." *Cornell Journal of Law and Public Policy.* 12 (Spring) (2003): 447.

[2] Several state constitutions contain explicit language regarding a right to privacy.

[3] NCISP, p. 5

[4] NCISP, p. 6

Increased Scrutiny of Law Enforcement Intelligence: The Challenge of Balancing Civil Liberties and Community Safety

Why is there increased scrutiny and criticism of law enforcement intelligence activities when there is a demonstrable threat of terrorism that can cause catastrophic effects, as evidence by the human, social, and economic impact of 9/11? There appear to be several factors.

Perhaps at the top of the list are abuses in the past. Unfortunately, there is a documented history of law enforcement (and other government agencies) that improperly collected, retained, and/or disseminated information and behavior about individuals whose public statements and actions were controversial, but not criminal. While in many of those instances law enforcement agencies believed that the intelligence target was undermining American sovereignty,[5] the fact remains that the agencies had no authority to collect or retain the information because it was a noncriminal expressive activity. It must be emphasized that law enforcement authority to perform any kind of intelligence activity is based solely in the statutory authority to enforce the criminal law, hence the obligation to follow the law of criminal procedure. As such, collecting information about citizens without an articulable criminal nexus is improper. Law enforcement agencies remain under scrutiny and are still paying the price for past abuses.

A second reason has its foundation in the civil rights revolution that had its birth in the 1960s and is exemplified by Supreme Court decisions under Chief Justice Earl Warren that expanded the application of civil rights and liberties.[6] The era experienced, for the first time, citizens overtly exercising and testing their rights in the form of public demonstrations and civil disobedience on a major scale as part of the civil rights movement and Vietnam War protests. This atmosphere prompted lawsuits by a new breed of activist civil rights attorneys against police departments and corrections agencies. These actions largely brought a long-standing statute, 42 USC 1983—Civil Action for Deprivation of Civil Rights, out of dormancy. Collectively, these events placed a new emphasis on the rights of Americans and added a new lexicon to the American citizenship experience.

A third factor is that many persons do not understand the distinction between law enforcement intelligence and national security intelligence. As such, they assume that actions of the intelligence community may also reflect actions of a local law enforcement agency. For example, the National Security Agency's capture of international telephone conversations or the FBI monitoring a suspicious person entering the United States identified by the CIA as a possible threat are examples of information collection that a state, local, or tribal law enforcement agency will neither perform nor typically have access to. Yet, there often is an assumption that law enforcement agencies are involved in such activities and, as such, must be monitored in order to protect civil rights.

Fourth, the 24-hour news cycle and evolving news outlets have also contributed to the increased scrutiny of law enforcement operations, including intelligence.

[5] This was particularly true with the fear of communism and members of the Communist Party in the United States, and their sympathizers during the 1950s and 1960s.

[6] As an example of how law enforcement adapts to change, when many of the Warren Court decisions expanded civil rights protections for the criminally accused, there was a loud cry by many that the Court was "handcuffing the police" and that this would lead to more crime. (The *Miranda* v. *Arizona,* 348 U.S. 436 (1966), decision was a particularly significant decision influencing the sentiment at that time.) Sentiments ran so strong that "Impeach Earl Warren" billboards appeared all across America. As new policy and training were put in place in law enforcement agencies, and particularly as new officers were hired, most of whom were college educated, the Warren Court decisions were embraced as "simply the rules we have to follow." It became, in a comparatively short amount of time, a nonissue.

Notwithstanding some changes in the print media, the evolution of the electronic media—both broadcast and Internet—have contributed significantly to the scrutiny of government activities. The increased electronic outlets have added spirited competition to news organizations, increasing competition to capture news stories that will pique the interests of consumers and meet the need for content on a 24/7/365 basis. As a result of these factors, there is more competition for controversial stories that will uniquely resonate with consumers. Moreover, because of the need to fill every hour with content, stories receive greater depth and are often repeated many times throughout a day. The consequent effect is a bombardment of news on a given topic that gives an impression of an issue that is somewhat disproportionate.

A fifth factor contributing to the scrutiny of law enforcement intelligence appears to be the increased partisanship among both elected officials and the electorate. This has developed a dichotomous environment on virtually every social, political, and economic issue where attitudes and behaviors tend to be drawn exclusively along partisan lines with extreme criticism and little conciliation toward opponents' views. Virtually any factor at issue—including law enforcement intelligence—can be caught in some type of partisan dispute.

Next, the growth of civil rights advocacy groups[7] has also clearly influenced public scrutiny of law enforcement. These groups identify incidents and trends that heighten their concerns about privacy protections. Through press releases, white papers, public presentations, and lawsuits, these groups publicize government behaviors they feel are improper. While not always publicly popular, these groups nonetheless bring the issue to the table to open a public debate and, oftentimes, seek to change public policy through litigation or political influence.

Finally, the movement of "open government" invites public scrutiny. Largely beginning in the 1970s with Watergate, a grassroots movement known as "open government" began slowly. The essential concern was that public officials were abusing the authority of their offices and had the obligation to demonstrate that actions of government officials were lawful and in the best interests of all citizens. The movement continued to gain widespread support with government officials slowly responding. Open records acts and open meetings acts were increasingly being passed, federal and state freedom of information acts (FOIA) were expanded, and judicial interpretations of FOIA legislation became increasingly broad. As a result of public demands, elected officials were required to issue financial disclosure statements and public watchdog groups began issuing reports on various actions of officials at all levels of government. Essentially, the movement seeks accountability in government.

Collectively, these factors have contributed to the public expectation of the right to know what's going on in government activities and have increasingly sought explanations and accountability through lawsuits. In recent years, fueled by the growth of the Internet and 24-hour news channels, accountability has grown to second-guessing many government decisions. For example, the recent publication of some classified documents by the media is one artifact

[7] See: Bill of Rights Defense Committee, www.bordc.org; American Civil Liberties Union, www.aclu.org; Electronic Frontier Foundation, www.eff.org; or Center for Democracy and Technology, www.cdt.org. Each has particular areas of concern about privacy, civil rights, and civil liberties as related to all types of governmental policy and actions, not just law enforcement. Each organization provides an important watchdog role, albeit oftentimes with controversy. Of course, an important watchdog or advocacy organization that stimulates controversy is probably not taking much action.

of this movement. As a general rule, mainstream open government advocates recognize the need to maintain secrecy of "content;" however, they expect openness as it relates to processes. That is, the public recognizes the need to keep explicit information confidential, but wants assurances that information is being collected, retained, used, and shared in a manner that protects their rights. These ideals affect law enforcement intelligence activities at all levels of government and necessitate the need to have open processes and privacy policies in place. The ideal that government is "of the people, by the people, for the people" is being increasingly demanded, and must be taken seriously by policymakers. Intelligence is no exception. Indeed, the inherent threat-based confidential nature of the intelligence process invites even more scrutiny. As evidence of this, the American Civil Liberties Union (ACLU) has stated:

> No American is beneath the law's protection. And no one … is above the law's limits. Our system of checks and balances must be maintained if American democracy is to be preserved.[8]

Similarly, the Bill of Rights Defense Committee has stated as its mission…

> ... to promote, organize, and support a diverse, effective, nonpartisan national grassroots movement to restore and protect civil rights and liberties guaranteed to all U.S. residents by the Bill of Rights. Our purpose is to educate people about the significance of those rights in our lives; to encourage widespread participation; and to cultivate and share the organizing tools and strategies needed for people to convert their concern, outrage, and fear into debate and action to restore Bill of Rights protections.[9]

It is important to recognize the need for accountability and the ramifications on a law enforcement agency if accountability is dismissed or ignored. Collectively, these factors represent a significant sociopolitical change in American life and, consequently, emerging law enforcement intelligence initiatives.

Consent Decree Defined

A consent decree is a settlement that is contained in a court order. The court orders injunctive relief against the defendant and agrees to maintain jurisdiction over the case to ensure that the settlement is followed. (Injunctive relief is a remedy imposed by a court in which a party is instructed to do or not do something. Failure to obey the order may lead the court to find the party in "contempt of the court" and to impose other penalties.) Plaintiffs in lawsuits generally prefer consent decrees because they have the power of the court behind the agreements. Defendants who wish to avoid publicity also tend to prefer such agreements because they limit the exposure of damaging details. A court will maintain jurisdiction and oversight to make sure the terms of the agreement are executed.

From Lexis-Nexis Legal, www.lexisnexis.com

---

[8] From www.aclutx.org/files/ACLU%20of%20TX%20DISPATCH%2002-2006.pdf, click Safe and Free, and from that page click Surveillance.

[9] www.bordc.org/about

Lawsuits and Decrees Related to Law Enforcement Intelligence Activities

Perhaps the most controversial area of information-gathering by law enforcement agencies deals with cases where individuals are involved in "expressive activity" that is often controversial, even extreme. People who express extreme views related to animal and environmental protection, antigovernment sentiments, anarchy, white supremacy, or any other belief system are often viewed as a threat, even though their specific actions are not criminal. Indeed, evidence has shown that there is an area of behavior between "extreme" and "criminal" that is dynamic and often difficult to define. The distinction between making a firm statement of belief and making a threat is often a matter of interpretation. In the post-9/11 environment we, as a country, have become hypersensitive about threats, which appears to be leading toward less tolerance of diverse, even extreme, views. The challenge for law enforcement is to make that distinction. The intelligence process seeks to collect information about individuals who pose threats to the community, but the behavior a law enforcement officer may define as having a criminal nexus may be behavior a civil libertarian calls a freedom of expression.

The need to understand the subtleties in these distinctions is important to ensure that law enforcement officers are performing their function lawfully while simultaneously protecting the community from harm. Unfortunately, as noted previously, there is a legacy of law enforcement abuses where agencies have collected information on individuals simply as a result of their political beliefs.[10] While law enforcement agencies have changed significantly during the past several decades, this legacy is difficult to overcome.

The Supreme Court's broad interpretation of the First Amendment-based right of association, as originally defined in *NAACP* v. *Alabama*[11] and most recently in *Boy Scouts of America* v. *Dale*,[12] can protect groups engaged in First Amendment conduct from unjustified political or religious surveillance that causes them cognizable harm. As a result, the state's interest in protecting the community may, in many instances, be outweighed by the protections afforded to expressive activity found in these court decisions. While limitations on surveillance cannot unduly restrict the government's ability to conduct necessary information-gathering, requiring a reasonable suspicion of criminal activity before investigating First Amendment activity can help achieve a suitable balance between public safety interests and associational rights.[13] This evidence of criminal activity, that is, the criminal predicate, establishes the compelling state interest that justifies law enforcement intelligence inquiries.

Two particularly noteworthy court cases concern expressive activity and the law enforcement intelligence function. Understanding the lessons learned from these cases provides insight useful for decision-making related to information collection and retention.

[10] See: Chevigny, Paul G., "National Security and Civil Liberties: Politics and Law in the Control of Local Surveillance." *Cornell Law Review* 69 (April) (1984): 735.

[11] *NAACP* v. *Alabama,* 357 U.S. 449 (1958).

[12] Boy Scouts of America, et al v. Dale, 530 U.S. 640 (2000).

[13] Fisher, Linda E., "Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups." *Arizona Law Review* 46 (Winter) (2004):. 621.

New York:

Handschu v. *Special Services Division,* 605 F. Supp. 1384(S.D.N.Y. 1985), affirmed, 787 828 (2d Cir. 1986). In the 1960s, the New York Police Department (NYPD) increased surveillance and other investigations to include:

> …more undercover and other surveillance of "groups that because of their conduct or rhetoric may pose a threat to life, property, or governmental administration"; of "malcontents"; and of "groups or individuals whose purpose is the disruption of governmental activities" for the peace and harmony of the community.[14]

While many activists maintained that the NYPD was collecting information on various activists who held nontraditional views but were not committing crimes, they had difficulty demonstrating evidence of this.

During a 1971 trial of 21 Black Panthers charged with attempting to blow up several police stations, information made public through the discovery process, evidence, and testimony revealed that the NYPD kept dossiers on groups defined as radical and activist, as well as others including gay groups, educational reform advocates, and some religious and civic groups.[15] As a result of this new information, the Handschu case was filed as a class action lawsuit against NYPD surveillance activities[16] by 16 individuals affiliated with various ideological associations and organizations.

> In the suit, plaintiffs contended that "informers and infiltrators provoked, solicited, and induced members of lawful political and social groups to engage in unlawful activities"; that files were maintained with respect to "persons, places, and activities entirely unrelated to legitimate law enforcement purposes, such as those attending meetings of lawful organizations"; and that information from these files was made available to academic officials, prospective employers, and licensing agencies and others. In addition, plaintiffs identified seven specific forms of police conduct: 1. the use of informers; .2. infiltration; 3. interrogation; 4. overt surveillance; 5. summary punishment; 6. intelligence-gathering; and 7. electronic surveillance. The complaint alleged, inter alia, that these police practices had had a "chilling effect" on the exercise of freedom of speech, assembly, and association; that they also violated constitutional prohibitions against unreasonable searches and seizures; and that they abridged rights of privacy and due process. The suit requested declaratory and injunctive relief to curtail these practices.[17]

Police officials conceded that their activities included information-gathering for the intelligence process and was "not limited to investigations of crime, but related to any activity likely to result in 'a serious police problem.'"[18] Essentially, the police department asserted that it had a need to collect information about people and their activities which, although absent a criminal predicate at the time, held a demonstrably strong potential for criminal activity and the information collection was necessary for community safety.

[14] *Handschu* v. *Special Services Division,* 605 F. Supp. 1384 at 1396 (S.D.N.Y. 1985).

[15] Lee, Chisun, "The NYPD Wants to Watch You." *The Village Voice.* Series of articles December 18–24, 2002.

[16] Specifically identified for these activities was the Special Services Division of the NYPD Intelligence Bureau.

[17] Koehnlein, Bill. *The History of the Handschu Decree.* New York Civil Liberties Union, 2003.

[18] Handschu, Ibid. p., 1396.

The consent decree in *Handschu* v. *Special Services Division*, which included what is referred to as the Handschu Settlement agreed to in 1985, governs NYPD investigations of groups or individuals engaging in various forms of political activity. The settlement established the Handschu Authority[19] to oversee the activities of the Public Security Section (PSS) of the Intelligence Division.[20] The NYPD could not engage in any investigation of political activity that the settlement defined as "the exercise of a right of expression or association for the purpose of maintaining or changing governmental policies or social conditions."[21] The settlement authorized the PSS to commence an investigation only after the NYPD established the following:

> … specific information [that] a person or group engaged in political activity is engaged in, about to engage in, or threatened to engage in conduct which constitutes a crime.[22]

Information obtained during investigations of individuals, groups, or organizations could be collected or maintained only in conformity with the settlement. Information "from publicly available sources" could not be maintained with the PSS. Officers were allowed to collect only certain, general information about a planned noncriminal event "in order to preserve the peace, deploy manpower for control of crowds, and protect the right[s] of individuals to freedom of speech and assembly."[23] The settlement prohibited developing a file on an individual or group based solely on that individual's or group's "political, religious, sexual, or economic preference." In sum, these are the five key elements of the Handschu consent decree:

1. Political groups can be investigated only when suspected criminal activity is alleged.
2. The NYPD must obtain a written authorization from a three-person panel—the Handschu Authority—after presenting its suspicions.
3. The NYPD is prohibited from videotaping and photographing public gatherings where there is no indication that any criminal activity is present.
4. The NYPD must obtain written agreement from any agency with which it intends to share this information, acknowledging that it will abide by the terms of the Handschu Agreement.
5. The court ordered the panel to prepare annual reports, open to the public, demonstrating the NYPD's requests for surveillance and the number of requests the panel granted.

In light of the threat environment after the 9/11 attacks—an environment which, of course, was particularly pronounced in New York—the NYPD sought and obtained modification of the consent decree.[24] While the NYPD requested fairly broad latitude for information collection about activities of persons who were likely political extremists, the court's modification of the consent decree was narrower, yet still permitting some expansion of the original restrictions. The court acknowledged that there was a change in the public safety environment in New York following the 9/11 attacks and modified the Handschu consent decree to be consistent with the FBI Guidelines[25] issued by the U.S. Attorney General.

[19] The Handschu Authority, similar to an oversight board, consisted of the First Deputy Commissioner of the Police Department, the Deputy Commissioner for Legal Affairs, and a civilian member appointed by the mayor for a term that was revocable at will.

[20] The Public Security Section (PSS) of the NYPD Intelligence Division was the new name of what had been the Special Services Division of the Intelligence Unit when the original class action lawsuit was filed.

[21] Steigman, Jerrold L., "Reversing Reform: The Handschu Settlement in Post-September 11 New York City." *Brooklyn Journal of Law and Policy* 11 (2003): 759.

[22] Ibid.

[23] Ibid., p. 760.

[24] Steigman, Ibid. p. 746.

[25] The Guidelines are available at: www.justice.gov/ag/readingroom/guidelines.pdf.

> The FBI Guidelines provide for three graduated levels of investigative activity: 1. [permit] checking initial leads [when] information is received of such a nature that some follow-up as to the possibility of criminal activity is warranted; 2. a preliminary inquiry [is] authorized when there is information or an allegation which indicates the possibility of criminal activity and whose responsible handling requires some further scrutiny beyond checking initial leads; and 3. a full investigation [is] authorized when facts or circumstances reasonably indicate that a federal crime has been, is being, or will be committed.[26]

The modification authorized by the court was viewed as a "mixed bag" by both the NYPD and civil libertarians; hence, one may conclude that it was a reasonable compromise. The Handschu Authority for oversight was retained in the modified consent decree. Another motion related to the consent decree requested the court to enjoin enforcement of New York City Police Department Interim Order 47 which established procedures and guidelines for the police department's use of photographic and video equipment, arguing that it was incompatible with NYPD guidelines, violated the plaintiff's First Amendment rights, and violated previous Handschu judgments.[27]

In February 2007, the court rejected the motions on the grounds that the investigations in question are not politically motivated. The court also stated that, since Order 47 did not constitute a First Amendment violation, it would not grant the plaintiffs' injunctive relief. Later in the year, the court further modified its February decision on the enforceability of the consent decree, requiring that plaintiffs show a systemic pattern of violations before the court will enjoin any police department policy.

The lessons learned from Handschu are that, regardless of the threat environment facing a community, surveillance of individuals by a law enforcement agency—including photographs, video, and collecting identities—still requires a criminal nexus. While some flexibility may be given in the post-9/11 environment, the constitutional guarantee of free speech and the freedom of expression remain paramount and must be respected by law enforcement agencies.

Denver:

American Friends Service Committee, et al v. *City and County of Denver,* 2004 U.S. Dist. LEXIS 18474. On March 11, 2002, the ACLU of Colorado publicly disclosed documents demonstrating that the Denver Police Department's (DPD) Intelligence Bureau had been monitoring and recording the peaceful protest activities of Denver-area residents and keeping files on the expressive activities of advocacy organizations about whom there was no evidence of criminal activity. In a letter dated March 11, 2002 to the Denver mayor, the ACLU asked the mayor to take immediate steps to stop the DPD's practice of keeping files on peaceful protest activities and to take four additional actions:

1. Prohibit the police from sharing their criminal intelligence information with other law enforcement agencies.
2. Order a full public accounting about the criminal intelligence information that would answer a number of questions.

[26] *Handschu* v. *Special Services Division,* 71 Civ. 2203 (Feb. 11, 2003) Slip Op. at 33–34.

[27] www.nyclu.org/node/1084, "*Handschu* v. *Special Services Division*"

3. Notify individuals named in the criminal intelligence information and permit them to review the information about them in the files.
4. Preserve the criminal intelligence information because it might be evidence in any forthcoming lawsuits. [28]

At a March 13, 2002 news conference, the Denver mayor made the following statement:

> After a preliminary review of the policy and reviewing a sampling of the files that have been kept on individuals and organizations, it is our conclusion that there was an overly-broad interpretation of the policy that resulted in cases where it may not have been justifiable to include certain individuals or organizations in our· intelligence-gathering activities.[29]

The plaintiffs filed a class action civil rights suit[30] against the DPD for violating U.S. and Colorado constitutional protections by not adhering to police department intelligence records policy and failing to manage its criminal intelligence records system in line with the guidelines in 28 CFR Part 23. The Plaintiffs' Class Action Complaint for Declaratory and Injunctive Relief[31] initially filed on March 28, 2002, challenged a practice of the Denver Police Department of monitoring the peaceful protest activities of Denver-area residents when there was no evidence of criminal activity; maintaining criminal intelligence records files[32] on...

> …the expressive activities of law-abiding individuals and advocacy organizations, many of which the Department has falsely branded with the label of "criminal extremist;" and providing copies of certain Spy Files to third parties.[33]

The complaint further alleged that the DPD had…:

> …singled out and selected the Plaintiffs and the plaintiff class for surveillance and monitoring based upon their advocacy of controversial or unpopular political positions and opinions.[34]

The plaintiffs also expressed concern that individuals would be less likely to join a rally or to participate in other expressive activities if they feared being photographed by the police or that their identities would appear in police criminal intelligence files. The complaint goes on to state that the criminal intelligence records on the plaintiffs…

> … contain nothing but identifying information and facts that show that the targets of the surveillance are engaged in peaceful and legitimate educational activities, political expression, petitioning the government, and political association. The pages contain no facts that suggest that any of the named plaintiffs are involved in criminal activity.
>
> The Department has recorded false and derogatory information about the Plaintiffs. It has mischaracterized the goals and purposes of the Plaintiffs' expressive activity and smeared their personal, political, and professional reputations.
>
> The Department has disseminated the information in the Spy Files to third parties."[35]

[28] *American Friends Service Committee, et al* v. *City and County of Denver,* Class Action Complaint for Declaratory and Injunctive Relief, p. 4.

[29] Ibid.

[30] 42 U.S.C. §1983 – Civil Action for Deprivation of Civil Rights

[31] www.aclu-co.org/Spyfiles/Documents/203SpyfileComplaint.pdf

[32] The criminal intelligence files in the complaint and subsequent news releases by the ACLU were referred to as the "Spy Files."

[33] American Friends Service Committee, Ibid. p. 2.

[34] Ibid.

[35] Ibid. p. 6.

Supporting their claims, the plaintiffs demonstrated practices in the department, including memoranda to officers from supervisors, that explicitly contradicted the DPD's criminal intelligence records policy, 28 CFR Part 23 and/or constitutional standards. One memorandum from the Intelligence Bureau commander to subordinates stated, in part:

> Please purge, i.e., shread, [sic] toss, or take home, ALL references and files earlier than a 1994 date. The heart of an Intelligence Bureau lies with the ability to maintain integrity of all files and references in the likely event of litigation by political or subversive groups.[36]

In light of the evidence presented in this case, while not admitting "…any fault or liability to Plaintiffs, nor any violation of law,"[37] the City of Denver entered into a Settlement Agreement with the plaintiffs. As part of the Settlement Agreement[38] the department established a new, more restrictive intelligence records policy,[39] created an oversight board, purchased a new computerized intelligence records system, and agreed to semiannual audits of compliance with the Settlement Agreement for 5 years.

The lessons learned from this case reinforces the requirement of a criminal predicate. Beyond this, the Denver case illustrates 1. The importance of supervision to enforce currently existing policy, 2. The importance of using the right-to-know and need-to-know standards of dissemination, and 3. The importance of complying with the 28 CFR Part 23 guidelines.

Implications from Handschu (New York) and American Friends (Denver)

At the heart of civil rights issues related to law enforcement intelligence are collection, retention, and dissemination of information which identifies individuals and organizations whose expressions and expressive activities pose a threat to public safety and security. The proverbial bottom line that is clear from these two cases reinforces the premise that any collection, retention, and dissemination of such information may occur when there is nexus between the behavior and a crime. Simply unpopular, unusual, or extreme expressions, along with assumptions that persons making such expressions may eventually lead to a crime, do not alone meet the test. There must be demonstrable evidence of a crime. Law enforcement officers should be trained to understand the issues associated expressive activity and a criminal predicate.

It is also clear from these cases that simply having a policy on criminal intelligence records is not enough, even if the policy is compliant with 28 CFR Part 23. There must also be supervision to ensure that the policy is followed. Law enforcement personnel must have explicit direction on their information-collection activities, and that direction must be consistent with standards that are characteristic of both professional good practice and the protection of civil rights and liberties. Similarly, it is important to reinforce that the dissemination of any such criminal intelligence information must meet the right-to-know and need-to-know standards.

[36] Denver Police Department Intelligence Bureau, Interoffice Correspondence to "All Troops" from the Intelligence Bureau Commander, Subject: Purge Days, November 2, 1998. www.aclu-co.org/spyfiles/Documents/MemoJoeBlack110298.pdf

[38] *American Friends Service Committee, et al* v. *City and County of Denver,* Settlement Agreement, April 17, 2003, p. 5, Section 7.3.

[39] www.aclu-co.org/spyfiles/Documents/SettleAgreement.pdf

[40] www.aclu-co.org/spyfiles/Documents/SettleAgreementExh1.pdf

These factors will be discussed in detail later. The important point to note is the role these factors played in these two important cases and the subsequent effects which resulted when the standards were not met.

Civil Rights Example: First Amendment Free Expression—Two Views

A common point of conflict over civil rights is found in actions related to free expression by persons involved in protests or demonstrations. Civil rights advocates maintain that their demonstrations are expressive activity protected by the First Amendment. As such, it is improper for law enforcement agencies to collect and retain information about persons who are involved in planning and participating in demonstrations, as well as about advocates of those individuals.

Law enforcement agencies maintain that the only information they collect and retain is that related to persons who commit crimes or pose threats to community safety. Civil rights advocates respond that minor crimes, such as trespassing or minor property destruction, are of such low magnitude that they do not counterbalance the violation of the broader First Amendment guarantees and that law enforcement uses minor crimes as an excuse to collect information about those with whom it disagrees. Law enforcement counters that it has the responsibility to protect the property of all victims and that any demonstration that permits property destruction can quickly spin out of control and result in even greater threats. The debate continues, often with opposing arguments, as illustrated in Table 7-1.

Table 7-1: Counterpositions on First Amendment Information Collection

Position of Protestors	Response of Law Enforcement
1. Government should not attempt to regulate expressive activity, no matter how repugnant, as long as the activity is done without committing a crime.	1. Often, it is difficult to determine, during the course of a protest or rally, if a crime is being committed or going to be committed. Anarchists, for example, have frequently spray-painted private property or have broken windows during the course of a protest. Spray-painting the property of another is "destruction of property," not an expressive activity.
2. Expressive activity is a fundamental right that is essential to the fabric of American life. As such, law enforcement should take no action to repress expressive activity.	2. Law enforcement has the obligation to protect the rights of all Americans, not just those engaged in expressive activity. As such, law enforcement agencies have the responsibility to take reasonable restrictive actions to protect the rights of others as well as to maintain community safety and security.
3. There should be no expressly defined "protest zones" that favor one group over another.	3. Some groups have a history of committing crimes during a protest, more so than others. Protest zones are used only in those cases where there is a history of crime or information that reasonably suggests a crime will be committed during a protest.
4. Law enforcement should not use pens, barricades, or force to regulate expressive activity.	4. In some cases, pens and barricades are used to protect the protestors or to prevent a conflict between protestors and those opposed to the group's expressive activity (e.g., Ku Klux Klan rallies).
5. Law enforcement should not use surveillance and infiltration of political or social groups involved in expressive activity.	5. Where there is reasonable suspicion to believe a crime will occur, the use of surveillance and infiltration is an accepted and lawful method to gather evidence for developing a criminal case for prosecution.
Believe these actions are required to protect civil rights	Balance is required to protect both	Believes this information is required to protect community

These are essentially diametrically opposed positions on the same issue. Which positions are correct? Like most issues where there are clear dichotomous perspectives, truth is somewhere in the middle of the continuum. The reality is that the burden typically falls on the law enforcement agency to show that its actions and the information collected was done in a manner that protects both civil rights and community safety. To minimize allegations of negligence and impropriety, as well as to demonstrate good faith actions by the law enforcement agency, a number of action steps could be performed, such as these:

1. Review the evidence and determine if there is trustworthy information on which a reasonable person would conclude that a crime may occur.
2. Use the least-intrusive means of information collection.
3. Provide specific direction on the types of criminal behavior that is suspected and types of information that needs to be collected to support the criminal predicate.
4. Ensure that supervision is present to monitor the law enforcement officers' information-collection activities.
5. When possible and appropriate, communicate with the protesting group to express concerns about crimes and the procedures that will be followed should a crime occur.
6. Ensure that all personnel understand the policy for information collection.
7. Ensure that all law enforcement activities are documented and explained as a matter of record.
8. Provide information and training to officers about the elements of crimes for which there is specific concern.
9. When the demonstration is over, review all information collected and destroy all information that is not needed to support a criminal case.
10. Prepare an after-action report that reviews processes, issues, and concerns—preferably with assistance from legal counsel—and amend processes that may place the agency in legal jeopardy.

The Need for More Controls of Intelligence Inquiries than Criminal Investigations[40]

At the heart of the diverse reasons why information collection by law enforcement agencies for the intelligence process is met with skepticism and suspiciousness is the belief by many that intelligence inquiries are more dangerous to liberty than criminal investigations. An intelligence inquiry attempts to assess the presence of a threat and the determination if a threat is real, unlike a criminal investigation that occurs after a crime has been discovered. Moreover, intelligence inquiries often engage First Amendment expression, they are more secretive, and they are less subject to after-the-fact scrutiny. Civil rights activists, therefore, argue that intelligence activities should require stronger compensating protections and remedies for violations. Three primary factors support these notions.

First, intelligence inquiries are broader. While they are limited by the criminal code, their breadth goes beyond crimes that have been committed and moves into the arena of threats. An explicit concern of civil rights activists is when law

[40] Based on a policy statement posted by the Center for Democracy and Technology, entitled "Bill Introduced to Reform FBI Data Demands", which can be found at www.cdt.org/publications/policyposts/2007/5

enforcement collects information about First Amendment activities. There often is disagreement about the interpretation of language and behaviors and whether the activity is the exercise of free speech or the exhortation of a threat.

Second, intelligence inquiries are conducted in much greater secrecy than criminal cases, even perpetual secrecy. When a person is accused in a criminal case, normally that person can make public statements about his or her innocence and publicly rebut the criminal assertions in open court proceedings. Moreover, in a criminal investigation the suspect is often aware of the investigation while it is underway. Similarly, most searches in criminal cases are carried out with simultaneous notice to the target. In intelligence cases, by contrast, the target and the individuals scrutinized because of their contacts with the target are rarely told that the government is collecting information about them. While the presumption of evidence is clearly respected in a criminal investigation, it is sometimes argued that there is a presumption of guilt in an intelligence inquiry. This perspective must change.

Third, in a criminal investigation almost everything the government does is ultimately exposed to scrutiny. A prosecutor knows that, at the end of the criminal process, his or her actions will be in public. If the prosecutor is overreaching or is on a fishing expedition, it will be aired with the prosecutor facing public scrutiny, ridicule, and perhaps disbarment.[41] That is a powerful constraint. Similarly, a police department must ultimately account to the public for crime rates and disorder in a community. Most intelligence inquiries never result in a trial or other public proceeding. The evidence may be used clandestinely. Sometimes the desired result is the mere sense that the government is watching.

Intelligence inquiries are broader, more secretive, and subject to less after-the-fact scrutiny; therefore, protections must be built in at the beginning. One important protection is a federal regulation related to criminal intelligence records that are held by state, local, and tribal law enforcement agencies.

Maintaining Privacy in the Intelligence Process

The concept of privacy is broad, encompassing different personal values and interests. A number of privacy-related factors become relevant in the current law enforcement intelligence environment and are intended to address "all crime and all threats."[42] Privacy interests may be characterized as representing a diverse array of issues, such as privacy of a person's beliefs, personal behavior, personal communications, personal attributes (such as health or handicaps), and personal data (information privacy). Private information includes not only information that a law enforcement agency may be collecting about a person's possible involvement in a criminal act, but also information relating to the following:

- Name, address, telephone number, or e-mail
- Race, national, or ethnic origin
- Religion
- Gender
- Marital status
- Fingerprints, blood type, or DNA

[41] This occurred with North Carolina prosecutor Michael Nifong in the allegations of sexual assault against Duke University lacrosse players. For more information, see "Duke Lacrosse Prosecutor Disbarred." CNN. www.cnn.com.

[42] Portions of this discussion are based on information in: National Criminal Justice Association (NCJA). *Justice Information Privacy Guide*. Washington, D.C.: NCJA, 2002, 12–13.

- Financial status, history, or credit condition
- Psychiatric or psychological conditions and history
- Criminal history
- Age
- Sexual orientation
- Education
- Medical history or conditions
- Employment history, including employment dispositions
- Identifying number, symbol, or other character assigned to identify a person (such as a social security number, driver's license number or university student identification number).

In the course of an intelligence inquiry, the law enforcement agency will collect different types of personal information, but has the obligation to maintain the privacy of the information regardless of whether the person is an intelligence target, witness, informant, or information provider (such as a citizen).

> Privacy of personal data (information privacy) is described as when, how, and to what extent you share personal information about yourself. Information privacy involves the right to control one's personal information and the ability to determine if and how that information should be obtained and used. It entails restrictions on a wide range of activities relating to personal information: its collection, use, retention, and disclosure.[43]

The law enforcement organization has an obligation to protect the privacy of all persons about whom the agency collects personal identifying information, including those suspected of committing crimes. Two primary methods are used: security and confidentiality.

Security of personal information means that mechanisms and processes have been put in place to ensure that there is no unauthorized access to private information. Whether the private information is in a computer system or in paper records, there must be an adequate mechanism in place to ensure that the information is not obtained by persons who do not have lawful access to them.

Confidentiality, particularly as related to information sharing, includes behaviors and processes that seek to prevent unauthorized disclosure of the information to third parties. After private information has been collected, the custodian of the information has the obligation to protect it from being shared with others unless there is a bona fide reason for a third party to receive the information. Once again, the standard of sharing personal information to others based on their right to know and need to know the information. This is an illustration of processes to ensure confidentiality. Moreover, there is an expectation that those who receive private information will maintain the confidentiality of personal information entrusted to them. Confidentiality is about limiting access to personal information 1. To those having specific permission for access[44] to the records and 2. Preventing its disclosure to unauthorized third parties.

[43] NCJA, 2002, p. 12.

[44] "Permission to access" private records can include consent by the individual and permission as provided through lawful regulatory procedures and/or the legal process.

To maximize privacy protection, law enforcement agencies should ensure that privacy protections are in place. The *National Strategy for Information Sharing* emphasized this by establishing core privacy principles that all agencies are required to adopt. These are:

- Share protected information only to the extent that it is terrorism information, homeland security information, or law enforcement information related to terrorism.
- Identify and review the protected information to be shared within the Information Sharing Environment (ISE).
- Enable ISE participants to determine the nature of the protected information to be shared and its legal restrictions (e.g., "this record contains individually identifiable information about a U.S. citizen").
- Assess, document, and comply with all applicable laws and policies.
- Establish data accuracy, quality, and retention procedures.
- Deploy adequate security measures to safeguard protected information.
- Implement adequate accountability, enforcement, and audit mechanisms to verify compliance.
- Establish a redress process consistent with legal authorities and mission requirements.
- Implement the guidelines through appropriate changes to business processes and systems, training, and technology.
- Make the public aware of the agency's policies and procedures, as appropriate.
- Ensure that agencies disclose protected information to nonfederal entities—including state, local, tribal, and foreign governments—only if the nonfederal entities provide comparable protections.
- State, local, and tribal governments are required to designate a senior official accountable for implementation.[45]

Protecting privacy is accomplished through the implementation of a privacy policy,[46] along with effective training and supervision.

A privacy policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information that it gathers and uses in the normal course of business. The policy should include information relating to the processes of information collection, analysis, maintenance, dissemination, access, expungement, and disposition.

The purpose of a privacy policy is to articulate publicly that the agency will adhere to legal requirements and agency policy determinations that enable gathering and sharing of information to occur in a manner that protects personal privacy interests. A well-developed and implemented privacy policy uses justice entity resources wisely and effectively; protects the agency, the individual, and the public; and promotes public trust.[47]

State, local, and tribal law enforcement (SLTLE) agencies have a mandate to establish a privacy policy not only from the NCISP, but also to participate in the ISE. It is clear that there are unequivocal expectations for law enforcement agencies

[45] *National Strategy for Information Sharing*. Washington, D.C.: Executive Office of the President, 2007, 27–28.

[46] The *Privacy Policy Development Guide* may be downloaded at it.ojp.gov/documents/Privacy_Guide_Final.pdf.

[47] Global Justice Information Sharing Initiative. *Privacy Policy Development Guide.* Washington, D.C.: Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, 2006, 4–1.

to meet national professional standards for privacy and civil rights protections. As such, the obligation is to not only implement the policy, but to also provide training and supervision to ensure that the policy is effectively applied.

28 CFR Part 23 – Criminal Intelligence Operating Policies

As is evident from the preceding discussions, at the heart of the civil rights issues is whether law enforcement agencies are collecting and retaining personal identifying information of persons who are involved in expressive activity. Often, it is difficult to distinguish between expressive activity and activity that is a precursor to a crime. If certain behaviors suggest that a crime is being planned, the law enforcement agency has the responsibility to collect information to verify this and take action, as appropriate. It is not always immediately clear if a crime is in the preparatory stage, so criminal intelligence records are retained until the veracity of the threat is verified or dismissed. Because of this fine line, guidelines must be established as a matter of policy to ensure the information is weighed and appropriately retained or destroyed, depending on what additionally collected information suggests about criminal liability.

The guiding regulation for managing a criminal intelligence records system for SLTLE agencies is the federal regulation entitled Criminal Intelligence Systems Operating Policies codified in the Code of Federal Regulations at 28 CFR Part 23.[48] The regulation was created largely as a response to past practices of law enforcement agencies collecting and retaining information about people based on their activities and/or expressed nontraditional beliefs that were often extreme or unpopular, but not criminal. The regulation seeks to provide procedural guidance for the management of criminal intelligence records systems that is consistent with constitutional guarantees. The federal government, however, cannot mandate this regulation to independently governed state and local governments. Nevertheless, adoption of the regulation is a condition that SLTLE agencies must agree to in order to receive certain federal grant funds. If a local police department, for example, accepted federal funds to purchase a computer system that would be used to maintain a criminal intelligence records system, adoption of 28 CFR Part 23 is a requirement for receiving the funds.

This regulation was the only clear guideline for managing criminal intelligence records and it became the de facto standard that most agencies adopted, whether federal funds were received or not. Broad adoption of the regulation gained further momentum when the NCISP recommended that all law enforcement agencies adopt 28 CFR Part 23. As a result, the regulation became a recognized national professional standard.

Although agencies that embraced the regulation understood the regulatory language, it was not easily translated to policy. Moreover, the regulation had some operational gaps. The Law Enforcement Intelligence Unit (LEIU), therefore, developed a model operational policy and procedures that translated both the language and spirit of the regulation to be more easily adopted by a law enforcement agency. This practical interpretation of 28 CFR Part 23 is known as the LEIU File Guidelines.[49]

[48] The Bureau of Justice Assistance has developed an online training about 28 CFR Part 23 which can be accessed through the secure National Criminal Intelligence Resource Center (www.ncirc.gov) web site, accessible through HSIN Intel, LEO, and RISS.

[49] The LEIU File Guidelines can be found at it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf.

The LEIU File Guidelines represent an important step in the management of criminal intelligence records systems to ensure constitutional integrity. Based on litigation, experience, and concern expressed by civil libertarians, the management of a criminal intelligence records system must also consider elements beyond this practical interpretation of 28 CFR Part 23; therefore, the current best practice is an amalgamation of different sources relying on a conservative integration of accepted practice and regulation. Those sources include 28 CFR Part 23, the LEIU File Guidelines, established law of criminal evidence and procedure, and precedent from lawsuits arising from civil rights lawsuits involving criminal intelligence records. It should be noted that this information reflects general practice, not unique state laws which may have different effects. The decision tree in Figure 7-1 is a visual representation of the following discussion concerning factors that should be considered before entering information into a criminal intelligence record system. This is a conservative interpretation of these factors in order to provide the safest guidance on retaining information in a criminal intelligence records system.

When information is collected, one of the first issues is to determine whether the information identifies either a person or an organization. Identity is not limited to a name but can include any descriptive information from which a person may identify an individual to the reasonable exclusion of others; for example, providing an address and physical description of a person living at that address may constitute identity. Determining if the information identifies an organization is somewhat more challenging because 28 CFR Part 23 includes organizations as protected criminal intelligence information but does not explicitly define organization. Based on precedent and experience, an organization is a distinguishable entity that has a definable purpose, an identifiable organizational leadership structure, and a process or method for members to affiliate with the organization, albeit informal. Certain entities exist, such as anarchist collectives wherein people tend to affiliate with each other around a common belief; however, they do not have the explicit characteristics defined above. In this illustration, the group is more of a movement than an organization. A movement that simply has a discernable ideology that people support, even as a collective, is not an organization.

A common question is why can information be retained in a criminal intelligence records system without establishing reasonable suspicion (i.e., a criminal predicate) if it does not identify a person or organization? Constitutional rights attach to individuals, not aggregate data, philosophical movements, criminal methods, or other information that is descriptive and useful for intelligence analysis but does not explicitly identify a person. Building on the concept from *Katz* v. *U.S.*[50] that the Fourth Amendment protects people, not places, logic says that constitutional protections are afforded to individuals, not aggregate behaviors or other information that are not explicitly linked to individuals. 28 CFR Part 23 explicitly extends protection to organizations as well as individuals.

If the information identifies an individual or organization, the next step is to determine if the information was collected in a manner consistent with lawful

[50] 389 U.S. 347 (1967)

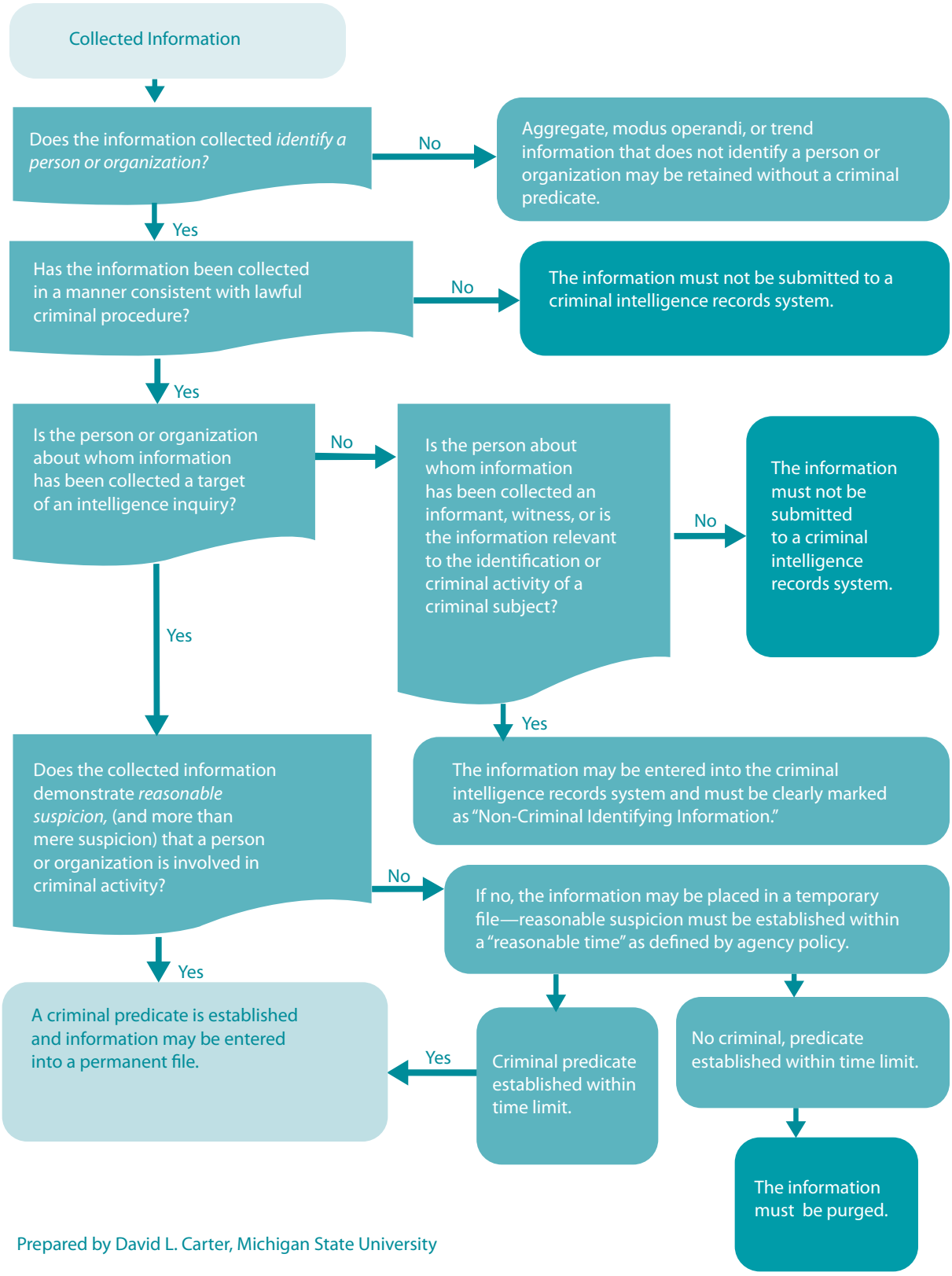
criminal procedure. While this is not a requirement of 28 CFR Part 23, precedence in both criminal and civil law suggests that this is good practice for an agency to follow in the process of deciding what information should be included in a criminal intelligence records system. There are several reasons. First, it is a constitutional protection that should be afforded to individuals; it is part of the fundamental fairness that the American justice system affords to individuals under the due process clauses of the Fifth and Fourteenth Amendments. Second, the sole authority for law enforcement to have criminal intelligence and investigative functions is based in the statutory authority to enforce the criminal law. As such, there is a reasonable probability that criminal intelligence and investigative inquiries may lead to prosecution. If there are violations of criminal procedure, the evidence will likely be excluded from trial. Third, it strengthens the legal integrity of the intelligence or investigative inquiry, thereby reducing the probability of civil liability. Processes that carefully adhere to constitutional guarantees demonstrate good faith and, conversely, are an affirmative defense to negligence by the agency. Fourth, given the scrutiny of law enforcement intelligence and investigative practices by many in the civil rights community, having this step in the process reduces criticism of law enforcement activities. Finally, the practice is consistent with the Privacy Guidelines of the Information Sharing Environment, which state, in part:

i. Seek or retain only protected information that is legally permissible for the agency to seek or retain under the laws, regulations, policies, and executive orders applicable to the agency.

ii. Ensure that the protected information that the agency makes available through the ISE has been lawfully obtained by the agency and may be lawfully made available through the ISE.[51]

[51] Program Manager for the Information Sharing Environment (PM-ISE). *Guidelines to Ensure that the Information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment.* Washington, D.C.: PM-ISE, Office of the Director of National Intelligence, Guidelines 2.b.(i) and (ii), September 4, 2006.

Figure 7-1: Intelligence Records Submission Decision Tree



Prepared by David L. Carter, Michigan State University

If information is collected about a person in the intelligence process and done so in a manner that is consistent with constitutional standards, the agency needs to have a reason for collecting it. That reason is to further an inquiry about threats to the community in the hopes of preventing that threat from reaching fruition. As a result, information is collected about individuals because they are either a target of an intelligence inquiry or have some type of information about the threat, even if they are not suspected of a crime. There is a need to lawfully retain both types of information in a criminal intelligence records system.

If a person is not the inquiry's target but has critical information, "Non-Criminal Identifying Information" (NCI) may be entered into a criminal intelligence information file if it is relevant to the identification of the subject or the subject's criminal activity, provided that: 1. Appropriate disclaimers accompany the information, noting that it is strictly identifying information carrying no criminal connotation; and 2. If the information pertains to the political, religious, or social views, associations, or activities of the criminal subject, it must relate directly to criminal conduct or activity. For example, if a criminal subject is known to attend a particular church, synagogue, or mosque, the inclusion of the religious affiliation in the system as NCI Information would be permitted only if it is directly related to the criminal conduct or activity, such as where the evidence indicates that the church, synagogue, or mosque is the site of the criminal activity. If an individual has material information about an acquaintance that supports the intelligence inquiry, this individual may also be entered into the criminal intelligence records system with a clear NCI identifier.

If the person about whom the information has been collected is the target of the inquiry, that information may be retained only if a *criminal predicate* is established. Determining a criminal predicate is a two-fold process. First, there must be a nexus between a person's behavior and a crime or an organization's operations and involvement in criminal activity. Second, for information to be submitted to a criminal intelligence records system as criminal intelligence information, the level of proof is "reasonable suspicion." Under 28 CFR Part 23, "Reasonable Suspicion or Criminal Predicate" is established when information exists that establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis to believe that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise. Reasonable suspicion is more than "mere suspicion;" that is, a person's behavior may seem suspicious; however, that information must meet the criminal nexus and level of proof tests prior to being retained in a criminal intelligence records system.

Often, intelligence personnel will receive a tip from the public or perhaps a Suspicious Activity Report (SAR) from a patrol officer. Typically, there is no criminal predicate documented in such information. Practically speaking, the intelligence officer should not simply dismiss the information; indeed, the officer has the responsibility to determine the veracity of the information as it relates to a criminal threat. The challenge to resolve is how the information can be lawfully retained if there is no criminal predicate. Since the 28 CFR Part 23 guidelines do

not address this circumstance, a practical interpretation of the regulation, which has been accepted by the courts, was created in the LEIU File Guidelines.[52] The guidelines recommend establishing two types of intelligence files: Temporary files and permanent intelligence files.

A *temporary file* is for information that does not rise to the level of reasonable suspicion but references an event or activity that indicates the possibility of criminal activity, such as a tip, lead, or SAR, none of which constitute criminal intelligence information under 28 CFR Part 23. Since this information is not criminal intelligence information, it must be clearly labeled as such in a temporary file (and defined by policy), whether stored in the same database or accessed or disseminated with criminal intelligence information. The temporary file must have a policy-defined time limit for retaining information in the file (a generally accepted time limit is 60 days). The purpose of the temporary file is simply to have a place to store raw information while an inquiry is made to determine if a criminal predicate can be established. If the criminal predicate is not established within the policy-defined time limit, the information should be purged.

Once a criminal predicate is established, the information is considered criminal intelligence information and may be stored in a *permanent file*. While it is commonly accepted phrasing, the term permanent file is somewhat misleading because the information in this file is subject to the 28 CFR Part 23 5-year review and purge requirement.

It should be stressed that these processes and rules apply only to a criminal intelligence records system that is managed by an SLTLE agency. The guidelines of 28 CFR Part 23 do not apply to a law enforcement agency's investigative records nor to a law enforcement agency's Records Management System[53] (RMS). Sometimes questions about different types of records law enforcement agencies maintain appear to be intelligence-related but are often kept separately from the RMS. The most common questions are associated with Field Interview records and gang records. Because law enforcement agencies vary widely in these types of records, some general questions (Table 7-2) can be asked to reasonably determine if the records are criminal intelligence information for purposes of 28 CFR Part 23.

This discussion was intended to provide general information about the management and use of criminal intelligence records. Often, there are explicit questions about specific systems of a given agency. The best resource for these questions is the 28 CFR Part 23 Training and Technical Assistance program funded by the Bureau of Justice Assistance.[54]

[52] See www.it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf.

[53] The RMS typically stores information such as offense reports, arrest records, traffic accident records, miscellaneous investigations, and similar types of records kept on the daily operations of managing and responding to calls for service and crime.

[54] For more information about this program see www.iir.com/28cfr, or visit www.ncirc.gov for BJA's online 28 CFR Part 23 Training.

Table 7-2: Questions to Determine if Records Must Comply with 28 CFR Part 23 Regulations

If the answer is "Yes" to any of the following questions, the records are criminal intelligence information and should be compliant with 28 CFR Part 23 regulations.	If the answer is "Yes" to any of the following questions, the records are most likely not criminal intelligence records for purposes of 28 CFR Part 23 regulations.
1. Are the records expressly called "intelligence records"? 2. Are the records retained in the same records system as criminal intelligence records? 3. Are the records kept primarily to assess threats with limited or no known criminal history of the intelligence targets? 4. Are records being retained that identify individuals or organizations suspected of criminal activity but are not the subject of a current criminal investigation?	1. Are the records kept for investigative support of known crimes? 2. Are the records kept in support of an active criminal investigation of a crime that has occurred and/or a known continuing criminal enterprise? 3. Are the records kept to monitor the behavior of convicted criminal offenders (e.g., sex offenders), including persons on probation or parole, who are reasonably believed to pose a hazard to public safety? 4. Are the records kept to identify individuals who are affiliated with a known crime group (e.g., persons who have tattoos known to be affiliated with a criminal gang)?

Federal Civil Rights Liability and Intelligence[55]

As evidenced by myriad lawsuits, such as the New York and Denver cases previously discussed, intelligence abuses have occurred. Unfortunately, critics often do not recognize the many changes that have occurred in law enforcement practices, coupled with the more specific professional direction of law enforcement intelligence. Higher educational standards, better training, adoption of ethical standards, and inculcation of law enforcement as a profession, are indicative that the culture of law enforcement has changed, rejecting past practices that contributed to the aforementioned abuses.

Beyond this history, the public generally has a misconception about the law enforcement intelligence function, envisioning it as involving spying, surreptitious activities, and acquisition of information by stealth. The public and media need to be reassured that law enforcement intelligence processes will strictly subscribe to individual constitutional protections when collecting, retaining, and disseminating information. Moreover, the public needs to understand that intelligence analysis is simply the scientific approach to problem solving, similar to the way analysis has been effectively used in community policing. The difference, however, is that community policing focused on crime and community disorder, while intelligence focuses on threats and methods that may be used to prevent such threats from reaching fruition. Generally speaking, critics are not against using information gathering and analysis to combat terrorism or solve crimes; rather, they simply demand that it be conducted in accordance with the constitutional parameters that law enforcement officers are duty-bound to follow.

[55] Based in part on: Carter, David L. and Thomas Martinelli. "Civil Rights and Law Enforcement Intelligence." *The Police Chief*, June 2007.

Because of the importance of protecting citizens' civil rights in all law enforcement activities, including intelligence operations, a remedy is available to citizens when an employee of a state, local and, in some cases, tribal law enforcement agency violates individual civil rights guarantees under the color of law. As noted earlier, this remedy is Title 42 of the United States Code, Section 1983 – Civil Action for Deprivation of Civil Rights (frequently referred to simply as Section 1983).

Section 1983 lawsuits provide civil action for the deprivation of constitutional and federal statutory rights by persons acting under the color of law. This statute was originally created as part of the Civil Rights Act of 1871, which was intended to curb oppressive conduct by government and private individuals participating in vigilante groups, such as the Ku Klux Klan. Section 1983 experienced a period of dormancy until 1961 and the landmark Supreme Court case, *Monroe* v. *Pape*, 365 U.S. 167 (1961) gave individuals a federal court remedy as a first resort rather than only in default of (or after) state action. Today, Section 1983 lawsuits against law enforcement agencies most commonly involve First Amendment issues such as freedom of speech, Fourth Amendment issues like search and seizure or use of force, and Fourteenth Amendment claims of due process violations.

The key elements of the statute:

- Was the individual deprived of a constitutional or federally protected right?
- Did the law enforcement employee act under color of state law?
- Did the law enforcement employee fail to provide the standard of care owed to the individual?
- Was the law enforcement employee's conduct the cause of the individual's deprivation of constitutional right or federal statutory protection?
- Did the law enforcement agency fail to provide due diligence to ensure that agency policy and personnel practices protect civil rights?

For a successful civil rights case to occur, the plaintiffs must show that the law enforcement agency was negligent and that there was a pattern of misconduct associated with that negligence. Typically, this is achieved by providing evidence that the law enforcement agency failed to provide due diligence in protecting individuals' civil rights. To accomplish this, the plaintiffs typically will attempt to demonstrate that the law enforcement agency showed deliberate indifference toward the protection of individuals' privacy and civil rights. In intelligence-related cases, this deliberate indifference may be a product of such things as these:

- Failure to train—the agency does not provide intelligence training to all law enforcement personnel in line with the recommendations of the Minimum Criminal Intelligence Training Standards that have been promulgated by the Global Advisory Committee.
- Failure to direct— the agency does not provide clear policy and procedures on criminal intelligence information collection, retention, review, and dissemination.
- Failure to supervise— the agency does not adequately monitor the intelligence- related activities of personnel and/or does not enforce intelligence policy.

- Failure to establish a privacy policy—the agency does not articulate a clear policy to protect the privacy, civil rights, and civil liberties of citizens as related to intelligence and records management activities.
- Failure to adopt accepted professional standards of good practice— the agency does not adopt the recommendations of the National Criminal Intelligence Sharing Plan or the Intelligence Standards of the Commission on Accreditation for Law Enforcement Agencies.

Hypothetical Example: Federal Civil Rights Liability and Intelligence Records

How could a state or local law enforcement agency be held liable in a federal civil rights lawsuit (42 U.S.C 1983 – Civil Action for Deprivation of Civil Rights) for improperly retaining personal identifying information in a criminal intelligence records system if the system's policies are 28 CFR Part 23 compliant?

- If the officers who were entering personal identifying information on suspicious persons in the criminal intelligence records system did not know that this information could not be entered because there was no criminal nexus, then there is a potential for negligence for failure to train.
- If a law enforcement employee did not understand that people involved in a protest were exercising their First Amendment rights to expressive activity, then there is a potential for negligence for failure to train.
- If the training was not adequate to teach the officers to do the job properly, there could also be negligence by failure to train.
- If a supervisor did not monitor the information being entered into the system or did not take corrective action for improperly entered information, then there is a potential for negligence for failure to supervise.
- If a law enforcement employee who clearly did not understand the policies of the intelligence unit or did not respect/follow the policies of the intelligence unit or if the person was unable to adequate apply the policies, then there is a potential for negligence for negligent retention.
- If command-level personnel learn of improper information being collected and retained and did not take actions to correct the problem, then there is a potential for negligence for failure to direct.

The resulting deliberate indifference is behaviors and processes that cause ongoing negligence in the protection of civil rights and liberties. The following are examples of behaviors or activities that are evidence of ongoing negligence.

- Retaining information that identifies people or organizations where there is no reasonable evidence supporting a criminal nexus.
- Profiling based solely on attributes such as race, religion, ethnicity, or country of origin rather than behaviors where there is a criminal nexus.
- Insinuating guilt by association or guilt based on mere suspicion.
- Inappropriate surveillance and information collection about an individual or organization.
- Knowingly keeping inaccurate information or information that should have been purged.
- Sharing information with other law enforcement agencies that identifies people or organizations with the inference of a criminal involvement when a criminal predicate does not exist and/or without establishing the recipient's right to know and need to know the information.

As noted in the New York and Denver cases, the loss of a civil rights lawsuit can be costly, embarrassing, disruptive of operations, and provide significant new restrictions on intelligence activities. As will be seen, this can be easily avoided with proper policy, training, and supervision in place.

Providing a Transparent Process

An important tool for gaining citizen support for the intelligence function while at the same time minimizing accusations of impropriety is to ensure that the intelligence process is public and transparent. Providing some insight into the need for transparency was a press release by the ACLU of Massachusetts commenting on the opening of the Massachusetts intelligence fusion center. The statement expressed concern about the center's role and activities, specifically stating the following:

> We need a lot more information about what precisely the fusion center will do, what information they will be collecting, who will have access to the information, and what safeguards will be put in place to prevent abuse.

These are reasonable and easily answerable questions. By simply providing this information to the community through a public information document or in town hall presentations, a great deal of conflict, criticism, and cynicism can be avoided. Uncertainty generates citizen consternation that translates into mistrust and allegations of impropriety. Educating the community about the intelligence process can reduce these tensions.

Hypothetical Example: Court Determination of a Criminal Intelligence Records System

A municipal law enforcement agency has a SAR records system that was developed using a federal grant. The agency states, as a matter of policy, that the SAR system is not a criminal intelligence records system. Is it conceivable that this SAR records system could be subject to the 28 CFR Part 23 guidelines?

It is possible that this could occur as a result of a lawsuit. For example, a plaintiff files a federal civil rights lawsuit (42 U.S.C. Section 1983) against a law enforcement agency alleging that the agency is collecting, retaining, and disseminating personal identifying information that is criminal intelligence. The complaint goes on to allege that the new records system is actually a criminal intelligence records system under the guise that the information is "only in SARs."

In its response to this complaint, the agency will no doubt say 28 CFR Part 23 applies only to the criminal intelligence records system and that the SAR records are not criminal intelligence records.

If the plaintiffs successfully argue that, since the primary persons accessing the SAR system are intelligence analysts and personnel assigned to the intelligence unit, this might be persuasive. Moreover, if the law enforcement agency employs an Intelligence-Led Policing philosophy wherein intelligence analysis permeates law enforcement operations and operational decision-making, this could be further evidence supporting the notion that the SAR system is indeed criminal intelligence. The argument would continue that it is irrelevant what the law enforcement agency called the system; rather, the single issue of determination is how the system is used.

If these arguments were successful, the court could rule that the SAR system is, indeed, a criminal intelligence records system irrespective of what the law enforcement agency called it. Consequently, as part of a settlement or injunctive relief, the guidelines of 28 CFR Part 23 could be applied to the SAR system.

In the last few years, many SLTLE agencies have reengineered their intelligence capacity largely through guidance provided by the National Criminal Intelligence Sharing Plan, the Law Enforcement Intelligence Unit File Guidelines, and various intelligence training programs developed under the sponsorship of the Bureau of Justice Assistance[56] and the Department of Homeland Security Training and Exercise Integration.[57] These intelligence programs include instruction on the constitutional guidelines regarding civil rights protections; however, new challenges are emerging that pose renewed concern about abuses.

In particular, there is increasing concern about the ISE[58] that is the product of the Intelligence Reform and Terrorism Prevention Action (IRTPA) of 2004. Largely based on the recommendations of the 9/11 Commission Report, the executive implementation of IRTPA is designed to maximize information-sharing between all levels of government, including sharing terrorism information between the Intelligence Community and SLTLE agencies. The reason, of course, was to ensure that America would be able to have the information and ability to connect the dots when a terrorism threat emerged. Despite this noble goal to protect America from terrorism, many critics felt the legislation went too far.

To address these diverse issues, three fundamental areas emerge where civil rights issues are of concern:

1. Ensure that the collection and retention of information in a criminal intelligence records system are done in a proper manner, both legally and ethically.
2. Ensure that individual privacy rights are protected for all information that has been collected and retained.
3. Ensure the integrity of data quality and data security.

While there are additional intelligence issues that have civil rights implications, these are among the most fundamental and challenging. It bears repeating that these issues are applicable to information and records that identify individuals.

Ensure that the collection and retention of information in a criminal intelligence records system is done in a proper manner, legally and ethically. As noted previously, the authority for SLTLE agencies to perform any type of intelligence operations lies in their statutory authority to enforce the criminal law. As such, any information that is collected and retained in a criminal intelligence records system must be based on a criminal predicate; that is, it must be demonstrated that there is a relationship between the person(s) identified in criminal intelligence records and criminal behavior. The level of that relationship is more than mere suspicion—there must be reasonable suspicion articulated to link the suspected individual to specific criminal behavior.

Ensure that privacy is protected for all information that has been collected and retained. Ensuring that information about individuals is collected and retained with proper legal basis is only one aspect of ensuring that citizens' civil rights are protected.

> A privacy and civil liberties policy is a written, published statement that articulates the policy position of an organization on how it handles the personally identifiable information it gathers and uses in the normal course of business.[59]

[56] These include the Criminal Intelligence for the Chief Executive (CICE) course, the State and Local Anti-Terrorism Training (SLATT) program, and the Criminal Intelligence Commanders course that is in preparation as of this writing. See www.slatt.org.

[57] Most notably the Intelligence Toolbox course. See intellprogram.msu.edu.

[58] See www.ise.gov.

[59] Global Justice Information Sharing Initiative. *Privacy and Civil Liberties Policy Development Guide and Implementation Templates.* Washington, D.C.: Office of Justice Programs, U.S. Department of Justice, rev. 2008, 4–1.

Law enforcement agencies must have mechanisms in place—including proper training, policies, procedures, supervision, and discipline—to make certain that this information is not disseminated to persons who do not have the right to know and the need to know the information. A privacy policy must be developed and implemented with proper safeguards in place. Incorporated within this policy must be a clearly defined process of discipline, demonstrating strict, swift, and certain sanctions for sworn members who fail to strictly comply with the policy's provisions.

Ensure the integrity of data quality and data security. Data quality refers to procedural mechanisms that ensure that raw information is collected and recorded in a valid, reliable, and objective manner. Its intent is to maximize the accuracy of raw information that will be used in the intelligence records system. Security includes processes and mechanisms to ensure that information is not accessed by, or disseminated to, persons who do not have the lawful right and need to know the information. Such security measures reinforce the procedural processes of individual privacy protections without divulging the substance of the intelligence gathered. Procedure over substance is a broad policy philosophy that can be shared with the community to quell mistrust and yet, it does not jeopardize an agency's efforts to protect data quality.

Steps to Ensure Protection of Citizens' Civil Rights

A wide range of issues has been discussed that represent legal flash points related to law enforcement intelligence activities. There are a number of mechanisms that may be easily implemented to ensure that civil rights protections remain intact while addressing the concerns of intelligence critics (See Figure 7-2).

1. Policy Implementation. Every law enforcement agency should implement a privacy policy, security policy, and accepted records management policy, such as the LEIU criminal intelligence file guidelines.[60] Relying on policy models and policy development processes recommended by the Global Intelligence Working Group provides a solid foundation on which to demonstrate that the agency is following accepted national standards. This has a twofold advantage: First, it demonstrates to the community that the law enforcement agency has an intelligence policy foundation that is consistent with nationally recognized standards. Second, in case of a lawsuit, it can be used as an affirmative defense that the agency's policies are consistent with professionally recognized good practice.

2. Training. Training has three fundamental levels. First, every agency should follow the training recommendations of the NCISP and the Minimum Criminal Intelligence Training Standards,[61] which includes an intelligence awareness training program for all officers.[62] Second, beyond these training standards, appropriate personnel within the agency need to receive training on agency policy and fusion center policy related to all aspects of the intelligence function. Special attention should be devoted to collection, retention, and dissemination of intelligence as well as special issues such as SARs, intelligence related to juveniles, and other unique forms of information. Last, as mentioned earlier, sworn personnel need to appreciate the gravity associated with constitutional rights violations as they pertain to intelligence

[60] www.it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf

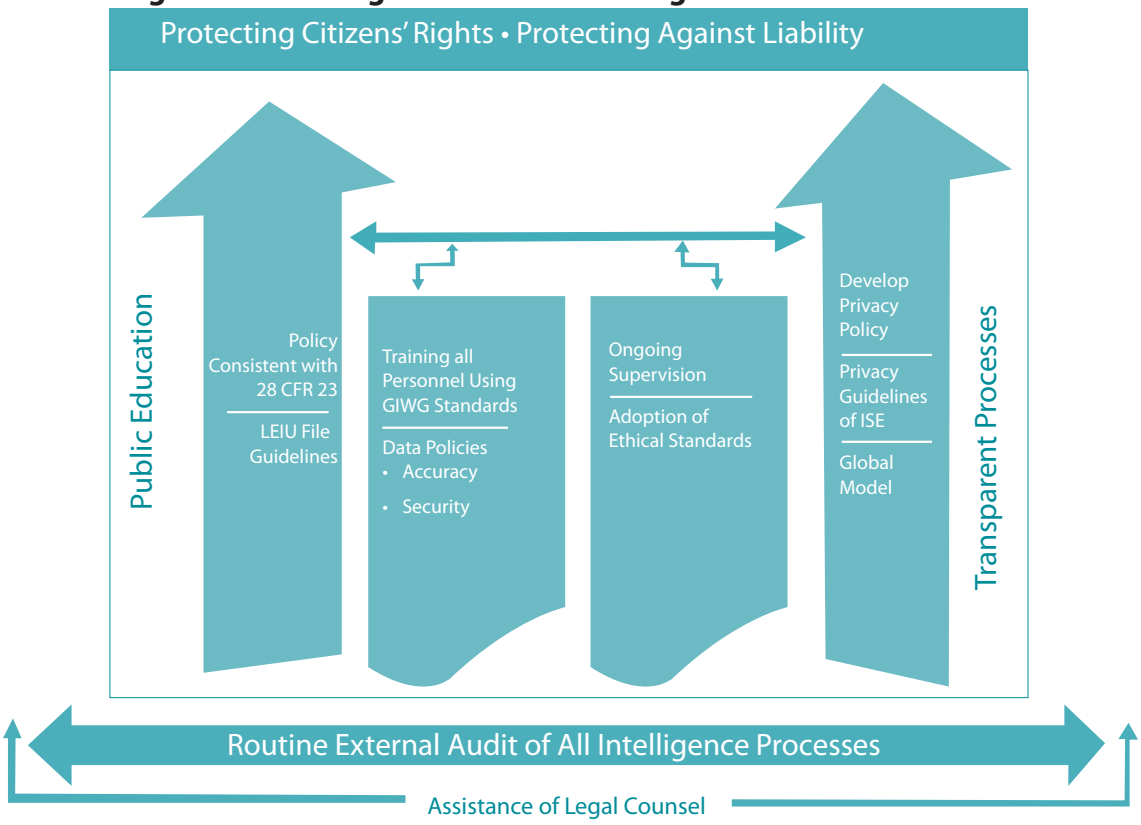
[61] https://it.ojp.gov/documents/min_crim_intel_stand.pdf

[62] Intelligence training resources can be found at: www.slatt.org, www.counterterrorismtraining.gov, and intellprogram.msu.edu.

gathering. Not unlike other critical issues in policing, a zero tolerance policy toward such infractions is mandatory. This policy demonstrates to law enforcement personnel, as well as to the community, that civil rights violations will not be tolerated and immediate disciplinary action will be taken.

3. Supervision. Good policy and training are only part of the equation; an agency must ensure that policies and procedures are being complied with as intended. If personnel are not following policy or are misinterpreting it, there exists a lack of systemic accountability and uniformity when it comes to meting out appropriate discipline. Street-level supervisors must be vigilant in their agency's commitment to constitutional policing and must hold their subordinates to the highest standards of the profession, specifically when dealing with intelligence gathering. When patterns and practices of civil rights violations are uncovered over a period of time, plaintiff attorneys simply have to demonstrate to juries that street-level supervisors and their bosses knew or should have known of these violations and deliberately chose not to take disciplinary action. Deliberate indifference has proven to be very costly for law enforcement agencies that have opted to look the other way when citizens or fellow officers have reported possible civil rights violations.[63]

Figure 7-2: Strategies to Ensure Civil Rights Protections



[63] Martinelli, T.J. and Joycelyn M. Pollock. "Law Enforcement Ethics, Lawsuits, and Liability: Defusing Deliberate Indifference." *The Police Chief* 67 (October, 2000) 10: 52–57

4. Public Education. A critical element of success for law enforcement intelligence is informing the public of law enforcement intelligence initiatives. Once again, there are two critical reasons for this. The first, as noted earlier regarding the ACLU's concerns, is to simply educate the public about the intelligence process. This eliminates erroneous assumptions and second-guessing. Much of the lay public assumes law enforcement agencies perform some type of widespread clandestine information collection and operate in a manner similar to the Intelligence Community. Correcting this misperception can go a long way toward developing positive support for the Intelligence Process. The second benefit to public education is to inform citizens of the signs and symbols of terrorism to assist in the information-collection process. For example, a trial program by the Regional Community Policing Institute at Wichita State University, in association with various police departments in Kansas, provided community training on terrorism and intelligence to educate the community on what to look for and how to report the information. Those attending the training were provided with a document called *Observe – Document – Report* and received instruction regarding the indicators of behavior that were considered suspicious, what kind of information needed to be documented, and how to report their observations to law enforcement. This model also helps citizens feel like they are contributing to the security of their own community and helps minimize the level of distrust toward their agency's efforts to combat crime and terrorism.

5. Transparent Processes. The intelligence function, like all other aspects of an American law enforcement agency, should have clearly understood and transparent processes. While certain information used in the intelligence function must be secured, the process that is used must be open. Critics of law enforcement intelligence argue that the Intelligence Process is secretive and that there is widespread spying on citizens.[64] This argument can be successfully countered by an agency that is open and transparent about how the Intelligence Process works, including relationships of an agency with other organizations, such as a fusion center. Without divulging the substance of intelligence records, an agency's efforts to educate its citizens about the procedural steps taken for information gathering and its data storage policies can go a long way toward achieving buy-in by the citizenry policed.

6. Accountability Audits. It should be a mandatory practice to have periodic internal audits of the intelligence processes within an agency. A two-step process may be involved. First, a supervisor or manager must review and document the intelligence processes following a recognized checklist of variables[65] written in the form of an inspection report. This would be followed by an external auditor, a balanced independent person such as a retired judge or other respected individual, who could review the report and ask challenging questions of both the auditor and chief executive. Important too, the audit should be viewed as a positive process designed to identify weaknesses or concerns that can be remedied. Taking proactive action such as an audit can ensure that all aspects of the process are operating as constitutionally mandated. It can identify unforeseen problems and serve as affirmative evidence that the agency is operating in good faith and without malice.

[64] As an illustration, the reader is urged to conduct an Internet search of the phrase "spy files." The results will provide insight on the breadth of concern about the intelligence process, as well as the issues of concern by many citizens.

[65] Two examples of Intelligence Audit checklists can be found at https://intellprogram.msu.edu/Carter_Intelligence_Guide.pdf and www.it.ojp.gov/documents/LEIU_audit_checklist.pdf.

7. Always Act in Good Faith. All actions of the agency and its personnel should clearly demonstrate that the decisions made in the intelligence process are expressly intended to meet lawful standards. Good faith can be demonstrated in a variety of ways including the implementing policies and procedures, providing training to personnel, and ensuring that appropriate supervision is being performed. Many areas of discretion in the intelligence process often lack definitive legal guidance. If the framework is in place to aid personnel in making the best discretionary decision that protects individuals' rights while maintaining community safety, then the probability of negligence is reduced through these good faith activities.
8. Assistance of Legal Counsel. The case law, as it pertains to police misconduct, relies on best police practice concepts such as good faith, reasonableness, and discretion without malice when judging an officer's conduct in hindsight. Juries typically do not want to find officers guilty for their alleged misdeeds or policy violations and, more times than not, will give the officers the benefit of the doubt. But without clearly drafted policies, in-depth training scenarios, and evidence of an organization's strict compliance with constitutional law issues, an agency's legal counsel may find it difficult to defend one of its own against an allegation of civil rights violations in a court of law. Competent legal counsel may be the best preventive measure that agencies can use to prepare for litigation involving allegations of civil rights violations. Whether it is a sole practitioner or an insurance carrier's legal counsel, an attorney well-versed in municipal law, Section 1983 actions, and police misconduct cases, can assist in drafting an agency's privacy and security policies, as well as formulating the process for gathering and analyzing intelligence data.

With this approach, an agency can be assured that every conceivable step has been taken to comply with the latest Supreme Court rulings pertaining to best police practices in accordance with society's increased need for vigilant police protection in this post-9/11 era. In the past, police ethics trainers have used case law examples and arbitration awards to demonstrate examples of police misconduct that resulted in suspensions or terminations. A municipal legal expert can draft street-level scenarios that engage police trainees in dialog that addresses both best police practices and the need to strictly adhere to the constitutional parameters of police work.

Conclusion

In the evolving world of information sharing that is increasingly being driven by intelligence fusion centers and the information-sharing environment, law enforcement executives face new challenges in managing sensitive information and intelligence. Professional law enforcement accepts the responsibility for protecting citizens' civil rights while protecting the community. Moreover, this same environment will draw greater scrutiny from civil rights activists to ensure that the types of information collected, retained, and disseminated by law enforcement agencies is done so in a lawful manner. We have the knowledge and tools to protect both the community and citizens' rights. The intent of this discussion was to ensure that these tools are accounted for and placed in perspective.

Chapter Annex 7-1: Protecting Civil Rights and Immunizing an Agency from Liability in the Law Enforcement Intelligence Process

The following is a series of action steps and policy actions to ensure that the law enforcement agency protects privacy and civil rights. These same actions will also help protect the agency from a civil rights lawsuit.

Many citizens do not understand the law enforcement intelligence process and express concerns often based on erroneous assumptions. As a foundation, the law enforcement agency should have a publicly available information document that answers these questions:

- What precisely does the intelligence unit or fusion center do?
- What type of information will be collected and retained in the intelligence records system by the law enforcement agency?
- Who will have access to the information?
- What safeguards are in place to ensure proper and lawful use of the information?

Law enforcement agencies can take a number of actions to ensure the protection of citizens' civil rights. The application of some of these items will be dependent on the specific agency, its size, its jurisdiction, and whether it has a full-time intelligence unit or a part-time intelligence capacity. The items below provide a framework for ensuring that civil rights are protected and, consequently, limiting a law enforcement agency's civil liability.

- Adopt the *National Criminal Intelligence Sharing Plan* (NCISP).
  - it.ojp.gov/ncisp
- Adopt and adhere to the Guidelines of 28 CFR Part 23.
  - www.iir.com/28cfr click on "Guidelines"
- Implement court-tested policies and procedures.
  - www.fas.org/irp/agency/doj/lei/app.pdf
- Provide a regular internal audit of the intelligence unit.
  - www.iir.com, under Information Sharing, Global Justice Information Sharing Initiative, National Criminal Intelligence Plan, "Law Enforcement Intelligence Unit (LEIU): Audit Checklist for the Criminal Intelligence Function." www.it.ojp.gov/documents/LEIU_audit_checklist.pdf
- Adopt a privacy policy.
  - it.ojp.gov/documents/Privacy_Civil_Rights_and_Civil_Liberties_Policy_Templates.pdf
- Adopt the IACP Oath of Honor and IACP Model Policy on Standards of Conduct as standards for ethical behavior.
  - www.theiacp.org/PoliceServices/ExecutiveServices/ProfessionalAssistance/Ethics/tabid/140/Default.aspx
  - www.theiacp.org/PoliceServices/ExecutiveServices/ProfessionalAssistance/Ethics/ModelPolicyonStandardsofConduct/tabid/196/Default.aspx

- Appoint an external auditor to regularly review intelligence processes.
- Clearly identify lines of authority and responsibility for intelligence records management, including a two-stage review and approval process for records entry.
- Use the law of criminal evidence and procedure as a guideline for information management whenever in doubt.
- Have a documented process for right to know and need to know.
- All personnel should sign a nondisclosure agreement related to information contained in the criminal intelligence records system.
- Always act in good faith: When a decision is made about information collection, retention, or dissemination where there is a lack of clarity caused by unusual circumstances, write a justification for the decision and the rationale as part of the case file. This memo to the file ensures clarity of the facts and circumstances at the time for the decision in case that decision is challenged or reviewed.
- Review federal and state FOIA and Privacy Act Guidelines and Exemptions. Have a clear policy and procedure to handle FOIA requests particularly related to the intelligence function.
- Provide training for all of the above.

Chapter 8:
The Intelligence Fusion Process

The Intelligence Fusion Process

The intelligence fusion process represents a new chapter in the evolution of law enforcement intelligence. Fusion centers represent a new intelligence structure for most state, local, and tribal law enforcement (SLTLE) agencies to understand and with whom they can interact. Contrary to intuition, the fusion process (developing intelligence from diverse resources) and the creation of fusion centers (the physical plant) is more involved than merely changing the organizational functions of an existing law enforcement intelligence unit. It typically involves either reengineering the entire conceptual framework of the intelligence function in an agency or creating an entirely new entity. It requires engaging a wide array of people and organizations to be contributors and consumers of the intelligence function; it involves changing attitudes and processes of personnel; it requires establishing new functional and information-sharing processes among SLTLE partners; it involves the development of new agreements and functional relationships; the development of new policies and processes; and the inculcation of the Intelligence Led-Policing[1] philosophy.

The challenges are multifold, not the least of which is opening oneself and one's agency to organizational change. Most humans are dogmatic, resisting change; however, if incongruent past practices and erroneous assumptions are not eliminated from intelligence processes, the likelihood of success is diminished. The following discussion is intended to provide insight into different dimensions of the fusion process as well as concerns that have been expressed about intelligence fusion.

Historical Perspective

Initially, intelligence fusion centers were generally referred to as Regional Intelligence Centers (RIC). They took different forms throughout the United States, with no single model for what the intelligence center did or how it should be organized. They evolved largely through local initiatives as a response to perceived threats related to crime, drug trafficking, and/or terrorism within a geographic region. The intent was to marshal the resources and expertise of multiple agencies within that region to deal with cross-jurisdictional crime problems. In some cases, a region was defined as a county (e.g., Rockland County, New York Intelligence Center[2]); as a major urban area (e.g., Los Angeles Joint Regional Intelligence Center[3]); a portion of a state (e.g., North Central Texas Fusion Center[4]), or an entire state (e.g., Minnesota Joint Analysis Center[5]).

The earliest RICs began as the product of counterdrug initiatives in the 1980s. Indeed, the High Intensity Drug Trafficking Area (HIDTA) intelligence centers[6] served as models for successful structures and initiatives as well as for identifying systemic issues that had to be overcome to make the intelligence center functional.[7] In the late 1990s, the Bureau of Alcohol, Tobacco and Firearms (ATF) developed a number of programmatic activities to reduce gun violence. Emerging from these initiatives were ATF Regional Crime Gun Centers. The centers, in some cases, were colocated with the HIDTA RIC and had a number of intelligence-related roles including "…analyzing trace data to identify gun traffickers,

[1] See www.theiacp.org/PublicationsGuides/NationalPolicySummits/tabid/298/Default.aspx or www.it.ojp.gov/documents/ncisp

[2] www.co.rockland.ny.us/DA/RC_DA_Programs.html

[3] www.llis.dhs.gov/channel/channelContentListing.do?channelId=90287&categoryId=5525 (must register)

[4] www.fusionsystem.us

[5] www.llis.dhs.gov/channel/channelContentListing.do?channelId=90287&categoryId=5912 (must register)

[6] www.whitehousedrugpolicy.gov/hidta/newyork_newjersey.html

[7] The Counterdrug Intelligence Executive Secretariat (1331 F Street, N.W., Suite 700, Washington, DC 20530; Telephone: 202.353.1875; Fax: 202.353.190), has an insightful unpublished report on *Metropolitan Area Consolidation/Collocation of Drug Intelligence Elements* that describes success and challenges for Regional Intelligence Centers.

disseminate investigative leads, and coordinate with the HIDTA RIC to identify drug traffickers and their sources of guns."[8] In virtually all cases, both the HIDTA and ATF intelligence centers had a great deal of interaction with SLTLE agencies. The intent was to integrate, that is, fuse, information from diverse sources to better understand and prevent multijurisdictional crime problems.

This laid the foundation for intelligence centers, but beyond idiosyncratic local crime issues, there was little incentive to expand the centers. Of course, this changed after September 11, 2001.

Because of their demonstrated successes and the information-sharing challenges of counterterrorism, additional state and local entities embraced the concept and began developing their own centers. These centers were initially developed by state and local governments. The federal government, at first by the Department of Homeland Security (DHS), saw the value of these initiatives and began providing funding support. Fusion centers were about to experience an expanding role.

> Recognizing that state and local fusion centers represent a critical source of local information about potential threats and a mechanism for providing terrorism-related information and intelligence from federal sources, the Program Manager for the ISE (PM-ISE), the Department of Homeland Security (DHS), and the Department of Justice (DOJ) are taking steps to partner with and leverage fusion centers as part of the overall information-sharing environment.[9]

Building on this observation, a report by the Government Accountability Office (GAO) documented a number of federal efforts underway designed to support fusion centers and address challenges or obstacles identified by fusion center directors. These include the following:

- The DHS, the FBI, and the PM-ISE have taken actions to assist fusion centers in gaining access to, and managing, multiple federal information systems, including classified systems.
- Both the DHS and the FBI have committed to providing security clearances to state, local, and tribal fusion center personnel and reducing the time it takes to process a clearance.
- The DHS and the FBI are assisting fusion centers in obtaining and retaining qualified personnel, both through assignments of federal employees to state fusion centers and through some DHS funding support.
- Federal funds in support of fusion centers have become more readily available and streamlined in operation to make grant awards faster and easier.
- Both the DOJ and the DHS have provided training and technical assistance in support of fusion center development and maturation.[10]

While progress has been made, many of the fusion centers and their governing officers appear to believe that there is still a long way to go before fusion centers will fulfill their envisioned role seamlessly.

[8] www.atf.gov/field/newyork/rcgc

[9] Government Accountability Office. *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers.* Washington, D.C.: Government Accountability Office, GAO-08-35 Homeland Security, October 2007, p. 2.

[10] GAO, Ibid., pp. 23–39.

Refining the Fusion Center Concept

It was clear after the 9/11 terrorists' attacks that there had been poor information sharing among and between all levels of law enforcement (and the Intelligence Community). As more information was learned about the terrorists and their minor encounters with state and local law enforcement in the weeks and months before the attacks, it was painfully evident that current information systems and processes were simply inadequate to deal with threats of this nature. It was also evident that if a diverse array of raw information was collected by different agencies, it would be essential to have a mechanism to provide data integration and analysis so its meaning would be of value to operational law enforcement personnel.

Increasingly, state and local law enforcement leaders recognized that the experiences of the HIDTAs and RICs could be applied to counterterrorism. Because of the need to have two-way information-sharing directly with federal law enforcement and indirectly with the Intelligence Community, the fusion centers, the FBI, and the DHS reached out to each other to develop fusion centers more holistically. Indeed, "federal departments and agencies—including DHS, FBI, and DOD [Department of Defense]—launched efforts to develop strategies to incorporate these fusion centers into their information and intelligence activities."[11]

The argument that fusion centers represent a vital part of our nation's homeland security relies on at least four presumptions:

1. Intelligence and the Intelligence Process play a vital role in preventing terrorist attacks.
2. It is essential to fuse a broader range of data, including nontraditional source data, to create a more comprehensive threat picture.
3. State, local, and tribal law enforcement and public-sector agencies are in a unique position to make observations and collect information that may be central to the type of threat assessment referenced above.
4. Having fusion activities take place at the subfederal level can benefit state and local communities, and possibly have national benefits, as well.[12]

The initial focus of many new fusion centers was exclusively on terrorism; indeed, that still remains the case for a few of the centers such as the Georgia Information Sharing and Analysis Center.[13] Most of the centers broadened their focus to embrace "all crime and all threats" for two reasons. First, it was recognized that most terrorist acts had a nexus with other crimes, and focusing exclusively on terrorism may miss some important indicators. Second, because there is a wide variety of crime, notably criminal enterprises, that were transjurisdictional and represented complex criminality,[14] it was recognized that the fusion process would be of value in dealing with these crimes.

Further evolution of fusion center responsibilities has moved into the arena of an all-hazards focus (in addition to "all crimes, all threats"). Inclusion of the all-hazards approach has come from two sources: One is a result of the special conditions on some DHS grants to fusion centers that specify all hazards. The second source is from state or fusion center governing board mandates.

[11] Program Manager-Information Sharing Environment. *Information Sharing Environment Implementation Plan*. Washington, D.C.: PM-ISE, Office of the Director of National Intelligence, 2006, p. 18.

[12] Masse, Todd and John Rollins, "A Summary of Fusion Centers: Core Issues and Options for Congress." *CRS Report for Congress*. Washington, D.C.: Congressional Research Service, United States Congress, September 19, 2007, p. 3.

[13] www.llis.dhs.gov/channel/channelContentListing.do?channelId=90287&categoryId=5546 (must register).

[14] "Complex criminality" refers to criminal enterprises that are involved in a wide range of criminal activities in support of their core enterprise. A drug trafficking organization, for example, may be involved in drug production, drug trafficking, money laundering, smuggling, corruption of public officials, fraud, and other offenses.

Recognizing that fusion centers were increasingly integrating the concepts of established law enforcement intelligence activities with the "all-crimes, all-threats, all-hazards" model of intelligence, the Homeland Security Advisory Council made the following observation:

Although the primary emphasis of intelligence/information fusion is to identify, deter, and respond to emerging terrorism-related threats and risks, a collateral benefit to state, tribal, and local entities is that it will support ongoing efforts to address nonterrorism related issues by:

- Allowing state and local entities to better identify and forecast emerging crime, public health, and quality-of-life trends
- Supporting targeted law enforcement and other multidisciplinary, proactive, risk-based and community-focused, problem-solving activities
- Improving the delivery of emergency and nonemergency services.[15]

There is no single model of a fusion center because of the diverse needs and environmental characteristics that will affect the structure, processes, and products of a center. In states such as Texas and California with their large land mass, large populations, and international borders, the structure and processes of fusion centers will be significantly different than predominantly land-locked rural states such as Wyoming or Nebraska.

A Congressional Research Service (CRS) report observed that questions have arisen regarding the current and/or potential efficacy of fusion centers. The report notes that in light of the growth of the fusion centers in state and local jurisdictions without a coordinated national plan, "…there appears to be no 'one-size-fits-all' structural or operational model for fusion centers."[16] From a centralized federal perspective—as reflected in the CRS report—the lack of a uniform model is assumed to be a significant flaw. The state and local perspective is somewhat different. Indeed, the ability to build a fusion center around grassroots needs is preferred because this permits state and local agencies to mold the fusion center into a model that best suits the needs and challenges that are idiosyncratic to each jurisdiction. As noted by Johnson and Dorn, describing the New York State Intelligence Center:

> Creating one center for intelligence and terrorism information— to combine and distribute that information to law enforcement agencies statewide—prevents duplication of effort by multiple agencies. Additionally, one state fusion center serving the entire New York law enforcement community provides a comprehensive picture of criminal and terrorists networks, aids in the fight against future terrorists events, and reduces crime.[17]

Within this same line of thought, fusion centers are also structured differently because of legislative or executive mandates. Montana's fusion center (Montana All Threat Intelligence Center), for example, is mandated to focus on "all threats;" the New Jersey Regional Operations Intelligence Center includes emergency operations as well as fusion; the Massachusetts Commonwealth Fusion Center focuses on all crimes; and the Oregon Terrorism Intelligence Threat Assessment

[15] Homeland Security Advisory Council. *Intelligence and Information Sharing Initiative: Homeland Security Intelligence and Information Fusion.* Washington, D.C.: U.S. Department of Homeland Security, 2005, p. 2.

[16] Masse and Rollins, Ibid., p. 18.

[17] Johnson, Bart R. and Shelagh Dorn. "Fusion Centers: New York State Intelligence Strategy Unifies Law Enforcement." *The Police Chief.* (February 2008): 38.

Network limits its focus to terrorism. The variability of fusion center structures is broad because of functional necessity and the inherent nature of local control and states' rights perspectives.

While the structure and operational processes of fusion centers may be different, national professional standards have nonetheless been articulated that outline good practice in critical administrative areas, regardless of the center's mission. That is the intent of the *Fusion Center Guidelines.*[18] See Table 8-1.

Table 8-1: Topics in the Fusion Center Guidelines

- The National Criminal Intelligence Sharing Plan and the Intelligence Process
- Mission Statement and Goals
- Governance
- Collaboration
- Memoranda of Understanding (MOU)
- Database Resources
- Interconnectivity
- Privacy
- Security
- Facility, Location and Physical Infrastructure
- Human Resources
- Training of center Personnel
- Multidisciplinary Awareness and Education
- Intelligence Services and Products
- Policies and Procedures
- Center Performance Measurement and Evaluation
- Funding

Despite some criticisms, the fact that fusion centers are structured differently is not a weakness, but a strength. It exemplifies that each center is designed to meet local and regional needs and to best integrate the fusion center with existing organizational components (and priorities).

The Michigan State Police, for example, have widespread responsibility for both traffic and criminal law enforcement throughout the state. As such, the Michigan Intelligence Operations Center is organizationally placed in the state police. Florida, however, has two predominant state law enforcement organizations: the Florida Highway Patrol, responsible for traffic law enforcement, and the Florida Department of Law Enforcement (FDLE), responsible for criminal law enforcement. As a result, the Florida Counter Terrorism Intelligence Center is organized as part of the FDLE Office of Statewide Intelligence. The two states structured their fusion center in a manner that best fits existing organizational structures and functional responsibilities.

[18] The *Fusion Center Guidelines* are often referred to as federal guidelines because they are a product of the Global Intelligence Working Group (GIWG) of the Global Justice Information Sharing Initiative (Global), which is funded by, and advisory to, the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice. It should be noted that the vast majority of GIWG members are from SLTLE agencies. Similarly, the group of subject matter experts assembled to develop the *Fusion Center Guidelines* also comprised predominantly state, local, and tribal representatives.

The point to note is that there are different operational and functional models of law enforcement throughout the United States. Fusion centers are no different because they are an element of state or local government and will have challenges to meet the unique needs of the jurisdiction they serve. As observed in one study:

> Fusion centers [must identify] their mission and their customers, at what level of analytic product they will produce, and to whom. Not all fusion centers will need the same amount of strategic analysis or tactical analysis, but, in order to determine what to produce, they will have to understand their customers' needs and ensure they are educated so they understand the difference between the two products. Fusion centers will also need to determine how they will integrate the emergency responder community.[19]

It is, perhaps, this last point that will be the most challenging to define because all-hazards intelligence and meeting the needs of the emergency responder community are not traditional roles for the law enforcement intelligence function. Some guidance to assist fusion centers in this area is being developed through the identification of "baseline capabilities."

Baseline Capabilities for Intelligence Fusion Centers

As a result of national plans that seek to increase the efficiency and effectiveness of information-sharing efforts, fusion centers will serve as the interlink between SLTLE and the federal Information Sharing Environment for the exchange of terrorism information. As such, it was recognized that there was a need to define fundamental baseline operational capabilities that should be used by fusion centers and major urban area intelligence units to meet the information needs of all consumers of the various intelligence centers. A joint project of the Global Intelligence Working Group, U.S. Department of Justice, U.S. Department of Homeland Security, and the Program Manager-Information Sharing Environment is currently working on the project. The end result will be a companion document to the *Fusion Center Guidelines* that will identify elements that serve as the foundation for integrating state and major urban area fusion centers into the national Information Sharing Environment. The project is based on the fusion process capabilities outlined in the 2007 Fusion Center Assessment and the 2007 and 2008 Homeland Security Grant Program, Fusion Capability Planning Tool Supplemental Resource. In addition to the 2007 Assessment, the baseline operational standards that will be outlined in the project are being developed using guidance provided in the *Fusion Center Guidelines,* the *National Criminal Intelligence Sharing Plan,* the *Information Sharing Environment Implementation Plan,* and the U.S. Department of Homeland Security's *National Preparedness Guidelines* and *Target Capabilities List*. Relying on the guidance of these national standards, development of the baseline capabilities for fusion centers will be guided by the requirements of the National Strategy for Information Sharing.

The baseline capabilities follow the structure of the *Fusion Center Guidelines* and represent a comprehensive articulation of functional standards and performance expectations. As a supplement to the *Baseline Capabilities for State and Major Urban Area Fusion Centers,* baseline capabilities have been prepared for Critical

[19] Nenneman, M. *An Examination of State and Local Fusion Centers and Data Collection Methods.* Monterey, California: A thesis prepared for the Naval Post Graduate School, 2008, p. 109.

Infrastructure and Key Resources, although at this writing the capabilities had not been approved for use. In addition, baseline capabilities for public health and for the Fire Service Intelligence Enterprise have been developed. These additional documents support the all-hazards responsibilities of fusion centers. The reader should monitor the Global Justice Information Sharing Initiative web site[20] and/or the National Criminal Intelligence Resource Center (NCIRC)[21] for the final approved supplement to *Baseline Capabilities for State and Major Urban Area Fusion Centers.*

What Is Intelligence Fusion?

The GIWG national *Fusion Center Guidelines* define a fusion center in the following manner:

> … a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity. The intelligence component of a fusion center focuses on the intelligence process, where information is collected, integrated, evaluated, analyzed, and disseminated. Nontraditional collectors of intelligence, such as public safety entities and private sector organizations, possess important information that can be "fused" with law enforcement data to provide meaningful information and intelligence about threats and criminal activity.[22]

The fusion process is an overarching methodology of managing the flow of information and intelligence across levels and sectors of government to integrate information for analysis.[23] The process relies on active involvement of state, local, tribal, and federal law enforcement agencies—and sometimes nonlaw enforcement agencies—to provide the raw information for intelligence analysis. As the array of diverse information sources increases, there will be more accurate and robust analysis that can be disseminated as intelligence. Information fusion utilizes the intelligence process[24] for information management and analysis. The fusion center is the physical location where the fusion process occurs.[25]

While the phrase "fusion center" has been used widely, often there are misconceptions about the function of the center. Perhaps the most common misconception is that the center is a large room full of workstations where the staff are constantly responding to inquiries from officers, investigators, and agents. This vision is more accurately a "watch center" or "investigative support center," not an intelligence fusion center. Another common misconception is that the fusion center is minimally staffed until there is a crisis wherein representatives from different public safety agencies converge to staff workstations to manage the crisis. This is an "emergency operations center," not an intelligence fusion center.

In the purest sense, the fusion center is not an operational center, but a support center. It is analysis-driven. The fusion process proactively seeks to identify criminal and homeland security threats and stop them before they occur. Prevention is the essence of the intelligence process. The distinction, however, is that the fusion center is typically organized by amalgamating representatives from different federal, state, local, and tribal law enforcement agencies (and, in

[20] www.it.ojp.gov/global

[21] The NCIRC is accessible through the RISS, NET portal and the FBI's LEO.

[22] Global Intelligence Working Group. *Guidelines for Establishing and Operating Fusion Centers at the Local, State, Tribal and Federal Level.* Washington, D.C.: U.S. Department of Justice and U.S. Department of Homeland Security, 2005, p. 8.

[23] *Local Anti-Terrorism Information and Intelligence Sharing: Information Sharing Overview.* Lessons Learned Information Sharing, U.S. Department of Homeland Security, 2005. www.llis.dhs.gov.

[24] The Intelligence Process, also known as the Intelligence Cycle, involves the systemic steps for collecting, assessing, analyzing, and disseminating intelligence.

[25] Global Justice Information Sharing Initiative. *Fusion Center Guidelines: Executive Summary*. Washington, D.C.: U.S. Department of Justice and U.S. Department of Homeland Security, 2006. it.ojp.gov/documents/fusion_center_executive_summary.pdf.

some cases, the private sector) into one physical location. Each representative is intended to be a conduit of raw information from his or her agency who can infuse that agency-specific information into the collective body of information for analysis. Conversely, when the fusion center has intelligence requirements,[26] the representative is the conduit back to the agency to communicate, monitor, and process the new information needs. Similarly, the agency representative ensures that analytic products and threat information are directed back to the parent agency for proper dissemination. Agency representatives may be physically assigned to the center, but a more common arrangement is for the agency representative—often called a terrorism liaison officer[27] or intelligence liaison officer—to performs his or her fusion center responsibilities along with the officer's other assignments at his or her home agency.

> In short, an intelligence fusion center must be able to: 1. Access and explore all government databases, including intelligence, regulatory, and law enforcement; 2. Integrate the information found in those databases; 3. Make independent judgments about that information; and 4. Provide warning.[28]

Delaware Information Analysis Center use of ATIX

The Delaware Information Analysis Center (DIAC) takes a proactive approach to information sharing and homeland security. To maximize timely, secure, two-way information exchange, the DIAC communicates with all of its local law enforcement partners and private sector critical infrastructure partners through the Internet using the Automated Trusted Information Exchange (ATIX) portal. ATIX provides a wide array of diverse threat and homeland security information as well as content and secure e-mail. A service provided at no charge by RISS.net, ATIX simply requires an Internet connection and the secure ATIX/RISS.NET software. Users, like DIAC, are also able to have secure information exchange "communities" to ensure that only DIAC and its partners have access to specified information. As the fusion center for Delaware, DIAC's proactive approach to local law enforcement through the use of ATIX has been a significant tool for success.

www.riss.net/atix.aspx
dsp.delaware.gov/Intelligence.shtml

Obviously, not every law enforcement agency can contribute a person to work in the fusion center. Instead, the center must develop mechanisms for two-way information sharing that captures information from the nontraditional collectors and provides threat-based intelligence and intelligence requirements back to those who have the need to know. As a result, multiple strategies and technologies need to be developed for diverse two-way information sharing.

Electronic two-way information sharing through various secure electronic information systems—Regional Information Sharing System Network (RISS.NET),[29] LEO,[30] Homeland Security Information Network (HSIN),[31] National Law Enforcement Telecommunications System (NLETS)[32] (now the International Justice and Public safety Network), or ATIX[33]—can be very effective. In the case of ATIX, individuals beyond the law enforcement community who have a demonstrated need—including some private sector persons—may also have access to the

[26] "Intelligence requirements" are information that is needed to help make a comprehensive and accurate analysis of a threat. See: Global Intelligence Working Group, Intelligence Requirements Subcommittee Report. *Recommendations for Intelligence Requirements for State, Local and Tribal Law Enforcement Agencies.* (October 2005).

[27] For example, see Arizona Counter Terrorism Information Center, Terrorism Liaison Officer Program, https://www.llis.dhs.gov/docdetails/detailsProfile.do?contentID=26251 (must register).

[28] Wortzel, Larry, *Creating an Intelligent Department of Homeland Security. Executive Memorandum 828*. Washington, D.C.: The Heritage Foundation, 2002. www.heritage.org.

[29] RISS.NET, www.riss.net.

[30] LEO (operated by the FBI), www.fbi.gov/hq/cjisd/leo.htm

[31] HSIN, www.gao.gov/new.items/d07822t.pdf.

[32] International Justice and Public Safety Network, www.nlets.org.

[33] ATIX, www.riss.net/Atix.aspx.

system and use it for secure two-way information sharing. Another example is the New York Police Department's Operation Nexus:

> The New York City Police Department's [NYPD] Operation Nexus is a nationwide network of businesses and enterprises joined in an effort to prevent another terrorist attack against our citizens. Our detectives [visit] firms that have joined us in this mutual effort. Members of Operation Nexus are committed to reporting suspicious business encounters that they believe may have possible links to terrorism. The NYPD believes terrorists may portray themselves as legitimate customers in order to purchase or lease certain materials or equipment, or to undergo certain formalized training to acquire important skills or licenses. … Through Operation Nexus, the NYPD actively encourages business owners, operators and their employees to apply their particular business and industry knowledge and experience against each customer transaction or encounter to discern anything unusual or suspicious and to report such instances to authorities.[34]

Another model has emerged that is being increasingly adopted throughout the United States. Developed in Los Angeles, the Terrorism Early Warning (TEW) group has multiple functions, including supporting the intelligence fusion center.

> The Los Angeles TEW includes analysts from local, state, and federal agencies to produce a range of intelligence products at all phases of response (pre-, trans-, and post attack) specifically tailored to the user's operational role and requirements. The TEW bridges criminal and operational intelligence to support strategic and tactical users. As part of this process, the TEW seeks to identify emerging threats and provide early warning by integrating inputs and analysis from a multidisciplinary, interagency team. Toward this end, the TEW has developed a local network of Terrorism Liaison Officers at law enforcement, fire, and health agencies, formed partnerships with the private sector to understand threats to critical infrastructure, and has developed and refined processes to analyze and synthesize threat data to support its client agencies.[35]

Regardless of the method of information-sharing, the key factors are: 1. There must be diverse raw input; 2. It must be analyzed; and 3. Actionable intelligence output must be shared with appropriate consumers.

Why Fusion Centers?

The heart of good intelligence analysis is a diverse array of valid and reliable raw information. The more robust the raw information, the more accurate the analytic output (i.e., intelligence). If one thinks of information input in terms of bandwidth, the typical law enforcement intelligence unit has a narrow bandwidth; that is, information is gathered from a fairly narrow array of sources, thereby limiting both the quality of the analysis and the ability to see the big picture of a criminal enterprise. Quite simply, the more limited the input of raw information, the more limited the quality of intelligence, but if the number of sources is broadened to include a wide range of agencies representing much broader geographic

[34] www.nypdshield.org/public/nexus.nypd

[35] Sullivan, John P. *Terrorism Early Warning and Co-Production of Counterterrorism Intelligence.* A paper presented at the Canadian Association of Security and Intelligence Studies. Montreal, Canada, 2005, p. 1.

and jurisdictional parameters, then the bandwidth is much wider. With wider bandwidth, there is a greater and more diverse information flow. With greater information flow, the analysis becomes more accurate and utilitarian. As the quality of analysis increases, the ability to prevent or mitigate the operations of a terrorist or criminal organization increases exponentially.

Recent analyses of both law enforcement and national security intelligence operations found a problem that has been referred to as the stovepipe of information in agencies.[36] That is, each agency would develop a large body of information and analytic products that it would retain and rarely share with other agencies. Analysis was generally limited to the information that came from internal sources and its dissemination was also largely internal. As a result, while agencies were developing information it was simply being stacked and stored in isolation, metaphorically as in a stovepipe. Current thought recognizes that far more value can be derived from information that is widely shared for analysis. Information from one agency may be a key in learning about a threat when integrated with information another agency: there was a need to fuse as much information as possible.

As noted in a report from The Heritage Foundation, the fusion center would not simply duplicate the activities of existing agencies, but would enhance and improve their efforts by providing a service that does not yet exist.[37] Another perspective on their development observed the following:

> Conceptually, fusion centers differ from [state police intelligence units] in that they are intended to broaden sources of data for analysis and integration beyond criminal intelligence, to include federal intelligence as well as public and private sector data. Furthermore, fusion centers broaden the scope of state and local analysis to include homeland security and counterterrorism issues.
>
> Despite being an expansion of existing subfederal intelligence/information activities, fusion centers represent a fundamental change in the philosophy toward homeland defense and law enforcement. The rise of fusion centers is representative of a recognition that nontraditional actors—state and local law enforcement and public safety agencies—have an important role to play in homeland defense and security.[38]

In exploring the need and structure of fusion centers, a project by the Police Executive Research Forum identified five critical questions:[39]

1. **Why do we need a fusion center?** Fusion centers embody the core function of collaboration, and as demands increase and resources decrease, fusion centers serve as an effective tool to maximize available resources and build trusted relationships. What distinguishes fusion centers from intelligence units within local law enforcement agencies is that fusion centers synthesize data gathered from multiple sources and disciplines.
2. **What is a fusion center's mission?** While opinions on the topic vary, many

[36] As an illustration see, Kindsvater, Larry C., "The Need to Reorganize the Intelligence Community". *Studies in Intelligence.* Vol. 47, No. 1, 2003. www.cia.gov

[37] Dillon, Dana R. "Breaking Down Intelligence Barriers for Homeland Security." *Backgrounder #1536.* Washington, D.C.: The Heritage Foundation, 2002. www.heritage.org.

[38] Masse and Rollins, Ibid., p. 2.

[39] *What is a Fusion Center?* Washington, D.C.: Police Executive Research Forum, 2008. Brochure available from www.llis.dhs.gov (Must register to access).

in the law enforcement community believe it makes more sense to establish a fusion center with a broader mission and scope, i.e., implement an all-crimes or all-hazards approach, while still maintaining the unique capability to monitor terrorist activity. The value of an all-crimes center is that it increases the ability of law enforcement to detect the traditional crimes that ultimately may be precursors of terrorist activity. The underlying purpose and goal of a fusion center is to provide law enforcement agencies with analyses of local, state and regional activities. Local law enforcement agencies, however, must do their part by feeding information to the center.

3. **Who governs the fusion centers?** Most fusion centers established memoranda of understanding with participating agencies and appointed a governing board of representatives from these agencies to provide oversight and ensure adherence to policies, as per the recommendations put forth in the *Fusion Center Guidelines*.

4. **What major functions and services do fusion centers perform?** Fusion centers are intended to be analytical support centers for law enforcement and other public safety agencies. A fusion center serves as a repository for all information available from open-source and law enforcement agencies throughout the state or region. Fusion centers and the agencies they serve work together to determine the best method for disseminating center analysis and products.

5. **How does law enforcement define value in its relationship with fusion centers?**
   - Providing daily information to law enforcement agencies
   - Interpreting diverse threat information from a local perspective
   - Providing timely actionable intelligence.
   - Connecting the dots from diverse jurisdictions that affect a local area
   - Serving as a one-stop shop for threat information.
   - Managing diverse pieces of information in a coherent form for local law enforcement agencies.

Fusion Centers and the Crime Laboratory: An Analogy

The relationship of the fusion center to a law enforcement agency may be seen in a somewhat familiar analogy: the crime laboratory. The vast majority of law enforcement agencies do not have a crime lab, just as they do not have an intelligence unit; however, they periodically need forensic analysis of evidence for a case. To use the crime lab effectively, each agency must have some type of forensic capacity so that physical evidence can be collected properly (i.e., prevent contamination and maintain the integrity of the chain of custody). The agency must also have established a relationship with the crime lab and know the processes for submitting evidence for analysis.

Most agencies use a state crime lab. While a small agency may use the laboratory only periodically, in those few times forensic analysis is needed. It is essential that the local agency has trained personnel and has access to appropriate resources to use the crime lab's services expeditiously and effectively. Table 8-2 provides a

comparative series of factors that are analogous between crime laboratories and fusion centers.

This analogy illustrates that there is a precedent for many organizational processes and practices that are required for fusion centers. Building on these experiences can make integration of the fusion center into law enforcement agency operations much easier.

Table 8-2: Analogy of a Crime Lab and a Fusion Center

Crime Laboratory	Fusion Center
• Central laboratory operated by the state. • In each law enforcement agency there must be a capacity to collect physical evidence to prevent contamination. • Retain physical evidence to meet chain-of-custody requirements. • Certified agency participant with crime laboratory in order to submit evidence for analysis. • Forensic analysis is performed by specifically trained analysts. • Crime lab provides analytic results of physical evidence.	• Fusion center operated by the state. • In each law enforcement agency there must be a capacity to lawfully collect raw information, building on the criminal predicate. • Retain information to meet 28 CFR Part 23 guidelines. • Certified as a fusion center participant to establish right to know and need to know to receive intelligence product. • Intelligence analysis is performed by specifically trained analysts. • Fusion center provides intelligence products.

Fusion Centers and the Information Sharing Environment

The *Information Sharing Environment (ISE) Implementation Plan* embraced the growth of fusion centers as a critical linchpin serving as information clearinghouses between federal entities (both federal law enforcement and the Intelligence Community), nonfederal law enforcement, and the private sector.

> [M]any states and localities emphatically moved to create and invest in fusion centers in the post-9/11 environment. These fusion centers now play a prominent role in collecting, analyzing, and sharing terrorism information. Individually, these centers represent vital assets for collecting terrorism-related information. Collectively, their collaboration with the Federal Government, with one another (state-to-state, state-to-locality), and with the private sector represents a tremendous increase in both the nation's overall analytic capacity and the multidirectional flow of information. It is important to note that these centers are not homogenous—considerable variations exist in terms of operations and mission focus (e.g., homeland security, law enforcement, emergency response). To date, more than 40 such centers have been established across the United States, and significant effort has gone into developing and adopting standards to facilitate easier information access, sharing, and use.[40]

[40] PM-ISE, (2006). Ibid, pp. 7–8.

To further this plan, the PM-ISE has established a National Fusion Center Coordination Group (NFCCG), led by DHS and DOJ, to identify federal resources to support the development of a national, integrated network of fusion centers. Moreover, the ISE…[41]

> …recognizes the "all-crimes and all-hazards" nature of State and local sharing, where SLT organizations may share and fuse together multiple types of information to address a variety of needs including law enforcement, preparedness, and response and recovery. In many instances, this information may not initially be recognized as terrorism information, but may be information that could ultimately prove crucial in preventing, preparing for, or responding to terrorism. The ISE focus on terrorism information will not impede or interrupt these additional fusion center functions.[42]

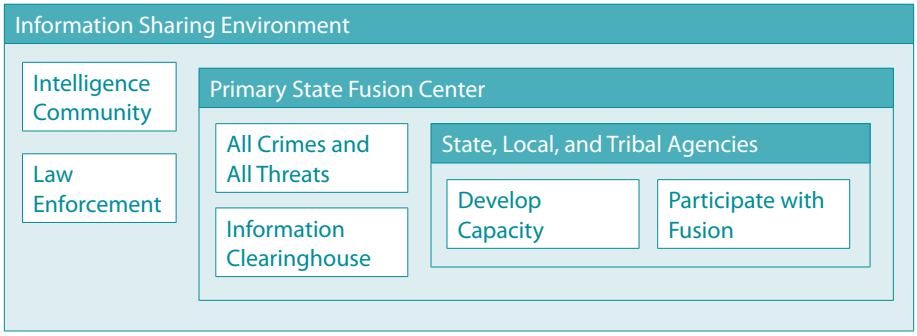
Operationalizing the Fusion Process

As depicted in Figure 8-1, three critical focal areas make the integrated information-sharing strategy functional. While all the factors are essential, the fusion center plays a uniquely critical role.

The process begins with the fundamental step of developing an intelligence capacity in all SLTLE agencies, regardless of size, as per Recommendation 1 in the *National Criminal Intelligence Sharing Plan*.[43] The intelligence capacity must be integrated with a law enforcement agency's proactive participation with the fusion center. The more agencies that participate as a fusion center partner, the greater the value of the center. As noted by the PM-ISE, "state and major urban area fusion centers will be central to implementation at the state and local levels…".[44] Creation of the fusion center, therefore, is only one ingredient; it is essential to have widespread participation.

The outer band of Figure 8-1 is the federal ISE, which consists of both the Intelligence Community and federal law enforcement. Both deal with national security and homeland security from a broad perspective and typically at a classified level. The challenge is to share appropriate threat information with local law enforcement. Similarly, when local law enforcement discovers information that is valuable to the ISE, there must be a mechanism to effectively share the information. The primary state fusion center is intended to fulfill these roles.

Figure 8-1: Organizational Interrelationships and Responsibilities for the Fusion Process and ISE



[41] GAO, Ibid., p. 12.

[42] PM-ISE, (2006). Ibid., p. 11.

[43] Global Intelligence Working Group. "*Recommendation 1.*" *National Criminal Intelligence Sharing Plan.* Washington, D.C.: Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, 2003, p. 21.

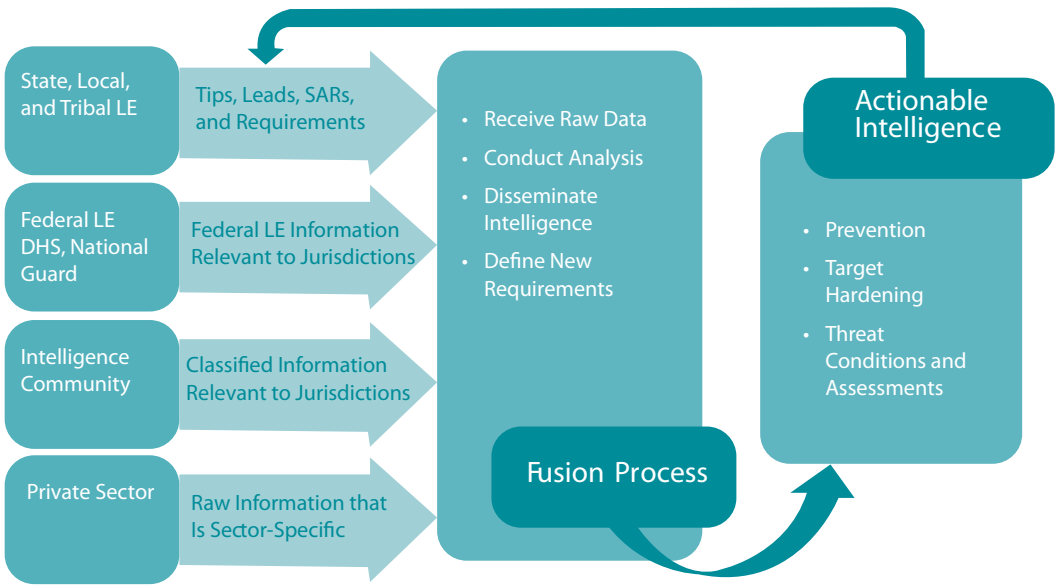
[44] Program Manager-Information Sharing Environment. *Common Terrorism Information Sharing Standards (CTISS) Program Manual.* Washington, D.C.: PM-ISE, 2007, p. 18.

The fusion center is envisioned as serving as an information clearinghouse between the ISE and local law enforcement. Generally speaking, the center will have representatives from all levels of government, experienced analysts, personnel with federal security clearances, and access to a wide range of information systems, sometimes including classified systems. With this foundation, the fusion center can disseminate critical intelligence to local and tribal partners as well as pass critical raw information to the federal ISE that is collected at the local, tribal, and private levels.

A simplified version of the fusion process to accomplish these objectives is depicted in Figure 8-2. A fundamental objective is to gain buy-in by all critical sectors within a state: law enforcement, federal partners within the state, the Intelligence Community[45] as applicable to each state and the private sector. The fusion process receives input (both raw data and intelligence as indicated in the block arrows of Figure 8-2) from a variety of agencies. The analysts integrate the diverse data and provide analytic output that may include information for prevention, target hardening, or threat assessment. In addition, the analysts may also define further intelligence requirements. After analyzing and redefining intelligence requirements, the fusion center disseminates relevant information and intelligence to its participants in the form of actionable intelligence.

It cannot be overemphasized that for intelligence fusion to be successful, as many law enforcement agencies as possible must participate in the process. Every nonparticipating agency represents a weakness in the ability to identify and prevent threats.

Figure 8-2: The Fusion Process



[45] The 16-member Intelligence Community (IC), which includes the FBI and the Drug Enforcement Administration, has a presence in every state; however, the specific IC agencies represented in each state, and consequently each fusion center, will vary widely. States with large international ports of entry or military bases, for example, will have a greater IC presence. See www.odni.gov/who_what/061222_DNIHandbook_Final.pdf.

Is there a Role for the Private Sector?

Often overlooked, the private sector can be a rich resource of information that adds a broadened dimension to information collection. Many large corporations have sophisticated security operations that monitor global threats to their facilities, products, and personnel posed by organized crime and criminal extremists, as well as predatory criminals. This type of information is often different from that collected by law enforcement organizations and can add a unique, and more insightful, component to the body of information being analyzed by the fusion center.

Similarly, the private sector is often a legitimate consumer of law enforcement intelligence meeting the right-to-know and need-to-know information-sharing standards. Eighty-five percent of the U.S. critical infrastructure is owned by the private sector. Moreover, the private sector has a large personnel force who, if given the proper information, can significantly increase the "eyes and ears on the street" to observe individuals and behaviors that pose threats. As noted in a "Best Practices" paper produced by the DHS, "a jurisdiction's analysis and synthesis entity [such as a fusion center], should also establish processes for sharing information with the local private sector."[46]

Of course, there are information-sharing issues that need to be resolved. For example, certain types of personal identifying information may be inappropriate for law enforcement to release to the private sector. Conversely, the private sector will be reluctant to share proprietary information related to corporate products and processes. Despite these limitations, the private sector has a legitimate role in fusion centers. Just as in the case of law enforcement partners, memoranda of agreement need to be in place that include provisions on information-sharing processes and restrictions.

[46] Lessons Learned Information Sharing Best Practices. *Local Anti-Terrorism Information and Intelligence Sharing: Dissemination.* Washington, D.C.: U.S. Department of Homeland Security, 2006. https://www.llis.dhs.gov/member/secure/detail.cfm?content_id=13091 (Must register to access).

Concerns About Fusion Centers

As might be expected, centralized intelligence fusion centers have heightened the concerns of some citizens who fear that the centers will collect, retain, and disseminate information that will further erode the privacy of law-abiding citizens who express support for unpopular or controversial causes. In some cases, a dialog with the community will reduce the concerns; in other cases, it will not. It is nonetheless important to understand these points of conflict. The following discussion presents the more common concerns expressed about fusion centers followed by the law enforcement response. The intent is to provide insight and communications between fusion centers and critics.

Concern: "There is a lack of an underlying philosophy. In the absence of a common understanding about what constitutes intelligence, fusion center development and progress may be impeded."[47]

Response: The purpose of a philosophy is to establish the underlying purpose, processes, and parameters in the execution of an enterprise. The philosophy of law enforcement intelligence, and by extension intelligence fusion centers, has never been clearer than it is today. The philosophy is being molded quite effectively, with a clear articulation of roles and responsibilities as found in the *National Criminal Intelligence Sharing Plan,* with further support provided by the *Information Sharing Environment Implementation Plan* and the DHS *Target Capabilities List*. Indeed, Fusion Center Guideline 1 states, "Adhere to the *National Criminal Intelligence Sharing Plan* and perform all steps of the intelligence process."[48] The *Guidelines* established the NCISP and the standards contained therein as an unequivocal philosophy.

Concern: "…arguably, the *2006 Fusion Center Guidelines* have the following limitations: 1. They are voluntary; 2. The philosophy outlined in them is generic and does not translate theory into practice; and 3. They are oriented toward the mechanics of fusion center establishment."[49]

Response: The *Fusion Center Guidelines* cannot be viewed in isolation, but must be viewed in the context of the other national standards described above. While they are voluntary—the federal government has no authority to mandate all state and local fusion centers to follow the guidelines—the guidelines nonetheless represent accepted national professional standards that are adopted for two reasons. First, the philosophical reason is to ensure ongoing professional practice. The second, more pragmatic reason, is that adoption of the *Guidelines* represents good faith and a component of due diligence that helps protect the fusion center from civil liability. While voluntary, the *Fusion Center Guidelines* represent the de facto national standard for state, local, and tribal law enforcement.

[47] Masse and Rollins, Ibid., p. 4.

[48] Global Intelligence Working Group (2005), Ibid., p. 25.

[49] Masse and Rollins, Ibid.

With respect to the philosophy, the *Guidelines state*, "…a fusion center is defined as a collaborative effort of two or more agencies that provide resources, expertise, and/or information to the center with the goal of maximizing the ability to detect, prevent, apprehend, and respond to criminal and terrorist activity."[50] These are explicit, practical objectives, not generic ones.

Finally, the criticism that the Guidelines "…are oriented toward the mechanics of fusion center establishment" is puzzling. The philosophy has been clearly established, as described above: It is a responsible, proactive, and effective fact that national standards for the mechanics of fusion centers have been established to help ensure consistency, efficiency and effectiveness. Indeed, the Guidelines represent important control mechanisms for fusion centers to help ensure adherence to the rule of law.

Concern: "Arguments against fusion centers often center on the idea that such centers are essentially preemptive law enforcement—that intelligence gathered in the absence of a criminal predicate is unlawfully gathered intelligence."[51]

Response: The fallacy of this argument rests on erroneous or misinformed assumptions about the law enforcement intelligence function. The first is that *information* is collected; *intelligence* is the output of the analytic process. This is an important distinction.

Certainly intelligence is preemptive. The intent of intelligence is to *prevent* crime. All crime-prevention programs are a form of preemptive law enforcement. The rationale of the criticism is inherently illogical. A cornerstone of law enforcement for decades has been a preemptive approach toward crime whenever possible. Indeed, this preemptive philosophy is the reason that the National Crime Prevention Council was created. Law enforcement intelligence is simply another dimension of prevention.

With respect to the concern about "unlawfully gathering" information, law enforcement personnel at all levels of government are acutely aware of the criminal predicate standard for intelligence. They adhere to privacy and civil rights standards in the intelligence process just as they adhere to constitutional standards of criminal procedure in the course of criminal investigations. Law enforcement organizations have privacy policies, intelligence records policies, and training, all of which meet constitutional and regulatory requirements. Law enforcement understands these obligations and fulfills them.

Concern: "Ambiguous lines of authority allow for 'policy shopping'. … Fusion centers … exist in a no-man's land between the Federal Government and the states, where policy and oversight is often uncertain and open to manipulation."[52]

[50] Global Intelligence Working Group. *Fusion Center Guidelines.* Washington, D.C.: Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, 2005, p. 5.

[51] Masse and Rollins, Ibid., p. 5.

[52] German, Michael and Jay Stanley. *What's Wrong with Fusion Centers?* New York American Civil Liberties Union, 2007, p. 9.

Response: All state and regional fusion centers are a part of state or local government; therefore, they have a chain of command and accountability to their parent governmental authority. All fusion centers have a policy manual that establishes, among other things, authority and responsibility. In some cases, fusion centers may be colocated with federal agencies, most notably with the FBI; however, there are clear lines of authority and responsibility for the management and accountability of the fusion center to the state or local government. Some have governing boards, others have direct lines of command to a state or local law enforcement organization or state office of homeland security. While there are different organizational configurations of fusion centers, the lines of authority are unequivocally clear. The practice of policy shopping simply does not occur.

Concern: "Private sector participation in fusion centers risks privacy and security. Fusion centers are poised to become part of a wide-ranging trend of recent years in the United States: the creation of a 'Surveillance-Industrial Complex' in which security agencies and the corporate sector join together in a frenzy of mass information gathering, tracking, and routine surveillance."[53]

Response: All nonlaw enforcement personnel in fusion centers, including public and private partners, must pass a background investigation before they are given access to information. Most have security clearances, which make them subject to federal laws governing the handling of classified and sensitive information and state and local privacy protection laws. In addition, private-sector representatives do not represent a single company, but the entire sector. The Washington Joint Analysis Center (WAJAC), for example, reached an agreement with The Boeing Company to assign a Boeing intelligence analyst to WAJAC. The analyst has a Defense Department security clearance and will represent aircraft manufacturers and their suppliers in the fusion center.

Information-collection for the intelligence process is a product of explicit procedures that are dictated by law and the scientific approach to problem solving—it is not collected in a frenzy. Indeed, mass information-gathering is avoided because it makes the intelligence process more difficult since it means that a greater mass of information would have to be sorted through to identify a threat. Indeed, the purpose of *intelligence requirements* is to identify and collect only that information which is needed for analysis.

The *National Criminal Intelligence Sharing Plan,* the *Fusion Center Guidelines,* the *Information Sharing Environment Implementation Plan,* and the DHS *Target Capabilities List* describe the importance of private-sector involvement in law enforcement intelligence.

[53] Ibid., p. 11.

Certainly there is sensitivity to the types of information to which the private sector participants have access; therefore, each fusion center has a privacy policy to which private-sector participants agree to adhere. Moreover, private-sector partners have to sign a memorandum of understanding (MOU) and a nondisclosure agreement, all of which help to protect individual privacy.

Concern: "Military participation in fusion centers violates fundamental tenets of liberty. Officials who regard American communities as battlegrounds in a 'war' can be tempted to dispense with 'inconvenient' checks and balances."[54]

Response: While the public may not be aware, both law enforcement agencies and military representatives in the law enforcement intelligence arena are hypersensitive to these issues.

Law enforcement does not have this war perspective, nor is law enforcement influenced by the military. Law enforcement agencies are acutely aware of the distinctions and simply use the military as a lawful support resource in the fusion centers just as the military has been used for years as a lawful resource in drug enforcement initiatives. Analysts, not information collectors or operational personnel, are assigned to fusion centers from the military; most typically, they are from the National Guard.

Concern: "Data fusion = data mining, which is bad for privacy and bad for security."[55]

Response: These two forms of research and analysis are *not* the same. *Data mining* (also known as Knowledge Discovery) has been defined as "the nontrivial extraction of implicit, previously unknown and potentially useful information from data".[56] It uses machine learning and statistical and visualization techniques to discover and present knowledge in a form which is easily comprehensible to humans.[57] *Data fusion* is the process of integrating information obtained from many heterogeneous sources into a single composite picture of the environment.[58]

Data mining is a proactive process using sophisticated software and mathematical models to develop new knowledge about an entity. Data fusion is an integration and analytic technique that increases the accuracy of analysis by relying on a wide array of diverse information sources. Generally speaking, law enforcement agencies and fusion centers have neither the resources nor the expertise for data mining activities; however, the inclusion of different agencies from different levels of government establishes the heterogeneous information sources characteristic of data fusion. Analysis is performed on this diverse data using the scientific approach to problem solving as is characteristic of all types of intelligence analysis.

[54] Ibid., p. 15.

[53] Ibid., p. 11.

[54] Ibid., p. 15.

[55] Ibid., p. 15.

[56] Frawley, W., G. Piatetsky-Shapiro, and C. Matheus. "Knowledge Discovery in Databases: An Overview." *Artificial Intelligence Magazine* (Fall 1992), 213–228.

[57] www.the-data-mine.com, *Introduction to Data Mining.*

[58] www.cas.edu.au/content.php/260.html

Concern: "Excessive secrecy undermines the mission of fusion centers."[59]

Response: Fusion centers operated by state and local law enforcement should have transparent processes; however, the content of much of their work must remain largely secret both to protect privacy and protect the integrity of inquiries. Some levels of secrecy increase when the fusion center is accredited as a Sensitive Compartmented Information Facility (SCIF).[60] In these cases, there will be more secrecy, as a matter of federal law, because the facility will contain classified information. While there are instances of excessive secrecy, the fundamental issue is that "excessive" will be interpreted differently, depending on one's position and perspective.

For many people, the past abuse of law enforcement intelligence will be the lens through which all law enforcement intelligence activities will be judged. The ongoing skepticism, while frustrating, is a reminder of the need to remain vigilant in training, supervising, and managing the intelligence process.

Similarly, critics need to realize the radical changes that have occurred in law enforcement organizations during the past 5 decades. Officers are significantly more educated, training has increased dramatically, and professional leadership has embraced modern management techniques, values, and responsibilities. This underlying fabric serves as an important foundation for the law enforcement intelligence function.

Fusion Centers and Civil Rights Issues

There is a concern among many privacy advocates that the growth of fusion centers will increase the jeopardy to citizens' civil rights and privacy. As noted in a National Governors Association best practices paper, "The risks to individuals' privacy begin when personal information of any kind is entered into criminal justice information systems."[61] Criminal intelligence records systems are certainly included in this description and warrant special attention because of the low level of proof— i.e., reasonable suspicion—required to enter personal identifying information into the system.

Complicating this issue is the fact that by not understanding the concept of the fusion process, many privacy advocates fear that the centers are the next iteration of centralized surveillance of citizens.

Perhaps the greatest concern of a fusion center in this regard is the participation of federal law enforcement agencies whose jurisdiction for information collection and retention is different from SLTLE agencies. Certainly, when an SLTLE agency is the custodian of an intelligence records' system, care must be taken to exclude information from the fusion center that does not meet the standards of 28 CFR Part 23.

Fundamentally, the privacy and civil rights issues of citizens related to fusion centers are the same as any other aspect of the intelligence process. Those relevant standards of the NCISP apply in the same manner and should be fully

[59] German and Stanley, Ibid., p. 9.

[60] For more information on SCIFs, see www.fas.org then search for "Physical Security Standards for Sensitive Compartmented Information Facilities"

[61] MacLellan, Thomas. *Protecting Privacy in Integrated Justice Systems.* Washington, D.C.: National Governors Association Center for Best Practices, 2006, p. 4

10 WAYS TO ENGAGE AND SUPPORT YOUR FUSION CENTER

- **Recognize the importance of information sharing.** Encourage the practice of sharing information with other law enforcement and public safety agencies. Use the guidelines and action steps of the NCISP to implement or enhance your organization's intelligence function.
- **Improve information flow.** Ensure that channels of communication exist to efficiently share information and intelligence, including Suspicious Activity Reports. Work with the fusion center to agree on a common lexicon and the most effective and efficient methods for the transfer of this information.
- **Support an information-sharing culture through training initiatives.** Provide training programs for everyone and explain intelligence, why it is valuable, and how it benefits the department.
- **Train new recruits.** Provide training to new recruits on the role of fusion centers, why the mission is important, what information to collect, and how to send information to the fusion center.
- **Communicate your needs to the fusion center or governing board.** Constantly communicate your information needs and requirements to the fusion center and offer definitions for actionable information. Ensure that your agency provides feedback on the value of products disseminated and offers recommendations for improvement when necessary.
- **Assign personnel to the fusion center.** Depending on the center, officers, investigators, and analysts may all be assigned and have skills and knowledge to contribute. There are many models for assignment—some agencies choose to assign personnel on a part-time basis (e.g., 1 day a week)—while others serve full-time for a 3- or 6-month rotation.
- **Establish or participate in a terrorism liaison officer (TLO) program.** For departments who cannot afford to lend personnel to a center, participate in a TLO program or intelligence liaison officer programs. Their purpose is to disseminate information distributed by the center to the "boots on the ground" and ensure that all appropriate information collected by his or her agency is effectively shared with the fusion center.
- **Educate political leaders.** Educating political leaders about fusion centers, their value, and their needs may encourage them to demonstrate commitment to the fusion concept and, thus, support your agency and that commitment through appropriate funding. Join the governing board of the fusion center, if one exists. Participating on an interagency governing board will demonstrate the importance of collaborating with the fusion center and allow for a greater understanding of the capabilities and products the center has to offer law enforcement.
- **Hire analysts, if possible.** Both intelligence and crime analysts require different skill sets than those required for patrol officers and investigators. Analysts can make officers work smarter, providing for both increased efficiency and effectiveness.

Based on: *10 Ways to Engage and Support Your Fusion Center*. Washington, D.C.: Police Executive Research Forum, 2008. https://www.llis.dhs.gov (Must register to access).

adhered to. Further, *Guideline 8* of the *Fusion Center Guidelines* states that the management of the fusion center should: "Develop, publish, and adhere to a privacy and civil rights policy."[62] Commentary on this guideline goes on to note the following:

> …one of the critical issues that could quickly stop intelligence sharing is the real or perceived violation of individuals' privacy and constitutional rights through the use of intelligence sharing systems. In order to balance law enforcement's ability to share information while ensuring that the rights of citizens are upheld, appropriate privacy policies must be in place.[63]

As a consequence, civil rights issues for fusion centers have components related to policy, training, supervision, and public information that must be addressed in the development and implementation stages.

Developing the Fusion Center

As noted previously, a fusion center's operations should be consistent with the recommendations of the *NCISP*[64] and the *Fusion Center Guidelines*[65] of the Global Intelligence Working Group. The *NCISP* provides standards for all aspects of the intelligence function to ensure best practices, effective operations, and adherence to civil rights. The *Fusion Center Guidelines* are designed to ensure the following:

> Information and intelligence sharing among states and jurisdictions will become seamless and efficient when each fusion center utilizes a common set of guidelines. The complete support of public safety leaders at all levels is critical to the successful implementation and operation of fusion centers.[66]

Adherence to established national standards will increase the quality of information sharing both within the fusion center's participants' jurisdictions, with intelligence entities outside of the region, and with the Information Sharing Environment. Further, the standards will institutionalize a consistent approach to information collection, retention, analysis, and dissemination that represent recognized and accepted processes as defined by the consensus of intelligence subject matter experts who helped design the standards.

Beyond relying on national standards, consideration must be given to defining who the center's stakeholders are and determining what it will take to get the stakeholders' buy-in to the center's operations. It is this simple: There is a direct correlation between stakeholders' (or consumers') participation in the fusion center and the success of the center. Similarly, stakeholders will not participate in the center unless the products they receive are useful.

To assist in the development and utility of fusion centers, the following common themes, and more important, common questions, should be examined:

- Do fusion centers solve the pre-9/11 information-sharing problems, and as such, make Americans safer?
- Can fusion centers work if they are not part of an integrated philosophy of intelligence and security?
- Who benefits from fusion centers?

[62] *Fusion Center Guidelines,* Ibid., p. 49.

[63] Ibid.

[64] See it.ojp.gov/documents/ncisp.

[65] See www.iir.com/global/guidelines.htm.

[66] Global Intelligence Working Group, 2005., Ibid., p. ii.

- Who should staff, fund, and oversee them?
- What role, if any, should fusion centers play in the Intelligence Community?
- What role should federal agencies play in fusion centers, including funding?
- Do fusion centers represent a shift in the security versus civil liberties pendulum?
- How active and proactive, if at all, should fusion centers be in the collection of intelligence that is not directly tied to a specific and identifiable criminal act?
- Is the current configuration of 40-plus fusion centers, in some cases several operating within one state, the most efficient organizational structure?
- Is the current approach to creating, authorizing, funding, and supporting fusion centers sustainable?
- What are the risks to the fusion center concept and how have those risks been specifically weighed and balanced against the stated goals of fusion center operations?[67]

The answers to these questions provide the foundation for shaping the guiding principles related to the creation and management of fusion centers:

1. Adhere to the tenets contained in the *NCISP*.
2. Collaboratively develop and embrace a mission statement.
3. Create a representative governance structure.
4. Use an MOU or other type of agreement, as appropriate.
5. Integrate SLTLE agencies.
6. Create an environment in which participants can seamlessly communicate.
7. Develop, publish, and adhere to a policies and procedures manual.
8. Develop, publish, and adhere to a privacy policy.
9. Ensure that appropriate security measures are in place for the facility, data, and personnel.
10. Integrate sworn and nonsworn personnel and ensure that all personnel are properly trained.
11. Leverage existing systems and databases and allow for future connectivity.
12. Offer a variety of intelligence services and monitor outputs and outcomes.[68]

[67] Masse and Rollins, Ibid., pp. 3—4.

[68] Modafferi, Peter and Kenneth Bouche. "Intelligence Sharing: Efforts to Develop Fusion Center Intelligence Standards." *The Police Chief* Vol. 7, No. 2, February 2005.

From an *operational* perspective, the experience of the North Central Texas Fusion Center has defined five guiding principles in support of the fusion center's performance:

Guiding Principle 1:	Processing tools and the aggregation of data across jurisdictions and across disciplines are required to achieve the benefits of fusion.
Guiding Principle 2:	Visualization and analysis tools are essential for "connecting the dots."
Guiding Principle 3:	The most important objective is disaster prevention, early warning, and mitigation.
Guiding Principle 4:	The more data the better.
Guiding Principle 5:	Cross-disciplinary analyst(s) need to be assigned to constantly explore the data and test hypotheses.[69]

Building on these principles, three broad phases, each with specific focal areas, are envisioned to accomplish the fusion center's development.

Phase 1. The foundation phase includes these components:

- **Reeducation.** Stakeholders must understand the contemporary role of law enforcement intelligence and the capabilities of the fusion center. Just as important, stakeholders must understand their role in making the intelligence function succeed at preventing acts of terrorism, prevent the occurrence of organized crime, and manage homeland security threats that may affect public safety. As recommended by the *NCISP* and the *Minimum Criminal Intelligence Training Standards,* personnel at all levels of the organization, from executives to line personnel, must receive awareness training as intelligence relates to their role.
- **Developing a mission, goals, and objectives.** What should the fusion center do? How will it operate? What crimes will it address? What will it produce? What is its role and relationship with its consumers? What are the priorities of the fusion center? These questions must be resolved and articulated in the mission, goals, and objectives. It is a laborious process requiring input from executives to stakeholders. It cannot be done effectively, however, until after the training component is completed because all personnel must understand the contemporary law enforcement intelligence function and ensure that their vision of the fusion center is consistent with contemporary standards.
- **What the fusion center will not do.** Just as important as what the fusion center will do, is some discussion of what the fusion center will not do. There will likely be changes in the historic intelligence activities of agencies that will not be continued in the fusion center; for example, many activities of state police intelligence units tended to be more akin to investigative support rather than intelligence activities. For the center to function most effectively, these factors must be clear. Similarly, stakeholders and consumers must understand what the fusion center will not do to avoid erroneous expectations.

[69] Stone, Kelly. *Deploying and Operating an Effective Regional Fusion System: Lessons Learned from the North Central Texas Fusion System.* Unpublished policy paper prepared by the North Central Texas Fusion System, McKinney, Texas, 2006, p. 5.

Phase 2. Proactive developmental activities that must be overtly addressed in this phase include the following:

- **Developing relationships.** Two critical elements to the success of any intelligence activity are information collection and information dissemination. Both must have detailed elements to ensure that everyone does his or her job with respect to intelligence activities. The fusion center must rely on management support from partnering agencies to support the fusion center. It must also rely on personnel to collect needed information, document it, and forward it to the fusion center. Similarly, to succeed, dissemination of information and products from the fusion center must be done in an effective manner that is easily accessible by consumers, in a format that is easy to use, and consistently contain useful information. To accomplish this, there must be overt initiatives to develop relationships among stakeholders within the fusion center and with its external constituency by developing commitments to participate in the center's activities.
- **Outputs/products.** The fusion center must identify specific outputs and products that will be produced on a regular basis. These are among the questions that need to be addressed and articulated as the fusion center's development process moves forward: Will both tactical and strategic reports be produced? Will bulletins and advisories be produced? Will summaries be produced? What is the schedule for outputs? How will responses to specific inquiries be produced? What is the process for determining *right-to-know* and *need-to-know* standards for products and outputs?

Phase 3. The third phase involves moving Phase 1 and Phase 2 activities into operational form, including everything from facilities and staffing to developing memoranda of agreement (see Chapter Annex 8-1), to the actual implementation of the fusion center's operations. This phase can consume a massive amount of time and logistics, particularly when the intelligence function is not only being revised, but reengineered, as well. Other activities in this phase include melding agencies and their data, protecting each agency's data, standardizing data for incorporation into a single system, ensuring quality control (i.e., accuracy) of data, security of the data, and establishing processes for auditing and accountability.

Outputs of the Fusion Center

The fusion center is not designed to respond to ongoing calls or inquiries about individuals or threats. While this will no doubt occur occasionally, if it happens too frequently the staff will be overwhelmed and unable to perform their analytic responsibilities. The most important output of the intelligence fusion center is actionable intelligence, meaning that the intelligence produced by the center will drive operational responses and a strategic awareness of threats.

An operational response occurs when the analysis determines that there is a threat against a specific type of target. Operationally, the law enforcement agency may then take necessary actions to harden the target or intercept the threat. Strategic awareness is broader information that provides information about threats and methodologies or indicators of terrorists and criminals.

The specific kinds of output from fusion centers are not universal. Different regions of the country, the character of targets in a region, and the unique character of threats must be taken into consideration when output is being

designed. In a given geographic region, for example, there may be a large presence of active right-wing extremists and, therefore, the fusion center would focus a significant amount of attention on their activities. Similarly, the U.S. border with Mexico would receive significant attention devoted to drug smuggling and human trafficking. Thus, while all fusion centers should have an all-crimes approach, strategic priorities within those crime categories would be appropriate.

In light of this, the fusion center's substantive outputs should be based on three basic factors:

1. Defined threats based on comprehensive and ongoing threat assessments within the jurisdiction of the fusion center.
2. Information and intelligence needs defined by stakeholders.
3. National priorities, including those of external funding, such as the National Preparedness Goal[70] or FBI intelligence requirements.

Beyond the substantive content, the format and frequency of outputs need to be identified, specifically in light of the types of analysis and products that are produced and the frequency of which they are produced. In some cases, the format of the output may be dependent on unique characteristics of the fusion center's jurisdiction. E-mail alerts, for example, may not be feasible in regions where there is limited electronic connectivity among law enforcement agencies. Similarly, intelligence alerts and bulletins that are designed as briefings and handed out at roll calls would not be feasible for rural or decentralized law enforcement agencies. Types of output may include any or all of the following:

- Summary briefs—incidents and activities, globally or locally, that may have some correlation to threats, particularly if the incidents reflect a trend.
- Threat assessment—a detailed description of threats, targets, the likelihood of an attack against a defined target, and the potential methods of attack.
- Situational awareness reports—the current status of known threats or changes in the status of known threats.
- Information bulletin—information on new or emerging threats, including threat indicators and methodologies.
- Intelligence assessments—comprehensive analysis, usually of a strategic nature, about a threat.
- Raw intelligence—information that is derived from a source deemed to be reliable but that has not been corroborated or analyzed. Typically, the threat is time-critical and potentially severe, hence the dissemination of the information.

In addition to these intelligence products, the fusion center will also produce case intelligence, which is intelligence related to specific threats, targets, and suspects. Case intelligence is produced and disseminated on a timely basis as facts warrant rather than on a fixed schedule. Dissemination is narrower and goes only to persons who have a demonstrable *right to know* and *need to know* the information.

The different intelligence outputs may use a variety of analytic techniques such as link analysis, financial analysis, association matrices, visual investigative analysis, threat profiling, and pattern analysis. Typically, a fusion center would also be

[70] www.llis.dhs.gov/member/secure/dynamicpage.cfm?pagetitle=Preparedness (Must register to access)

involved in other processes that enhance the criminal inquiries of intelligence targets, such as deconfliction, case correlation (particularly between jurisdictions), and intelligence support of investigations related to criminal enterprises and terrorism.

Conclusion

The intelligence fusion process holds a great deal of promise for effective intelligence operations. This is particularly true, given the multijurisdictional character of terrorists' operations and criminal enterprises, as well as hazards that will require public safety operations. The four greatest challenges are: 1. Develop a cooperative and committed relationship between all stakeholders; 2. Ensure privacy and protection of personal identifying information; 3. Establish policies and processes that support efficient, effective, and lawful intelligence operations; and 4. Stay on message as an analytic center.

Chapter Annex 8-1: Developing a Memorandum of Understanding[71]

Fusion centers inherently require the sharing of information and, oftentimes, resources between law enforcement agencies. In either case, there are important obligations on the part of the fusion center and each agency that enters into an agreement with the fusion center. An agreement needs to be in place to formalize and institutionalize obligations and responsibilities of all parties involved. These agreements have different names: memorandum of understanding (MOU), memorandum of agreement, letter of understanding, or statement of understanding. Regardless of the name, all refer to a written agreement between two or more parties that articulates a specific relationship.

Because the nature of the agreements will vary widely, this description focuses on the basic principles and types of content that should be included in an MOA.

Guiding Principles of an MOU:

- *The MOU Is a Statement of Commitment*—The MOU defines the actual agreements and responsibilities in the relationship. The commitment statement can set the context, quality, or sentiment behind the relationship.
- *The MOU Requires Explicit Statements of Expectations and Obligations*—Specific activities, expertise, and resources need to be articulated in the agreement with as much detail as possible.
- *The MOU Must State What Is Not Intended To Be Covered*—If there are specific activities and responsibilities that might be assumed to be covered by the MOU but are not intended to be covered by the agreement, they should be spelled out.

Contents of an MOU:

1. Introduction
    a. What is the intent, capability, or resource for which the MOU is being created?
    b. Specify the agencies that are participating in the MOU. An MOU may between two entities, such as the fusion center and a single law enforcement agency, or it may include multiple parties.
    c. Provide a statement of why the MOU necessary. This is essentially the spirit of the agreement, which can be useful if questions of interpretation later arise about certain provisions in the agreement.
    d. What agreements are set forth by this MOU?
2. Purpose
    a. To what capability does the MOU apply? When answering this question, consider these questions:
        i. What is the intended level of commitment?
        ii. What is the command structure that will make decisions about, and enforce components of, the agreement?

[71] For further information see: 1. Office for Interoperability and Compatibility. *Writing Guide for a Memorandum of Understanding (MOU).* Washington, D.C.: U.S. Department of Homeland Security, undated. www.safecomprogram.gov/SAFECOM/library/default.htm
2. *Partnering for Strength: Getting your Relationships in Print*. Collaborating Agencies Responding to Disasters (CARD), undated. www.cardcanhelp.org/resources.html.

3. Scope
    a. Who are the public safety, public service, and other governmental and nongovernmental agencies that will use the capability/resource?
    b. Are there organizations or agencies that must be excluded that would otherwise be a participant?
4. Definitions
    a. What are the technical and operational aspects of responsibilities, capabilities, and resources? Consider including definitions for each.
    b. Be certain to define/explain acronyms that may be commonly used.
5. Policy
    a. Specify the circumstances for use of fusion center resources, including special requests.
    b. Specify authorization required for contacting and use of the fusion center.
    c. Specify the operating procedures associated with the fusion center as related to the parties of the MOU.
6. User Procedure Requirements
    a. What are the training, exercise, and equipment requirements associated with participating in this MOU?
7. Financial Relations
    a. If the MOU includes a fee-for-service arrangement or other financial obligations, a method for determining financial payments should be clearly established. Any and all financial commitments should be spelled out clearly, with appropriate approvals and monitoring systems in place.
    b. Articulate any financial obligations that must be considered.
        i. What is going to be done?
        ii. Who is going to do it?
        iii. Under what conditions and when will it happen?
        iv. Who pays for what?
8. Maintenance
    a. What are the maintenance requirements associated with participating in this MOU?
    b. If any licenses are required for activities (e.g., software licensing) who will own the licenses?
    c. Who will maintain the equipment?
9. Oversight
    a. What governance structure oversees the fusion center?
    b. What is the relationship of the governance structure to the parties of the MOU?
    c. What are the participation requirements in this governance structure of agencies entering this MOU?
    d. How are issues affecting policy, recommendations, and/or subsequent change implemented by the governance structure?

10. Responsibility For Standard Operating Procedure (SOP) Compliance
    a. Who is responsible for ensuring that the SOPs associated with this capability/resource are followed and that individual agency personnel are trained appropriately?
    b. How will compliance be carried out?
11. Updates To The MOU
    a. Who has the authority to update or modify this MOU?
    b. How will this MOU be updated or modified?
    c. Will updates or modifications require this MOU to have a new signature page verifying the understanding of changes by each participating agency?
12. Separation From The MOU
    a. Under what circumstances may a signatory agency withdraw from the MOU?
    b. What are the penalties or obligations (both funding and other resources), if any, for separation prior to the termination date of the MOU?
13. Authorized Signatures and Dates
    a. All parties to the MOU must have a signature of agreement and commitment by an individual who has the authority to make such commitments.
    b. Explicit dates should be specified as to when the MOU goes into effect.

Chapter Annex 8-2: Common Terrorism Information-Sharing Standards Program

Program Manager/Information-Sharing Environment

Common Terrorism Information-Sharing Standards (CTISS) Program

The Program Manager-Information Sharing Environment released standards that state, local, and federal law enforcement officials must follow when they share information about suspicious activity that could have links to terrorism. Those standards define fusion centers as central nodes for sharing information. The role of fusion centers in collection, integration, analysis, and redistribution of incident information is envisioned to follow these processes:

1. **Observation.** A person witnesses suspicious activity and reports it to a law enforcement agency.
2. **Initial response and investigation.** A law enforcement officer collects additional information from interviews and databases.
3. **Local and regional information processing.** The reporting agency stores that information in its records management system.
4. **Creation of a Suspicious Activity Report (SAR).** A person assigned to the intelligence fusion center assesses the information using standards developed by Office of the Director of National Intelligence (ODNI). If the reported activity could have links to terrorism, the official creates an Information Sharing Environment Suspicious Activity Reporting (ISE-SAR) record.
5. **Information sharing and dissemination.** That ISE-SAR record is shared with FBI and Homeland Security Department employees who work at the fusion center. The employees enter the information into FBI and DHS databases.
6. **Information processing at the federal headquarters level.** The ISE-SAR record is combined with information from other state and local authorities to create an agency-specific national threat assessment, which is shared with agencies that participate in the ISE.
7. **National Counterterrorism Center (NCTC) analysis.** The ODNI's NCTC analyzes the data using information from the intelligence, defense, law enforcement, foreign affairs, and homeland security communities.
8. **NCTC threat alerts and warnings.** The NCTC products are shared with all appropriate federal departments and agencies and with SLT through the state or major urban area fusion centers. The sharing with state, local, and tribal entities and the private sector occurs through the federal departments or agencies that have been assigned the responsibility and have connectivity with the state or major urban area fusion centers.
9. **Focused collection.** The information has come full circle and the process begins again, informed by an NCTC or other federal organization's product and the identified information needs of state, local, and tribal entities and federal field components.

www.ise.gov/pages/ctiss.html

Chapter 9:

Developing Public-Private Partnerships for Law Enforcement Intelligence

Developing Public-Private Partnerships for Law Enforcement Intelligence

Conceptually, it could be argued that the idea for public-private partnerships in law enforcement goes back to one of the most fundamental principles of policing articulated by Sir Robert Peel in 1829 in the United Kingdom. Peel noted that the government alone could not perform all policing duties—assistance was needed by members of the public and, by extension, the private business sector, to help keep communities safe from crime. Indeed, Peel argued that in a democratic society, the police derived its authority from the public; hence, the public had an obligation to assist the police on matters of public safety. His principle, "The police are the public and the public are the police" infers a reciprocal responsibility.[1] In the 21st century, this can be inferred to include two-way information sharing and joint public safety initiatives—responsibilities that both law enforcement and the private sector should embrace.

Reinforcing this notion was an observation reported in a study by the Vera Institute of Justice, which concluded:

> The police depend on citizens to assist in almost every aspect of crime prevention and investigation. Mobilizing that public support is essential to the core mission.[2]

Traditionally, the relationship between law enforcement and the private sector concerning crime control and community safety initiatives has been relatively superficial. Typically, such initiatives have been related to crime issues that were largely idiosyncratic to a given community. In some cases, the law enforcement-private sector relationship has even been contentious. For example, alarm companies and law enforcement have often had problems related to responses to false alarms just as law enforcement and private investigators or security guards have been at professional odds, often with law enforcement viewing these two groups despairingly as "police wannabes."

In other cases, new law enforcement-private sector relationships have been derailed by legitimate obstacles such as civil rights and privacy concerns by law enforcement or the potential to undermine profit and investments by private entities. While not insurmountable, resolution of these issues requires creativity and innovation, both of which are often labor-intensive. All too often the initiative has dwindled away, with both groups saying "we tried" rather than forging forward to resolve the barriers. In some cases, it was perceived that the potential outcomes were not worth the time and resource investment needed to make the initiative work. These perspectives are beginning to be reshaped in the post-9/11 era, albeit slowly.

[1] Carter, David L. *Police and the Community.* 7th ed. Englewood Cliffs, New Jersey: Prentice Hall, Inc., 2000.

[2] Bhanu, Chitra and Christopher Stone. *Public-Private Partnerships for Police Reform.* New York: Vera Institute of Justice, 2004, p. 3.

Working cooperatively with the private sector to accomplish functional goals can be highly productive. As observed by the Vera Institute:

> Perhaps the most promising but least studied source of external support for police reform is the private business community. Not only do private sector companies command political attention, they hold talent, dynamism, creativity, and a wealth of resources that can be useful to reformers within police agencies.[3]

Similarly, a study by the RAND Corporation found the following:

> Private organizations also have proved to be a good source of information for local police. Private security officers, reservation and store clerks, and baggage handlers are good examples of private sources with helpful information; they are much more likely than an officer to see or sense something suspicious. Some agencies are trying to develop such relationships by creating seminars to teach businesses about the kinds of information that are most helpful. These seminars have the twofold objective of easing the anxiety of participants while enhancing the likelihood that they will call the police with information.[4]

As law enforcement reengineers its intelligence initiatives for homeland security, it has become obvious that the need for effective public-private partnerships is more important than ever. Moreover, the partnerships need to be configured in an array of different models depending on the threat picture within a region. The obstacles still remain; however, increasingly it is understood that the value derived from such relationships is indeed worth the investment of time and resources. While there are many programmatic approaches related to the private sector associated with prevention, disaster preparedness, incident management, and response, the current discussion will be limited to public-private partnerships for intelligence (P3I).

Background and Perspective

Much of the current thought on public-private partnerships has been shaped by initiatives related to the development of the European Union. A brief look at this history provides some perspective.

As a means to increase their economic strength on a global basis, 13 Western European countries developed an agreement that was originally known as the European Economic Commonwealth. It evolved into the European Community and, as it is known today, the European Union.[5] One of the foundations of developing a viable and economically strong union of diverse, multilingual governments was to embrace public-private partnerships. The conceptual framework developed by the European Union has broad applicability to the U.S.

> A public-private partnership is an agreement of cooperation between autonomous private and public parties working together to achieve joint objectives, on the basis of a clear division of responsibilities, tasks and authority, and with no hierarchy amongst the parties. The most important preconditions for the success of a public-private partnership are mutual trust and recognition of the possibilities for the future.[6]

[3] Bhanu and Stone. Ibid., p. 1.

[4] Riley, K. Jack, Gregory Treverton, Jeremy Wilson, and Lois Davis. *State and Local Intelligence in the War on Terrorism.* Santa Monica, California: RAND Corporation, 2005, p. 40.

[5] The current European Union membership is 27 countries, with three candidate countries awaiting admission. The history of the European Union is too complex and unnecessary for the current discussion. A good history, including milestone events, can be found at europa.eu/abc/history/index_en.htm.

[6] European Commission. *Report of the Seminar on Public Private Partnerships.* The Hague, Netherlands: 2003, www.theccv.eu/binaries/English_documents/Crime_prevention/seminar_ppp.pdf, p. 6.

In expanding the concept of public-private partnerships to public safety and security issues, the European Commission report stated the following:

Security—or safety—is a fundamental right, … meaning that the State bears responsibility for the preservation of this right. Four notions are important in this respect:

1. The State cannot solve the security problems in society alone.
2. When there is a specific risk, the people in charge must take the necessary measures.
3. Repression is not the only solution; there is a need to develop prevention.
4. The problems on a local level must be tackled by a common endorsement of all the participants [public and private alike].[7]

Three conditions for effective partnerships were articulated for public-private partnerships to be functional:

1. Effective cooperation, which includes the willingness to listen, to get to know each other, to respect each other, to recognize the limits of each partner, to share useful information, leading to discretion, confidentiality and the willingness to share information.
2. Working methodically: which means not to wait for a crisis before working together, to meet regularly, to plan processes of meeting, to use tools agreed on by all the partners to collect information.
3. Strengthening and a territorial disposition adapted to the history of the [community] and to its administrative and social reality.[8]

On the last point, for P3I in the U.S., this would include consideration of civil rights and privacy issues, protection of corporate proprietary information, adherence to national standards for security of sensitive information, and participation in the Information Sharing Environment (ISE).

U.S. National Standards and Recommendations for Public-Private Partnerships

In the U.S., the need to proactively incorporate the private sector as a functional partner in the information/intelligence-sharing process has been consistently recognized by a wide range of inquiries. The *9/11 Commission Final Report* noted this:

> The mandate of the Department of Homeland Security does not end with the government; the department is also responsible for working with the private sector to ensure preparedness. This is entirely appropriate, for the private sector controls 85% of the critical infrastructure in the nation. Indeed, unless a terrorist's target is a military or other secure governmental facility, the "first" responders will almost certainly be civilians. Homeland security and national preparedness therefore often begins with the private sector.[9]

[7] European Commission. (2003). Op. cit., p. 15.

[8] European Commission. (2003). Op. cit., p. 15\6.

[9] National Commission on Terrorist Attacks upon the United States. *9/11 Commission Final Report.* Washington, D.C.: 2004, 397–398.

There is no more critical need for information-sharing with the private sector than to develop intelligence to prevent terrorists' attacks from touching U.S. soil. The 9/11 Commission goes on to observe the following on the matter of public-private information sharing:

> The necessary technology already exists. What does not [already exist] are the rules for acquiring, accessing, sharing, and using the vast stores of public and private data that may be available. When information sharing works, it is a powerful tool.[10]

In examining the successes of government information-sharing, the Government Accountability Office made the following observation:

> One of the challenges in securing our homeland is ensuring that critical information collected and analyzed by the Department of Homeland Security (DHS) and Department of Justice (DOJ) is shared in a timely and secure manner with a variety of parties within federal, state, and local governments, as well as the private sector.[11]

To deal with these issues, the *National Strategy for Homeland Security* stated, "Government at the federal, state, and local level must actively collaborate and partner with the private sector…". [12] Similarly, the *National Strategy for Information Sharing* observed, "Private sector information represents a crucial element in both understanding the current threat environment and protecting our nation's critical infrastructure from targeted attacks."[13]

The Global Intelligence Working Group recommended that law enforcement include the private sector in the law enforcement intelligence mission. Recommendation 7 of the *National Criminal Intelligence Sharing Plan,* for example, states the following:

> Local, state, tribal, and federal law enforcement agencies must recognize and partner with the public and private sectors in order to detect and prevent attacks to the nation's critical infrastructures. Steps should be taken to establish regular communications and methods of information exchange.[14]

Similarly, the *Fusion Center Guidelines* observed:

> The public safety and private sector components are integral in the fusion process because they provide fusion centers with crime-related information, including risk and threat assessments, and subject.

As evidence by the various reports cited thus far, it is clear that public-private information-sharing is critical for homeland security. It is recommended in virtually every inquiry and assessment of intelligence effectiveness, yet in the years since the 9/11 attacks, accomplishments have not reached the magnitude that was envisioned. As noted by a 2005 Bureau of Justice Assistance report exclusively devoted to public-private relationships in homeland security, "Barriers to information sharing between law enforcement and private security clearly exist."[15] The report goes on to conclude:

[10] Ibid., p 419.

[11] Government Accountability Office. *TECHNOLOGY: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives.* Washington, D.C.: Government Accountability Office, 2007, p. 9.

[12] *National Strategy for Homeland Security.* Washington, D.C.: Executive Office of the President, 2002, p. 33.

[13] *National Strategy for Information Sharing. Washington,* D.C.: Executive Office of the President, 2007, p. 4.

[14] Global Intelligence Working Group. *National Criminal Intelligence Sharing Plan.* Washington, D.C.: Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice,2003, p. 27.

[15] Morabito, Andrew and Sheldon Greenberg. *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships.* Washington, D.C.: Bureau of Justice Assistance, 2005, p. 4.

[16] Ibid., p. 7.

> The lifeblood of any policing agency is information; thus, information sharing (and its analyzed counterpart, intelligence sharing) should be a central component of any law enforcement-private security partnership.[16]

Not only has the DOJ noted the importance of public-private information sharing, a recent array of DHS inquiries has also emphasized the importance of this relationship. For example, one of the objectives of the DHS Intelligence Enterprise Strategic Plan is as follows:

> Objective 1.4: Reporting: Manage Homeland Security intelligence-related information reporting, seamlessly linking all levels of government and the private sector.[17]

Similarly, one of the DHS Lessons Learned/Best Practices papers, states:

> A jurisdiction's analysis and synthesis entity should also establish processes for sharing information with the local private sector. Private businesses and public safety agencies can provide each other with valuable threat and vulnerability information. However, public and private entities often have restrictions on information sharing with each other because of concerns over the release of sensitive or proprietary information.[18]

Yet another DHS Lessons Learned/Best Practices document recommends: "Local businesses and industries should also be incorporated into any local information sharing network".[19] One of the caveats, however, is that, "Public safety and private security officials should cooperatively establish guidelines that strike a balance between the need to inform the private sector of potential threats and the need to ensure that proprietary information is not improperly disseminated".[20] Another report addressed this issue, noting:

> Currently, no formal process exists for state, local, tribal, and private sector entities to task federal agencies with specific intelligence requirements. Failing to understand these entities' requirements inhibits the federal government's ability to understand the threats facing the Nation, much less provide actionable, timely, preferably UNCLASSIFIED, and frequently updated homeland security information and intelligence to those on the front lines of the domestic War on Terrorism.[21]

It is clear from these recommendations and assessments that the private sector must be integrated into information-sharing partnerships. Despite this plethora of recommendations, integration has been surprisingly limited. Moreover, the economic lifeblood of many communities lies in the corporate sector. Many corporations and industries—beyond those that are part of the critical infrastructure—have been identified as targets of terrorist attacks. Information-sharing between public and private entities simply has not evolved as recommended and expected. It is incumbent upon law enforcement leaders to develop a process and training to remedy that problem.

[17] Office of the Chief Intelligence Officer. *DHS Intelligence Enterprise Strategic Plan.* Washington, D.C.: U.S. Department of Homeland Security, 2006, p. 7.

[18] Lessons Learned Information Sharing Best Practices. *Local Anti-Terrorism Information and Intelligence Sharing: Dissemination.* 2006. www.llis.dhs.gov/member/secure/detail.cfm?content_id=13091. (Must register to access)

[19] Lessons Learned Information Sharing Best Practices. *Local Anti-Terrorism Information and Intelligence Sharing: Information Sharing Networks.* 2006. www.llis.dhs.gov/member/secure/detail.cfm?content_id=13088. (Must register to access)

[20] Ibid.

[21] Lessons Learned Information Sharing Best Practices. *Homeland Security Intelligence Requirements Process.* 2006. www.llis.dhs.gov/member/secure/detail.cfm?content_id=15327. (Must register to access)

P3I and the Intelligence Process

The current model of intelligence, related particularly to homeland security, addresses "all crimes, all hazards and all threats." From this perspective, state, local, and tribal law enforcement agencies are concerned with two types of intelligence: law enforcement and homeland security.

As a brief review, law enforcement intelligence is the analytic output of raw information that describes threats to a community that have a nexus with crime. This traditional form of intelligence focuses on criminal behaviors such as those related to terrorism or criminal enterprises. The less-traditional homeland security intelligence is the analytic output of raw information that describes noncriminal threats to the critical infrastructure, public health, or community safety for which a law enforcement agency will have some type of public order, public safety, and/or order-maintenance responsibility. If a pandemic flu strikes a community, for example, law enforcement agencies will likely have to assist with victims, aid in quarantines, and assist in expediting and protecting medical supplies. As another illustration, homeland security intelligence may determine that, as a result of new industry, larger barges will travel a major waterway near a community which, in turn, increases the likelihood of a barge striking a major bridge. As a result, law enforcement strategic planning would have to deal with rescue and recovery plans, traffic control plans, and security of the accident scene.

Linking both types of intelligence into a targeted capability outcome, the DHS *Target Capability List* states the following:

> Effective and timely sharing of information and intelligence occurs across Federal, State, local, tribal, territorial, regional, and private sector entities to achieve coordinated awareness of, prevention of, protection against, and response to a threatened or actual domestic terrorist attack, major disaster, or other emergency.[22]

Some challenges for P3I may occur for health professionals with unique types of personal identifying information (such as information on public health and the Health Insurance Portability and Accountability Act of 2006).[23] Plans and processes for lawfully dealing with sharing this type of information and avoiding barriers should a public health tragedy emerge are much easier to resolve before a crisis than during a crisis. If a public health emergency occurs, it would be essential for health care professionals to identify individuals to law enforcement who pose a risk or who are at risk. If processes are put in place with both law enforcement and public health professionals trained, conflict resolution and service delivery will be expedited.

The intent of this discussion has been to place some basic definitions and concepts in context to provide perspective for the P3I. A transitional issue is the relationship of public-private partnerships to the ISE from the context of state, local, and tribal law enforcement agencies.

[22] National Preparedness Directorate. *Targeted Capabilities List.* Washington, D.C.: U.S. Department of Homeland Security, 2007, p. 69.

[23] See the Office of Civil Rights, U.S. Department of Health and Human Services, www.hhs.gov/ocr/hipaa, for more information.

The Information-Sharing Environment and the Private Sector

A new challenge for both law enforcement and the private sector results from the creation of the ISE. The ISE is a formal set of guidelines and processes to enhance the sharing of intelligence across five critical sectors: 1. The Intelligence Community; 2. Federal law enforcement; 3. State, local, and tribal law enforcement; 4. The private sector; and 5. Foreign partners.

> Recognizing the need to go beyond individual solutions to create an environment—the aggregation of legal, policy, cultural, organizational, and technological conditions—for improving information sharing, Congress passed and the President signed the landmark Intelligence Reform and Terrorism Prevention Act of 2004 (IRTPA). The Act requires the President to establish an Information Sharing Environment (ISE), "for the sharing of terrorism information in a manner consistent with national security and with applicable legal standards relating to privacy and civil liberties."[24]

Based on this legislative mandate, the program manager for the ISE guided the development of an implementation plan to provide the mechanism by which the ISE would accomplish its legislative mandate. A critical starting point was defining a vision that has essentially become the ISE's ultimate goal:

> We envision a future ISE that represents a *trusted partnership among all levels of government in the United States, the private sector, and our foreign partners, to detect, prevent, disrupt, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States of America.*[25] (Emphasis in original.)

Key to realizing this vision was to create a culture of information sharing among the Intelligence Community, law enforcement agencies, and the private sector. This ambitious plan includes developing the willingness among all entities to be involved proactively in two-way information sharing, increasing technological connectivity between the entities to appropriately and lawfully share information and to develop a common lexicon to increase the quality of information while maintaining security.

As part of this challenge, the *ISE Implementation Plan* stated that the private sector should be part of "… a coordinated [information sharing] source … for access to terrorism information, alerts, warnings, and situational awareness".[26] The *Implementation Plan* went on to note that private-sector information represents a crucial element in both understanding the current threat environment and preventing the nation's critical infrastructure from being the target of attacks.

> Protecting the interconnected and interdependent U.S. infrastructure also requires a robust public-private partnership that provides the private sector with information on incidents, threats, and vulnerabilities, as well as protects private-sector information in such a way that the private sector is willing to share it with government partners.[27]

[24] Program Manager–Information Sharing Environment. *Implementation Plan for the Information Sharing Environment.* Washington, D.C.: PM–ISE, Office of the Director of National Intelligence, 2006, p. xiii.

[25] Ibid.

[26] Ibid., p. 12.

[27] Ibid., p. 19.

While going beyond the needs of the intelligence process, the primary conduits for sharing terrorism information currently are the Sector Coordinating Councils (SCC) and sector-specific Information Sharing and Analysis Centers established by the *National Infrastructure Protection Plan* (NIPP) and the National Infrastructure Coordination Center. To date, however, sharing through these mechanisms has yielded mixed results. One of the reasons stems from the ambiguity inherent in the public-private relationship. Another important factor is that the private-sector participants report the demand from federal, state, and local governments for critical infrastructure and other information since 9/11 has multiplied many times over, imposing more demands on industry to collect information and report it. Added to the complexity of these factors is that requests for private-sector information are rarely coordinated or consistent, resulting in duplicative requests.[28] If P3I is going to be successful, a consistent collection plan needs to be established. The NIPP[29] articulated six objectives that can serve as guideposts for the collection plan:

1. Sharing information to manage risks to business enterprises and in a manner that protects the information privacy and other legal rights of Americans.
2. Creating a national framework and culture for sharing information that rationalizes requests for terrorism information to the private sector and that adequately protects the risks and proprietary interests of corporations.
3. Creating an integrated, trusted environment in which information can be shared, maintained, and protected.
4. Ensuring access to the integration and analysis of data from multiple sources to provide industry with indicators of impending threats or current attacks.
5. Receiving actionable alerts and warnings concerning specific industries that improve their situational awareness of terrorist threats and enable them to prioritize risks and security investments, and shape the development of plans to ensure the security, continuity, and resiliency of infrastructure operations.
6. Implementing policies and mechanisms that provide liability and antitrust protections to the private sector in connection with sharing information in good faith.[30]

One initiative that is intended to help facilitate these initiatives is the United States Public Private Partnership (USP3). USP3 was designed to serve as a coordination conduit for private and public outreach programs creating a national cross-sector membership. Members in USP3 are involved in information sharing among the partnership.[31] While the concept is sound and there has been good support for the initiative, notably by the DHS, the project has had limited participation. Nonetheless, USP3 should be monitored and supported by local law enforcement as a foundation for developing solid partnerships with the private sector.

The challenge is to understand the complete character of P3I, defining the critical issues that must be resolved, and achieving these objectives in a manner that protects the critical interests of both private entities and law enforcement organizations. These are often competing interests; however, some principles can be relied on to guide both types of organizations through this largely uncharted territory.

[28] Ibid.

[29] The NIPP can be downloaded at www.dhs.gov/xlibrary/assets/NIPP_Plan.pdf.

[30] Ibid., p. 20.

[31] www.usp3.org

Fundamental Principles of Public-Private Partnerships for Intelligence

The P3I is intended to prevent or mitigate criminal and homeland security threats to a community through a two-way flow of raw information and intelligence. In its Homeland Security Policy Statement, the National Governors Association observed that:

> …private sector partners play a key role in providing experts, technology, and infrastructure resources to establish and maintain our nation's security. The role of the business community and the impact on the economic viability of a community when faced with [the prospect of] a terrorist attack must be considered.[32]

One perspective of understanding private-sector targets within a community is to use the framework on which the DHS relies for identifying critical infrastructures and key resources. Certain national infrastructures are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States.

- Telecommunications
- Electrical power systems
- Gas and oil storage and transportation
- Banking and finance
- Transportation
- Water supply systems
- Emergency services (including medical, police, fire, and rescue)
- Continuity of government.[33]

These elements of the critical infrastructure affect every community in the United States and, therefore, are of primary national concern.

The term "key resources" means publicly or privately controlled resources essential to the minimal operations of the economy and government.[34] A key resource can vary between communities. Hallmark Cards, for example, is not part of the U.S. critical infrastructure; however, the company employs more than 4,000 competitively paid workers at its Kansas City, Missouri, headquarters and, therefore, is a key resource for the economy of Kansas City. A key resource may also go beyond a single business and include an entire sector within a community. For example, the beef cattle industry in Dodge City, Kansas, includes cattle feed lots owned by a wide array of individuals and businesses, a cattle auction house, and multiple beef processing companies. Collectively, these businesses are the economic engine, hence key resources, for southwestern Kansas. (See Chapter Annex 9-1 for a public-private case study of this in Dodge City.)

As noted previously, while there are many roles the private sector may fulfill in homeland security, the current discussion is focusing solely on the intelligence role for prevention. As such, both private critical infrastructures and knowledge resources should be identified by their likelihood of becoming a target in light of the reasonable threats within the region.

[32] National Governors Association. "Section 5.5 – Coordination with the Private Sector." *Policy Position: EC-05.* Homeland Security Policy. Washington, D.C.: National Governors Association, 2007.

[33] *Executive Order No. 13010. Critical Infrastructure Protection.* See 42 U.S.C. 5195c(e).

[34] Homeland Security Act of 2002 codified as 6 U.S.C. 101(9).

One might also consider the nonlaw enforcement public sector within the same framework as private because much of its information processing and roles are more like the private sector than law enforcement. Moreover, these organizations will have access to unique types of information; for example, public health, agriculture and veterinary medicine, mass transportation, and aviation departments possess a significant amount of information that could provide value to both law enforcement and homeland security intelligence.

Intelligence relies on raw information. From this perspective, an important element to consider is that the private sector has access to raw information not readily available to law enforcement that can be important for responding to intelligence requirements related to threats within a community or a region. This information may come from independent sources (domestically or internationally) that a corporate security organization has developed through its own sources. These are some examples:

- An automobile manufacturer's corporate security division learns through an investigation of trans-shipment thefts from an overseas parts supplier that the same criminals are smuggling explosive components to a person within the U.S.
- Corporate security of a multinational banking firm learns of suspicious financial transactions originating in your city that involve transferring funds to a bank in Iran suspected of hosting bank accounts of persons suspected of terrorism.
- Corporate security of a large retail company discovers that drugs being smuggled from Thailand to your community are hidden in legitimate shipments of merchandise.

Information from the private sector may also be developed as the result of a request from law enforcement to be on the look out (BOLO) for certain terrorism or criminal indicators. Examples:

- Law enforcement intelligence provides training on criminal indicators to freight or package delivery companies and asks their delivery persons to report suspicious activities based on those indicators.
- Law enforcement intelligence asks retailers to notify it if certain commodities known to be used in terrorism financing or part of another type of criminal enterprise are being sold in, or stolen from, their stores (e.g., Enfamil infant formula[35]).
- Law enforcement intelligence asks a representative of large corporate retailers of certain chemicals to report unusual purchases of selected products that could be used to commit a terrorist attack.

"Business leaders often ask what—other than extra funds—they can contribute to effective police reform. One answer is skills."[36] The private sector has expertise not readily available in law enforcement. This can range from unique technologies, international audio and video communications, abilities to assess hazardous materials, and access to a wide array of equipment ranging from chemical detectors to satellites.

[35] See www.ice.gov/pi/news/newsreleases/articles/babyformula.htm.

[36] Bhanu and Stone, Op. cit., p. 3.

Types of Partnerships

Partnerships may be developed in different forms according to resources, threats, and information needs. They will be determined by such factors as the nature of threats within a community; the types of critical infrastructures and key resources in a region and their vulnerability; and the willingness of public and private organizational leaders to enter into an information-sharing partnership.

Full Partnerships through Personnel Assignment

Full partnerships occur when a person from the private sector is assigned full-time to a fusion center or intelligence unit. Typically, the individual will represent a business sector, not just the company where he or she is employed. The Boeing Corporation, for example, has assigned an intelligence analyst (who has a Department of Defense security clearance) full-time to the Washington Joint Analysis Center (WAJAC). The Boeing employee represents the entire aircraft manufacturing industry (including suppliers), not just the Boeing Corporation. The criterion for a private sector representative to be assigned to WAJAC is stipulated in its operations manual:

> "Private Entities: WAJAC shall consider the assignment of personnel from privately owned corporations who have a stake in homeland security and meet the approval of the WAJAC Advisory Board." (p. A-4).

Having a private-sector employee represent an entire sector, with the approval of the WAJAC Advisory Board, avoids allegations of playing favorites to any specific company. Moreover, it is simply more efficient and effective to have one sector representative rather than multiple representatives from one sector. Of course, a challenge is to ensure that the sector representative has an agreement with other members of the sector to share needed information.

A full partnership assignment should include, at the minimum: 1. A background investigation of the person being assigned; 2. A memorandum of agreement (MOA) between the public and private entities that spells out duties, responsibilities, and processes of both parties as related to the employee's assignment; and 3. A signed nondisclosure agreement.

The law enforcement intelligence entity needs to assess the sectors in its region to determine the most critical to have represented in the fusion center or unit. Of course, those which have major installations in the region are the most likely candidates. Table 9-1 lists the range of sectors that may provide value to an intelligence unit.

Table: 9-1: Sectors of Private Industry

• Agriculture, food, water, environment • Banking and finance • Chemical industry and hazardous materials • Criminal justice (nonlaw enforcement) • Education • Emergency services (nonlaw enforcement) • Energy • Government • Health and public health • Hospitality and lodging • Information and telecommunications • Military facilities and defense industrial base	• Postal and shipping • Private security • Public works • Real estate • Retail • Transportation – Aviation (all commercial) • Transportation – Aviation (general) • Transportation – Buses and light rail • Transportation – Maritime • Transportation – Rail • Transportation – Roads and bridges

Full-time Information-Sharing Partnership

Under a full-time arrangement there is two-way information sharing between law enforcement and private sector partners that occurs on an ongoing basis, just as the agency does with law enforcement partners. The distinction between this and the full partnership is that in the current case a person is not assigned to a fusion center or intelligence unit—he or she remains at his or her place of employment. This is particularly valuable when standing intelligence requirements are related to the private sector. The most common model where this is used is when an intelligence liaison officer[37] (ILO) program has been established.

The ILO concept establishes a formal relationship with the private-sector organization designating an individual who will be the contact point on all two-way information-sharing. Typically, the ILO is vetted for security purposes; receives training along with law enforcement officers on intelligence, counterterrorism, and homeland security intelligence issues; is given defined areas of responsibility for information-sharing; and is often given access to a secure e-mail system, such

[37] This concept is used in a variety of different agencies and has different names: Terrorism liaison officer (TLO) and industry liaison officer (ILO) are common examples. Regardless of the name of the program, the concept is the same. Similarly, the concept is not limited to the private sector. A state fusion center, for example, may designate an ILO from different law enforcement agencies throughout the state.

as the Automated Trusted Information Exchange (ATIX). ILOs should also meet regularly with the intelligence group to discuss issues and processes in order to maximize effectiveness as well as to maintain a strong relationship that is essential for sustaining the ILO program. As was the case with the full partnership, all participating organizations should sign an MOA and the ILO should sign a nondisclosure agreement.

Since the ILO will physically remain at his or her place of employment, information security becomes a greater issue for both parties. Information security processes, therefore, should be outlined in the MOA.

The ILO program is a functional option when the private sector does not have sufficient personnel to assign a person to the law enforcement agency, yet its information is critical for community safety.

The ILO fulfills a number of important roles which include, but are not limited to these:[38]

- Collect, report, retrieve, and share training materials related to threats faced by the sector.
- Serve as a source person for internal and external inquiries from the fusion center or intelligence unit.
- Collect, report, retrieve, and share information and intelligence related to potential threats to the sector.
- Identify, communicate, and serve as a liaison with stakeholders in the sector.
- Serve as the contact person for persons in the sector who have questions about, or information to share about, a threat.
- Conduct, coordinate, and/or facilitate training regarding threats in the sector. The training should be for law enforcement and/or the sector.
- Serve as the designated sector representative for meetings, associations, task forces, or any other entity related to sector threats.
- Monitor and share information with the fusion center or intelligence unit about the existence and/or changes of sector critical infrastructure and key resources.
- Conduct and maintain threat and vulnerability assessments for the sector.
- Keep up to date on terrorist and criminal threats to the sector by monitoring all sources, including open sources.
- Familiar with all law and national standards related to the intelligence function.
- Serve as a sector subject matter expert on all technical and industry-specific language, equipment, and processes for the sector.

Ad Hoc Partnerships

The ad hoc partnership is used on an as-needed basis. This is a particularly viable alternative when no standing intelligence requirements are needed from a particular industry in the private sector. When threat circumstances arise relating to the sector or organization, a mechanism is in place for rapid information-sharing. In extreme cases, a private-sector representative may be placed on a

[38] Based on the Arizona Counterterrorism Information Center bulletin on the terrorism liaison officer program.

temporary duty assignment to the law enforcement agency. Similar vetting processes should be used as in the case of the ILO as well as the memorandum of understanding (MOU) and nondisclosure agreement.

Obstacles to Law Enforcement-Private Partnerships

The inherent nature of P3I requires the open two-way exchange of threat-based information and intelligence between law enforcement agencies and the private sector for both law enforcement and homeland security purposes. As such, processes need to ensure that the exchange is open and that both law enforcement and the private sector receive the information they need. Unfortunately, this is not easy. In exploring the law enforcement-private sector relationship, the Bureau of Justice Assistance (BJA) identified three key obstacles that must be overcome when establishing effective partnerships.[39]

Obstacle 1: Barriers to Information-Sharing. A number of information-sharing barriers must be overcome by both law enforcement and the private sector if effective information sharing is to take place.

The barriers emanating from a law enforcement agency to the private sector include the following:

- Uncertainty about what types of information may be shared with the private sector because of privacy and civil rights concerns.
- Uncertainty about how to share information designated for law enforcement distribution only. In this regard, one question to resolve is whether the assignment of a private-sector representative in a formal arrangement under the authority of an MOU establishes that person as an agent for the law enforcement organization. In many cases, this will be largely influenced by state law.
- Determination of an acceptable method to share sensitive information and intelligence. (Once again, ATIX may provide the best answer.)

Conversely, private-sector barriers to law enforcement include these:

- The reluctance to share proprietary information even if related to a potential threat.
- Foreign-owned companies are reticent to share any information with the government in the U.S.
- As a rule, the private sector does not want to risk information becoming public that could harm profits.

While these information-sharing barriers are not insurmountable, they require nontraditional and creative resolution to address legal controls, information security concerns, and legitimate corporate interests.

Obstacle 2: Lack of Trust. Surveys by the Justice Department[40] have consistently found that the level of trust between law enforcement and private sector security is quite low. The two sectors often view each other as having separate goals and different constituencies. The law enforcement agency's constituency is the community it serves, whereas the constituency of the private sector includes

[39] Morabito, Andrew, and Shelton Greenberg. *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships.* Washington, D.C.: Office of Justice Assistance, U.S. Department of Justice, 2005, p. 4.

[40] Ibid.

not only a broader community but also its investors who go far beyond the local community. There is also an often unstated belief by both law enforcement and the private sector that if one cooperates, the other may not reciprocate. Contributing to the distrust is that, in some instances, private security is seen as not being equal to sworn law enforcement. Of course, private security capability is quite broad, ranging from security guards to sophisticated investigators and analysts.

BJA noted that to develop trust, law enforcement executives and their staffs must do the following:

- Create a vision and passion that brings workers together.
- Deliver what is promised.
- Ensure consistency. Constant change or change that is not understood destroys credibility.
- Communicate.
- Draw out and address past suspicions and concerns.
- Pay attention to detail.
- Train law enforcement personnel and private-sector partners together.
- Ensure equity and equality. Both sides must produce their share of work and be recognized for it.
- Reinforce the importance of the partnership (with an emphasis on sharing the credit for successes).
- Admit mistakes and learn from them. Both sides will make errors.

Obstacle 3: Misinformation and Misunderstanding. Among the major causes of lack of trust are misinformation and misunderstanding. Often, neither law enforcement nor the private sector has a complete understanding of what the other does or can do. Collectively, these have often been viewed as insurmountable by both parties. Successful partnerships demonstrate that the barriers can be overcome, but it requires leadership, commitment, and work to resolve the barriers.

How can these obstacles be overcome? BJA recommends use of the "4 C's":[41]

- Communication—Goals, plans, the types of information to be shared, and concerns should be clearly and unequivocally stated by both parties.
- Cooperation—Overt efforts must be made to reach out to the other. Each party will have wins and losses. The need to develop creative ways to share information should be paramount to establishing a trusting relationship.
- Coordination—Be certain that the actions and responsibilities of each party are clearly articulated to ensure there is no duplication and that all activities mesh well in a seamless public-private Information Sharing Environment.
- Collaboration—Not only work together, but plan together. Each should rely on the expertise and strengths of the other.

[41] Morabito and Greenberg, Ibid., p. 5.

Summary of Critical Elements when Establishing P3I

- Documentation and Agreements
  - » Operational plan to integrate private sector in intelligence operations
  - » Memorandum of agreement for activities, obligations, and services
  - » Nondisclosure agreements by both parties
  - » Liability waiver
- Processes
  - » Application review process
  - » Vetting of private-sector applicants
  - » Training
  - » Access to secure communications (consider ATIX)

Two Critical Issues to Resolve: Sharing Criminal Information and Private Proprietary Information

Sharing criminal information with a private partner has concerns and restrictions that are related to civil rights, state law, criminal intelligence records regulations and policy, and operational security. Most issues can be resolved but they will require carefully crafted policies, MOU provisions, and training. A critical issue for law enforcement is the sharing of information when individuals or organizations are identified: this is the point where constitutional protections attach.

Perhaps the easiest issue is how to share information related to criminal intelligence when individuals and organizations are *not* identified. This may be information about threat conditions, threat indicators, and advisories related to unspecified threats. In these cases, the information-sharing restrictions essentially focus on the right-to-know and need-to-know requirements. The MOA between both parties should be written in such a manner as to make the private-sector representative an agent of the law enforcement entity, thereby giving him or her the right to know. The need to know is determined on a case-by-case basis, just as it should be for law enforcement personnel.

The greater challenge is how to lawfully share information with private-sector partners that identifies individuals and organizations. When a person or organization is identified, constitutional rights and more stringent restrictions attach to the information and information-sharing process. The ability to share this information with private-sector personnel hinges on two important concerns. The first is how state law deals with privacy issues and, in particular, whether a private-sector partner is deemed to be an agent of the law enforcement agency. The second issue is the right-to-know and need-to-know standards that apply in the same manner as described above. Essential to success is the careful crafting of the MOA, training for all parties, and a secure information-sharing process.

Just as there are legal and operational restrictions on sharing criminal information, there are corporate restrictions on sharing proprietary information that belongs to private entities.

Essential Questions to Ask

- Do you know the private-sector entities in your jurisdiction that should be involved?
- Do you have an established contact with any of these private-sector entities?
- Have representatives of these entities been vetted?
- Do you have an MOA with any of these entities?
- Have the entities with which you have a relationship signed a nondisclosure agreement?

Proprietary information is information that is patented, copyrighted, and/or trademarked, and describes a product, process, design and/or formula that was developed or purchased by a private organization and is part of that organization's business processes. It includes, but is not limited to: financial information; data or statements; trade secrets; product research and development; existing and future product designs and performance specifications; marketing plans or techniques; schematics; client lists; computer programs; processes; and know-how that have been clearly identified and properly marked by the company as proprietary information, trade secrets, or company confidential information

To be proprietary, the information must have been developed by the private entity and is not available to the government or to the public without restriction from another source. The formula for a soft drink, software code, the business plan of a company, a business marketing list ,or the components of a computing device are examples of proprietary information. The nature of proprietary information can range on a very broad spectrum. Essentially, every product and every business in the world conceivably has some form of proprietary information that typically is not shared because of concern over aiding competitors or undermining one's success in the marketplace.

In some cases, proprietary information may be relevant to the prevention or mitigation of a criminal incident or emergency; for example, the design of a production or shipping facility, the location of storage and backup sites, the compounds in a chemical product, or the process to disable some type of device. In such a circumstance, it is hoped that the private entity would share proprietary information with law enforcement. To accomplish this, the law enforcement agency must recognize the magnitude that such a request holds. The disclosure of the information could undermine the success of the company. While the law enforcement agency sees the value of learning such information, it must also be cognizant of the risk that it poses to the private-sector partner. It is good practice to have a procedure for the release of proprietary information and a statement of release and nondisclosure that is signed by both parties. Examples of components of such a document are listed in Table 9-2.

Table 9-2: Sample Components of a Release and Nondisclosure Agreement Regarding Proprietary Information

- Identify the specific type of proprietary information needed.
- Provide a clear state of justification of why the information is needed to prevent or mitigate terrorism or criminal offense or the public safety need for such information.
- Define the conditions under which the private-sector entity would release the information.
- Articulate any unique stipulations to the distribution of the information.
- Define the information security requirements for protecting the proprietary information.
- Describe the time frame, if any, for which the information release is authorized.
- Describe how the information is to be handled after the threat requiring the information has passed.
- Stipulate sanctions, processes, or other remedies to impose should the information be inappropriately disclosed or disseminated.
- Signed and dated by both the public sector and private sector authorizing agents.

Developing the Message to Private-Sector Partners

- There should be a consistent message to private-sector partners, but recognize the following:
- Different types of substantive information may be disseminated to the different partners.
  - » Somewhat different information will be sought from the different partners.
- The message should emphasize their responsibility to contribute to community safety.
  - » This is somewhat of a parallel to Neighborhood Watch or Business Watch.
- Key components of the message:
  - » We need your help to protect our community by reporting suspicious activity that you observe.
  - » We will provide information on what to look for.
  - » We will provide you with details on the reporting process.
  - » The process is designed to protect the rights of innocent persons.
- Goal: To convey to partners their obligation to community safety through a structured process that protects citizens civil rights.

Developing a Successful Public-Private Partnership for Intelligence

Successes in P3I require a collaborative effort and an effective plan. In its study of public-private relationships, the Bureau of Justice Assistance identified 12 essential components to develop. These components can be used as a road map for creating a public-private partnership. To begin, the law enforcement agency must articulate its vision and responsibilities for each of the factors listed

below (See Figure 9-1). The response to each factor is reviewed and refined by those responsible for establishing and managing the partnership. The final implementation plan, including commitments of personnel and resources, is reviewed, refined (as necessary), and affirmed by the chief executive. The critical factors to be addressed in this process are the following:

- Negotiate and develop common goals.
- Identify and develop common tasks for both law enforcement and private-sector personnel.
- Develop knowledge of the capabilities and goals of participating agencies and businesses.
- Articulate well-defined projected outcomes.
- Establish a reasonable timetable for implementation.
- Provide training on the concepts, purpose, and tasks for all involved.
- Clearly identify the tangible purposes of the partnership.
- Clearly identify leaders and those responsible for tasks and goals.
- Create an operational guide on how the partnership will function after it is implemented.
- Secure an agreement by all partners about how the partnership will proceed, including resources and responsibilities.
- Articulate a mutual commitment to providing necessary resources.
- Establish an assessment and reporting process.[42]

Denver Police Department Public-Private Partnership (DP3)
The acronym DP3 stands for Denver Public-Private Partnership. DP3 represents the Denver Police Department's effort at forming a partnership with private security professionals in the City and County of Denver.

The centerpiece of DP3 is a broadcast alert communication network whereby DP3 members receive up-to-the-minute information regarding security threats, crime trends and incidents-in-progress, upcoming major events, BOLO announcements, and the like.

Additionally, DP3's web site will post crime-prevention information and have links to partner organizations' web sites. These sites have many valuable resources relating to security, domestic preparedness, and major incident planning.

Benefits of Membership
The DP3 homepage will post public information and links, but members will have additional privileges. DP3 members, after a limited background and records check, will receive e-mail or text messages and alerts. Members will also have access to the DP3 archives of past alerts and the document library.

Who Should Join
Eligibility for membership in DP3 is limited to security directors and supervisors having an established proprietary or contractual security force within the City and County of Denver. They may also designate members of their staff as being eligible for membership. Access to the DP3 site, however, is open. A brief e-mail to DP3@ci.denver.co.us expressing interest in membership is all that is required, and you will be contacted with instructions and an application. Applicants will undergo a brief computer records and background check as part of the application and approval process.

www.denvergov.org/DP3

---

[42] Adapted from: Morabito and Greenberg, Ibid, pp. 5–6.

Following this process provides a solid foundation and a clear purpose for the partnership with a demonstration of support and commitment by the chief executive. Collectively, this represents an explicit development plan that may be submitted to potential private-sector partners. If the partnership is going to move forward, the private sector must review, refine, and agree to its responsibilities associated with the above factors. There may need to be a negotiation process on certain elements of the plan, which the law enforcement agency must reasonably consider. In the end, each party must agree to its responsibilities and commitments before the partnership is finalized. The development and implementation plan should then move into a joint operational plan with a signed MOA, as appropriate (see Figure 9-1 again).

It is a recipe for failure if either the law enforcement agency or private entity attempts to implement critical factors without input from the other party. Remember that in many cases, the private partner will often have to sell the partnership to a larger corporate structure. As such, demonstrating substantive input into the partnership development process by the private entity can be an important factor in securing corporate commitments.

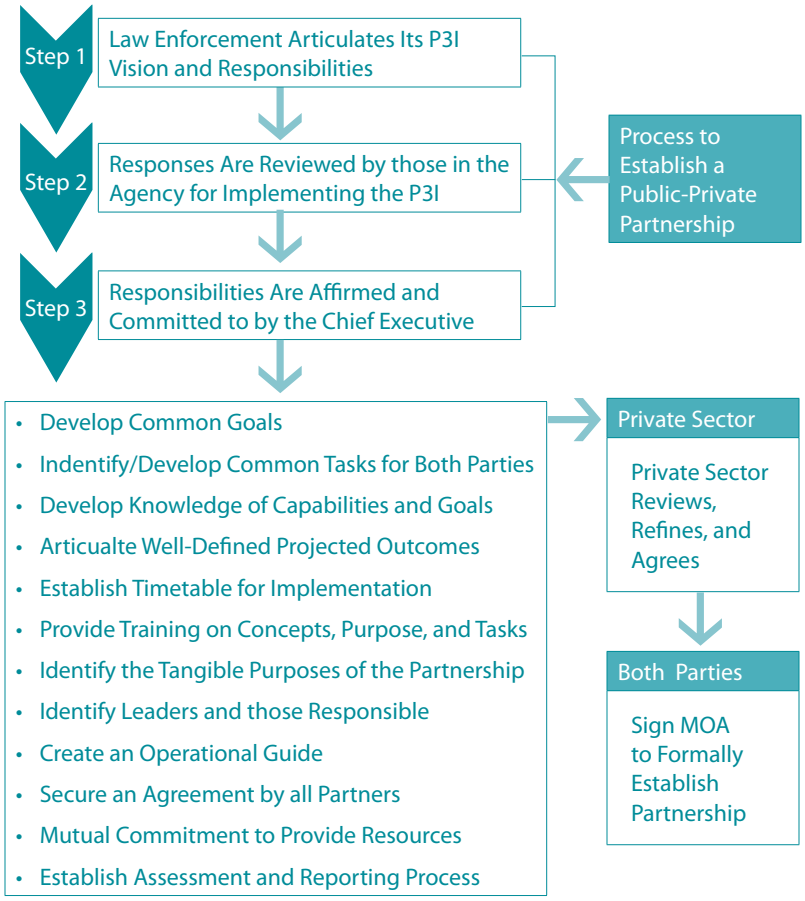
In developing a public-private partnership in support of the intelligence function, Matthew Simeone of the Nassau County, New York, Police Department identified several key factors executives should consider:

- First who, then what: Make sure the right people were in the right positions in the organization before they decide on strategy.
- Tipping Point Leadership: Within every organization there are people, acts, and activities that exert a disproportionate amount of influence on performance. Consequently, focusing efforts on identifying and then leveraging these factors can enable great change.
- Instilling a Need for Change: An initiative involving the private sector and information sharing is likely to bring about debate within the agency regarding the type of information that will be shared. Preparing an internal campaign that addresses the anticipated concerns of officers and the value they will receive from the partnership is essential for the partnership to be effective.
- Committing the Resource: As has been discussed on previous issues, the failure to commit resources to the partnership is essentially condemning the partnership to failure.
- Leveraging the Natural Leaders: The person responsible for developing and implementing the public-private partnership must believe in the concept, understand the concept, have the interpersonal and intellectual skills to move the partnership forward, and be respected within the agency as an informal leader.
- Be Open to Innovation: Agencies should be open to user innovation and should encourage creativity and sharing within the agreed-on guidelines. Just because something has not been done before does not mean it is a bad idea or that it will not work.
- Build on Established Experiences: While public-private partnerships for intelligence may be new, the agency may have previous public-private experiences related to crime prevention or community policing that can serve as a springboard for the intelligence initiative.[43]

Some examples of different law enforcement-private partnership models will provide additional insight.

[43] Adapted from: Simeone, Matthew J. *The Integration of Virtual Public-Private Partnerships in Law Enforcement to Achieve Enhanced Intelligence-Led Policing.* Monterey, California: A thesis prepared for the Naval Postgraduate School, 2007, 103–108.

Figure 9-1: Establishing a Public-Private Partnership for Intelligence



InfraGard[44]

In the 1990s, with the rapid growth of computer networking and reliance on computerization for managing many aspects of government and commerce, it was recognized that the U.S. cyber infrastructure responsible for sustaining the fundamental elements of American life was increasingly vulnerable to terrorist attacks, criminal incursions, and natural disasters. To address this issue, a new initiative in critical infrastructure protection was developed by the Federal Bureau of Investigation (FBI) with the expressed purpose of understanding potential threats and developing ways to prevent or mitigate threats. The greatest emphasis was focused on cyber threats and cyber security.

As this initiative developed, it became apparent that a significant portion of the critical infrastructure was owned by the private sector. As such, it was concluded that critical infrastructure could be adequately protected only by developing a two-way information-sharing partnership between the government and the private sector. It was in this environment that InfraGard was developed.

InfraGard is an information-sharing and analysis effort serving the interests and combining the knowledge base of a wide range of members. At its most basic level, InfraGard is a partnership between the FBI and the private sector. It is an

[44] For more information about InfraGard see www.infragard.net/about.php?mn=1&sm=1-0.

association of businesses, academic institutions, state and local law enforcement agencies, and other participants dedicated to sharing information and intelligence to prevent hostile acts against the United States. InfraGard chapters are geographically linked with FBI Field Office territories, with an FBI special agent coordinator assigned to it. The FBI coordinator works closely with program managers in the Cyber Division at FBI Headquarters.

In its early development, InfraGard was under the direction of the National Infrastructure Protection Center (NIPC) with its focus on cyber infrastructure protection. After September 11, 2001, NIPC expanded its efforts to include physical as well as cyber threats to critical infrastructures. InfraGard's mission expanded accordingly.

In March 2003, the NIPC was transferred to the DHS, which now has responsibility for Critical Infrastructure Protection (CIP) matters. The FBI retained InfraGard as an FBI-sponsored program and works with DHS in support of its CIP mission, facilitating InfraGard's continuing role in CIP activities. In addition, the FBI has further developed InfraGard's ability to support the FBI's investigative mission, especially as it pertains to counterterrorism and cyber crimes.

The goal of InfraGard is to have ongoing, two-way, substantive information sharing between the FBI and its private-sector critical infrastructure partners. InfraGard members gain access to information that enables them to protect their assets and, in turn, give information to the government that facilitates its responsibilities to prevent and address terrorism and other crimes. This information exchange occurs at both the national and local levels for a more comprehensive approach to infrastructure protection.

To accomplish its goal, the FBI established the following objectives:

- Increase the level of information and reporting between InfraGard members and the FBI on matters related to counterterrorism, cyber crime, and other major crime programs.
- Increase interaction and information-sharing among InfraGard members and the FBI regarding threats to the critical infrastructures, vulnerabilities, and interdependencies.
- Provide members with value-added threat advisories, alerts, and warnings.
- Promote effective liaison with local, state, and federal agencies including the DHS.
- Provide members with a forum for education and training on counterterrorism, counterintelligence cyber crime, and other matters relevant to informed reporting of potential crimes and attacks on the nation and U.S. interests.

InfraGard is a solidly conceived and developed program. As might be expected, more substantive information exchanges tend to occur at the local level, while the national level initiatives are important for setting the tone for the public-private partnership. Critical to the success is having a special agent coordinator who fully understands the concept and its value and immerses himself or herself in the partnership to ensure that it is a productive relationship.

Security/Police Information Network: Nassau County, New York

The Nassau County Security/Police Information Network (SPIN) is a dynamic, multidimensional crime-prevention partnership between the Nassau County Police Department and the private sector that seeks to increase public safety through the sharing of important and timely information. This program is designed to promote homeland security initiatives and business continuity, as well as to foster the exchange of information that is critical to the success of protecting Nassau County residents and businesses.

The goals of SPIN are to share information, identify and discuss crime trends and solutions, and work together toward the common goal of protecting persons and assets. SPIN enables the police department or any other county agency to send information to the general distribution group or to a specific sector (i.e., colleges/universities, hospitals, schools, malls/retail, utilities, petroleum, technology, hotels/motels, financial institutions, corporate security, and civic leaders). In addition, SPIN connects local, state, and federal law enforcement agencies operating in Nassau County, as well as public transportation and other government agencies. As a result, SPIN's multitiered approach allows messages to be tailored to law enforcement, vetted security directors, or chambers of commerce and civic organizations.

SPIN members are contacted by e-mail of unfolding situations as they occur. Messages include notifications of bank robberies, major road closings, disruptions in public transportation, major fires or explosions, civil disturbance, public health or weather-related emergencies, or any other situations involving public safety or affecting continuity of business. In addition, Sex Offender Registry notifications are sent to vulnerable entities using SPIN. Members can use SPIN to share information or inquire about safety matters or concerns.

The establishment of such a comprehensive network has applications that are far-reaching in scope, such as: aiding in the capture of felony suspects; notifying participants of the latest crime trends; helping the continuity of business through traffic delay notifications; and facilitating the large-scale exchange of information. The network also provides the police department with the ability to provide training materials to participants that will enhance the safety of all who live and work in Nassau County. Informational meetings are held as necessary to discuss timely security-related issues. Meeting topics have included domestic terrorism, the Republican National Convention, gang awareness, and the *National Response Plan*.

Recognizing the vast amount of knowledge, expertise, and resources in the private sector, SPIN recently expanded the scope of its public-private partnership with the formation of a Security Advisory Council. Utilizing the expertise of security professionals and police officers, the Council is focused on the establishment of guidelines promoting homeland security, crime-prevention and crime-reduction techniques, as well as working toward a coordinated response to critical incidents. The Security Advisory Council's first project, *Digital Video*

Surveillance Guidelines, was recently completed. The guidelines were presented at a SPIN meeting and then posted to the departmental web site.

SPIN, in partnership with the Nassau County Office of Emergency Management, has the ability to send out information to the entire SPIN membership, or to any specific sector of private industry, which are sorted into their own e-mail distribution groups.

The design of SPIN (see Figure 9-2) is not only logical; it is easily adaptable and scalable to meet the needs of agencies of diverse sizes.

Surrounding its law enforcement core are nonlaw enforcement government agencies and responsibilities that are among the easiest with which to establish a partnership, as well as to meet and communicate on a regular basis.

Relying on e-mail and a web portal, SPIN has been comparatively inexpensive to implement, it is less labor-intensive than face-to-face initiatives, it is fast, and it is easier for many private-sector entities, particularly those with a small workforce, to participate. Yet, it has empirically been demonstrated to be highly effective.[45]

Jani-King Janitorial Services Terrorism Awareness Program
Dallas-based Jani-King International, Inc., the world's largest commercial cleaning franchisor, has announced a training program for its franchisees and employees to provide an additional level of security to the more than 50,000 buildings that Jani-King cleans. Some 10,000 franchisees will be trained to assess potential building and workplace security threats and report them to authorities.

Jani-King believes that an aggressive and proactive approach to terrorism prevention is critical and of benefit to everyone. "The key word here is prevention," says Jani-King President Jerry Crawford. "We want to create a security force multiplier to help reduce the risk of terror threats."

"Jani-King is one of the only businesses where banking institutions, major corporations, educational facilities, nuclear power plants, and utilities literally hand over the keys to their buildings and provide access to secure areas," says Crawford. "We feel an obligation to put into action additional measures to help keep these buildings safe."

Crawford explained that Jani-King's training program would specifically educate employees and franchisees on three key areas that are important to terror prevention: awareness, identification, and reporting. "The training will consist of awareness of potential security threats, recognition skills, and proper reporting channels," says Crawford. "Franchise owners will not be trained to confront suspicious persons." Crawford gave an example. "Our crews clean the same buildings night after night. We see the normal activity. We want our employees to understand how to spot suspicious activity and then how to report it."

www.bizjournals.com/dallas/stories/2004/09/13/daily13.html

---

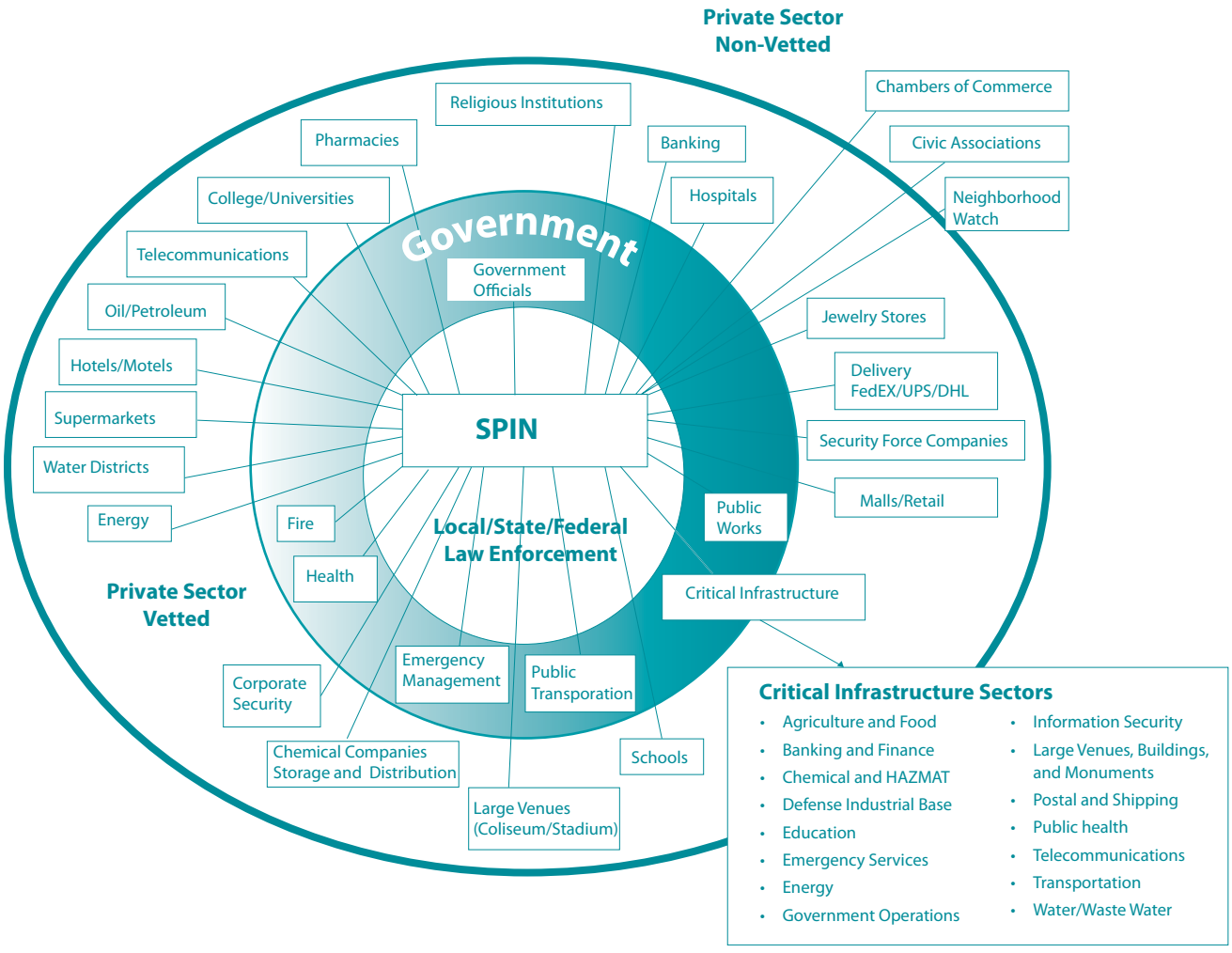
[45] For a comprehensive discussion of SPIN, see: Simeone, 2007, Op. cit.

Homeland Security, Information-Sharing, and the Private Sector

While there is an important role in all aspects of the intelligence process for public-private partnerships, it has been most comprehensively structured through initiatives of the DHS. Directed by legislation, Executive Orders, and Homeland Security Presidential Directives, DHS has developed a comprehensive structure for information sharing. Each holds potential for the intelligence process.

The DHS model has established different formal mechanisms to address its relationship with the private sector. These mechanism are intended to reach beyond the intelligence process and include the diverse elements of the *National Strategy for Homeland Security,* that include processes "to protect, prevent, respond to and recover from" terrorism and other man-made or natural threats to the homeland. The focus of the current discussion is to examine these processes from an intelligence perspective.

Figure 9-2: Nassau County (New York) Police Department SPIN Project Diagram



Critical Infrastructure Sector Partnership[46]

Critical infrastructure protection is a shared responsibility among federal, state, local, and tribal governments and the owners and operators of the nation's critical infrastructure and knowledge resources. Partnership between the public and private sectors is essential for three interactive reasons:

1. The private sector owns and operates approximately 85 percent of the nation's critical infrastructure.
2. Government agencies have access to important information about threats that may disable or destroy the critical infrastructure.
3. Both the private sector and the government control security programs, research and development, and other resources that may be more effective if discussed and shared, as appropriate, in a partnership setting.

Many factors inhibit information sharing for critical infrastructure protection, ranging from limitations by the government for sharing certain types of sensitive information to reservations by the private sector about making business processes available to persons outside of the corporate structure. Because of the important, yet tentative, understanding by both parties, mechanisms had to be put in place to enhance the sharing of important information, yet protect the responsibilities of each. *Homeland Security Presidential Directive 7* and the *NIPP* provide the overarching framework for a structured partnership between government and the private sector for protection of the CI and KRs. This sector partnership structure encourages formation of Sector Coordinating Councils and Government Coordinating Councils to facilitate communications and enhance information-sharing policies and practices.

Sector Coordinating Councils. A "sector" refers to businesses that share a common or closely related product or service. Often, members of a sector are business competitors—such as Delta Airlines and United Airlines in the aviation sector—yet they also share common risk and security problems. In the case of homeland security, sectors are identified as they relate to the protection of U.S. sovereignty and citizens, ranging from the provision of important services to the continuity of both government and the economy. The Sector Coordinating Councils (SCC) foster and facilitate the coordination of sector-wide activities and initiatives designed to improve the security of the nation's critical infrastructure. They are self-organized, self-led, broadly representative of owners and operators (and their associations) within the sector, and are focused on homeland security and critical infrastructure protection. The DHS has a strong preference that each SCC be chaired by an owner and/or operator. Government agencies may suggest the inclusion of various parts of a sector, but it is the responsibility of each SCC to identify the sector's boundaries, establish the criteria for membership, seek broad participation and representation of the diversity of the sector, and establish the governance, business case, and work processes of the sector's SCC.

Government Coordinating Councils. The Government Coordinating Councils (GCC) bring together diverse federal, state, local, and tribal interests to identify and develop collaborative strategies that advance the protection of critical infrastructures. GCCs serve as a counterpart to the SCC for each critical

[46] www.dhs.gov/xprevprot/partnerships/editorial_0206.shtm

infrastructure and key resource sector. They provide interagency coordination around CI and KR strategies and activities, policy, and communication across government and between government and the sector to support the nation's homeland security mission. GCCs coordinate with, and support the efforts of, the SCCs to plan, implement, and execute sufficient and necessary sector-wide security to support the CI and KR sector. GCCs can leverage complementary resources within government and between government and CI and KR owners and operators.

Critical Infrastructure Partnership Advisory Council

The DHS established the Critical Infrastructure Partnership Advisory Council (CIPAC) to facilitate the effective defense of our nation's critical infrastructure by coordinating federal infrastructure protection programs with the infrastructure protection activities of the private sector and of state, local, territorial, and tribal governments.

CIPAC membership encompasses CI and KR owner/operator institutions and their designated trade or equivalent organizations identified as members of existing SCCs. The GCC members of CIPAC are representatives of federal, state, local, and tribal government entities.

CIPAC provides the framework for members of SCCs and GCCs to engage in intragovernment and public-private cooperation, information sharing, and engagement across the entire range of critical infrastructure protection activities. It enables them to interact freely and share sensitive information and advice about threats, vulnerabilities, protective measures, mutual actions, and lessons learned. CIPAC, therefore is exempt from the requirements of the Federal Advisory Committee Act that require public disclosure of an advisory committee's activities.

CIPAC consists of Joint Sector Committees in which GCC and SCC members participate. The Food and Agriculture Joint Sector Committee, for example, comprises food and agriculture GCC and SCC members. The CIPAC also includes one Joint Cross-Sector Committee consisting of the designated private-sector and agency leads from each Joint Sector Committee. The 16 sectors and 7 subsectors of CIPAC are as follows:

- Chemical Sector
- Commercial Facilities Sector
- Communications Sector
- Dams Sector
- Defense Industrial Base Sector
- Emergency Services Sector
- Energy Sector
    - Electricity Subsector
    - Oil and Natural Gas Subsector
- Financial Services Sector
- Food and Agriculture Sector

- Health Care and Public Health Sector
- Information Technology Sector
- Nuclear Sector
- Postal and Shipping Sector
- State, Local, Tribal, and Territorial Government Coordinating Council
- Transportation Sector
  - Aviation Modal Subsector
  - Highway and Motor Carrier Modal Subsector
  - Maritime Modal Subsector
  - Mass Transit Modal Subsector
  - Railroad Modal Subsector
- Water Sector

Special Note: Terrorism Early Warning Group

While the structure and processes of the Terrorism Early Warning (TEW) groups concept go far beyond both private-sector and intelligence issues, it is important to note the private-sector role.[47] TEW groups include analysts from local, state, and federal agencies as well as input from the private sector and the nonlaw enforcement public sector to produce a range of intelligence products at all phases of response (pre-, trans-, and post-attack) specifically tailored to the user's operational role and requirements. TEW groups seek to identify emerging threats and provide early warning by integrating inputs and analysis from multidisciplinary, interagency teams. Using all-source/all-phase fusion, where intelligence is derived from all potential sources (classified, sensitive but unclassified, and open sources), provides information and decision support at all phases of a threat or response to a threat.[48]

In many ways, a TEW epitomizes the concept of thinking globally, acting locally because it seeks to identify global-distributed threats and achieve an understanding of their impact on a local community. This requires more than simple information sharing: it demands collaborative information fusion and the production of intelligence among cooperative nodes that are distributed among locations where terrorists operate, plan, or seek to attack.[49] As a result, there is a need to develop a diverse array of intelligence in a collaborative and integrated process that encompasses multiple sources, including the private sector.

The TEW concept and approach are based on the recognition that local and regional agencies are producers as well as users of intelligence. The following precepts form a foundation for both individual TEWs and the need to link these TEWs into a national network.

- Intelligence for domestic civil protection (homeland security) is not solely a top-down, federally-driven process.
- Intelligence must move top-down, bottom-up, and laterally. There is also a need for bilateral police information sharing and cooperation, independent of federal agencies.

[47] The "Lessons Learned Information Sharing" web site operated by the DHS has extensive resources on all aspects of the TEW. For more information search "TEW" at www.llis.gov.

[48] TEW Information based on: Sullivan, John P. *Terrorism Early Warning and Co-Production of Counterterrorism Intelligence.* Paper presented at the Canadian Association for Security and Intelligence Studies, Montreal, Quebec, Canada, 2005.

[49] Ibid.

- Local police and public safety and health agencies may be first to observe indicators.
- The need for local responsibility to protect public and craft response.
- There is a need for accountability, structure, and guidelines (i.e., doctrine) for access to national intelligence products.
- Regional entities (such as TEW groups) are partners in processing and disseminating intelligence (including providing local context and analyzing products). Local knowledge adds significant value.

Further, while an emphasis on prevention and deterrence is a critical aspect to TEW operations, the domestic intelligence effort is not exclusively related to supporting criminal investigations or pre-attack, pre-event prevention. Intelligence sharing and access to a wide range of intelligence products is needed during attacks in order to develop effective consequence management efforts.[50]

Anecdotal evidence suggests the TEW is an effective process for managing complex diverse information, particularly in large, multijurisdictional areas. As mentioned previously, the TEW concept encompasses far more than the intelligence process. As such, it requires greater degrees of collaboration among partners. Nonetheless, it is an initiative that should be explored when considering any aspect of public-private partnerships for counterterrorism.

Conclusion

The intent of this discussion was to emphasize the importance of P3I and the value such partnerships can bring to the intelligence process. Processes were described on how to develop and implement a public-private partnership as well as challenges that will be encountered. Even with the value of P3I, such partnerships nonetheless require creativity, collaboration, and flexibility by all parties to be developed effectively. There will be challenges which lack clear direction to resolve and new relationships that alter the status quo. Nonetheless, the value gained can be of significant importance for the protection of our communities.

[50] Sullivan, John P., et. al. (undated). *Los Angeles TEW Concept of Operations,* p. 10. www.llis.dhs.gov.

Chapter Annex 9-1: Public-Private Partnership Exercise

Sudden Impact: Threat Planning for Infectious Disease in Cattle

Communicable Cattle Disease Exercise
Dodge City, Ford County, Kansas
(Funded by the National Institute of Justice)

Intelligence Case Study

The following is an actual case study from Ford County (Dodge City) Kansas. Ford County is one of the largest cattle production areas in the U.S. Tens of thousands head of cattle are raised and processed here every year. Because of the critical role cattle play in the American food supply as well as the economic impact of the cattle industry in Kansas, the Kansas Bureau of Investigation (KBI) and the Ford County Sheriff's Office developed a program, with funding support from the National Institute of Justice, to determine how public safety organizations could best work with the private-sector cattle farms, sale barns, and processing plants in case an infectious disease was introduced either intentionally or through natural causes.

Particular challenges:

- Information sharing
  - Would the cattle producers provide sufficient critical information, including proprietary information, to public safety officials related to the identification or discovery of an infectious disease and the status of cattle from feedlots to processing to shipping?
  - What kind of information could the public safety sector provide to the cattle industry regarding threats, particularly concerning sensitive information and with consideration of privacy issues?
  - What kind of public health information would be needed and how could it be shared, particularly related to health privacy laws (notably the Health Insurance Portability and Accountability Act)?
- Interruption of operations
  - How would the cattle industry respond to public safety requests to reduce or stop operations should an emergency occur?
  - What authority does public safety agencies have to mandate the closure of private-sector operations in such an emergency?
  - At what point is the public safety threat sufficient to warrant a halt in cattle production operations?
  - What effect would such actions have on the local economy and to what extent should such factors be considered in halting operations?

While there were many other aspects, particularly related to emergency responses, these emerged as the most critical for the current illustration. Following a comprehensive simulation exercise, it was apparent that the private-sector businesses and public safety officials had distinctively different perspectives on

these issues, despite the fact that extensive meetings and agreements had taken place prior to the simulation.

Some of the issues that emerged:

- Law enforcement tended to take an aggressive stance and gave orders rather than working cooperatively.
- Law enforcement was reluctant to share certain types of information about threats, suspects, and associated facts under the assumption it was improper to share this information with the private sector.
- The private companies tended to withhold certain types of critical information under the assumption it would not be understood by public safety officials.
- Private companies resisted shutting down all operations because of the economic impact of such actions.
- Private companies argued against stop orders of cattle that were already in shipment because of the economic impact. Conversely, law enforcement tended to dismiss the economic variables.

The lesson learned from this exercise was that despite extensive planning by a wide variety of people who had the intent to find the best method to handle an emergency, additional planning was necessary. Both groups viewed the issues from significantly different perspectives.

Public-private partnerships are necessary and can be effective, but they are not easy. The stress and disagreement that arose from an exercise would be magnified under the conditions of an actual threat. Hence, the need for extensive planning, communications, training, and exercising is essential.

Chapter 10:

Managing Information: A Closer Look at Suspicious Activity Reports, Intelligence Requirements, Collection, Analysis, and Products

Managing Information: A Closer Look at Suspicious Activity Reports, Intelligence Requirements, Collection, Analysis, and Products

It is all about the information. Raw information is the fuel that drives the intelligence process. The information flow should be constant, bidirectional, and originate from a diverse array of sources. Managing this information relies on a number of processes that have been introduced in previous chapters. The intent of this chapter is to build on the discussions of these processes with more detail, providing insight into current intelligence applications for information management. Because of the rapid evolution of law enforcement intelligence—particularly as influenced by fusion center development, Intelligence-Led Policing (ILP) and the Information Sharing Environment (ISE)—there is value in a closer examination of these integrated processes as tools for both the information collector and the intelligence consumer.

Suspicious Activity Reporting

Law enforcement intelligence has long used information, both solicited and unsolicited, to learn about criminal threats. Traditionally referred to as "tips and leads," this information was most commonly provided to the intelligence function by officers, informants, and sometimes by the community. In some cases, intelligence personnel would disseminate specific types of information that was needed to answer specific questions about national threats; i.e., intelligence requirements. While criminal investigators and patrol officers rely on the public as a source of information, through Neighborhood Watch or Crime Stoppers, this practice is not as common for the intelligence function.

As the philosophy and processes of intelligence have changed, so have the processes related to tips and leads. It has been recognized that there is value in a proactive approach to generate more of this type of information for the intelligence function. Beyond simply capturing more information, a more structured process was needed to capture, evaluate, store, and share this information. The process is evolving with coordinated development by the Global Intelligence Working Group (GIWG) on behalf of the Department of Justice (DOJ), the Program Manager's Office for the Information Sharing Environment (PM-ISE), and the Intelligence and Analysis Directorate (I&A) of the Department of Homeland Security (DHS). These new initiatives collectively refer to the management of suspicious behaviors through the use of Suspicious Activity Reports (SAR).[1]

[1] There are two types of SARs: one type deals specifically with financial transactions where financial institutions must report large cash transactions as suspicious activity. For more information about the financial SAR see www.fincen.gov/reg_sar.html. Another type of SAR pertains to criminal behavior.

Suspicious Activity Reporting for a Law Enforcement Agency

A further description of suspicious activity reporting gives perspective as described in a project by the Major Cities Chiefs Association:

> The Suspicious Activity Report (SAR) process,… focuses on what law enforcement agencies have been doing for years—gathering information regarding behaviors and incidents associated with crime—and establishing a process whereby information can be shared to detect and prevent criminal activity, including that associated with domestic and international terrorism.[2]

Suspicious activity reporting is a formalized process to *document* and *share* observed behaviors which are indicative of criminal activity. Information—including "tips and leads"—may come from law enforcement personnel, private-sector partners, or citizens. This information should be placed in written form and processed through the agency in order to have the SAR integrated into the analytic process of the intelligence function.

There are three types of Suspicious Activity Reports. The first is the *financial* SAR. This was mandated by the Bank Secrecy Act wherein a wide range of financial institutions must report certain types of transactions to the Treasury Department. The suspicious activity most commonly associated with financial SARs is money laundering or trafficking in unlawful commodities.

The second is the *all-crimes* SAR. This is simply the documentation and reporting of suspicious activity related to any crime. The activity may be observed by a law enforcement officer or reported to an officer. This is similar to what many law enforcement agencies have used, traditionally known by various names such as a Field Intelligence Report, Field Interview Report or Miscellaneous Investigation Report.

The third type is the *Information Sharing Environment Suspicious Activity Report* (ISE-SAR). This is the documentation of suspicious activity specifically related to terrorism or crimes that support or facilitate terrorist planning and acts. As will be described later, an all-crimes SAR and an ISE-SAR are handled differently.

At a law enforcement agency, the form and processes for line officers are typically the same for both the all-crimes and ISE-SARs; however, when the SAR is processed through the intelligence unit or fusion center, the ISE-SAR is processed and shared differently. The reason for the different processing is based on the responsibility of the ISE to deal with terrorism and crimes supporting terrorism.

The first step for a law enforcement agency is to have an intelligence policy to manage suspicious activity reporting. Several organization components need to be in place to have an effective suspicious activity reporting process. Included are:

1. *An agency-wide process for documenting suspicious activity.* A policy guiding the format, use of case numbers, and processing of the SAR must be a formal part of the agency's records system.
2. *An agency-wide process of sharing SARs with other components of the agency and shared externally with other agencies— such as a fusion center—as appropriate.* A report of suspicious activity is of little value if it is just recorded, but not shared.

[2] *Suspicious Activity Report Support and Implementation Project. Final Report.* Washington, D.C.: Major Cities Chiefs Association; U.S. Department of Justice and U.S. Department of Homeland Security, 2008, p 1.

3. *Training personnel on the indicators of the crimes of concern.* Indicators are the signs, symbols, material, and behaviors that are known to be linked to crimes. For example, certain symbols are known to be linked expressly to right-wing extremist groups just like the possession of certain precursor chemicals are known to be associated with "cooking" methamphetamine. Virtually any type of crime will have some type of indicators. As a result, personnel must be trained to recognize these indicators to support suspicious activity reporting. Important, training should include the fact that activities should be viewed as suspicious in light of the "totality of the circumstances," not just on the observation of an indicator alone.
4. *A SAR review and purge process.* Not all activities that initially appear suspicious are criminal. Consequently, the SAR policy should have a process to review the SAR, and ensure there is a reasonable criminal nexus. If not, the SAR should be purged. Important, the agency's privacy policy should be a key component in the review and purge process

---

Financial SAR

To assist law enforcement agencies in its efforts to combat money laundering, terrorist financing, and other financial crimes, the Bank Secrecy Act (BSA) requires financial institutions to file SARs to inform the federal government of transactions related to possible violations of law or regulation. The financial SAR was created replace multiple reports required by different financial regulatory agencies to report, and subsequently investigate, financial transactions that may have a criminal nexus. To further increase efficacy of criminal financial investigations, all financial SARs are filed through the Financial Crimes Enforcement Network (FinCEN).

While it is the financial institutions' responsibility to file the financial SAR, law enforcement intelligence units deal with these reports extensively in the course of identifying illegal activity, identifying offenders, developing cases against continuing criminal enterprises and identifying emerging threats based on trend and pattern analysis of reported financial irregularities.

The financial SAR can be an important resource for the intelligence process because virtually every criminal enterprise has to have a financial network. The SAR is an important tool for tool for intelligence analysis because it reaches into a wide variety of financial institutions and processes, including:"

- Depository institutions, e.g., banks, credit unions, and thrifts
- Brokers or dealers in securities and/or futures
- Money services businesses, e.g., sellers of money orders and travelers' checks; check cashers and currency exchangers
- Casinos and card clubs
- Insurance companies
- Mutual funds
- Individual(s) transporting more than $10,000 in currency or other monetary instruments into/out of the U.S.
- Shippers/receivers of more than $10,000 in currency or other monetary instruments into/out of the U.S.

SARs are a critical source of information for the intelligence cycle. Oftentimes, the reports identify behavior related to previously unknown threats. In other cases, the SAR provides information about an inquiry that helps more clearly understand a known threat or new dimensions of a known threat. The SAR also aids in defining new intelligence requirements. While the SAR is certainly not the only source of new information for the intelligence cycle, it fulfills a critical role, particularly when supported by officers who are comprehensively trained on terrorism and crime indicators and who consistently report that suspicious activity.

Suspicious Activity Reporting Processes

An important part of the suspicious activity reporting process is the underlying assumption that many people observe suspicious activity in their daily lives but either do not recognize it or think the suspicious behavior is not of sufficient consequence to report. As will be seen, a goal is to generate increased reporting of suspicious activity with the belief that as these reports increase, the probability of gaining critical threat information will also increase. The keys to success are the following:

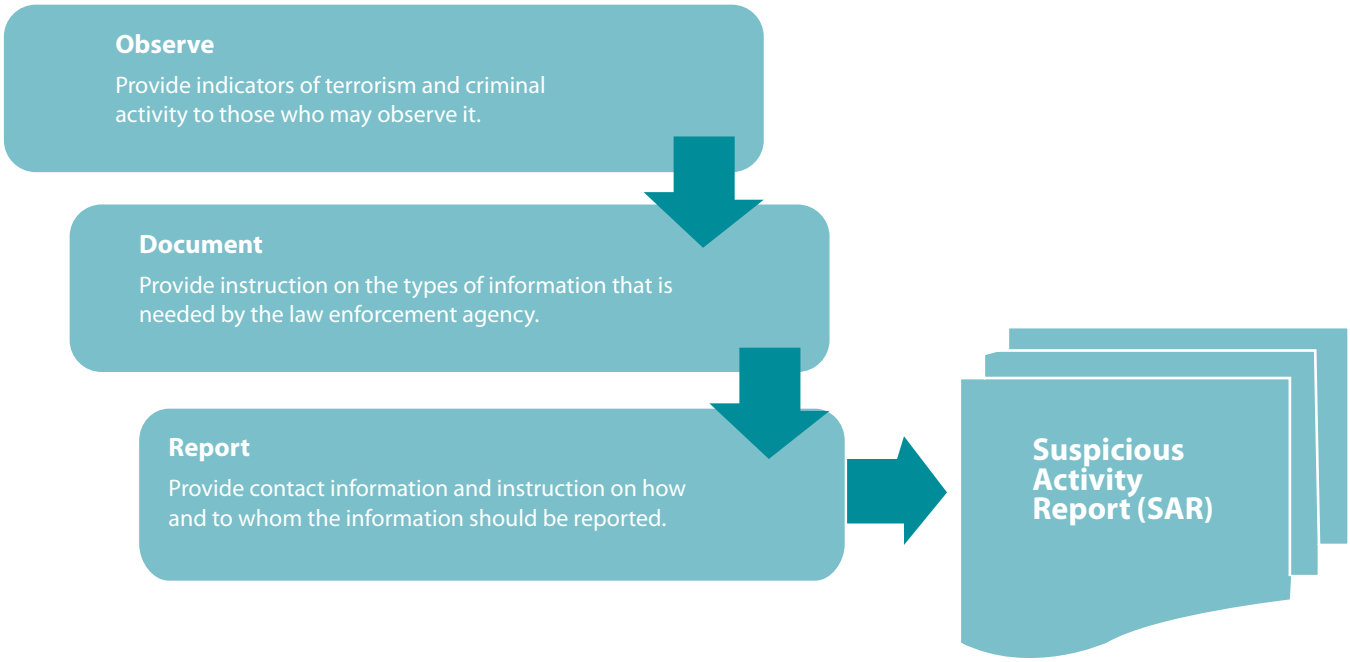
- Recognize "focused" suspicious activity
- Capture substantive information about suspicious activity
- Ensure that all activity is reported through the proper internal intelligence channels or external channels, such as a fusion center (instead of simply being recorded in a law enforcement agency's records management system)
- Review and analyze the information and, if creditable, share it or store it in a searchable database.

This new vision of suspicious activity reporting has two integrated dimensions. The first dimension is development of a model for refining suspicious activity processes. The second dimension is broadening the scope of persons who are encouraged to report suspicious activity, such as community members and private-sector partners.

With the first dimension, "suspicious activity" can encompass a broad array of behavior. Moreover, what a person defines as suspicious will vary, depending on a person's life experiences, values, and other social factors. Direction must be given so that suspicious activity is defined (and viewed) in the context of the types of information that is needed for the intelligence process. To accomplish this, a three-part model can be used: Observe, Document, and Report (see Figure 10-1).[3]

[3] This model is based on a community training model for counterterrorism developed by the Regional Community Policing Training Institute at Wichita State University, Dr. Andra Katz-Bannister, Director.

Figure 10-1: Suspicious Activity Reporting Model



Observe

People must be observant, but observations need to be targeted. Awareness training is needed to ensure that the behavior that is observed has a potential criminal nexus. Often, training includes providing information about "indicators"—behaviors that are reasonably linked to potentially criminal activities. There are two critical components of indicators: First, the focus must be on *behavior*— not the attributes of an individual. Moreover, there must be a reasonable likelihood that the behavior could be related to a crime; that the behavior is not just "odd" or "unusual." "Attributes of an individual" would include perceived[4] race, ethnicity, gender, religion, and so forth. That is, a person *should not* be deemed "suspicious" simply because he or she possesses these attributes—suspicion must be based on *behavior*. If suspicious behaviors are observed and documented as they relate to the preparation or commission of a crime, then the attributes can be properly used as part of the description of the suspicious person. Of course, these guidelines are general and must be applied in light of circumstances and other information the observer has.

The second critical component is for the observer to understand the *types of behaviors and symbols* (e.g., gang markings, tattoos, slogans of criminal extremists, etc.) that are particularly indicative of criminal activity. This means that observers can benefit from some type of training or information about suspicious activities.

For law enforcement officers, training programs are available, both in class and online, that can provide important contemporary information about threat indicators. One such program has been the *State and Local Anti-Terrorism Training (SLATT)* program funded by the U.S. Bureau of Justice Assistance (BJA). SLATT training provides detailed information to officers on indicators of both international and domestic terrorism/criminal extremism from the perspective

[4] The word "perceived" is used here because often an observer sees a characteristic that is mistaken for an attribute. For example, an untrained observer may see a person that the observer concludes is from the Middle East when, in fact, the person is of a different ethnicity.

of how patrol officers, for example, may encounter and observe such behaviors during their regular work shift.[5]

> Communities Against Terrorism (CAT), also funded by the BJA, is a program directed toward the nonlaw enforcement community to provide suspicious activity indicators The CAT program assists law enforcement in the development of partnerships with community members because when community members are aware of potential indicators of terrorism activities, they may provide law enforcement with valuable information. To assist law enforcement in the outreach effort, the CAT offers has templates of flyers containing potential indicators that law enforcement can distribute to specific industries.[6]

Document

When suspicious activity is observed, the value of the SAR is increased if the observer provides explicit information about the suspicious persons and the specific nature of the suspicious activity. While law enforcement officers are trained to collect such information, the public, which reports a significant amount of suspicious activity, typically does not have this knowledge. Public education programs need to inform community members of the kinds of information that are most valuable: Detailed descriptions of the suspicious persons and their vehicles, location of the activity, the actions that appeared suspicious, and any objects the person might have that added to the suspicious activity are all types of information that must be documented. Once again, the CAT program provides the details that are specific to different kinds of businesses.

Report

For law enforcement officers, new processes—described later as the Nationwide SAR Initiative—are being developed to establish common standards for capturing and reporting SARs that will enhance SAR information-sharing. At the outset, the process has a particular focus on terrorism because it is being driven by the ISE.[7] However, since the standards are being prepared with support from the GIWG and the Criminal Intelligence Coordinating Council (CICC), the framework for suspicious activity reporting is envisioned to eventually apply to "all crimes and all threats". A goal is to have the reporting of suspicious activities become more standardized, with officers using a consistent reporting process.

Reporting suspicious activities has been more problematic for community members. In many cases, information has not been reported because the community simply did not know how or to whom to report this information. Law enforcement agencies have been improving their capacity to assist citizen reporting; for example, increasing numbers of law enforcement agencies have developed SAR web sites, special telephone numbers, and initiatives related to agencies' community-based programming.

[5] See www.slatt.org. The web site not only provides training schedules but also online training and a wide range of resource materials. For full access to the web site, one must register with employment verification that the user has a bona fide need for access to the site. Because the program is funded by BJA, there is no charge for the training.

[6] CAT brochures may be downloaded by registered users of slatt.org at www.slatt.org/secured/cat.aspx.

[7] See www.ise.gov/pages/ctiss.html for more information on the ISE initiatives and standards related to SARs.

The goal is to educate and encourage people to be aware of behavior that is likely to be criminal, capture critical facts about the behavior, and submit the information to a law enforcement agency. In many cases, the information can provide important missing puzzle pieces to the intelligence analyst. In other cases, the information may inform the law enforcement agency about potential criminal activity about which the agency was previously unaware.

As initiatives are developed to encourage people to report suspicious behavior, law enforcement is more likely to identify and mitigate threats. A significant element of this process is to ensure that suspicions are based *on behavior* and that the observer captures as much accurate information as possible to report the suspicious activity. Once this information is in the hands of the intelligence function, it must be integrated to learn what else is known about the suspicious activity and to define future information needs to clearly understand if a threat exists and, if so, how it can be stopped.

SARs and Personal Identifying Information

An important issue related to SARs is whether the report contains Personal Identifying Information (PII). PII may be defined as any information or data from which a reasonable person may identify a specific individual. When PII is collected, civil rights protections and privacy standards must be applied.

A PII-SAR is a report that names an individual or provides sufficiently specific information where identity could reasonably be established, such as the physical description of an individual and the address where the person lives. In these cases, retention, security, and dissemination guidelines must be restrictive, with the safest approach of using information management standards that are consistent with the 28 CFR Part 23 guidelines.[8] It should be stressed that SARS typically are not defined as criminal intelligence and the 28 CFR Part 23 guidelines are not required for SARs. However, the guidelines serve as a good model to use for protecting privacy and civil rights. In addition, several agencies are developing SAR-specific guidelines to ensure the protection of privacy and civil liberties. A non-PII-SAR is a report that describes suspicious circumstances, indicators, and/or behaviors of unknown persons. If PII is not included in the report, then the law enforcement agency has significant latitude for retaining and disseminating the information.

Regardless of the SAR model used by a law enforcement agency, distinct policies with respect to the handling of SARs that have PII and those that do not should be made.

Establishing Controls on Suspicious Activity Reports/ Information

Information contained in SARs is sensitive for several reasons: The basis or motivation for reporting the information and the inherent accuracy of the information is often unknown. As such, law enforcement must determine whether lawful activity was misperceived as being criminal and whether the information was reported accurately. Despite these potentially limiting factors, when suspicious activity is reported to law enforcement, the agency has a public

[8] The reader is reminded that 28 CFR Part 23 applies only to criminal intelligence information. Even if the SAR is not retained as part of the criminal intelligence records system, the guidelines afford recognized civil rights and privacy standards to demonstrate that the law enforcement agency is doing due diligence in protecting individuals' rights. Actual policies should be reviewed by counsel with specific reference to the laws of each state.

safety responsibility to determine if there is a reasonable suspicion that a crime is being planned or has been committed. If so, the information should be retained and serve as the basis for a further criminal inquiry and operational planning to protect the public.

Because of this sensitivity, the Global Justice Information Sharing Initiative's Privacy Committee identified six critical factors, or points in the SAR process, wherein information management controls should be implemented to ensure the security and privacy of PII while at the same time permitting the agency to further its inquiry into the behavior. These controls are based on the same principles of information management used to protect information in a criminal intelligence records system. With some modification from the Privacy Committee's report, the six controls include the following:

1. Receipt/Collection. At the time of receipt or collection, suspicious activity information should be assessed and reviewed for sensitivity and confidentiality using corroborative information, if possible. Every effort should be made to validate or refute the information in order to resolve as quickly as possible whether there is a criminal predicate or whether the SAR is unfounded. Collecting information that is purely expressive activity protected by the First Amendment should be prohibited.
2. Storage. Storage of suspicious activity information should be handled similarly to data that rise to the level of reasonable suspicion. Those requirements should include an audit and inspection process, supporting documentation, and logical separation or labeling of the unconfirmed SAR from other information.
3. Access. Because of uncertainty about the information's credibility and/or accuracy, access to suspicious activity information should be handled similarly to access to information that rises to the level of reasonable suspicion. Access should be allowed only where there is a right to know and a need to know the information in the performance of a law enforcement, homeland security, or public safety activity.
4. Dissemination. Suspicious activity information, if systematically collected and stored for interagency distribution, should be disseminated primarily in response to an inquiry, and only for law enforcement, homeland security, and public safety purposes. Uncorroborated suspicious activity with PII should not be regularly disseminated in bulletins or other similar products, but it may be included in secure information databases and disseminated to relevant law enforcement, homeland security, and public safety agencies that have the right to know and need to know the information for public safety purposes.
5. Retention. The retention period for suspicious activity information should be established by policy and be of sufficient time to determine the veracity of the information in light of the agency's expertise and resources. Suspicious activity records should have a "disposition" label, such as "undetermined/unresolved" or "cleared/unfounded," to clearly notify the user of the information's status. Agencies should also consider the need for maintaining some type of suspicious activity data for purposes of statistical reporting and performance measurement when setting retention and purge procedures.
6. Security. Physical and electronic security measures should be similar to those used for information that is rising to the level of reasonable suspicion.[9]

[9] These factors are based on the following document with some modification: Global Intelligence Working Group. *Privacy Committee Report: Tips and Leads Issues Paper.* Washington, D.C.:, Global Justice Information Sharing Initiative, U.S. Department of Justice, 2007, pp. 7–8.

Permeating each factor in this process should be constant attention to privacy, accuracy, and corroborating the information in the SAR, as reinforced by a report to Congress by the PM-ISE:

> Protecting the information privacy and legal rights of Americans is a top priority: At the local level, SARs will be incorporated into existing processes and systems used to manage other crime-related information and criminal intelligence so as to leverage existing policies and protocols utilized to protect the information privacy, civil liberties, and other legal rights of the general public. Multiple levels of review and vetting will be established to ensure that information is legally gathered and managed, and reports containing personally identifiable information that are unfounded, or that cannot be reasonably associated with criminal activity, will not be shared beyond the originating entity.[10]

Complicating these processes among many law enforcement officers is that all information may be useful sometime in the unknown future. This belief produces a great reluctance to destroy any information or reports. Iit must be remembered that SARs are largely unsolicited tips and leads from sources that have a wide range of credibility. If the follow-up shows that the allegation in the SAR is unfounded, there is no reason to retain any PII.

Policy Recommendations for Developing and Managing a Suspicious Activity Reporting System

As has been evident in this discussion, law enforcement agencies are increasingly developing a more comprehensive system to stimulate the reporting of suspicious activity as well as to have a more structured process to manage SAR records. The Major Cities Chiefs Association and the Global Justice Information Sharing Initiative approached this task with support from the Department of Justice (DOJ) and the Department of Homeland Security (DHS). A number of substantive recommendations were made from this project including, in part, the following:

- Agencies should educate and gain the support of policymakers about issues and processes related to suspicious activity reporting.
- All privacy and civil liberties policies and training should be reviewed to verify that they are consistent with current law and national standards.
- Information management of the SARs process should be integrated with existing processes and systems that manage criminal investigative information and criminal intelligence, thereby leveraging existing policies and protocols to protect privacy and civil rights.
- The SAR policy should be communicated to the public because transparency is the key to acceptance.
- Gathering, processing, reporting, analyzing, and sharing suspicious activity information is critical to preventing crimes, including those associated with domestic and international terrorism. The SAR process should have an all-crimes orientation.
- The SARs process should use criminal information management processes, applying SARs to the appropriate criminal records management system or criminal intelligence records system.

[10] McNamara, Thomas E. *Annual Report to the Congress on the Information Sharing Environment.* Washington, D.C.: Program Manager–Information Sharing Environment, 2008, p. 29.

- Suspicious activity submissions should not bypass the local law enforcement agency or agency of original jurisdiction and the standard 911 reporting systems.
- When an agency receives information that affects another jurisdiction, it is the responsibility of the receiving agency to immediately notify the affected agency and discuss coordination, deconfliction, investigation, and vetting procedures with the affected agency. Once vetted, further dissemination of the information would be the responsibility of the affected agency.
- A process should be established to ensure that SARs are made available to fusion centers and local Joint Terrorism Task Forces (JTTF) in a timely manner.
- An ongoing emphasis should be placed on defining and communicating trends in terrorism activity, geographically-specific threat reporting, dangers to critical infrastructure, and general situational awareness.
- There is a need for a common national methodology, including common data codes, for sharing suspicious activity data in order to discern patterns across the country.
- Training is a key component of the SAR process. All relevant agency personnel must be trained to recognize behavior and incidents indicative of criminal activity associated with international and domestic terrorism.
- Incorporating outreach to the public, law enforcement, and the private sector in the collection process is important to the success of the program.
- Develop a common national methodology to horizontally and vertically share SAR data in a timely manner that is consistent with privacy and civil liberty guarantees.
- Develop a standardized training program to provide consistent nationwide SAR training.[11]

The intent of these recommendations is to maximize the utility of suspicious activity information while at the same time protecting civil liberties. While these recommendations are intended to bring about standardization of the SAR process, the report notes that every jurisdiction will have to develop policies and procedures that take into account the unique circumstances and relationships within that community.[12]

The Nationwide Suspicious Activity Reporting Initiative

The Nationwide Suspicious Activity Reporting (SAR) Initiative (NSI) directly supports efforts to protect local communities from terrorism and other violent crime while at the same time protecting the privacy and civil liberties of Americans. An outgrowth of a number of separate but related activities during the last several years, the NSI responds directly to the mandate to establish unified, standardized, and integrated process to gather, document, process, analyze, and share information regarding circumstances potentially associated with terrorism-related criminal activity in a manner that rigorously protects the privacy and civil liberties of Americans, as called for in the National Strategy for Information Sharing (NSIS). The NSI process is a cycle of 12 interrelated operational activities that address the requirements outlined in the NSIS. The NSI long-term

[11] *Suspicious Activity Report Support and Implementation Project,* Op. cit., 2008, pp 2–5.

[12] Ibid., p. 6.

goal is that most federal, state, local, and tribal law enforcement organizations will participate in a standardized, integrated approach to gathering, documenting, processing, analyzing, and sharing information about suspicious activity.

Suspicious activity is defined as "observed behavior reasonably indicative of pre-operational planning related to terrorism or other criminal activity."[13] Although the Nationwide SAR Cycle was developed to enhance our abilities to identify, document and share terrorism-related suspicious activity, the process and technological concepts can be applied to address any emerging crime problem. The NSI cycle intentionally used this approach because individuals and groups involved in terrorism may engage in broad range of criminal activity as they plan, prepare for, and carry out a terrorist attack.

The Challenge. The lack of unified operational processes and a standardized technological approach for gathering, handling, and sharing terrorism-related suspicious activities has impeded the use of locally generated information to identify and mitigate emerging crime trends, including those potentially related to terrorism. Furthermore, the lack of standardized privacy and civil liberty rules can lead to the inappropriate collection and retention of data, and potentially infringe on the privacy and civil liberties of Americans.

The Solution. The NSI builds on what law enforcement and other agencies have been doing for years—gathering information regarding the behaviors and incidents reasonably indicative of criminal activity. As part of this standardized process, frontline and analytic personnel are trained to identify and distinguish between legal and illegal behaviors. Furthermore, through the establishment of clearly defined business rules, potential SARs are reviewed and vetted before they are made available to other analytic and investigative personnel. The use of common data and technical architecture standards enable terrorism-related SARs to be accessed by fusion centers, authorized federal, state, local, and tribal law enforcement agencies, DHS Headquarters, and the FBI's JTTFs and Field Intelligence Groups, thereby enabling the discovery of patterns and trends by analyzing information at a broader level than typically recognized within a single jurisdiction, state, or territory.

The NSI cycle (Figure 10-2) accommodates the specific risks and threats of local, state, and tribal law enforcement agencies. The first part of the cycle encourages jurisdictions to conduct risk assessments and use that information to identify and document priority information needs for that jurisdiction. Those information needs are guide the training provided to frontline law enforcement officers and analysts regarding those behaviors and incidents reasonably indicative of pre-operational planning related to criminal activity—including those potentially related to terrorism. So whether the identified risk is related to illegal drugs, violent gang activity, terrorism or other crime—the NSI process and technological concepts can be applied to address any emerging crime problem.

[13] *Information Sharing Environment, Functional Standard, Suspicious Activity Reporting*. ISE-FS-200, Version 1.5, 2009, Section 5, h. See www.ise.gov/docs/ctiss/ISE-FS-200_ISE-SAR_Functional_Standard_V1_5_Issued.pdf.

The Benefit. Better recognition by law enforcement of behaviors and incidents indicative of criminal activity in a manner that more effectively protects privacy and civil liberties. Investigators, analysts, and homeland security professionals have improved access to critical information, enabling more rapid identification of emerging threats facing our local communities. Preliminary results have already proven value to local counterterrorism efforts. For example, in one jurisdiction during a 12-month period, 1,500 SAR were documented, and of those 1,500 more than 65 have been referred to the JTTF, resulting in 21 prosecutions and convictions in state court for terrorism-related offenses.

While there is widespread recognition of the importance of identifying and reporting suspicious activities, the initiative is not without its critics. The American Civil Liberties Union made the following comment about suspicious activity reporting:

> This overbroad reporting authority gives law enforcement officers justification to harass practically anyone they choose, to collect personal information, and to pass such information along to the intelligence community. Suspicious activity report (SAR) policing opens the door to racial profiling and other improper police behavior, and exposes law-abiding people to government prying into their private affairs without just cause.[14]

Because of these concerns, training is essential. It must be emphasized that the focus is on collecting information about behaviors that represent pre-operational indicators of criminal activity. Unusual or odd behavior or circumstances would not be included unless there is some articulable relationship between that behavior and a potential crime. Beyond training, it is essential to have ongoing supervision and a substantive assessment mechanism to document the effectiveness of the process.

Summary

Suspicious activity reporting is being embraced as a key element in the contemporary intelligence process. With appropriate methods and systems in place, it serves as a valuable tool for gaining critical raw information. The reader is cautioned that the processes are still in development. Moreover, SARs are sensitive from a civil rights perspective and require careful development and controls. While noteworthy progress has been made, challenges remain. The PM-ISE has noted the following:

> Fostering an information-sharing culture may be the most formidable challenge confronting the ISE. In the post-9/11 world, a predisposition to share the right information with those who need it is not merely an option but a fundamental principle firmly grounded in law and regulation. The goal is clear, but achieving it will take dedicated effort. The NSIS states "We will…change government culture to one in which information is regularly and responsibly shared and only withheld by exception." ISE cultural change initiatives aim to ensure that this principle is clearly understood and that managers are held accountable for driving change in their agencies.[15]

[14] German, Mike and Jay Stanley. *Fusion Center Update.* Washington, D.C.: American Civil Liberties Union, 2008, p. 2.

[15] McNamara, *Annual Report to the Congress,* Op cit., 2008, p. 47.

10 WAYS TO INTEGRATE SUSPICIOUS ACTIVITY REPORTING INTO YOUR AGENCY'S OPERATIONS

1. RECOGNIZE the importance of SAR, understand your role in the SAR process, and know that your involvement makes a difference. Strong leadership is an essential element. Gain support from personnel, leadership, and policymakers both internally and externally.

2. DEVELOP a data-collection process and secure standardized reporting format for sharing suspicious activity. Define and communicate trends in terrorism-related activity, geographically specific threat reporting, dangers to critical infrastructure, and general situational awareness.

3. LEVERAGE and adopt the use of common national standards to enhance the capability to quickly and accurately analyze suspicious activity data such as the ISE Functional Standard for Suspicious Activity Reporting, the State and Local Agency Information Exchange Package Document (IEPD) for SAR Reporting, the National Information Exchange Model (NIEM), and the Records Management System (RMS) and Computer Aided Dispatch (CAD) functional standards.

4. INCORPORATE appropriate guidelines and concepts into your operations, such as Intelligence-Led Policing, the *National Criminal Intelligence Sharing Plan, the Fusion Center Guidelines, the Findings and Recommendations of the Suspicious Activity Report (SAR) Support and Implementation Project,* and privacy and civil liberties templates. Use the IEPD for the *SAR for Local and State Entities* to establish and integrate the SAR process.

5. IMPLEMENT and adhere to your agency's privacy policy and ensure that the privacy and civil liberties of citizens are protected. Evaluate and update, if necessary, your privacy and civil liberties policy to ensure that the gathering, documenting, processing, and sharing of information regarding terrorism-related criminal activity is specifically addressed. Communicate the policy to the public.

6. TRAIN personnel and institutionalize the SAR process within your agency. Ensure that law enforcement and public safety personnel understand the SAR process and what internal policies or protocols exist to share appropriate information. Learn about available training to increase or enhance abilities, such as the State and Local Anti-Terrorism Training (SLATT) Program.

7. INSTITUTIONALIZE the gathering of suspicious activity information at the street level and standardize the reporting of such data so that it may be shared with other appropriate public safety partners, such as your criminal intelligence unit, state or regional fusion center, Joint Terrorism Task Force (JTTF), and other law enforcement and public safety partners.

8. EDUCATE citizens, businesses, and partners on suspicious activity reporting and how to report activity to appropriate officials. Integrate programs such as the Communities Against Terrorism (CAT) program in your community. Develop outreach materials to educate the public on recognizing and reporting behaviors and incidents indicative of criminal activity associated with international and domestic terrorism.

9. PARTNER with other law enforcement, public safety, private sector, and state or major urban area fusion centers. Foster interagency collaborations to maximize each other's resources and create an effective and efficient information sharing environment.

10. CONNECT to a major information sharing network, such as the Regional Information Sharing Systems (RISS), the Federal Bureau of Investigation's Law Enforcement Online (LEO), and the U.S. Department of Homeland Security's Homeland Security Information Network (HSIN). Leverage proven and trusted technology to share information, communicate, and access additional resources.

From: *10 Ways to Integrate Suspicious Activity Reporting into Your Agency's Operations.* Washington, D.C.: Bureau of Justice Assistance, U.S. Department of Justice, 2008. (Brochure)

Figure 10-2: Nationwide Suspicious Activity Reporting Cycle

Intelligence Requirements

With the growth of the ISE and fusion centers, law enforcement is increasingly relying on the use of intelligence requirements as a method for defining the types of raw information that are needed to develop a more robust analysis of threats. An "intelligence gap" is missing information that is needed for effective intelligence analysis. An "intelligence requirement" is the information needed to fill the gap. When managing information, both the gaps and requirements must be identified and defined.

To illustrate requirements, a statement by former Secretary of Defense Donald Rumsfeld, which was panned by many pundits as being nonsense, demonstrates the concept when dissected. Secretary Rumsfeld stated the following:

> "There are known knowns. There are things we know that we know. There are known unknowns. That is to say, there are things that we now know we don't know. But there are also unknown unknowns. There are things we do not know we don't know."[16]

Table 10-1 illustrates Secretary Rumsfeld's statement as applied to different intelligence challenges—international terrorism (such as al-Qaeda) and violent crime within a community—followed by a statement of the intelligence action related to requirements which must be taken.

Table 10-1: Interpretation and Illustration of the Rumsfeld Quote

	Al-Qaeda Example	Violent Crime Example	Intelligence Action
There are known knowns	We know that al-Qaeda's intent is to commit more terrorist attacks against the U.S. and U.S. interests.	We know there is an increase in violent crime using guns within a community.	The information we know must be consistently monitored and verified (i.e., "standing requirements") to determine any changes in the status of the information we know.
There are known unknowns	We know that al-Qaeda has plans for future terrorist attacks, but the timing, method, and locations are unknown.	We know there is an increase in black market guns, but it is unknown who the supplier is, where the guns come from, or how the transactions are made.	We know that we have intelligence gaps. Intelligence requirements, sources, and methods must be defined so that we may learn the currently unknown information.
There are unknown unknowns	If al-Qaeda has developed new alliances or new methods to commit attacks, these are unknown to us.	There are factors driving the increase in violence beyond the availability of guns; however, these other factors are unknown to us at the time.	Information must be collected from all sources and analyzed in an attempt to identify new threat information.

[16] Department of Defense News Briefing, February 12, 2002. See www.slate.com/id/2081042.

The intelligence analyst must integrate currently held information to determine what we know about a threat: these are the "known knowns." Because the threat environment is dynamic, these known factors must be constantly monitored to verify the threat and determine if a change is occurring to the threat picture. In many instances, while we know that a general threat exists, the specific character of the threat—the method of attack, specific target of attack, and when the attack may be attempted—is unknown. These are "known unknowns." Finally, there are threats which may be developing, either by a known suspect or a suspect completely unknown to us, that we are simply unaware of—these are the "unknown unknowns." The goal is to continually monitor suspicious activities and collect information from diverse sources that may give us an indicator of a new threat. When these new indicators are learned, requirements are defined to better identify the threat and those who pose the threat.

One can understand how the layman may interpret Secretary Rumsfeld's statement as nonsense, but he was essentially describing intelligence gaps and intelligence requirements.

The use of intelligence requirements is a concept that is largely new to law enforcement intelligence, although it has long been used in national security intelligence to specify information needs about threats. It is a holistic approach to collecting and analyzing information so that the most comprehensive picture of a threat emerges, as well as alternatives for countering the threat. The use of requirements also increases the efficacy of the intelligence process by expressly focusing on information needs rather than using a broad dragnet approach to information collection or simply awaiting the serendipitous discovery of critical data.

To use an analogy, the job of an intelligence analyst is akin to putting together a jigsaw puzzle without knowing what the final picture in the puzzle looks like. Each piece of information is like a puzzle piece and the analyst must see where it fits to create a discernable image. The missing pieces are information gaps; the intelligence requirements are to identify and collect the missing pieces, filling gaps, to make the picture more complete. As more pieces are identified, new requirements often emerge. Once sufficient information has been collected, the picture becomes clear and the threat is more clearly understood. Of course, in practice it is not that simple; therefore, there is the need to elaborate on the issues and processes related to requirements-driven intelligence.

Filling Gaps/Fulfilling Requirements

The information-collection process has to be focused so that specific information needs are fulfilled. This increases the efficiency of the process and ensures that the right information needs are being targeted. Historically, law enforcement used an approach that was based largely on intuition of what was suspicious. Often it was mere suspicion based on statements or behaviors that seemed out of the norm, extreme, or unusual. This process was neither objective nor scientific and was often influenced by bias (typically, unintended bias) imposed by the officer's attitudes, values, and beliefs. This process collected volumes of

diverse raw information that was forwarded to analysts and investigators who could examine the information in hopes of discovering that substantive threat information may emerge. As illustrated in Table 10-2, there are a number of differences between this tradition-driven approach and the requirements-driven approach to information collection. In essence, the requirements-driven approach is more scientific and, therefore, more objective, more focused, more efficacious, and less problematic on matters related to civil rights. On this last point, given that intelligence requirements are often the product of an ongoing criminal inquiry, the criminal predicate is more easily articulated.

Essentially, the tradition-driven approach is like throwing out a net, seeking to collect as much information as possible under the assumption that threat information and evidence of crime will emerge from the vast body of information. It is less efficient, less effective, and more likely to lead to civil rights liability. Requirements-driven intelligence is more laser-like. It focuses specifically on the types of information we need to give us an understanding about a narrowly defined area of threat.

Table 10- 2: Traditional Collection versus Requirements-Driven Collection

Tradition-Driven	Requirements-Driven
• Data-driven	• Analysis-driven
• Exploratory	• Specifically focused
• Emphasizes amassing data	• Emphasizes a focused, selective approach to information collection and analysis
• Assumes collected information will identify criminals	• Analytic inference of criminal suspects from collected information
• An aggregate approach to information collection (dragnet); even mere suspicion	• Targeting/specificity on information regarding reasonable suspicion of crimes
• Explores all general inferences about potential criminality	• Selectively explores crime and threat leads based on priorities and evidence
• Explores collected information to see if there are questions to answer	• Answers questions by collecting and analyzing specifically collected information
• Develops intelligence records for contingency needs, (i.e., just in case information is needed)	• Develops intelligence records in support of active threats and criminal enterprises

Applying the Concept to Law Enforcement

As part of the FBI Intelligence Directorate's reengineering process, former Executive Assistant Director Maureen Baginski used requirements-driven intelligence. This concept is epitomized by the statement frequently made by Baginski, and previously referenced in Chapter 4's discussion of the intelligence process, "The absence of evidence is not the absence of a threat."

This is an insightful observation for understanding why requirements-driven intelligence is important. Let us say that a law enforcement executive asks the Regional Intelligence Fusion Center if there is a terrorism threat within the agency's region. The response may be, "There is no evidence to suggest a terrorist threat within the region." However, there may be an unknown threat in the community for which no evidence has been discovered (e.g., "unknown unknowns"). One such unknown threat in the community was Timothy McVeigh who placed the bomb at the Murrah Federal Building in Oklahoma City. Another unknown threat was Muhammad Atta, who had a base of operations within U.S. communities to aid in planning the attacks of September 11, 2001. These were both clear threats to their communities but the evidence of these threats had not been discovered.

We must have a means of identifying these unknown threats, assessing the danger posed, and taking appropriate action to prevent or mitigate the threat. The process is not easy, especially for a state, local, or tribal law enforcement (SLTLE) agency that may have limited information-collection and analytic capabilities. Identifying evidence of such threats is both labor-intensive and resource-intensive, requiring good information-sharing, effective linkages with intelligence networks, constant monitoring and exchange of information, and ongoing information collection, assessment, and analysis within an agency's jurisdiction. These needs reinforce the value of fusion centers, which will have all of these characteristics, and the need for agencies to be a fusion center partner. The fusion process is particularly structured to use the intelligence requirements model effectively.

While requirements-driven intelligence will work well for a law enforcement agency, it requires a commitment of time and resources to accomplish its goals. At the very least, a law enforcement agency needs a minimalist intelligence capacity to contribute to the process at a state or regional level, particularly to be an effective intelligence fusion center partner.

Comparing Intelligence Requirements and Crime Analysis

Intelligence requirements may be conceptualized as information that is needed to make decisions on how to best protect a community from threats posed by organized crime and terrorism. When requirements are filled, executives and managers have sufficient reliable information to direct an operational response to a threat.

As an illustration, SLTLE agencies often make operational decisions related to incidents of predatory crime based on crime analysis requirements. Indeed, this is the fuel of the CompStat process. Specifically, as a result of the timely analysis of reported crime, certain types of crime trends emerge. Relying on information derived from that analysis such as type of crime, modus operandi, time and geographic factors, suspect descriptions, etc., response strategies are developed to deal with the crimes that have occurred and the likely forecast (i.e., future) of crime that will occur if the crime series is left unchecked. The agency may use saturation patrol, undercover officers, decoys, surveillance, or a combination of strategies to capture these repeat offenders. Without the information from the crime analysis output, the most effective operational decisions cannot be made.

Of course, crime analysis requirements are much easier to provide than intelligence requirements because of the inherent differences between criminal investigation and criminal intelligence. Essentially, investigations are crime-driven while intelligence is threat-driven. Thus, investigations are reactive, responding to crimes that have occurred and a known quantifiable universe of data that have been identified through the investigation. Conversely, intelligence is proactive by intervening when a threat is identified. Essentially, intelligence is pre-crime and far more probabilistic—factors that pose both operational challenges and civil rights issues.

Requirements and Strategic Priorities

Intelligence activities should be based on the mission of the unit or fusion center; for example, the mission of a High Intensity Drug Trafficking Area intelligence center would be focused on the production and distribution of illegal drugs. Similarly, intelligence activities of the Immigration and Customs Enforcement service of the DHS are focused on smuggling humans and contraband across U.S. borders. Most state, local, and tribal intelligence activities, however, have adopted an all-crimes, all-threats, all-hazards approach. In reality, all-crimes for intelligence purposes is somewhat of a misnomer. Because this encompasses a wide breadth of crime types, pragmatically, even an all-crimes intelligence operation must prioritize the types of crime that will be the focus of intelligence activities. As noted in the Chapter 6 discussion of strategic priorities, this priority will be based on geography, criminal history of the region, and special issues that help facilitate organized crime and terror threats, such as the presence of seaports, international airports, or unique commercial industries, such as critical infrastructure or key resources.

Intelligence requirements should also be mission-related. Known as *priority intelligence requirements,* the intent is to maintain focus on crime and threats that have been assessed as having the impact of greatest concern in the jurisdiction. We know, however, that crimes and threats change over time. In the case of drugs, for example, trends change in different geographic areas of the country quite frequently. In some areas, methamphetamines are a major problem, in another region the drug problem may be crack cocaine. In both cases, the primary drug problem will evolve. As a result of such changes in crime problems, reprioritizing intelligence targets should be part of the reevaluation component of the intelligence process, as well as of strategic intelligence analysis.

Typologies of Requirements

There are various ways to describe intelligence requirements, meaning that there is no uniform standard for describing the different types of requirements used by law enforcement agencies. This discussion seeks to take the different models and terms currently used and not only explain them, but also illustrate their relationships.

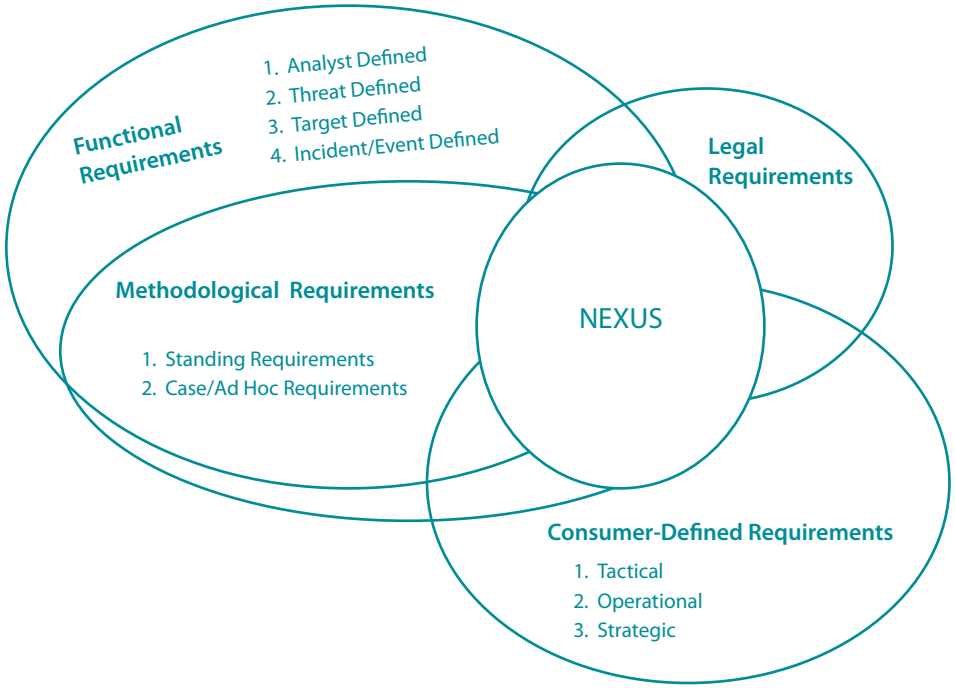
Requirements may be characterized in different ways based on their role. These different characterizations are not mutually exclusive. Indeed, as illustrated in the Venn diagram of Figure 10-3, there is a nexus among the different types, with the various characterizations fundamentally relating to their purposes.

Functional requirements are defined by the intelligence unit or fusion center for the purpose of learning about different dimensions of a threat. Information is collected through SARs and the collection plan associated with ongoing inquiries to help the analyst understand the functional evolution of threats. This is often a systemic process wherein as more information is received and analyzed, a better understanding of the threat emerges which, in turn, helps define additional requirements. This is an iterative process that continues to refine the threat picture until the threat is compromised or until it dissipates.

There are four types of functional requirements:

1. Analyst defined. During the course of the analysis the intelligence analyst discovers a gap in the information that needs to be filled for a comprehensive and accurate analysis to be completed. An analyst has three SARs that suggest an interrelationship among the three as preparation to commit a crime. The intelligence requirements are information that is needed to confirm this linkage.
2. Threat defined. Known threats within the jurisdiction that are monitored on a consistent basis to continually assess the threat. For example, if a jurisdiction has a known white supremacist group that has made criminal threats, monitoring that group to understand changes in its structure, membership, and/or activities can help identify imminent threats.
3. Target defined. Based on the nature of known threats, targets are monitored to assess vulnerability and risk. The Earth Liberation Front threatens to burn down houses and destroy construction equipment in a new subdivision that it says is in an environmentally sensitive area. The requirements would be to collect information on the vulnerability of the targets for a threat assessment.
4. Incident/event defined. If an event is planned or an incident occurs, requirements will be defined to determine potential threats associated with the event or future implications of the incident. For example, if the president of the World Bank is invited to give the commencement address at a local university, there is a high likelihood that anarchists will attend the commencement to demonstrate their disdain for the World Bank. Some anarchists will lawfully demonstrate while others are likely to commit property crimes and disrupt the event. The intelligence requirements are derived from the fact that the event was scheduled.

Figure 10-3: Characterizations of Law Enforcement Intelligence Requirements



For each type of functional requirement, there are critical information needs to enable an understanding of all dimensions of a threat. Threat requirements apply to both law enforcement and homeland security/all-hazards intelligence. As the name implies, these are information needs that help an analyst define a threat with as much precision as possible. Whether the threat is from a terrorist group or from pandemic flu, the analyst needs a wide array of valid information from reliable sources that can provide as much insight as possible about the threat picture.

The method by which the information is solicited is referred to as the methodological requirements. Generally speaking, there are two types:

1. Standing requirements. Information that needs to be collected on an ongoing basis to monitor known and consistently present threats within a community.
2. Case (or ad hoc) requirements. Information that is needed by analysts to determine the existence and character of a threat that is based on unsolicited tips, leads, suspicious activity reports, and/or other information developed through the intelligence process.

Another dimension of requirements is based on an analysis request by intelligence consumers; for example, a partner agency in a fusion center may request a certain type of analysis for its jurisdiction. This request, therefore, will drive the requirements process. These are the types of requirements:

1. Tactical. What information is needed to prevent or mitigate an imminent or short-term threat?

2. Operational. What information is needed to prevent or mitigate a developing or long-term threat?
3. Strategic. What changes in the threat picture exist in the coming months or years that can have an impact on operational planning and resource allocation?

Overlapping these is a type of requirement that is unique to law enforcement: *legal requirements.* Recall that the sole authority for law enforcement agencies to have an intelligence function is their statutory authority to enforce the criminal law. As a result, conceptually all information collected must be viewed as if it may eventually result in a criminal prosecution. Consequently, information is needed, at the least, to aid in establishing the criminal predicate and eventually sufficient evidence to establish the burden of proof in a trial. Requirements will need to be defined that help establish the corpus delecti or the elements of a specific crime as it relates to the intelligence targets.

Requirements and Criminal Evidence

This issue warrants special attention because it is unique to law enforcement intelligence. In the national security intelligence community, requirements serve as information to help make decisions about threat prevention, policy development, and strategic responses. In law enforcement intelligence, however, while many of these same needs are fulfilled, there is the added dimension that information collected from requirements may also be used as criminal evidence. Given the civil rights responsibilities that law enforcement officers must uphold, intelligence requirements for a law enforcement agency must also ensure that information collected during the requirements process follows the law of criminal procedure.

This can be a challenging process for law enforcement because there is a constant balancing process. In some cases, information collected about an individual must be balanced and documented with the threat to public safety. In other cases, the officers may be following up on a SAR to determine the veracity of the lead and establish both a criminal predicate and determination of a threat. There are many scenarios where decisions are made about information collection and retention that are in the arena of uncertainty. Relying on a cautious perspective, some fundamental guidelines should help guide the information collection process for legal requirements:

- Follow the law of criminal evidence and procedure.
- Always act in good faith with documented evidence and rationale that are the basis for information-collection and retention.
- If there is a threat to community safety, document the evidence and rationale associated with that threat and corroborate it to the extent possible.

Summary

Information is needed to make decisions: the higher the quality and the more comprehensive the information, the more sound the decision. Similarly, information that answers a specific question is more useful than information that is general. If an executive is going to make a decision about implementing a new program, he or she needs information about the specific costs, benefits, and risks of the program as well as the more difficult dimension of what benefits will be lost if the program is not implemented. Typically, the information sought is not conclusive, but based on probability, the experience of others, experimentation, logic or, sometimes, an educated guess. Not having sufficient reliable information makes the decision process more difficult and risky.

The same process applies to the operational environment of criminal intelligence. To adequately assess the threats from a terrorist group or criminal enterprise, information is needed for a comprehensive analysis. Often during the course of the analytic process, critical information is missing that prevents a complete and accurate assessment of the issue. The collection process focuses on collecting the specific information identified in the requirement in order to answer questions related to criminal or terrorist threats.[17] The fulfillment of the intelligence requirement provides critical information for making strategic or operational decisions about how to respond to the threat.

The intent of this discussion was to provide some perspective of intelligence requirements as specifically related to law enforcement intelligence. Once those information needs are identified, the next step is to collect them.

Collection

Collection of information has been discussed in the context of the intelligence process (Chapter 4) and information needs for ILP (Chapter 6). The current discussion builds on the previous by looking at information from a broader perspective. Collection refers to information that is brought into the intelligence process for analysis. It is the generation of raw data and, as will be seen, it is not always an overt action by the law enforcement agency to reach out and gather information.

Essentially, information enters the intelligence process in one of three ways:

1. It is deliberately sought out and collected—tasked collection.
2. It is collected as a result of another law enforcement activity—routine collection.
3. It is given to law enforcement—volunteered information.

Tasked collection is in response to intelligence requirements and is typically gathered as a result of a collection plan, defined as follows:

> A plan for gathering information from all available sources to meet an intelligence requirement. Specifically, a logical plan for transforming the essential elements of information into orders or requests to sources within a required time limit.[18]

[17] FBI Office of Intelligence. *The FBI Intelligence Cycle: Answering the Questions. A Desk Reference Guide for Law Enforcement.* (Pamphlet), July 2004.

[18] www.acpo.police.uk/asp/policies/Data/nim2005.pdf

The collection plan, previously referred to in Chapter 6, typically will be determined by an analyst, sometimes with input from a supervisor, to determine what types of information are needed, where (sources) the information may be obtained, and how (methods) the information will be gathered. The analyst will have an array of options from which to choose, ranging from open sources (discussed in detail in Chapter 11) to restricted databases,[19] to interviewing people, and more. The key lies in the question: "Where might I find this information and how will I get it?" The collection plan is the road map to answering this question.

In some cases, the assistance of operational units will be needed. In these circumstances, intelligence personnel should coordinate with operational managers or supervisors to explain what information is needed, why it is needed, and the role of the operational units in collecting the information. Even in cases where the "why" must remain confidential, a general description of the "why" will help in gaining cooperation and commitment.

When operational units assist in collection, explicit descriptions of the types of information needed should be provided. Similarly, time constraints for when the information is needed should be established. Operational units should also be provided with precautions, if any, during the collection process. In some cases, precautions may be related to officer safety; in other cases, the precaution may be to collect the information in a subtle manner so as not to tip off an inquiry. The key, of course, is effective communications between intelligence personnel and operational personnel.

The second method, *routine collection,* refers to the collection of information as part of routine operational and law enforcement activity. It focuses on the standing intelligence requirements or other issues of intelligence significance that are known and require a constant input of raw information. Information collected in this way usually is submitted as an information/intelligence report, but it may also be recorded elsewhere such as information within or from the following:

- Crime reporting
- Criminal investigations, including stand-alone proactive or reactive operational databases/case management systems
- Firearms licensing to monitor trends and to flag names of known offenders
- Community and partnership activities and meetings
- Custody records.

Routine collection can take many forms. As one example, the intelligence commander in one state has configured e-mail notification from the Open Source Center[20] (OSC) so that whenever any kind of information naming his or her state is entered into the OSC, the commander routinely receives an e-mail about the entry. In many cases, the information would have limited or no value from a criminal intelligence perspective, but where there is value, the information may have been missed without routine collection.

[19] Chapters 12 and 13 will discuss these in detail.

[20] OSC is an information system operated by the Office of the Director of National Intelligence. Open source information is the topic of the following chapter.

Volunteered information is offered to law enforcement by the general public, community contacts, and private partners. Its collection is focused (but not exclusively based) on the intelligence requirement. Information obtained usually is recorded and submitted on a SAR or some form of information report, depending on the nature of the information.

Collecting Information from Corrections Agencies

Correctional agencies are an often overlooked source of information in the collection process. Increasingly, corrections departments are creating and using a Security Intelligence Threat Group, an intelligence-based approach to information collection and analysis to determine threats that reside in prison facilities.

Despite common misperceptions, many inmates retain strong connections with criminal groups on the outside during their incarceration. There is ample evidence that gangs and drug traffickers as well as radical ideological groups (such as the Aryan Brotherhood or Islamic extremists) have outside connections and tend to know, and sometimes have influence on, the criminal organization's activities. Corrections agencies have greater breadth for information collection and can be an important data source for the intelligence process.

> Significant elements of nontraditional information and intelligence resides within corrections IT systems. In fact, corrections is uniquely positioned to gather information that other law enforcement entities are not able to gather. Information like inmate visitor data, criminal associate data, and telephone record data are but a few of the intelligence sources that have the potential to provide valuable insight to law enforcement and homeland security agents seeking to develop a framework for social networking to better determine the synergistic relationship between the criminal enterprise and the terrorist network(s) that threaten our country.[21]

The types of information that correctional agencies are able to collect and retain are invaluable. While the information has often been successfully exploited for dealing with gangs, such initiatives need to be broadened. The National Institute of Justice has established the Corrections/Law Enforcement Intelligence Gathering and Sharing Project[22] as a means of enhancing threat identification. Beyond working with corrections agencies within a law enforcement agency's region, monitoring projects such as this can provide additional value for developing information-sharing.

Summary

Regardless of the method that is used to collect information, it is important to remember for law enforcement intelligence that there is a different standard for information that is collected for use in a criminal intelligence records system between information that identifies individuals and groups and information that contains no identifying information. (These differences are discussed in detail in Chapter 7.)

[21] Herzog, Thomas J. *Integrating Correctional Authorities into the Fusion Center Rubric.* Palm Coast, Florida: Corrections Technology Association, 2007, p. 4.

[22] www.justnet.org/TechBeat%20Files/DataMining.pdf

Analysis

Without analysis, there is no intelligence. No single methodology is used for intelligence analysis; rather, various approaches and analytic tools are used, depending on the type of data/information that are available and the type of analysis (tactical or strategic) that is being performed.

The intent of this discussion is not to teach analytic methods, but to provide the consumer of analysis with insights into the process. Such insights should make the end-user a more enlightened consumer. Moreover, with a better understanding of analysis, a law enforcement officer will have better insights when responding to intelligence requirements.

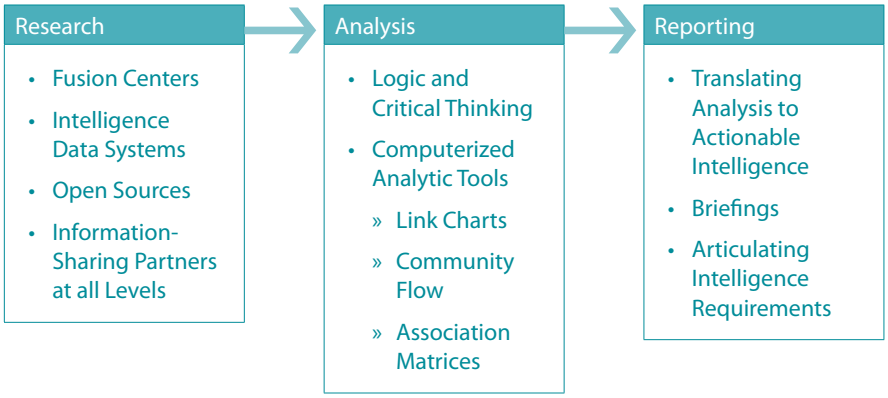
Intelligence analysis is often referred to as a unidimensional activity that is the central step in the intelligence process. When examining the analysis function more closely, one finds that it is a process that requires three broad skill sets. (See Figure 10-4) As such, the development of knowledge, skills, and abilities (KSA) must correlate with these skill sets.

The first skill, *research,* involves collecting diverse pieces of information and assessing the value (validity and reliability), as well as the relevancy and materiality to the assessment. Research is somewhat different from collection. Research involves gaining information that clarifies issues and provides perspectives on an issue of interest. Examples: searching the web blogs of anarchists to learn more about their beliefs and train of thought; reviewing research on the characteristics and common processes of human smuggling; reviewing reports and articles on a specific issue, such as the behavioral characteristics of a person planning a suicide attack; or any other type of data collection that provides insight—as opposed to evidence— about a targeted issue. Certainly there could be an overlap between research and collection; however, the roles are more complementary than duplicative. Analysts' KSAs must include both research and assessment methodologies. The analyst must be aware of the diverse sources of information—both open source information and law enforcement proprietary information—and know how to gain access to them. While collection of information will occur from a wide array of sources beyond the analyst, the need for research skills to be able to drill down into the information is essential.

The intelligence analyst must be more than a recipient of information. The analyst must be proactive in two methods: The first is to define and disseminate intelligence requirements to fill gaps in the information in order to have a more comprehensive and robust analysis of a threat, individual, or target. The second method is to elicit information from diverse sources. Whether this is a data base, a fusion center, a private partner, or an investigator, the analyst must proactively seek the information. Information-sharing systems and practices have increased dramatically as a result of post-9/11 intelligence reengineering. Nonetheless, no system or process can ensure that all the needed information will reach the analyst's desk. Proactive efforts by the analyst will add redundancy to the collection process to ensure that it is as comprehensive as possible. This is reinforced by the *Law Enforcement Analytic Standard #11–Collection Follow-Up Standard:*

In the course of collection by investigators and others, analysts shall evaluate the progress of the collection to determine if the collection plan/requirements are being met and shall identify additional sources of information, as well as identify information that may be useful to other cases or activities. Where possible, analysts shall relay that information to an appropriate body for follow-up.[23]

Figure 10-4: The Analytic Process



An important part of this process is that policies and procedures must give analysts the authority to seek needed information and have some type of accountability mechanism to ensure that the information is being provided. An unfortunate reality in many law enforcement organizations is that the intelligence analyst is often viewed as having a lower professional status than a sworn officer, sometimes making it difficult for analysts to give direction to investigators. While this artifact of organizational culture is slowly changing as analysts are increasingly viewed as practicing professionals, remnants of this perspective remain. Consequently, it is important for the intelligence process to ensure that analysts have the organizational authority to gain the information they need.

The second skill set, *analysis,* is essentially the scientific approach to problem solving. It relies on inductive and deductive reasoning; a balanced assessment of raw data; objectivity in the interpretation of facts; hypothesis testing; critical thinking; and decision making based on evidence. The late Carl Sagan, a world-renowned astrophysicist, explained the scientific process this way:

> Science is a way of thinking much more than it is a body of knowledge. Its goal is to find out how the world works, to seek what regularities there may be, to penetrate to the connection of things—from subnuclear particles, … to living organisms, the human social community, and thence to the cosmos as a whole. Our intuition is by no means an infallible guide. Our perceptions may be distorted by training and prejudice or merely because of the limitations of our sense organs, … Science is based on experiment, on a willingness to challenge old dogma, on an openness to see the universe as it really is. Accordingly, science requires courage—at the very least the courage to question the conventional wisdom. … [T]he scientific cast of mind examines

[23] Global Justice Information Sharing Initiative and the International Association of Law Enforcement Intelligence Analysts, Inc. *Law Enforcement Analytic Standards.* Washington, D.C.: Global Justice Information Sharing Initiative, 2004.

> the world critically as if many alternative worlds might exist. … If you spend any time spinning hypotheses, checking to see whether they make sense, whether they conform to what else we know, thinking of tests you can pose to substantiate or deflate your hypotheses, you will find yourself doing science.[24]

This process described by Sagan is essentially what intelligence analysts do when attempting to derive meaning from a diverse array of facts. Sagan noted that science seeks to determine "…what regularities there may be…". In law enforcement, we seek to identify criminals' modus operandi because these regularities in criminal processes are important for forecasting crime and determining prevention strategies. Similarly, Sagan observed that science seeks "…to penetrate to the connection of things." Law enforcement intelligence analysts seek to find the connection between criminal conspirators (e.g., via link analysis), between different types of evidence (e.g., via association matrices) and between criminal transactions (e.g., via commodity flow diagrams).

Intelligence analysis is an intellectual exercise that has pragmatic applications. For most people, it does not come easily. It requires *structure*, *critical thinking*, *self-discipline*, and *strong substantive knowledge of the target*. "Structure" refers to the ability to be organized and follow accepted analytical methods without taking shortcuts and ensuring that all information and evidence is included in the analysis. "Critical thinking" means that the analyst will follow the rules of logical reasoning, not intuition. It also means that the analyst will draw conclusions based on the known evidence, not assumed evidence. "Self discipline" is essential for the analyst to remain objective and not be influenced by emotion or external pressures. This objectivity also means that the evidence is considered with respect to its "weight" (reliability, validity, and corroboration). Beyond having the analytic KSAs, the analyst needs to have "substantive knowledge" of the targeted crime(s). Whether the target is a Jihadist network, drug trafficking cartel, or money laundering network, the analyst needs to understand the terminology, beliefs, and mechanics associated with the criminal enterprise.

Training, programs, continuing education, and self-directed education are valuable for developing the substantive knowledge needed for effective analysis; however, the thinking skills, which must be integrated with the substantive knowledge, are more challenging. A person can be taught the processes and tools of analysis, but critical thinking is most effectively produced through "mental calisthenics" and experience. Mental calisthenics refers to series of written exercises or problems that challenge a person to find a solution. There may be multiple solutions, of which the next challenge is to find the best or most probable solution. This process is frequently used in Problem-Based Learning, which is a strategy that builds a curriculum around a central question. The question may force the student to either solve a problem or make a decision.[25] The analytic skill set is the most difficult to effectively develop in an analyst; it is also the most critical.

The third skill set is *reporting*. Throughout the analytic process, there are stages where the findings must be reported to decision-makers and investigators.

[24] Sagan, Carl. *Broca's Brain: Reflections on the Romance of Science*. New York: The Ballantine Publishing Group, 1979.

[25] Friedman, Robert S. and Fadi Peek, "Problem-Based Learning and Problem-Solving Tools: Synthesis and Direction for Distributed Education Environments," *Journal of Interactive Learning Research* 13,(3)(2002): 239–257.

Reporting is translating the analytic output into descriptive status reports or actionable intelligence. A descriptive status report essentially describes the character and process of an intelligence target, probable effects, and probable future activities. The report may also include evidence currently possessed, intelligence requirements, and unexplained crime-related phenomena that need closer assessment. Typically, these reports are designed to assist in planning and directing an inquiry, allocating resources, assessing risk to potential victims, gaining insights about threat timetables, planning for intervention and mitigation strategies. In contemporary intelligence, the reporting process is when the analyst develops "intelligence products." This will be discussed in detail in the next section of this chapter.

Suggested Software Needed for Effective Analysis

- Word processing program
- Spreadsheet program
- Relational database
- Presentation software
- Flowcharting software
- Link analysis software
- Database reporting/visualization software
- Mapping software
- Photo enhancement software
- Telephone analysis software
- Portable Document Format (PDF) creation software
- Security software (virus, adware, spyware software; firewall and Virtual Private Network [VPN] security)
- Publication software
- Statistical analysis software
- Text mining software

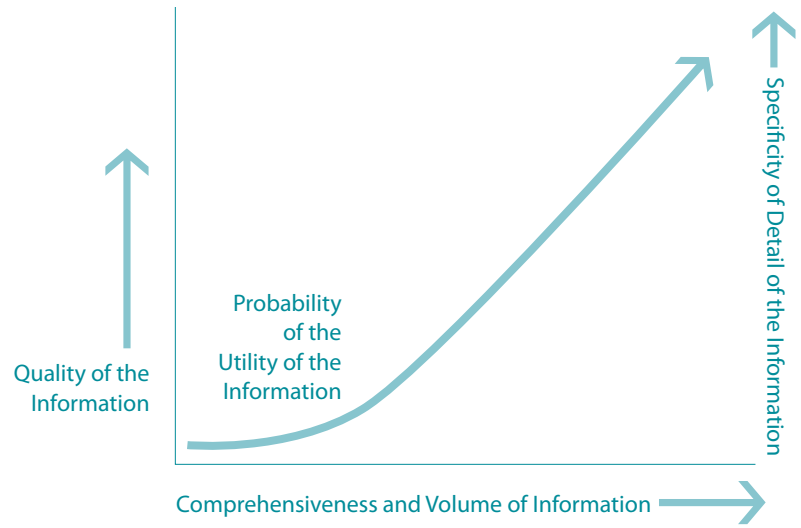
Resource: *The Analyst Toolbox,* Global Intelligence Working Group. it.ojp.gov/documents/analyst_toolbox.pdf

---

With actionable intelligence, a law enforcement agency has sufficient information to develop an operational response to threats. Within this framework, three factors contribute to effective analysis:

1. The overall quality of the information used to make a decision. Accuracy of information is essential. When information is analyzed, conclusions are drawn based on the facts that the analyst has. If the information is wrong or biased, this will inherently affect the quality of the analysis.
2. An increased body of information to make the information more comprehensive; hence, corroborating other facts. As the volume of high-quality information increases, the more accurate the analysis. Raw information is clarified and the quality of analysis will increase as volume increases. The key is to ensure that the quantity of information is accurate and relevant, a factor that is at the heart of the fusion process.
3. Increased specificity of the information. The more detailed the raw information, the greater the likelihood of identifying subtle factors about a threat.

Figure 10-5: Critical Characteristics of Information Quality



As illustrated in Figure 10-5, as each factor increases, the value of the analysis increases. Regardless of the skill of the analyst and the analytic tools available, the character of the raw information is fundamental to actionable analysis.

Analytic Tools

A number of analytic tools are available to the intelligence analyst. "Tools" essentially refers to methodological techniques that help *organize*, *integrate*, *compare*, *correlate*, and *illustrate* a body of raw information. None of the analyst tools will produce actionable intelligence alone; each adds a component of new knowledge—or at least new insight—about the data which, collectively, contribute to the analysis and/or lead to the definition of new intelligence requirements.

The actual analysis relies on the critical thinking skills of the analyst along with his or her ability to integrate the output of these diverse methodologies into a cohesive, actionable intelligence product. These products may include portions of the analytic tools output to illustrate complex relationships, such as an illicit commodity flow chart or a link analysis chart showing the relationships and hierarchy of people involved in a criminal enterprise.

While the intelligence consumer does not need to know how to perform these various types of analyses, there is value in understanding the different analytic tools available and the types of information they provide. While not an exhaustive list, the more common tools[26] an intelligence consumer may encounter include the following:

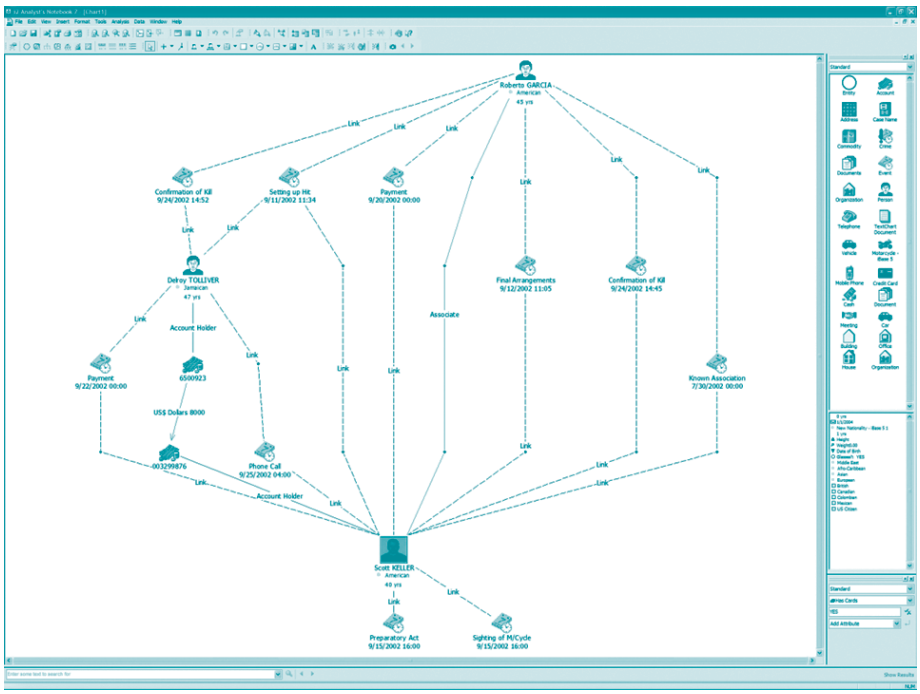
- Activity flow. Similar to a modus operandi or method of operation, the activity flow shows the steps a criminal enterprise uses, indicating exact incidents, dates, and a description of the activities that occurred. The incidents are linked in a flow chart to help understand the progression of the enterprise. The activity flow pieces together a complex criminal organization and may be used for intervention in the enterprise as well as to determine where gaps exist. If gaps are identified, intelligence requirements will be used to fill the gaps so that the activity of the enterprise can be fully mapped to aid in prevention and in prosecution.
- Association matrix. This matrix seeks to correlate two or more factors in a criminal enterprise, documenting the frequencies with which certain factors (e.g., persons, organizations, phone numbers, addresses, and similar variables) occur at the same time in order to isolate the correlating factors that are instrumental in the criminal enterprise operations and eliminate factors that have no correlation. The factors may be alike, such as correlating a series of telephone numbers. The factors may also be inherently independent but provide insight when they are correlated, such as charting the travel patterns of two intelligence targets when a telephone call or bank transaction precedes the travel.
- Commodity flow/visual investigative analysis. A diagram that illustrates how an unlawful commodity is moved through a criminal enterprise and the transactions that are made in the commodity movement. For example, the commodity flow of Afghan heroin would show each transaction and method of smuggling, along with the transaction costs, from Afghanistan to a city in Middle America.
- Communications traffic analysis. Important information can be gained from a traffic analysis of telephones, text messaging, and e-mail. By identifying with whom intelligence targets are communicating, the frequency of the communications, their origins and destinations, length of the communications, and whether there were attachments to e-mails, an analysis can provide significant corroboration and evidence of criminality. While the content of communications, obviously, will provide important information, an analysis of communications traffic can also be valuable.
- Crime pattern analysis. A generic term for a number of related disciplines such as crime or incident series identification, crime trend analysis, hot spot analysis, and general profile analysis and can include mapping.
- Criminal business profiles. Such profiles contain detailed analyses of how criminal operations or techniques work, in the same way that a legitimate business might be explained.
- Demographic/social trends analysis. An analytic method centered on demographic changes and their impact on criminality. It also analyzes social factors such as unemployment and homelessness, and considers the significance of population shifts, attitudes, and activities as they may affect crime.

[26] Many of these analytic tools are illustrated in: Peterson, Marilyn, et al. *Successful Law Enforcement Using Analytic Methods.* South Florida, Florida: International Association of Law Enforcement Intelligence Analysts, Inc., 1996.

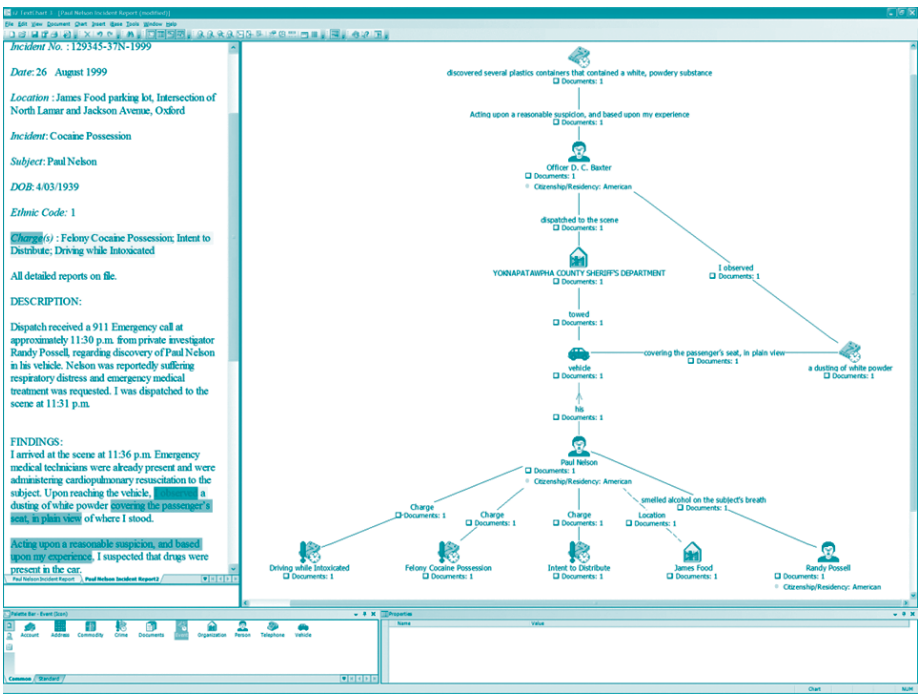
- Event flow analysis. Charts that provide a visual depiction of a series of important occurrences or incidents (such as a criminal transaction) and the sequential relationship of these occurrences, such as travel of a criminal participant, monetary transactions, or other events that are critical in facilitating the crime.
- Financial analysis. There are a variety of financial analysis techniques that collectively seek to correlate diverse financial transactions including the nature of the transactions; parties involved; origin, intermediary, and destinations of transactions; and comparative analysis of income and expenditures. Collectively, the intent is to document transaction trends of intelligence targets (both individuals and organizations) and identify discrepancies or suspicious financial activities. Given that virtually all crimes have some form of financial element, financial analysis is an important tool.
- Hypothesis testing. The analyst will make a hypothesis about the linkages of people and organizations in the criminal enterprise, necessary transactions for the enterprise to operate, and critical commodities or resources necessary for the enterprise to be successful. Unlike the previous items in this list, which are visual depictions of various elements of the enterprise, hypothesis testing uses the depictions to determine if all the elements in the enterprise have been identified that can be used to prevent the enterprise from continuing and, ideally, determining the criminal liability of participants.
- Link Analysis. A chart that identifies all confirmed and suspected persons and organizations in the criminal enterprise and illustrates their relationship to each other.
- Market profiles. The profiles are assessments that survey the criminal market around a particular commodity in an area, such as drugs or stolen vehicles, or of a service, such as prostitution. They are continually reviewed and updated.
- Network analysis. This analysis not only describes the links between people who form criminal networks, but also the significance of the links, the roles played by individuals, and the strengths and weaknesses of a criminal organization.
- Operational intelligence assessment. Such an assessment evaluates incoming intelligence to maintain the focus of an operation on previously agreed objectives, particularly in the case of a sizeable intelligence collection plan or other large-scale operation.
- Results analysis. An analysis that evaluates the effectiveness of law enforcement activities; for example, the effectiveness of patrol strategies, crime-reduction initiatives, or a particular method of investigation.
- Risk analysis. An analysis that assesses the scale of risks posed by individual offenders or organizations to individual potential victims, the general public, and to law enforcement agencies.
- Target profile analysis. An analysis that embraces a range of analytical techniques to describe criminals, their criminal activity, lifestyle, associations, the risk they pose, and their strengths and weaknesses to give focus to the investigation targeting them. Profiles may also focus on victims and vulnerable persons.

Each of these techniques is used to better understand raw information and its relationships and to illustrate a criminal phenomenon. Figure 10-6 presents examples of two kinds of analytical charting.

Figure 10-6: Illustrations of Analytical Charting[27]



Link Analysis Chart



Text Analysis Chart

[27] The charting illustrations are from i2's Analyst Notebook software. Images courtesy of i2.

Predictive Analysis

Predictive analysis has become increasingly popular as a tool for intelligence analysis; therefore, a brief description of the concept can be of value to the intelligence consumer. Predictive analysis is borrowed largely from the private sector where econometric models are used to forecast market changes. By analyzing economic factors in a current market, buoyed by analysis of known trend data—such as changes in a sector's economics during different times of the year—a manufacturing firm may alter its production, workforce size, and supply chain to enable it to continue profitable operations while meeting supply demands throughout varying conditions. In that situation, the analysis provides strategic direction for both management and operations to make decisions about alternative futures that will help them avoid unnecessary profit losses while still fully serving customer needs.

Can such a quantitative-based approach work in the largely qualitative world of law enforcement intelligence analysis? While predictive analysis has important applications to intelligence analysis, it will not provide an analysis as robust as in more quantitative fields that have more predictable change cycles, such as in the business world. Nonetheless, it has important applications to intelligence, but will require a diverse and often labor-intensive research effort; a multifaceted analytic methodology, and a broadened method of reporting that offers differential outcomes based on the evolution of social and political trends. As time passes, these trends can be monitored by the intelligence analyst to refine the status and threat implications of the trends being observed.

Predictive analysis is a critical-thinking methodology that integrates known quantitative and qualitative variables—including incidents, events, and political and social dynamics—into a logical forecast of threat parameters. In many ways, the label "predictive" is misleading because it is virtually impossible to truly predict events that are based on human behavior and the infinite number of variables that can influence that behavior. The process is a probabilistic analytic exercise that gathers diverse data, constantly monitors changes in the data, and refines the forecast based on the new inputs. Just like the intelligence process itself, predictive analysis is reiterative, constantly seeking new inputs of information to refine the forecast.

The reiterative nature of predictive analysis complements requirements-driven intelligence. This process continuously seeks to identify information to fill intelligence gaps or voids in our knowledge base about threats, and then identify, collectand analyze information to fill those gaps. Intelligence requirements—the information that is required to fill a gap—provides constant input into the intelligence cycle to help ensure that there is a base of knowledge that is as comprehensive as possible.

Predictive analysis in law enforcement can have the greatest impact on strategic intelligence, although it can also have an application to aid in defining standing intelligence requirements. This analytic technique will not forecast threats, per se, but it can forecast changes in the environment that may alter conditions that contribute to threats.

Critical Variables for the Analysis of a Threat

Critical to analytic techniques that seek to help us understand any kind of threat, is the ability to collect information about a series of key variables related to the intelligence target(s). Once again, each variable has significant implications for intelligence requirements.

- Intent. What is the stated intent of the intelligence target? Has it changed? How might any of the current events or activities influence the stated intent of the target?
- History. What has the intelligence target or group done in the past? Often, history can provide insight into future behaviors, methods, and targets. This includes identifying and assessing triggering events from previous attacks or violent behaviors of the intelligence target.
- Capability. What capabilities does the target or group have? Have they been trained to execute terrorist attacks or crimes? Do they have critical assets available, including people, munitions, money, documents, and travel to commit the crime?
- Opportunity. Are there any unusual or unique opportunities arising that will help facilitate an attack? If so, what kind of access to that opportunity will the intelligence target have? Is there evidence to suggest that planning for an attack or crime to coincide with an opportunity has occurred?
- Resolve. Does the intelligence target or group actually have the commitment to execute the attack? Is the intelligence target simply making a threat or does the target actually pose a threat? Are there insights into how the resolve to commit an attack may be mitigated? Particularly in the case of ideological groups, a critical variable related to "resolve" is learning the characteristics of the leader. If the group has a charismatic leader, then the likelihood increases that the group will act on its intent.

Intelligence requirements and analysis are inherently related to threat assessments. The interrelationship is systemic: a change in one component will affect the others.

> Intelligence analysis is a complex task involving the examination and assessment of information to draw conclusions about a particular topic. It is not an academic exercise because it does not involve philosophical theories. Instead, intelligence analysis is a function heavily dependent on realism and requires an objective approach to thinking. It is predominantly process driven, and it requires continuous exhaustive research using information from a variety of classified and nonclassified sources. Analysis also involves the collation of information to identify relationships, expose indicators and filter factual evidence. This is a process that forces the questioning of information to confirm truths and probabilities. The next process is to scrutinize the information to recognize trends that will lead to an event or pattern. Once a conclusion about the information has been formed, an assessment is made which is then presented to customers so they can make well-informed decisions based on our findings.[28]

[28] Australia's Defence Intelligence Organisation, www.defence.gov.au/dio/analysis.html.

Summary

Intelligence analysis is both the development of cognition and a cognitive process. It is a cognitive process because the analyst is learning as he or she conducts the analysis. But it is also the development of cognition because the output of the analysis— conclusions, estimates, and forecasts—is new knowledge that will be shared with others in reports and briefings. Effective analysis, therefore, should serve the law enforcement agency in the following ways:

- Identifying points of opportunity for intervention that might change the state of affairs in some way, especially before a conflict occurs
- Helping states attain a comparative advantage in decision-making, thus the term "actionable intelligence"
- Protecting the state and its citizens to maximize security
- Optimizing resources
- Integrating information to enhance understanding of threat environments.

Analysis is a critical factor in information management because it provides the intelligence that describes criminal threats and the alternatives to manage those threats. This information must be expressed in the form of intelligence products.

Intelligence Outputs and Products

The output of analysis, that is, intelligence, must be placed in a reporting format that maximizes the consumption and use of the information. This is referred to as the intelligence product. In describing the relationship of analysis to products, Ratcliffe, in *Integrated Intelligence and Crime Analysis,* observed the following:

> …criminal intelligence is the creation of an intelligence knowledge product that supports decision-making in the areas of law enforcement, crime reduction, and crime prevention. In this context, an intelligence knowledge product is a product that can influence the thinking of a decision-maker. It is the result of a criminal intelligence analysis and could be a written bulletin, a presentation, a verbal report, or some combination of these in a briefing. An intelligence knowledge product could even be a brief telephone conversation if the intelligence is timely and has an effect on the decision-making of the recipient of the intelligence.[29]

Typically, different types of products are developed to meet the needs of different consumers and different types of analysis. A tactical analytic product will differ from a strategic analytic product. The product developed for a comprehensive assessment of a targeted criminal enterprise will differ from a product intended to make officers aware of criminal indicators. An executive briefing of a criminal threat will differ from a patrol briefing of a criminal threat. Regardless of the type of product, all should contain five fundamental elements in the context of the product's intent:

1. Identify the targeted consumer of the information (patrol officers, administrators, private sector, others).
2. Convey clearly the critical information needed by the intended consumer.

[29] Ratcliffe, Jerry H. *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders.* Washington, D.C.: Office of Community Oriented Policing Services, U.S. Department of Justice, 2007, p. 8.

3. Identify time parameters wherein the intelligence is actionable.
4. Define additional intelligence requirements, if needed.
5. Provide operational recommendations in light of the analysis.

Ideally, products are a series of regularly produced intelligence reports that have a specific format and type of message to convey. They are most useful when each product has a specific purpose; is in a consistent, clear, and aesthetic format; and contain all critical information the consumer needs with no superfluous information. As a general rule, at least three types of products should be developed by an intelligence unit or fusion center:

1. Products directed toward the prevention of known threats.
2. Products that provide threat advisories which provide indicators of threatening behaviors and threatened targets.
3. Products that describe changes of the terrorist or criminal threat picture to a jurisdiction.

While most law enforcement officers are very familiar with investigative reports and records, they are less familiar with intelligence products. As indicated in Table 10-3, there are notable differences that are important for the consumer to understand. With a clear understanding of the distinction, there will be greater use of the products.

Table 10-3: Differences between Investigation and Intelligence Reports

Criminal Investigation Reports and Records	Law Enforcement Intelligence Reports, Records, and Products
• Primary goal is prosecution • Report is documentation of a criminal incident that occurred • Report is an official record and is evidentiary • Motive is irrelevant as a legal element of the crime • Evidence is documented to prove the corpus delicti	• Primary goal is threat-based prevention • Report focuses on suspected criminal threats • Report documents information associated with a threat inquiry • Motive is an important tool for forecasting • Information is documented to build hypotheses about criminal threats

Two broad distinctions in law enforcement intelligence outputs are characterized in Table 10-4. The first is "case intelligence." A critical characteristic of case intelligence is that it identifies individuals or organizations. Conceptually, its ultimate goal is arrest and prosecution of particularly-described persons as a means of preventing a threat from reaching fruition.[30] An important factor to note is that with case intelligence, civil rights attach to individuals who have been identified in any type of intelligence report. The second type, "intelligence advisory products," describes (i.e., advises) general indicators of crime and threats for which officers must be aware. The goal is for law enforcement personnel to be

[30] It should be remembered that the only authority for law enforcement agencies to be in the "intelligence business" is based on their statutory authority to enforce the criminal law; therefore, development of a criminal case is a sound model to follow.

aware of the indicators and, if observed, take appropriate action to ensure public safety and prevent a criminal incident from occurring. As a general rule, there are no explicit civil rights issues of advisory products until a person or organization is identified as related to the criminal indicators.

Table 10-4: Case Intelligence versus Intelligence Products

Case Intelligence	Intelligence Advisory Products
• Individuals are identified • Specific offenses are identified • Intelligence develops evidence of criminal liability • The goal is to develop a criminal case for prosecution	• Trends in crime and/or their methodologies are identified • A change in criminal trends is forecast • Indicators of the new crime types are identified for awareness by law enforcement personnel • The goal is to prevent the crime from occurring

Any intelligence unit or fusion center can determine the type of products it needs to develop based on the administrative mandate of the unit. Some are designed to meet unique jurisdictional needs, such as a transit law enforcement agency. As a general rule, law enforcement intelligence reports may be in a typology with two broad components: 1. The nature of the report and 2. The nature of the analysis.

Nature of the Intelligence Report

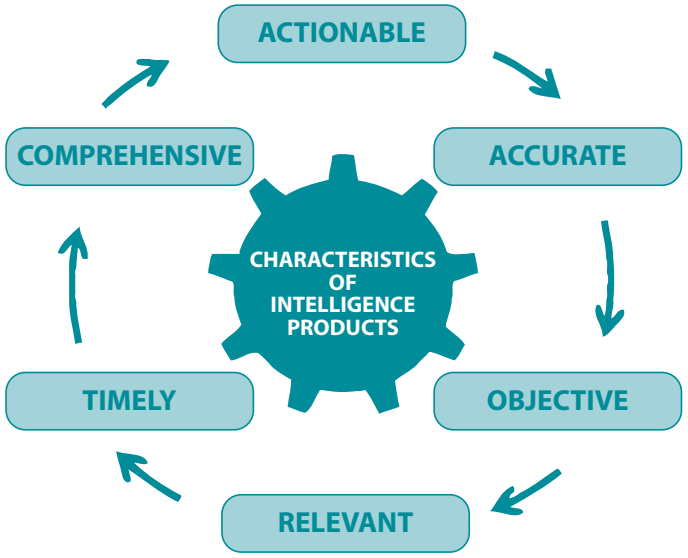
Different kinds of intelligence reports are created to meet the needs of specific audiences. An "Intelligence Alert" may be a short report giving the basic facts about indicators or persons related to a threat that is time-critical. An "Intelligence Bulletin" may provide more detailed information about indicators or threats that are not imminent but those which personnel may encounter. An "Intelligence Assessment" typically provides a historical perspective of a threat and how the current status of the threat has changed. At this point there are no uniform classifications of intelligence reports across all agency types and levels of government; rather each agency or fusion center produces reports that tend to meet these general guidelines. Law enforcement personnel should receive training on the types of products that are used in their jurisdictions and the intent of each report type.

Nature of the Analysis

Perhaps adding confusion to the universe of intelligence reporting is that some terminology has different meaning to the intelligence community, the military, and federal law enforcement when compared to state, local, and tribal law enforcement. The current discussion is directed toward the latter. Previously, the differences between tactical analysis and strategic analysis were described from the law enforcement perspective. Again, while there are no uniform categories of specific report types based on the kinds of analysis that was performed, suffice it to note that intelligence consumers should be aware that some report outputs will describe threats in need of an operational response (tactical) while other reports will describes changes in the threat picture (strategic).

Other report types exist or will emerge. Intelligence briefings are oral summaries of analyses that require yet a different approach to reporting that pay homage to the often repeated comment of Sgt. Joe Friday in the old television series Dragnet: "I want the facts, just the facts." We are increasingly seeing new report types emerging that are based on technology and range from text messaging to Podcasts. Regardless of the method of reporting, it is essential that each report type contains the information that is needed for the intended consumer to be effective in fulfilling his or her responsibilities.

Figure 10-7: Characteristics of Intelligence Products



As illustrated in Figure 10-7 and discussed below, regardless of the type of product, each should reflect six core characteristics.

1. Actionable. The product should provide sufficiently definitive information that some kind of operational activity or response may be developed from the intelligence.
2. Accurate. The nature of the analytic process is often probabilistic; therefore, concrete conclusions and forecasts can rarely be made. Despite this, every effort should be made to be as accurate as possible, with weaknesses in the conclusions clearly documented.
3. Objective. Intelligence products should be free of bias. All information should be provided in a balanced manner clearly articulating knowns and unknowns as well as strengths and weaknesses in the analysis.
4. Relevant. The analysis, and the products, should focus on threats that are part of the strategic priorities and/or emerging threats that could have a significant effect on public safety in the region.
5. Timely. Timeliness has two components. First, the intelligence product should be of a threat that is of current concern. Second, when practicable, the product should be made available to maximize the time permitted for operational units to develop a response and put it in place.
6. Comprehensive. The intelligence product should provide as much information as possible about all dimensions of the threat.

Practices to Avoid with Intelligence Products

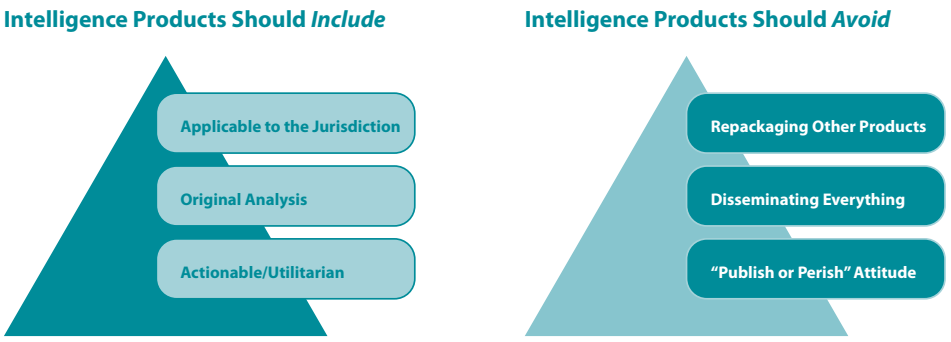
In the post-9/11 environment where the critical phrase is "information sharing," some practices related to intelligence products have emerged that create more problems than solutions. Information should be "targeted," that is, useful information needs to be shared with people who can use it. Unfortunately, this axiom has gone unheeded too frequently.

Three fundamental practices related to analysis and intelligence products should be avoided. They might be expressed as the "three don'ts of information sharing."

1. Don't repackage the intelligence products of another organization. Most agencies will have received the original product; hence, repackaging it is duplicative and can be confusing. A repackaged product adds little value and may have a misleading effect if the same information is distributed as the product of two different agencies. Further, if another agency's product is simply repackaged, the agency will not be able to provide any follow-up detail should inquiries be made.
2. Don't disseminate everything to everybody. Receiving too much information can be just as ineffective as receiving no information. If personnel are inundated with a cascade of information that has little value to them, they tend to pay little attention to any information. The intelligence function, not the consumer, must separate the wheat from the chaff. Targeted dissemination of information to people who need it is critical.
3. Don't develop a "publish or perish" attitude. This can be a systemic problem. Managers want to see productivity by intelligence analysts; however, productivity is difficult to quantify in the intelligence function. One activity which can be easily counted is the production of intelligence products and some intelligence units and fusion centers have used "products" as a measure of effectiveness. While it is understandable how this has evolved, the publication of products alone is not a measure of success. Even if the product is "interesting" it provides little value unless it is actionable. It is not the quantity of products that should be measured, but their *quality* and *utility*. Of course, this is difficult and somewhat subjective. The evaluation process is often difficult to perform effectively.

Figure 10-8 summarizes what intelligence products should and should not contain.

Figure 10-8: Attributes of Intelligence Products



To avoid the problems embodied in the "don'ts" of intelligence products, those responsible for the intelligence function should answer these questions affirmatively as they relate to intelligence products:

1. Tactical and Operational Intelligence. Does the intelligence product provide sufficient detail about a threat within your region or service area so that operational personnel can develop tactical plans or activities to prevent or mitigate an identified threat?
2. Strategic Intelligence. Does the intelligence product describe the characteristics, modus operandi, or change in the threat picture in sufficient detail as related to your region or service area so that effective decisions can be made about strategic priorities and resource allocation?
3. Actionable Dissemination. In light of the nature of the threat and content of the intelligence product, who within your region or service area has the right to know and need to know this information for threat prevention, mitigation, and/or planning?

Summary

Intelligence products are the means by which critical threat information reaches the street. The importance of developing the kinds of products of greatest use to an intelligence unit or fusion center's consumer and placing the right product in the hands of the people who need it is a critical process.

Conclusion

As specified in the *National Strategy for Information Sharing* (NSIS), two fundamental objectives are related to SLTLE agencies with respect to sharing information from the federal government:[31]

1. Ensuring that the Federal Government provides information in ways that better meet the needs of SLT partners through the establishment of an Interagency Threat Assessment and Coordination Group (ITACG) within the National Counterterrorism Center (NCTC). This integrated approach allows Federal agencies to work together to disseminate a federally-validated perspective on available threat information.[32]
2. Supporting improved collaboration at the State and local levels by designating fusion centers "as the primary focal points within the State and local environment for the receipt and sharing of terrorism-related information" and by establishing and sustaining a national integrated network of these centers.[33]

In July 2007, Congress passed the 9/11 Commission Act of 2007 that statutorily created the ITACG and designated the PM-ISE "to monitor and assess" the ITACG's efficacy.[34] The Act also called for a DHS State, Local, and Regional Fusion Center Initiative which, among other requirements, must "support efforts to include state, local, and regional fusion centers into efforts to establish an information sharing environment."[35] The NSIS further advanced these initiatives by providing a detailed description of the role of the ITACG and the roles and responsibilities of Federal and SLTLE agencies. Significant advances have been made in implementing the NSIS objectives[36] at all levels of government; however, there is variability of successes around the U.S. at the state, local, and tribal levels.

[31] National Strategy for Information Sharing, 2007, p. 30.

[32] NSIS, p. 18.

[33] NSIS, p. 20.

[34] 9/11 Commission Act of 2007 (P.L. 110-53), §521(c), The ITACG was established as part of the ISE Implementation Plan and Guideline 2, but the statute strengthened several of its functions and provided for additional oversight.

[35] 9/11 Commission Act of 2007, Op cit. §511(b)(2).

[36] McNamara, *Annual Report to the Congress on the Information Sharing Environment,* 2008, Op cit., p. 24.

For effective information management in the intelligence process there must be a common foundation and ideological thread permeating the law enforcement organization. To meet the needs of contemporary law enforcement intelligence, including newly established national standards, the management of information requires the following:

1. Reengineering some of the organization's structure and information processes. SLTLE agencies should examine their current intelligence processes, if any, to determine if they are consistent with the NCISP and currently accepted national standards for law enforcement intelligence. If not, adjustments should be made to the organization and/or processes. This consistency is important so that there is a common understanding and acceptance of information validity, reliability, and consistency with civil rights standards. A common perspective of the intelligence process and a body of policies and procedures, all of which meet the same national standards, greatly enhances two-way information-sharing—an essential element of requirements-driven intelligence.
2. Developing a shared vision of the terrorist or criminal threat. All agencies at all levels of government must define and understand the threats that face them. This does not mean that all communities are threatened in the same way, but that all agencies understand the common enemies. This includes a common understanding of threats and general agreement on the types of threats facing America. Important strides have occurred as cooperative initiatives and information sharing have taken place: for example, the growth of the Intelligence Fusion Centers, and initiatives such as the Global Intelligence Working Group, Criminal Intelligence Coordinating Committee, the Information sharing Environment, and the Counterterrorism Training Coordination Working Group. With diverse membership from law enforcement agencies at all levels of government, the common lexicon is growing and communication is increasing.
3. A commitment to participate and follow through with threat information. Effective information sharing can exist only if there is a true commitment by an agency to participate, not just lip service to intelligence initiatives. To enhance output of these different national initiatives, an executive must ensure that personnel are trained in the intelligence process and that policies are in place for effective, lawful, and reliable information collection and sharing (in accordance with standards in the NCISP). Commitment also means that the chain of command reinforces the need for employee information collection and sharing processes. Too often the policies that are in place are irregularly applied. When this occurs, the intelligence process breaks down and the ability to connect the dots is jeopardized.
4. The commitment of an agency's resources, time, and energy to the intelligence function. A commitment to participate necessarily requires a commitment of resources. Intelligence is prevention-oriented. Often, it is difficult to see what has been prevented. Similarly, a great deal of information that is collected and shared leads to nothing—a fact of life in the intelligence enterprise—but the critical few pieces of information that lead to the prevention of a terrorist attack are well worth the investment. The intelligence function should be a budget line in the agency's regular budget, not an activity that is relegated to soft money or piggy-backed on other agency activities. The lack of a budget line for intelligence is tantamount to the lack of full commitment.

5. Proactive people using creative thought to identify what we don't know about terrorism and organized crime. Requirements-driven intelligence seeks to fully understand the environment of a community and how changes in that environment may influence threats or crime. Creativity requires viewing community conditions and potential threats through a lens that seeks to interpret information in different ways. Terrorists and criminals have shown they can be creative in the planning and execution of their crimes. Law enforcement must be similarly creative to identify changes in the threat environment and develop proactive operational initiatives to prevent threats from reaching fruition.
6. A law enforcement agency to think globally and act locally. Most people view issues in life from a provincial perspective. This is normal because our greatest concerns are those that affect us in the most direct manner. Unfortunately, the provincial view does not always serve us well when we view events around the globe with the mistaken belief that they won't affect us. Global events in terrorism and crime can affect us on local basis just as global economic events have an influence in our communities. As a simple example, terrorist events, war, economic markets, and political conflicts in OPEC will have an effect on the prices we pay at our local gas pumps. We must recognize that international planning, financing, and logistical support of terrorism, and criminal incidents can have an impact on our communities. Thus, local intelligence analysts must consider the extended effect of global incidents, such as the conflict between Israel and Hezbollah, and how that can be translated to local and regional reactions to those who support Islamic extremism. If the analyst does not have this information, then these are intelligence gaps that must be filled and applied locally.

Chapter 11:

Open Source Information and Intelligence: A Perspective for State, Local, and Tribal Law Enforcement Agencies

Open Source Information and Intelligence: A Perspective for State, Local, and Tribal Law Enforcement Agencies[1]

When considering the collection of information for the intelligence process, a historically undervalued resource has been open sources of information.[2] In many ways, open source information holds some of the greatest value for intelligence because of the vast array of diverse, reliable information available for analysis. This is particularly true with the rapid growth of networking. A great deal has been written about open source information,[3] particularly as it is used in business intelligence, and increasingly for its use in national security intelligence. The current discussion will provide perspective for open source application in the law enforcement community, including important limitations that may be imposed on the retention of certain types of open source information.

It should go without saying: The growth of technology has radically changed the character of open source information. To provide perspective, as the public embraced the World Wide Web en mass beginning in the mid-to-late 1990s, the Internet emerged as the primary source to search for all types of information. As computer memory and processing speeds increased, more information was being stored and processed, including audio and video files. The integration of computing into nearly every aspect of daily life, spurred by the prevalence of wireless computing has caused the development of faster, more discriminating search software. Similarly, content providers have increased the type and mass of content available. Collectively, technological development and the willingness of the public to embrace this technology have contributed dramatically to the ease and value of open source information.

There is a caveat, however: Quantity of information does not equal quality of information. Open source users must take care by assuring that the information collected from open sources for use in decision-making is accurate and dependable. Information absent quality control is of little value. The challenge, particularly when massive amounts of information are at one's fingertips, is to make good end-user decisions about what information should be kept and which information should be discarded.

Understanding "Open Source"

The concept of open source information and intelligence is in a state of renewed interest, particularly as applied to the intelligence community and law enforcement. A brief discussion on the concept and its application in the current context will provide perspective.

Why Is there Value in Open Source Information?

Open source information has often held a second-class status in the intelligence world because of the erroneous assumption that people, movements, and conditions that pose threats would not have information that is available about their intent, characteristics, or behavior in the open.

[1] For an effective discussion of open source information, certain topics are most effectively illustrated using examples from commercial services and web sites. Attempts were made to be objective in the illustrations and where possible use multiple sources. References to businesses and web sites are for illustration purposes only and should not be construed as an endorsement in any form.

[2] Best, Richard and Alfred Cumming. *Open Source Intelligence (OSINT): Issues for Congress.* Washington, D.C.: Congressional Research Service, 2007, p. 4.

[3] For example, see www.oss.net/extra/document/?module_instance=3 and www.firstmonday.org/issues/issue76/stalder.

This assumption is erroneous for six fundamental reasons.

- First, individuals and groups who pose threats because they have an extremist ideology—even those who support violence to fulfill their ideological goal—and typically want to share their beliefs and goals, usually with the intent of persuading others to adopt their beliefs. They often post such information on web sites, in print, in broadcast media that are sympathetic to their cause, and via shortwave broadcasts.[4]
- Second, criminals use the web as a largely anonymous instrumentality to traffic in contraband. Offenders can easily reach a U.S. market from overseas and use techniques to make them difficult to track, both of which add to the lure.[5]
- Third, certain types of information that are useful for the intelligence process, including information that identifies individuals, are openly available because policy, regulation, or law permits the custodian of such information to make it publicly available in some states; for example, public databases contain information about motor vehicle licenses, property ownership, voter registration, sex offenders, salaries of public employees, and a wide array of other information for which an individual has little, if any, control over its public release.[6]
- Fourth, people want selected information to be public. This can occur for a multitude of reasons: telephone numbers, business names and addresses, various reports of research, and marketing are but a few examples. Not only do the individual pieces of information provide insight, surprising amounts of new knowledge can be gained when such information is analyzed in the aggregate.[7]
- Fifth, nonlaw enforcement entities, such as the news media or advocacy groups, may conduct inquiries that become open sources. These sources may provide personal information, descriptions of behavior, personal relationships, activities of a given group, and descriptions of an incident to satisfy the purpose of their business or cause.[8]
- Finally, information often becomes openly available because of an individual's carelessness. A politician making an embarrassing statement in the presence of an open microphone in a public venue or a person writing incriminating information in a blog are examples. In these cases, valuable information that may be used in the intelligence process is often available through open sources.[9]

[4] For example, see media files supporting the World Jihad at www.memri.org.

[5] For example, see the Drug Enforcement Administration's Operation Cyber-Chase arrests of illegal web-based pharmacies at www.usdoj.gov/dea/pubs/pressrel/pr042005.html.

[6] For example, see the Michigan Internet Criminal History Access Tool (ICHAT) at apps.michigan.gov/ICHAT/Home.aspx.

[7] For example, see the aggregated data base to locate people and businesses at www.switchboard.com.

[8] For example, NBC's news stories on pedophiles – see www.msnbc.msn.com/id/6083442.

[9] One source for inadvertently released information, among a wide array of other information, is www.cryptome.org.

[10] *Intelligence Community Directive, Number 301.* National Open Source Enterprise. Section F(3), July 11, 2006.

Definitions and Categories

Open source information is any type of lawfully and ethically obtainable information that describes persons, behaviors, locations, groups, events, or trends. The Office of the Director of National Intelligence (ODNI) simply defines open source information as follows:

> Publicly available information that anyone can lawfully obtain by request, purchase, or observation.[10]

As can be seen by either of these definitions, the array of information that falls within the open source arena is very broad. From a law enforcement perspective, one of the values of open source information is that it can be searched for and collected without legal process. As will be described later, civil rights issues emerge related to the retention of open source information for the intelligence process.

As one should assume, when raw open source information is evaluated, integrated, and analyzed it provides new insight about intelligence targets and trends—this is open source intelligence.

Open source information is wide-ranging. To provide perspective, examples of categories of open source information include these:

- All types of media.[11]
- Shortwave broadcasts and conversations.[12]
- Publicly available databases.[13]
- Directories.[14]
- Databases of people, places, and events.[15]
- Open discussions, whether in forums, classes, presentations, online discussions on blogs, or general conversations.
- Government reports and documents.[16]
- Scientific research and reports.[17]
- Statistical databases.[18]
- Commercial vendors of information.[19]
- Web sites that are open to the general public even if there is an access fee or a registration requirement.[20]
- Search engines of Internet site contents.[21]

The main qualifier that classifies information as open source is that no legal process or clandestine collection techniques are required to obtain the data. While open source data has virtually always existed, networking has increased its accessibility significantly. For example, if an analyst was preparing a strategic intelligence report on trends in international terrorism, he or she may go to the U.S. Department of State Counterterrorism Office[22] web site, the FBI terrorism reports[23] web site, the Department of Homeland Security-funded terrorism database,[24] and the Israeli Defense Forces terrorism statistics center web site[25] to download the various reports and data. If the analyst was preparing a report on right-wing extremists, he or she may visit the Southern Poverty Law Center[26] web site to download reports or go to a white supremacy web site, such as Stormfront,[27] to read materials and then conduct further research by following hyperlinks to gain more raw data to prepare an independent report.

Source of First Resort

Open sources are increasingly referred to as the source of first resort. This means that analysts and information collectors should exploit open sources of information as the first step in the information-collection process. Particularly when intelligence gaps, whether tactical or strategic, are identified, open sources can provide important insights which may give functional direction to a line of inquiry.

If a unique crime trend emerges within a community, for example, an open source search of newspapers nationwide can identify other locations where crimes with similar modus operandi have occurred.[28] Similarly, unknown graffiti or a unique

[11] See www.newslink.org.

[12] See www.shortwave.be and www.blackcatsystems.com/radio/shortwave.html.

[13] See as an example www.searchsystems.net and www.factfind.com/database.htm.

[14] One of the most extensive directories is in www.yahoo.com. However, other sources of directories exist, such as www.mypeoplesearch.com.

[15] See as an example www.namebase.org, www.searchsystems.net and www.blackbookonline.info.

[16] See www.thecre.com/links/fedgov-links.html, www.firstgov.gov/Topics/Reference_Shelf.shtml and www.firstgov.gov/Citizen/Topics/PublicSafety.shtml.

[17] See www.fas.org.

[18] See www.lib.umich.edu/govdocs-stats-pilot and www.ojp.usdoj.gov/bjs.

[19] See as an example www.accoleads.com.

[20] As an example, Islamic radical web sites can be found at www.e-prism.org.

[21] Beyond the commonly used Internet search engines such as Google, Lycos, Yahoo, Ask, and others, a unique web search site is www.itools.com.

[22] www.state.gov/s/ct

[23] www.fbi.gov/terrorism/terrorism.htm

[24] www.start.umd.edu.

[25] dover.idf.il/IDF/English

[26] www.splcenter.org

[27] www.stormfront.org

tattoo may be searched via image files.[29] A blog search can provide unique insights about virtually any extremist group just as information may be obtained about a unique problem.[30] Similarly, insightful information about Hezbollah[31] can be found on YouTube and information about the MS-13 gangs[32] can be found on MySpace.

Similarly, because of the threat posed by jihadists, there is value in knowing the beliefs, language, arguments, and perspectives of jihadists to:

> …improve strategic understanding of the of the jihadist threat by more effectively mining the Internet and other open sources for information. Such an effort, it is suggested, also will enable … a better tactical understanding of how jihadists use the Internet's web-television capabilities, chat rooms, and "news" sites, to train forces and raise money. Ultimately, these observers suggest, the United States must develop the capability to understand and influence foreign populations — "not in their council of states but in their villages and slums" — if it is to effectively counter the threat posed by jihadists. In such circumstances, it is argued, the information that should matter most to policymakers can be derived from open sources.[33]

The value of open sources as the first resort is multifold. When an issue or threat emerges, open sources can often provide an efficient, effective, and fast insight into the issue that may often validate the need for further inquiry. Similarly, open sources can provide a broad view of a person or threat as a means of establishing context and perspective. Moreover, open sources can often provide insights and relationships that may be missed by the inherent nature of many closed sources.

> Allen Dulles estimated in 1947 that over eighty percent of the "information required for guidance of our national policy" was available in open sources. George Kennan revised the estimate to upwards of ninety-five percent in a 1997 *New York Times interview*.[34]

With this estimated amount of valuable information available through open sources, it is only reasonable to use these sources as a starting point in a line of inquiry. The application to law enforcement is just as valid as it is for national security. The below scenarios, all of which are based on actual cases, illustrate this point:

- A land developer reports that he has received a threat from an obscure radical environmental group saying that if he does not stop construction of condominiums at an environmentally sensitive location, "he will pay the price". A quick search of news stories identifies the presence of the environmental group in other locations, its past activities and attacks, and the methods of attack. This can be an important element for defining specific intelligence requirements and methods of prevention in the current case.
- A tip is provided to law enforcement that a radical Islamic cleric who preaches violence is going to be in its community to speak to a local group. An open source search provides information about the individual's past speeches, the content of the speeches and any public safety issues that emerged associated with the speech.

[28] For example, one such source is library.pressdisplay.com which can be accessed at no charge through www.opensource.gov.

[29] All major web search engines include an image search capability. In addition, there are specialized image search engines such as www.picsearch.com and www.thrall.org/proimage.html.

[30] For example, if protestors from the Westboro Baptist church are anticipated at a funeral for an American service veteran, information about tactics, can be found at www.godhatesamerica.com and their protest schedule can be found at www.godhatesfags.com.

[31] See youtube.com/watch?v=P28KJvu46DY .

[32] See profile.myspace.com/index.cfm?fuseaction=user.viewprofile&friendid=91546354.

[33] Ibid., Best and Cumming, 2007, p. 2.

[34] Office of the Director of National Intelligence. *National Open Source Enterprise.* Washington, D.C.: Office of the Director of National Intelligence, 2007, p. 3.

- The manager of a nursery reports that a man driving a rental van just purchased an unusually large quantity of fertilizer. While a criminal history check was negative, an open source search of a commercial integrated database identified the individual's address and persons known to use the same address. An Internet search engine identifies some of the man's associates on a right-wing extremist web site.
- A confidential informant states that members of a violent gang are slowly moving into the region. An intelligence analyst conducts an open source search to learn more about the gang, identify gang characteristics, and locates samples of the gang's graffiti and tattoos and distributes the information to patrol officers so they can record the presence of gang symbols in the community.
- A group of anarchists announce that they are going to demonstrate against the president of the World Bank who is speaking at the commencement exercise at a local university. A search of anarchist blogs finds a discussion of plans by the anarchists to cause major disruption during the protests by destroying targeted property and resisting arrest.

In each case, the initial tip or lead was followed by a quick open source search to gather more information. Not only did the open source information provide more insight about the threat, the information aided analysts in defining explicit intelligence requirements to help in fully articulating the threat picture.

As a source of first resort, open sources are not only fast; they also represent a minimal intrusion on civil liberties. Furthermore, open sources are less expensive than traditional law enforcement information-collection methods.

National Initiatives: The National Open Source Enterprise

The Office of the Director of National Intelligence (ODNI) was created by the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. Among the mandates for the ODNI was the development of a comprehensive National Intelligence Strategy; including development of an Information Sharing Environment (ISE) that maximizes intelligence and information sharing among the Intelligence Community, law enforcement, the private sector, and foreign partners. The ISE includes development of a consistent intelligence lexicon and standardized information-sharing and security standards. To maximize efficient, effective, and comprehensive information collection in support of the intelligence process, one strategy of the ODNI was to create the National Open Source Enterprise (NOSE).[35]

In the development of this enterprise, the ODNI notes:

> Given the challenges and threats the United States faces in the 21st century, it is essential our decision-makers, war-fighters, law enforcement, and homeland security authorities receive accurate, actionable and timely intelligence support. … Part of this new approach to intelligence is the collection of national intelligence via an integrated collection enterprise, fundamental to which is a robust, distributed, open source exploitation capability, known as the National Open Source Enterprise (NOSE).[36]

[35] See *Intelligence Community Directive, No. 301, National Open Source Enterprise* (July 11, 2006).

[36] Office of the Director of National Intelligence, p. 3.

The NOSE builds on observations from *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction* (2005) which observed:

> The need for exploiting open-source material is greater now than ever before…The ever-shifting nature of our intelligence needs compels the Intelligence Community to quickly and easily understand a wide range of foreign countries and cultures…information often detailed in open sources…"[37]

Based on *Intelligence Community Directive 301*, which created NOSE, the following are among the new responsibilities of Intelligence Community members:

- Conduct acquisition, analysis, and dissemination of open source materials.
- Make all open source information, products, and services available across the Intelligence Community (unless expressly prohibited by law).
- Coordinate all open source resources and activities through the Assistant Deputy Director of National Intelligence for Open Source.
- Designate a primary open source coordinator in each department or agency.
- Support staffing requirements of the Director of National Intelligence's (DNI) Open Source Center.
- Make full use of open source information, expertise, and capabilities to conduct analysis and inform collection strategies.
- Use a formal intelligence requirements mechanism for open sources.[38]

These responsibilities represent a major commitment to open source activities. A significant initiative in this regard was creation of the OSC,[39] formerly the Foreign Broadcast Information Service of which the CIA serves as the Executive Agent.

> OSC offers extensive coverage of open source intelligence information monitored worldwide on topics such as military affairs, politics, the environment, societal issues, economics, and science and technology. The information is obtained from radio, television, press, periodicals, books and other sources of unrestricted information such as databases and gray literature (open source information not available by subscription).

The web site has a massive amount of information, in both text and multimedia, and is accessible through a standard Internet connection. State, local, and tribal law enforcement (SLTLE) personnel can gain access to the web site by registering, which includes verification of employment (i.e., right to know) and that the requester has the need to know sensitive homeland security information. While there is a great deal of information at the OSC that will be of interest, although marginally relevant to many SLTLE agencies, the greatest value of the OSC to law enforcement is the free access to many commercial databases.

The direction of these and additional open source activities demonstrate the importance and value that are being committed to the development of a new open source capability. Moreover, in light of the implementation of the ISE, the goals of information sharing across the Intelligence Community and with SLTLE and the private sector,[41] the NOSE takes on even greater meaning.

[37] *The Commission on the Intelligence Capabilities of the United States Regarding Weapons of Mass Destruction,* 2005

[38] *Intelligence Community Directive 301. National Open Source Enterprise.* Section E(6), July 11, 2006.

[39] www.opensource.gov

[40] infoserve.sandia.gov/electronic/fbis.html

Open Source and Law Enforcement Intelligence (Tradecraft)

"Tradecraft" is a collective term used by the Intelligence Community to refer to the methods used in the Intelligence Process, particularly collection and analysis, on both broad and specific scales. While the term is rarely used in law enforcement, it is useful to understand its meaning in light of developments in the ISE.

Therefore, open source tradecraft has two meanings for law enforcement. At the macro level, it broadly refers to how open sources can be used in the Intelligence Process. At the micro level, it means the explicit procedures in conducting open source searches as well as capturing and interpreting raw open source information. The remaining discussions deal with open source tradecraft for law enforcement at both levels.

The fact that information is collected from an open source should not dissuade a law enforcement officer or analyst from using it. Indeed, there is often high-quality, insightful evidence available from open sources. So much so, that the 9/11 Commission's Final Report recommended that a new "Open Source Agency" be added to the U.S. intelligence structure.[42] This is essentially being implemented with NOSE. However, like virtually every other aspect of intelligence issues, the use of open sources in law enforcement intelligence has unique applications and parameters that vary somewhat from open source exploitation by Intelligence Community agencies. Fundamentally, the distinction lies in the fact that the SLTLE agency should be collecting and retaining only open source information identifying individuals and/or organizations where there is a criminal nexus. As will be described below, a great deal of open source applications for law enforcement intelligence should be incorporated as standard protocol in the intelligence process.

Criminals Also Use Open Source

A 15-year-old Sierra Vista High School student who was shot October 13, 2007 in front of his southwest Las Vegas home was a key witness in a 2006 Crips gang-related double slaying in Riverside County. Prosecutors in California think another teen shot Demontre Carroll in the back to silence him. The teen, who had relocated to Las Vegas from Southern California because of threats on his life, was located by the assailant using the victim's MySpace page.

Las Vegas Review Journal, November 7, 2007, p. 1A.

---

[41] See: Program Manager-Information Sharing Environment. *ISE Implementation Plan*. Washington, D.C.: Program Manager-Information Sharing Environment, 2006, at www.ise.gov.

[42] National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*. Washington, D.C.: U.S. Government Printing Office, 2004, p. 413. Also online at www.9-11commission.gov/report/911Report.pdf.

Law Enforcement Applications of Open Source

There are both tactical and strategic applications of open source for law enforcement intelligence, such as the following:

- *Identifying and verifying facts.* Perhaps one of the most common uses of open sources in law enforcement is to identify and verify a wide range of facts. Personal identity information, addresses and phone numbers, e-mail addresses, vehicles known to have been used, property records, are among a wide variety of other facts can easily be identified through open source public and commercial databases and directories.
- *Social networking.* Social networking sites such as MySpace, provide a wealth of information about individuals and persons with whom they interact. Social networking web sites contain identity information of the user and his or her friends, often with photographs, as well as private messages and statements about beliefs and behavior. Likes and dislikes are often enumerated, ranging from entertainment to politics to people, as well as contact information. While some information, such as a private message, is subject to legal process, a great deal of information is available as an open source.
- *Identifying criminal offenders.* In a surprising number of cases, people will make incriminating statements in open sources. It has occurred in media reports but most commonly in either social networking sites or on web sites devoted to a particular deviant or unlawful behavior. Sexual predators, drug traffickers, persons trafficking in stolen property, and criminal extremists are all examples that have been found in the "deep web." While incriminating statements alone will not meet the burden of proof for conviction, they clearly establish a criminal predicate and basis for further inquiry.
- *Understanding and interpreting ideologies*. An important element of analysis that aids in defining and forecasting threats is to understand the motivation or rationale of individuals involved in criminal behavior. Particularly in the case of ideological extremists, web sites can be a valuable source. Extremist web sites typically articulate their beliefs as well as what behaviors or changes their movement will cause. Moreover, drilling down and reading blogs can provide more information about individuals' beliefs and behaviors, including incriminating statements.
- *Identifying criminal methodologies.* Collecting information from media sources, web sites, and/or blogs can provide important insight into methods and targets of criminal acts. The modus operandi of violent serial offenders, criminal extremists, and criminal enterprises can be identified readily in many cases. This can be valuable information for developing preventive strategies; for example, a technique used by anarchists is the "black bloc" that includes property destruction and other activities that could be criminal. The tactics can be learned through various open sources.[43]
- *Identifying emerging crime issues and trends.* Just as criminal methodologies can be learned from open sources, so can new and emerging crime trends. In many cases, certain types of crime will disperse geographically in a consistent pattern. Drug trafficking and gang activity serve as good

[43] flag.blackened.net/revolt/rbr/rbr6/black.html

examples. Monitoring new and emerging crimes or changes in crimes on a broad geographic basis can often provide insight about crime problems that are on the horizon for a community. Methamphetamine hydrochloride, for example, first emerged in urban areas on both coasts of the United States. Its movement to rural areas and to the midwest was on a fairly definable path permitting forecasting. Much of the information was easily identifiable through media reports.

An Example of "Pushed" Open Source Information

In March 2008 there was a series of direct action demonstrations in San Francisco. Predominantly focused on the war in Iraq, other issues were also being expressed by demonstrators including opposition to the U.S. policy toward Israel, economic issues, and global warming. Some demonstrators stated on "direct action" web sites they would be involved in civil disobedience and arrests were anticipated.

To learn more about the protests and the plans, the author searched several direct action web sites related to the demonstration. One web site provided cell phone text messages on plans and events throughout the day. The author signed up for the text service and had information on the demonstration "pushed" to his cell phone, therefore not only monitoring the events, but arriving at locations where civil disobedience was planned prior to most demonstrators.

The texts were open sources in near real time and it illustrates that with technology, open source information can take diverse forms.

An important word of caution: Just as law enforcement seeks information that provides insights into criminal behavior, individuals who are involved in criminal behavior may also attempt to provide disinformation on their web sites in an attempt to mislead law enforcement authorities. This is of particular concern regarding ideological groups who may seek to either induce law enforcement into some form of unjustified action or to simply distract law enforcement away from the heart of a group's real activities. This reinforces the need to verify sources and content.

Open Sources and Civil Rights

Unlike Intelligence Community agencies and the private sector, SLTLE agencies must be vigilant in the management of open source information because of unique rules that apply to information retention in a criminal intelligence records system.

Raw information obtained from open sources tends to fall into two categories that have important significance for an SLTLE agency: 1. Information about individuals and organizations and 2. Aggregate nonidentifying information. As a general rule, when a law enforcement agency conducts an open source search for information, the agency should assumed that civil rights protections attach to any information that identifies individuals or organizations, no matter how innocuous that individual piece of information appears to be. Conversely, as a general rule, no civil rights attach to aggregate information or descriptions of issues, trends, ideologies, and so forth that does not identify an individual or organization.

Of particular importance is when the information involves expressive activity that is protected by the First Amendment. It is easy to find information posted on blogs and web sites that express extreme statements about a diverse array of behavior, such as support for international terrorism, advocacy of legalization of drugs, vehement opposition to policies of government officials, advocacy of pedophilia, racist beliefs, and so forth. The difficulty is to distinguish between extreme expressive beliefs and statements that have a criminal nexus.

The statements in Table 11-1 illustrate expressive beliefs (left column) and statements with a likely criminal nexus (right column). Assume that the statements are made by a person who has been identified by an SLTLE officer.

Table 11-1: Comparison of Expressive Statements and Statements with a Criminal Nexus

Expressive Statement	Statement with Criminal Nexus
• "All politicians are corrupt and ought to be shot."	• "The only way to stop this war is for us to kill the President."
• "Doctors who perform abortions are committing murder and must be stopped."	• "The only way to stop that doctor from performing abortions is for us to blow up his clinic."
• "Everyone should smoke marijuana."	• "I can get you some marijuana to smoke."
• "Violence is the only message they understand."	• "I urge you to kill our oppressors."

The differences are often subtle. The expressive statements, while extreme, are less explicit. Moreover, even in these illustrations, additional facts and circumstances would be needed to establish a criminal predicate.

It is good practice to assume that any information identifying individuals or organizations collected from open sources must be 28 CFR Part 23-compliant.[44] Thus, there must be evidence establishing a reasonable suspicion that there is a nexus between the person or organization identified in the open source and a crime; that is, the "criminal predicate test." The essential principle is not the source of the information, but *what information is being retained* by a law enforcement agency in its criminal intelligence records system. Illustrations of open source applications include the following:

- If information is being collected from open sources as part of the criminal investigation of a crime that has already occurred, the criminal predicate test for intelligence records typically does not apply. Information from a criminal investigation would be placed in the law enforcement agency's Records Management System, rather than the criminal intelligence records system.
- If a group plans a protest or demonstration in a jurisdiction, open source information may be used to determine how past protests or demonstrations have been conducted, tactics used in other protests and demonstrations, outcomes and behaviors of the protesters and demonstrators with no criminal predicate required.

[44] The reader is reminded that 28 CFR Part 23 applies only to information that is placed in a criminal intelligence records system.

- While there is some debate, the general rule is that an open source inquiry identifies people who have been arrested during a protest or demonstration; this information may be retained without a separate criminal predicate being established. If a person has been arrested, probable cause has been established, which is a higher standard than the "reasonable suspicion" required for the criminal predicate.
- If the law enforcement agency receives a Suspicious Activity Report that an identified person may commit a crime during the course of the protest or demonstration, that information may be retained in a temporary criminal intelligence file in order to collect further information to verify the veracity of the suspicious activity information. In these cases, the law enforcement agency's criminal intelligence records policy should be followed.

• Descriptive information about extremist ideological beliefs, behaviors of those supporting those beliefs, changes and trends in extremists beliefs or collective behavior, methods advocated for accomplishing the goals of the extremist ideology, and potential targets of the extremists' actions may all be collected, analyzed and retained by a law enforcement agency without a criminal predicate as long as specific individuals or organizations are not identified.

Creating intelligence dossiers on persons who are merely suspicious is both tempting and easy using open source data. Similarly, exploring a social networking site through its search utility to determine if something interesting is located about a person is similarly easy. Nevertheless, law enforcement personnel must follow 28 CFR Part 23-compliant procedures for collecting and retaining open source information in a criminal intelligence records system just as it would for any other form of criminal intelligence information. It warrants repeating: The issue is not whether the information is from an open source, but whether a law enforcement agency can properly keep the information. Decisions must focus on the reason for which information is being retained, not the source of the information.

An important point to remember is that laws vary by state and locality, whether it is intelligence records laws, open records legislation, a state freedom of information act, or state privacy act. There is sufficient variability among the states to warrant a careful review of state law as it relates to criminal intelligence records.

Working with Internet Service Providers and Web-Based Companies

Often, open source searches will lead to the need to use the legal process to gain further information about an inquiry. Of course, when a law enforcement agency seeks information about the specific behaviors of an individual who is a customer or client of a private company, significant privacy concerns arise.

While this process moves beyond open sources, it should be noted that Internet service providers and companies that operate social networking web sites typically have a published policy and guide to work specifically with law enforcement agencies. While it is important for the reader to be aware of this,

since legal process has to be used and information is being sought that is not openly available, it is not open source information when the process goes beyond information that is openly available on the Internet.

Attribution and Copyrighted Materials in the Intelligence Process and Reports

Much of the open source information acquired through the intelligence process is in the public domain, that is, information for which no copyright is claimed. In other cases, as with certain commercial databases, rights to the information have been obtained by contract in accordance with usual government procurement procedures. In many other cases, however, agencies acquire copyright information without the authorization of the copyright holder.[45]

Too often products from law enforcement agencies, ranging from intelligence products to training materials, contain information that is drawn from other sources; however, there is no attribution to the original source. Attribution is important for four basic reasons:

1. It gives corroboration and support for the line of logic, inference, or conclusion that is presented in the report.
2. It permits the consumer to go to the original source for further information on the subject as well as giving the consumer the opportunity to independently evaluate the original source.
3. Attribution will typically meet the standards of law for copyrighted materials.
4. Attribution is the ethical and correct method of operation by giving appropriate recognition to the thoughts, ideas, creativity and work of others.

The importance for attribution has been reinforced by the ODNI through Intelligence Community Directive (ICD) 206, *Sourcing Requirements for Disseminated Analytic Products.*[47] The Directive states:

> Source reference citations shall be included as endnotes in disseminated analytic products. These endnotes shall be provided for all significant, substantive reporting or other information upon which the product's analytic judgments, assessments, estimates, alternative hypotheses and views, or confidence levels depend.[47]

The importance of attributing information to the original source is based on the following notion:

> Thorough and consistent documentation enhances the credibility and transparency of intelligence analysis and enables consumers to better understand the quantity and quality of information underlying the analysis.[48]

Of course, not all attributed material is copyrighted work, particularly in the case of public records. Most public documents and information that have been originally collected by the law enforcement agency are not copyrighted. In these cases, attribution is important for validity purposes.

Beyond public records there is information that should be attributed, particularly if it is from a copyrighted source. For example, information in a strategic

[45] Weimer, Douglas R., *The Copyright Doctrine of Fair Use and the Internet: Case Law.* Washington, D.C.: Congressional Research Service, 2005, pp.1–2.

[46] www.fas.org/irp/dni/icd/index.html

[47] Office of the Director of National Intelligence. ICD 206. *Sourcing Requirements for Disseminated Analytic Requirements.* Paragraph D.2, October 17, 2007, p. 2.

[48] Ibid., Paragraph B., p. 1.

intelligence product is drawn from a book on terrorism, a video from a television network that is used to illustrate terrorist attack methods, or the original concept and ideas of a consultant that is used in an intelligence report. All should be considered as copyrighted materials and attributable to the original source.

A copyright is a form of protection provided by the laws of the United States[49] to the authors of original works, including not only written materials, both published and unpublished, but also video and audio materials. Under the protection of federal copyright law,[50] the owner of copyright has the exclusive right of use, distribution, limitation to distribution, and to authorize others to reproduce copies; use the copyrighted material; prepare derivative works based on the original; and rent, sell or transfer the copyright.

Law enforcement agencies are obliged to follow copyright law just as any other individual or organization. While it is important to understand and respect copyrighted works, the "fair use" exemption permits use of the materials without seeking permission of the copyright owner.[51]

> The fair use of a copyrighted work, including such use by reproduction in copies or phonorecords[52] or by any other means specified by that section, for purposes such as criticism, comment, news reporting, teaching (including multiple copies for classroom use), scholarship, or research, is not an infringement of copyright. In determining whether the use made of a work in any particular case is a fair use the factors to be considered shall include:
>
> 1. The purpose and character of the use, including whether such use is of a commercial nature or is for nonprofit educational purposes.
> 2. The nature of the copyrighted work.
> 3. The amount and substantiality of the portion used in relation to the copyrighted work as a whole.
> 4. The effect of the use upon the potential market for or value of the copyrighted work.
>
> The fact that a work is unpublished shall not itself bar a finding of fair use if such finding is made upon consideration of all the above factors.[53]

With specific reference to copyright law and open source intelligence, a Congressional Research Service report stated:

> In using such copyrighted information, intelligence agencies, like other users of public information, are governed by the doctrine of "fair use" (based on common law and codified in the Copyright Act of 1976 (17 USC 107)).[54]

Clearly, law enforcement agencies are also obliged to conform to copyright law. Beyond the legal requirements, it is simply good practice to offer attribution of information where applicable.

Copyright and attribution issues are complicated when law enforcement agencies use the services of a commercial vendor whose work product has copyright protection. Care must be taken to ensure that users of the information understand the copyright implications in the service contract.

[49] United States Code, Title 17.

[50] United States Code, Title 17, Section 106 with reference the Copyright Act of 1976.

[51] Ibid., Section 107.

[52] "Phonorecords" is language from the 1976 law and has been interpreted to include all forms of audio and video media that meet the other standards for copyright protection. Similarly, digital materials such as web pages are also included.

[53] www.copyright.gov/title17/92chap1.html#107

[54] Weimer (2005), Ibid.

In the process of collecting information and preparing intelligence reports, law enforcement personnel should always include copyrighted material in their searches, be certain to provide proper sourcing[55] of the information, and be aware of the proper procedures in the fair use exemption.[56]

Metrics for Open Source Use

A great deal of information has been discussed about the effectiveness of open source information; however, the only true measure of effectiveness is to ensure that it is designed and evaluated to specifically meet the needs of the intelligence environment in which it is being used. A challenge, however, is the absence of widely accepted measurements or metrics related to open source intelligence. Responsible managers must develop outcome measures for intelligence practices to ensure they are accomplishing their intended goals (i.e., effectiveness) and are doing so in a manner that does not waste resources (i.e., efficiency).

Simple open source metrics may include the following:

- A count of open sources attributed in intelligence reports
- The proportion of all analysis where open sources are used
- Proportion of time when open sources are the source of first resort for intelligence requirements
- Time requirements for locating needed information in the open source environment versus the closed source environment.

While somewhat superficial, these metrics represent more than is currently used. Moreover, inasmuch as open source information is used by all-source analysts in connection with information from closed sources, it is difficult to measure how much open source information contributes to a specific intelligence product.

> It is anticipated that open source information will increasingly be relied upon given its greater availability, the nature of issues that today's analysts must cover, and the heavier emphasis placed on it by senior intelligence leaders.[57]

The ultimate open source metric is the qualitative contribution open sources make to the analysis. While this is difficult to measure, long-term evaluative assessments should be developed in order to focus the type of open sources and the methodology of their inclusion in the intelligence process which is most productive.

Open Source Content for the Intelligence Process

While open sources include information beyond the web, it is apparent that information about virtually any topic can be found on the Internet. Indeed, the quantity of information can be overwhelming. Having some perspective about different kinds of open source content that have particular value for law enforcement intelligence can begin to make the navigation and collection process more manageable.

[55] *Intelligence Community Directive 206* provides a significant amount of detail of information that should be included in the attribution.

[56] The United States Copyright Office web site, www.copyright.gov is very comprehensive and should provide answers to most copyright questions, including the fair use doctrine.

[57] Ibid. Best and Cumming, 2007, p. 17.

Open Source Information Identifying People and Organizations from Subscription Services and the Media

Two open sources that frequently identify people and organizations that warrant special attention are subscription database services and media reports. These are often subject to question about the propriety of their use. Both may be used properly and can be of great value to law enforcement intelligence. Just as in the case of any open source, the nature of the sources must be understood and the regulations concerning retention in criminal intelligence records systems must be applied in the same manner as any other information.

Searching media sources[58] can also provide a significant amount of information about individuals, organizations, trends in crime, movements, and criminal extremist ideologies. News services have global networks of sophisticated communications and informants with trained staff to conduct research and investigate virtually all issues that would be of interest to a consuming public. As a general rule, responsible news organizations also have editorial policies to ensure that the information used in news stories is valid, reliable, and corroborated (i.e., "well-sourced"). Crime and criminal extremism are important news; hence, journalists often seek to learn as much as possible about these incidents. The depth of information frequently includes details that are useful in the intelligence process. The news media can openly identify individuals and organizations involved in criminal incidents and often link similar individuals and incidents in diverse geographic locales. A search of news stories can provide both important leads and important undiscovered detail about a line of inquiry. A word of caution, however: not all media sources adhere to the same high standards. The practices and reputation of the media source must be evaluated just as any other source.

A number of companies have developed systems that permit a search for information from public and commercial databases using proprietary data integration software. Examples of the types of data that may be obtained are listed in Table 11-2. Companies such as AutoTrack,[59] Accurint,[60] Lexis-Nexis,[61] and RiverGlass[62] permit the development of extraordinarily detailed information about people into a summary report. Even though a fee is charged for these services, they are still open source because anyone can purchase the data and neither a legal process nor surreptitious collection methods are used.

Since both subscription services and media sources can provide a significant amount of detail about individuals and organizations, it is important to repeat once again that the criminal predicate rule is still applicable for information placed in law enforcement intelligence records.

National Media Exploitation Center

On a related point, initiatives by the Intelligence Community related to media information are worthy of note. Because of the vast amount of information that is available and easily accessible from the global news media, the National Media Exploitation Center (NMEC) was established in late 2001 at the Central Intelligence Agency[63] (CIA). NMEC's role is to coordinate FBI, CIA, the Defense Intelligence

[58] Such as News Directory www.newsdirectory.com or World: News, Media and Communications www.geocities.com/albaruthenia/AW/news.html.

[59] www.autotrack.com

[60] www.accurint.com

[61] www.lexisnexis.com

[62] www.riverglassinc.com

[63] Don Cryer, Special Assistant to the Director of Central Intelligence for Diversity Management. (November 5, 2003). *Prepared Statement, Hearing before the Permanent Select Committee on Intelligence, 108th Congress.*

Agency, and National Security Agency efforts to analyze and disseminate information gleaned from millions of pages of paper documents, electronic media, videotapes, audiotapes, and electronic equipment.[64]

Table 11-2: Examples of Information Obtainable from Subscription Database Services

- Full names
- Date of birth
- Place of birth
- Parents, spouses, siblings, and children
- Known associates
- Known addresses associated with all the names
- Social security numbers
- Mortgage and lien information
- Credit report
- Credit cards and credit card usage
- Professional affiliations
- Occupations and employers
- Licenses of all types
- Vehicle, watercraft, and aircraft registrations

In this venue, exploitation refers to the collection of open source information relevant to defined requirements, integrating it with other known information and deriving new knowledge from this process; that is, developing open source intelligence. The NMEC has a great deal of expertise and resources. SLTLE agencies may take advantage of the NMEC through federal partners—typically the FBI or DHS—at the primary state fusion center.

The Social Networking Concept and Issues for Open Source

A social network is a linked, interactive structure of people consisting of "nodes" that may be either an individual or group. The basis of the linkage is a shared interest of virtually any definable character—music, occupation, personal philosophy, political affiliation, sexual orientation, hobbies, and so forth. Each node may have multiple connections based on the different variables. For example, one person (i.e., a node) may be a member of multiple social networks. A person who is an accountant may also be a motorcycle enthusiast, enjoy country music, and be an avid fantasy football player. Each variable could represent membership in different social networks. Similar social network models can be defined for people who support extremist ideologies, are gang members, or are involved in illegal activities, such as drug use or pedophilia.

While social networks have existed in some form since the dawn of humankind, the growth of the Internet has resulted in new social networks that are virtual, notably represented by web sites such as MySpace,[65] FaceBook,[66] Bebo,[67] Twitter,[68]

[64] Federal Bureau of Investigation. "The FBI's Counterterrorism Program Since September 2001." *A Report to the National Commission on Terrorists Attacks Upon the United States.* Washington, D.C.: Federal Bureau of Investigation, undated, p. 16.

[65] www.myspace.com

[66] www.facebook.com

[67] www.bebo.com

[68] www.twitter.com

and SocialGrid.[69] Other social networking web sites not as sophisticated or widely known also represent diverse interests. Ironically, social network members will frequently post information that is incriminating or, at the least, sufficiently strong to establish a criminal predicate as related to their behavior. While in some cases one may find gang members or supporters of the Earth Liberation Front on popular web sites such as MySpace, there are many more underground web sites that will have postings indicating criminal behaviors. That is why creative search strategies become important. Typically, intuitive search criteria will not produce the results being sought; rather, use of terms and phrases unique to the social structure are required. As a result, background research to understand a social network becomes an important starting point.

A different form of social networking is found in YouTube.[70] As most readers will know, individuals may post videos on this web site for public viewing. The videos range from humor to personal statements about all kinds of issues. Included are videos related to Hamas,[71] Hezbollah,[72] MS-13[73] and others. In some cases, the videos are critical while in other cases, they are supportive of the cause. Reviewing the videos can provide unique insights and images, including signs and symbols of the group being examined.

To be most successful in searching a social network, the user must create an identity and become a member of the network. For purposes of intelligence inquiries, a false identity and e-mail address should be created by the law enforcement user.[74] Important, there are certain ethical and legal limits that should be fully explored before going forward. Of particular concern is the need to be certain that statements and actions by a law enforcement employee do not induce a person to commit an act that the person would not have otherwise done without the inducement. That is entrapment. A law enforcement agency should develop a policy and procedures to guide the use of creating a false identity and using that identity for intelligence inquiries including social networking.[75] Despite the caveat, the value of using the search engine of each social networking web site should not be underestimated.

Newsletters and Blogs

Monitoring a variety of variables related to a threat is an important part of strategic intelligence. Essentially, these are standing intelligence requirements. Open source materials that are particularly useful for this purpose are newsletters and blogs. While newsletters exist in both printed and electronic form, the latter is increasingly prevalent because they are more timely and frequently provide hyperlinks leading the reader to sources that will provide greater detail about the subject.

Newsletters are designed to highlight issues, trends, and developments within a specific topic area. Blogs are web-based opinion discussions also typically focused on a specific topic area where writers and readers express opinions, perspectives, and beliefs. In many cases, a single source will have both a newsletter and a blog; for example, a particularly useful newsletter and blog for intelligence issues is *Secrecy News*[76] from the Federation of American Scientists.[77]

[69] www.socialgrid.com

[70] www.youtube.com

[71] www.youtube.com/watch?v=TrieBhaGgHM

[72] www.youtube.com/watch?v=P28KJvu46DY

[73] www.youtube.com/watch?v=MDUIxJJbP00

[74] The processes and "lessons learned in the creation of a false identity for law enforcement inquiries will not be discussed because this is a publicly available document.

[75] As a technical point, searching a social networking site is an open source. Establishing a false identity on the site to lure an individual into making incriminating statements is surreptitious and, therefore, not an open source.

[76] See www.fas.org/sgp/news/secrecy and www.fas.org/blog/secrecy, respectively.

[77] The Federation of American Scientists web site contains a great deal of interesting and useful information related to intelligence issues, including downloadable documents, many of which are often difficult to gain access to. See www.fas.org.

Generally speaking, there are four broad categories of newsletters and blogs:

1. *Professional/academic and government.* These sources tend to be among the most objective, although never rule out the ideological influence, even if unintentional, of an author or editor. Despite this caveat, these sources are most likely to make statements based on corroborated information and use an approach to analysis and conclusion based on logic and the scientific method rather than emotional arguments. Typically, these sources report facts and data more objectively and most commonly include attribution of facts and data.
2. *Commercial sources.* As the name implies, these are profit-driven sources often intended to provide information that supports the sale of products or services. Despite the fact that the motive of the source is to make a profit, the sources can nonetheless be very reliable. Indeed, the reliability of these sources is often an important selling point for the business. While the information is typically accurate, information about alternatives is not likely to be included.
3. *Advocacy groups.* These sources are agenda-driven based on the ideology and goals of the source. A newsletter from a right-wing extremist source will reflect information that supports that ideology. Similarly, discussions in a blog on environmental extremism will support the goals of that group. The reader should recognize where they are coming from and factor that into one's analysis. Using this approach, these sources can be quite insightful for understanding an ideology or advocacy position.
4. *Pundits.* A wide range of individuals blog on the web as critics and commentators on virtually every subject. Pundits work for a wide variety of organizations—news, entertainment media, professional organizations, etc.—and some are independent commentators working only for themselves, oftentimes not as a source of income, but as a means to discuss an interest or belief. What is important to recognize is that pundits typically do not seek to be objective, but to comment on a topic of interest from their particular ideology or perspective. This is also true for pundits who blog for news organizations. Often their arguments and observations are persuasive and useful, but typically they are not objective. Pundits tend to be news and policy wonks; hence, their research will often identify issues and sources of information that might otherwise be easily missed. As such, they are often good sources of raw information that can be corroborated through objective sources.

Subscribing to newsletters and monitoring blogs on a consistent basis can provide a wealth of information about trends, issues, and anomalies. When a new issue of concern begins to emerge on a consistent basis, and particularly if it is reflected in multiple sources, the issue should be proactively explored through other information sources to determine its reliability and validity and to assess the probable impact on one's area of responsibility.

The number of blogs and newsletters on the web is unknown; moreover, they are dynamic in both their presence and content; as a result, there is value in relying on web sites that aggregate blogs, newsletters, and news. These sites typically organize their content into broad categories and have search engines that limit queries to the site's contents. Both factors aid in narrowing the breadth of a search. Two such sites that are comprehensive in their aggregation are

BlogRunner[78] and TalkDigger.[79] Each uses a slightly different approach, thereby providing a more comprehensive search methodology.

Wikis

A wiki is software that allows users to easily create, edit, and link pages. Wikis are often used to create collaborative web sites and to power community web sites, often also referred to as wikis. These collaborations are increasingly being used by businesses to provide affordable and effective Intranets and for knowledge management.[80] More specifically, the collective business knowledge of all members of an organization can be documented, refined, and shared in a dynamic virtual environment.

Wikis generally are designed with the philosophy of making it easy to correct mistakes, rather than making it difficult to make them. Thus, while wikis are open, they provide a means to verify the validity of recent additions to the body of pages. The most prominent, on almost every wiki, is the "Recent Changes" page—a specific list numbering recent edits, or a list of all the edits made within a given time frame.

Critics of publicly-editable wiki systems argue that these systems could be easily tampered with, while proponents argue that the community of users can catch malicious content and correct it. The safe lesson on a public wiki is to use it as a pointer system and corroborate the content of interest.

Perhaps the best known wiki is the online encyclopedia *Wikipedia*;[81] however, there are many types of wikis, some with a very specific focus.[82] For example, the ODNI OSC provides access to a wiki that is specifically focused on intelligence called *Intellipedia*.[83] While primarily focused on the Intelligence Community, it contains information that is also useful to SLTLE. Wikis can be a valuable source when dealing with a topic or issue about which the information collector has limited information. Most wikis include external references to materials which helps in the corroboration process.

From an intelligence perspective, the wiki can provide subject matter knowledge on an issue as well as direction to more information.[84]

RSS Feeds

RSS (Really Simple Syndication) is a family of web feed formats used to publish frequently updated content including, but not limited to, blog entries, news headlines, and podcasts. An RSS document (which is called a feed, web feed, or channel) contains either a summary of content from an associated web site or the full text. RSS makes it possible for people to keep up with web sites in an automated manner that can be sent to the subscriber.[85]

From an open source perspective, the value of RSS feeds, when available on a web site, is that any new information or changes in content are sent to those registered for the service without the need to check each site. It increases both the efficiency and timeliness of information for the user.[86]

[78] www.blogrunner.com

[79] www.talkdigger.com

[80] en.wikipedia.org/wiki/Wiki

[81] en.wikipedia.org/wiki/Main_Page

[82] A wide variety of wikis can be searched through www.wiki.com.

[83] www.opensource.gov/providers/intelinku/wiki/Main_Page (access only)

[84] For example, see the crime wiki at unclesam.pbwiki.com/Crime.

[85] en.wikipedia.org/wiki/RSS_(file_format)

[86] As an example, see the terrorism news and analysis RSS feeds at www.2rss.com/rss_5352.html.

Gray Literature

Gray literature is open source information that typically is not published but made openly available, usually to a specific audience. While it is open, the information is often not easily identified or retrieved. The American Library Association observes:

> The greatest challenges involved with [gray literature is] the process of identification, since there is limited indexing, and acquisition, since availability is usually marred with uncertainty. Added to this is the absence of editorial control, raising questions about authenticity and reliability.[87]

Traditionally, gray literature was defined as any documentary material that is not commercially published and is typically composed of technical reports, working papers, business documents, and conference proceedings. More of these types of documents are becoming available online, but often are not discovered by traditional search engines.

This author views the concept of gray literature more broadly, particularly as applied to the law enforcement intelligence process. The basic idea of gray literature has three components: 1. Documents of interest that exist; 2. The information is open; and 3. The information is not widely distributed and therefore difficult to locate. The concept of gray literature, therefore, should not be limited to academic or scientific works, but applied to any documents characterized by these three elements.

Brochures printed by a right-wing extremist are handed out a local gun show or fliers printed by anarchists and distributed at a demonstration could also be considered gray. In both cases, the documents are not commercially published but are intended to be disseminated openly and as broadly as possible (the limitation often being a budgetary one). The limited supply of these unpublished materials makes them difficult to identify or locate. Collecting gray literature is a challenge and must be explored in light of the types of potential literature that exist and where they might be located, most likely by a human collector rather than by networking.

The Deep Web

The web is a complex entity that contains widely diverse information in a variety of formats. Most people tend to view the web in the context of web sites with a combination of fixed and dynamic content. The fixed content tends to have minimal change and is the most common content found in standard searches. The dynamic content on many web sites is far larger than the fixed documents and is more likely to be missed in standard searching, with the exception of file names and file extensions.

[87] www.ala.org/ala/mgrps/divs/acrl/publications/crlnews/2004/mar/graglit.cfm

The deep web or invisible web refers to the following:

> …the vast repository of information that search engines and directories don't have direct access to, like databases. Unlike pages on the visible Web (that is, the Web that you can access from search engines and directories), information in databases is generally inaccessible to the software spiders and crawlers that create search engine indexes.[88]

Common estimates suggest that the deep web contains 500 times the content that is found in the visible web. Five broad types of content[89] constitute the invisible web:

1. *The content of web-based databases.* Information stored in databases is accessible only by query to the database and are not picked up by the web crawlers used by search engines. This is distinct from static, fixed web pages, which contain documents that can be accessed directly. A significant amount of valuable information on the web can be generated from databases.
2. *Nontextual files.* These include multimedia files, graphics files, software, and documents in formats such as Portable Document Format (PDF). Web crawling has a limitation in searching the content of these types of files. Web crawlers can identify file names and extensions (e.g., .jpg, .wmv, .pdf, etc.) of such files, but cannot identify the content of these files during the web crawling process. Essentially, they are files that are not in HTML[90] format, therefore, a great deal of information and data are not picked up from these files by traditional searches.
3. *Script-based web pages.* These are web pages that are written in script coding, other than HTML and/or those with URLs[91] that contain a "?".
4. *Content available on sites protected by passwords or other restrictions.* The content of web sites protected by some degree of access through rigorous password protection or a Virtual Private Network (VPN) will not be identified by search engines. There is a continuum of identifiable and nonidentifiable information from these types of web sites depending on what types of information the site owners elect to be publicly accessible (often for marketing purposes) as well as the degree of security applied to the site (in some instances the web site's security is limited and some data can be identified). Suffice it to note, a significant amount of information from these sites is not identifiable through traditional search engines.
5. *Pages deliberately excluded by their owners.* A web page creator who does not want his or her page captured in search engines can insert special meta tags that will cause most search engines' crawlers to avoid the page.

Obviously, a great deal of open source information from the deep web could be valuable to the intelligence process if it could be identified and retrieved. The deep web is searchable, but not using standard search techniques. The goal is to find tools that can locate valuable open source deep web information.[92] The most effective ways to search the deep web is to use search utilities that are designed to explore specific databases. While this still reaches only a portion of the deep web, the information gained from these databases can be extremely valuable, although not necessarily convenient. Deep web searching of databases typically requires accessing a variety of web sites to search for the desired information.

Language Distribution on the Internet

According to one web-based study, languages were distributed among web pages in these percentages:

English	56.4%
German	7.7%
French	5.6%
Japanese	4.9%
Spanish	3.4%
Chinese	2.4%
Italian	2.0%
Other	17.6%

If an information collector is searching only in English, then the search has immediately eliminated 43.6 percent of the visible web.

Source: www.netz-tipp.de/languages.html

[88] websearch.about.com/od/invisibleweb/a/invisible_web.htm

[89] See www.internettutorials.net/deepweb.asp.

[90] HTML is Hypertext Markup Language.

[91] A URL is Uniform Resource Locater, which is the web address.

[92] For a guide to assist your search strategy, see: www.lib.berkeley.edu/TeachingLib/Guides/Internet/Strategies.html.

Both as a resource and as a means to illustrate the breadth of databases in the deep web, the following is a list of deep web/database search utilities. It is not a comprehensive list; rather, the sites are among those most likely to have some form of utility for law enforcement intelligence.

1. Clusty[93]—A metasearch engine that combines the results of several top search engines.
2. Intute[94]—A searchable database of trusted web sites reviewed and monitored by subject specialists.
3. Infomine[95]—A virtual library of Internet resources relevant to university students and faculty. Built by librarians from the University of California, California State University, the University of Detroit–Mercy, and Wake Forest University.
4. Librarians Internet Index[96]—A search engine listing sites deemed trustworthy by human librarians, not just an Internet bot.
5. Internet Archive[97]—A database of tens of thousands of movies, live music, audio, texts, and home of the Wayback Machine that allows you to find old versions of web pages, more than 55 billion.
6. Direct Search[98]—A list of hundreds of specialty databases and search engines. No longer maintained, but still perhaps the most complete list of the deep web.
7. Scitopia.org [99]—A federated search engine that consists of a real time search through a disparate group of databases. The user enters a set of query parameters, which are broadcast to the selected databases; the results are collated and presented back to the user in a unified format.
8. Science.gov [100]—A search engine for government science information and research results. Launched in February 2002, it is in its fourth generation, providing a search of more than 50 million pages of science information with just one query, and is a gateway to more than 1,800 scientific web sites.
9. Pipl[101]—As an alternative method to search for people, Pipl searches databases for names of individuals rather than names that are simply incorporated on web pages.
10. StumbleUpon[102]—Using the technique of web harvesting, this deep web search engine relies on a combination of human opinions and machine learning to immediately deliver relevant content.
11. GPO's Catalog of U.S. Government Publications[103]—A searchable database of federal publications, with links to those available online.
12. Smithsonian Institution Libraries[104] —A collection of 20 libraries from the world's largest museum complex.
13. The National Archives[105]—A list of all National Archives research tools and databases.
14. HighWire Press[106] —A searchable catalog of the largest repository of free full-text, peer-reviewed content, from more than 900 journals.
15. Education Resources Information Center (ERIC) [107]—A catalog of more than 1.2 million bibliographic records, providing links to the full text where available. Sponsored by the U.S. Department of Education and the Institute of Education Sciences.
16. Encyclopedia Britannica[108]—The authoritative encyclopedia searchable with full text online.

[93] www.clusty.com

[94] www.intute.ac.uk

[95] infomine.ucr.edu

[96] www.lii.org

[97] www.archive.org/index.php

[98] www.freepint.com/gary/direct.htm

[99] www.scitopia.org

[100] www.science.gov

[101] www.pipl.com

[102] www.stumbleupon.com

[103] catalog.gpo.gov

[104] www.sil.si.edu

[105] www.archives.gov/research/tools/index.html

[106] highwire.stanford.edu

[107] www.eric.ed.gov/ERICWebPortal/Home.portal

[108] www.britannica.com

17. Topix.net [109]—A news search engine.
18. Internet Public Library[110]—The Internet's public library, which is fully searchable.
19. The Online Books Page[111]—A searchable database of more than 25,000 English works with full text available free online.
20. ebrary[112]—A searchable database of more than 20,000 full-text books.
21. Hoover's[113]—A searchable database of businesses.
22. ThomasNet[114]—An industrial product search directory.
23. GuideStar.org[115]—A searchable database of nonprofit organizations.
24. American FactFinder[116]—A repository of aggregate census bureau data searchable by city, county, or ZIP Code.
25. FedStats[117]—A gateway to statistics from more than 100 U.S. federal agencies.
26. United States Government Printing Office (GPO)[118]—A search engine for multiple government databases, including U.S. budgets, campaign reform hearings, code of federal regulations, congressional bills, unified agendas, and more.
27. CIA Electronic Reading Room[119]—A searchable database of declassified CIA documents.
28. International Data Base (IDB)[120]—A computerized data bank of statistical tables and demographic information for 228 countries and areas.
29. FIRST[121]—A database of military aggression and weapons holdings.
30. CIA Factbook[122]—A reference material published by the CIA, containing information on every country in the world.
31. THOMAS (Library of Congress)[123]—A searchable database of legislative information from the Library of Congress.
32. Law Library of Congress[124]—The largest collection of legal materials in the world, containing more than 2 million volumes.
33. Global Legal Information Network[125]—A searchable public database of laws, regulations, judicial decisions, and other legal sources.
34. FindLaw[126]—A free legal database with searchable collections of cases and codes, legal news, and an online career center.
35. Bureau of Justice Statistics[127]—A directory of legal and judicial statistics, ranging from crime to law enforcement, to courts and sentencing.
36. Library of Congress[128]—A searchable catalog of the world's largest library, containing more than 130 million items.
37. Library of Congress Digital Collections[129]—A searchable database of Library of Congress items that have been digitized and fully available online.
38. Library of Congress Prints and Photographs Reading Room[130]—A searchable catalog of Library of Congress prints and photographs including thumbnail reproductions of the items.
39. National Institutes of Health[131]—A searchable encyclopedia of health topics.
40. FAA Flight Delay Information[132]—A map of the United States with flight delay information from the nation's largest airports.
41. National Highway Traffic Safety Administration[133]—A database of car and car part defects, searchable by item number or car make and model.

[109] www.topix.net

[110] www.ipl.org

[111] digital.library.upenn.edu/books/search.html

[112] shop.ebrary.com

[113] www.hoovers.com

[114] www.thomasnet.com/index.html

[115] www.guidestar.org

[116] factfinder.census.gov/home/saff/main.html?_lang=en

[117] www.fedstats.gov

[118] www.gpoaccess.gov/multidb.html

[119] www.foia.cia.gov

[120] www.census.gov/ipc/www/idb/index.php

[121] first.sipri.org/index.php

[122] www.cia.gov/cia/publications/factbook/index.html

[123] thomas.loc.gov

[124] www.loc.gov/law/index.php

[125] www.glin.gov

[126] www.findlaw.com

[127] www.ojp.gov/bjs

[128] www.loc.gov/search/new

[129] www.loc.gov/library/libarch-digital.html

[130] www.loc.gov/rr/print/catalog.html

[131] health.nih.gov

[132] www.fly.faa.gov

[133] www-odi.nhtsa.dot.gov/cars/problems/tsb/tsbsearch.cfm

Beyond these diverse resources, a number of fee-based deep web search utilities are available. The advantage to these search utilities is that they identify and seek information from multiple databases without the need to make separate inquiries, and proactively search for data in non-HTML formats (beyond databases). The following are among the most comprehensive::

1. Xrefer[134] —A searchable database of 236 titles and more than 2.8 million entries.

2. LexisNexis[135]—The world's largest collection of public records, unpublished opinions, forms, legal, news, and business information. More than 35,000 sources are searchable with full-text available online.

3. Forrester Research[136]—An independent technology and market research company publishing in-depth research reports on a variety of subjects.

4. Factiva[137] —A searchable collection of more than 10,000 individual sources.

5. Copernic[138]—Provides indexing, searching, and tracking of databases and deep web resources by using software that seeks and identifies web resources beyond those in HTML.

6. BrightPlanet[139]—Searches, harvests, consolidates, indexes, merges, analyzes, and categorizes documents and associated metadata in any format and language, from visible and deep sources on the web and from inside and outside the firewall.

   Both the BrightPlanet and Copernic utilities are particularly comprehensive deep web search tools that go beyond databases that are useful for law enforcement intelligence.

What should be apparent is that much of the deep web is not hidden in a surreptitious manner. Rather, it is hidden because it contains information in formats or architectures that are not readily identifiable by standard search engine technologies. As a result, it takes specially designed search utilities and greater effort by the user to identify and capture deep web information.

The Underground Web

The underground web is a cultural dynamic that has evolved on the Internet, just as it has in the physical society. An article in *Business Week* described it this way:

> Warning: You are about to enter the dark side of the Internet. It's a place where crime is rampant and every twisted urge can be satisfied. Thousands of virtual streets are lined with casinos, porn shops, and drug dealers. Scam artists and terrorists skulk behind seemingly lawful Web sites. And cops wander through once in a while, mostly looking lost.[140]

Many visible web sites reflect the underground culture where transactions constantly traverse the line between lawful and unlawful behavior. While they are virtually impossible to police, these visible sites—whether trafficking in illegal commodities or purveying any other kind of illegal activity—are often relatively

[134] www.xrefer.com

[135] www.lexisnexis.com

[136] www.forrester.com

[137] www.factiva.com

[138] www.copernic.com

[139] www.brightplanet.com and www.completeplanet.com

[140] www.businessweek.com/magazine/content/02_35/b3797001.htm

easy to find through diligent standard search techniques. Often operated offshore, the sites' owners do not want to be overly visible drawing attention to their activities, but they need to be found with relative ease to make a profit for their operations.

Other types of underground deep web sites exist with the intent to keep their activities as secret as possible from the visible web world. Nonetheless, they must be accessible for their clientele, with URLs often passed between individual referrals by those who are participants in the underground activities. Identity thieves selling stolen credit card information, pedophiles exchanging photographs, traffickers unlawfully selling controlled substances, and criminal extremists planning an event are examples of open source information that exist in the underground deep web.

While this kind of information is of great interest to law enforcement intelligence, it is difficult and time-consuming to locate. Painstaking searches of the deep web and labor-intensive reading of deep web content and blogs can produce evidence and leads for a criminal inquiry. Nonetheless, this process will be faster and more effective in identifying criminal threats than traditional methods of inquiry.

There is some optimism that this process could become easier. In mid-2006 the Symantec Corporation beta-tested new software called Dark Vision that mines underground web sites and chat rooms for sensitive information that is being sold.[141] The original plan was to target carder web sites—deep underground web sites where identity thieves sell stolen credit card information. While Symantec is uncertain when or if the software will be rolled out, it nonetheless represents a breakthrough that could be applied to other criminal activity.

A vast amount of open source incriminating information is available in the deep underground web. The challenge is to develop the searching expertise and investing the time to find this critical information.

A Broadened Perspective of Open Source for Law Enforcement

The value of many web resources, such as directories, extremist web sites, and social networking sites, for law enforcement intelligence is evident; however, there is a wide array of data that have value for the intelligence process that are less intuitively evident, for example:

- Information about a possible threat that includes the name of an unknown geographic feature.
- Information about the demographic characteristics in a geographic area that is needed in a strategic intelligence assessment.
- Information from a foreign source about money, distance, weight, temperatures or the size of clothing (among other things) that needs to be converted to U.S. standards.
- Real time information to track either a commercial flight or private aircraft.
- Legal description of the GPS coordinates and/or image of a house in question.
- A satellite image of a given location.
- The need to convert a digital video so it can be viewed on a law enforcement computer.
- The need to identify relatives of an intelligence target.

[141] www.infoworld.com/article/07/07/31/Symantec-Dark-Vision-mines-sites_1.html

These requirements, and much more, can be found in an eclectic array of web-based open sources. (See Chapter Annex 11-1 for the descriptions and locations of these web sites.)

The point of note is simple: One of the important values of online open sources is easy access to information that is unique yet critical to a comprehensive analysis.

Homeland Security Intelligence and Open Sources

Beyond enforcing the criminal law, America's law enforcement agencies have a wide range of well-established responsibilities related to public safety and order maintenance. Whenever there is a natural disaster, such as a flood, tornado, or hurricane, law enforcement has the responsibility to aid in the rescue and recovery of victims, protect unharmed citizens from injury and protect property. Similarly, in a catastrophe, such as the crash of an airliner or the collapse of a building or a public health emergency, law enforcement agencies have historically had significant responsibilities for public safety and order maintenance.

With the creation of new national initiatives related to homeland security after 9/11, many of these public safety responsibilities have become more structured. Particularly with the growth of intelligence fusion centers that have an operating philosophy of all crimes, all hazards and all threats, a new form of noncriminal intelligence has emerged: homeland security intelligence.

It should be reinforced that intelligence is based on prevention and is inherently a pre-incident function; whether that incident is criminal or all hazards/noncriminal. To reiterate, homeland security intelligence may be defined as "the analytic output of raw information that describes noncriminal threats to critical infrastructure, public health or community safety." Law enforcement needs to obtain a wide range of information to effectively prepare for homeland security threats identified through analysis. Open sources can be particularly valuable to aid in the intelligence process and to understand the characteristics and threats posed by pandemic flu, hazardous materials, or other direct or incidental threats posed by a homeland security emergency.

A wide range of information related to hazardous materials may be found at Environmental Chemistry;[142] information on threats to public health can be obtained from the Centers for Disease Control;[143] and a wide range of diverse useful information is available from a collection of online searchable databases provided by the National Center for Biotechnology Information of the National Institutes of Health.[144]

The broad range of homeland security threats is too exhaustive for a comprehensive discussion. The point to note is essentially this: Since the responsibility for homeland security intelligence has become a part of the law enforcement intelligence process, particularly at the state fusion center level, analysts and information collectors should aggressively use open sources as the first step in collecting this critical information.

[142] www.environmentalchemistry.com

[143] www.cdc.gov

[144] www.ncbi.nlm.nih.gov/sites/gquery

Open Source Processes and Protocols

A number of tools and techniques may be relied on to make the open source collection process more productive as well as to enhance the quality of information. The following discussion is a primer for insights into the process.

Using an Open Source Collection Plan

As anyone knows who has browsed the Internet, the ability to search diverse information and travel down an unanticipated path of hyperlinks can easily draw one away from their original line of inquiry into an area of often interesting but frequently irrelevant information. From an intelligence perspective, this is unproductive and risks the collection of unneeded and sometimes distracting information. The user is urged to develop an open source collection plan when using networking to seek open source information.

A collection plan is essentially a research methodology that seeks to focus the open source information collection process. Rather than relying on a dragnet approach, the collection plan focuses on source searching that is defined by specifically identified agenda items, such as the following:

- Intelligence requirements
- Research an identified emerging threat issue
- Identifying information in support of tips and leads that have been received
- Research information about a known local threat to determine its presence and effects in other geographical areas
- Research diverse and creative tactics for managing threats
- Gain a body of information about a specific intelligence target
- Gain knowledge about the current and changing nature of threat conditions in your region.

The plan should include the following:

- Specific types of information needed (i.e., names, locations, characteristics, or indicators of the threat or criminal behavior, signs and symbols of the threat, effects of the threat).
- Identification of the sources where the specified information is most likely to reside.
- Critical information associated with a given threat (e.g., methods, geography, modus operandi, and so forth).
- Logistical information associated with threats.
- Materiel used in the commission of a crime or terrorist act and how that materiel is used.
- Unique characteristics related to the intelligence target (i.e., important dates, times, symbolism, and so forth).

The significant point to note is that open source information collection through networking can be of the greatest utility when it has a specifically directed agenda.[145]

[145] See Chapter Annex 11-1 for a series of questions and methodology to help form a precise search plan.

Techniques and Tools

Perhaps the most important foundation skill to develop for any type of networking environment is to become adept at searching. The most common approach is to open one's search engine of choice and use the default search utility for the information that is needed. Some successes are achieved with this method, but the results often can provide a large quantity of related information that often lacks the specificity needed. Narrowing the search can be more productive in seeking the information that is needed. The first step is to develop a pre-search plan to focus on search requirements (See Chapter Annex 11-2). Beyond this plan, here are some tips for narrowing the search:

- Understand the culture of the intelligence target to both identify and accurately interpret relevant information. With a clear understanding of the culture of the target or the information that is being sought, a wider array of search terms and phrases can be developed. Moreover, narrowing the terms may assist in defining the sources or search engine to use.
- Based on the cultural assessment, carefully define the types of information that is being sought. To do this, rely on the concept of being collectively exhaustive; that is, make an attempt to search all derivative terms that describe the data or phenomenon being sought in the search.
- Once the information is defined, dissect it to develop alternative terms, synonyms, jargon, symbols, abbreviations, and alternative spellings.
- Examine different formats of the information being sought. For example, if searching for the name John Alexander Doe, the search should take several forms, such as:
  - John Doe
  - J Alexander Doe
  - J. Doe
  - J. Doe
  - Johnny Doe
  - Alexander Doe
  - J.A. Doe
  - J. "Alex" Doe

This is particularly important for deep web searches.

- Specialty search engines[146] can help focus a search by limiting searches to explicitly defined areas. Using a search engine that focuses only on news web sites[147] can pick up useful information from trends in terrorism or crime to the names of individuals or organizations that may be associated with threats. Moreover, news web sites often make an assessment of the quality of information easier than many other sites.
- Language translation from multiple languages to English is increasingly available at no charge online. These sites typically will permit the entry of text for translation or entry of a web site address to translate the information contained in the URL.

National Virtual Translation Center

Building on this last point, when foreign language translations are necessary, the National Virtual Translation Center[148] (NVTC) may be an additional resource to explore. Established by Congress in 2003, the NVTC role is to provide timely and accurate translations of diverse raw information for all elements of the Intelligence Community. A virtual workplace, NVTC personnel and linguists are located throughout the United States and connect through various networks with the NVTC program office in Washington, D.C. As a member of the Intelligence Community, the NVTC is part of the ISE and, therefore, may become a resource

[146] A wide variety of general and specialty Internet search engines can be found at www.searchengineguide.com/searchengines.html.

[147] An example is NewsDirectory at www.newsdirectory.com.

[148] www.nvtc.gov

for SLTLE, and particularly fusion centers, on inquiries that may coincide with Intelligence Community concerns. SLTLE agencies should work with their FBI or DHS fusion center partners to secure assistance with the fee-based NVTC.

The Need to Determine Accuracy, Reliability, and Validity

As is the case with any information collected for the Intelligence Process, it is essential to evaluate the accuracy of facts, the reliability of the source of information and validity of the information's content. These concepts are the same as for any type of information in the Intelligence Process:

- *Accuracy:* The information is true and may be corroborated.
- *Source Reliability:* The source of the information is dependable for providing accurate information.
- *Information Validity:* The information actually depicts or portrays what it purports.

A good method for measuring these standards in open sources is to seek multisource reporting of information for validity. It is important to ensure that multisource reporting is not merely repetitive reporting; for example, *USAToday*, CNN, Fox News, and MSNBC may report the same news story. If all of these news outlets are simply reporting the same facts derived solely from an Associated Press story, then this is not multisource validity. This is referred to as the echo chamber, which is described as follows:

> …a group of media outlets that tend to parrot each other's uncritical reports on the views of a single source, or that otherwise relies on unquestioning repetition of official sources.[149]

In the example above, if each network reports the Associated Press story and independently confirms it relying on its own reporters, then this is multisource validation. A useful tool for assessing validity and reliability can also be found online through web sites such as Truth or Fiction,[150] About.com: Urban Legends,[151] or Snopes.[152] These web sites contain surprisingly comprehensive and well-sourced information about rumors, legends, and information that has been quoted as fact. The web sites typically describe the veracity of the story, with some form of explanation.

Web content is bursting with hyperbole, innuendo, and false information. One must be diligent to ensure that collected information is accurate, reliable, and valid.[153]

[149] www.sourcewatch.org/index.php?title=Echo_chamber

[150] www.truthorfiction.com

[151] urbanlegends.about.com

[152] www.snopes.com

[153] For a comprehensive discussion of reliability, particularly as related to the web and open source information, see sourcesandmethods.blogspot.com/2008/10/how-to-determining-source-reliability.html.

Avoiding Traffic Analysis: Becoming Anonymous on the Web

Online intelligence and investigation procedures should mask the Internet Protocol (IP) address of the computer being used. This can easily be accomplished in two ways. One way is simply to have a stand-alone computer that is generically registered using a false identity with an Internet Service Provider (ISP).[154] The computer should not be connected to any other network and not used for personal activities, such as accessing accounts requiring a user name and password.

Another method is to use a proxy server that will mask the IP address of the computer being used.[155] There are commercial enterprises that will provide this service for a fee, such as Anonymizer[156] or The Cloak.[157] There are also free methods such as using a free proxy web site as found on Proxify[158] or ProxyIndex.[159] Another method is to identify anonymous server IP addresses and insert the IP number and port number into the proxy server option in your web browser. The process is actually quite simple. First go to a web site that lists proxy servers, such as Public Proxy Servers,[160] and select a server from the list. In your Internet browser, go to the proxy settings dialog box. In Microsoft Internet Explorer[161] (IE), the path is usually the following:

Tools > Internet Options > Connections > LAN Settings

In LAN settings, check the proxy server box and enter the IP address and port number (both will be on the proxy server list). Figure 11-1 illustrates how a proxy server from the Russian Federation (highlighted at the bottom of the image) was entered into the proxy server option in Microsoft IE.

The reason that the IP address should be masked is because tools are available on the Internet to trace domain names, IP addresses, connection routes, e-mail addresses, general geographic locations of the computer, and other electronic transaction information. These tools can also be used effectively by law enforcement and can be found at such web sites as DomainTools,[162] Better-WhoIs,[163] and Geektools.[164] It should be noted that different WhoIs web sites will have different databases to search and multiple sources may need to be used. If, however, the IP being searched for has been cleaned through a proxy server, the WhoIs search will not be fruitful.

Finally, the computer's cookies and Internet cache should be cleaned regularly. This will help ensure anonymity, particularly in light of the inevitable fact that someone will use the computer for personal business. While cookies and the cache can be cleaned manually, the most effective way is to use software designed for that purpose.[165]

[154] This is sometimes referred to as a "hello computer" much like and generically registered "hello telephone" used in law enforcement undercover operations.

[155] To maximize safety, use a proxy server even on a hello computer.

[156] www.anonymizer.com

[157] www.the-cloak.com/pay-terms

[158] www.proxify.com

[159] www.proxyindex.com

[160] www.publicproxyservers.com

[161] The path to LAN settings may differ somewhat between versions of IE. Other Internet browsers such as Netscape and Firefox, will have a similar ability to create a proxy server.

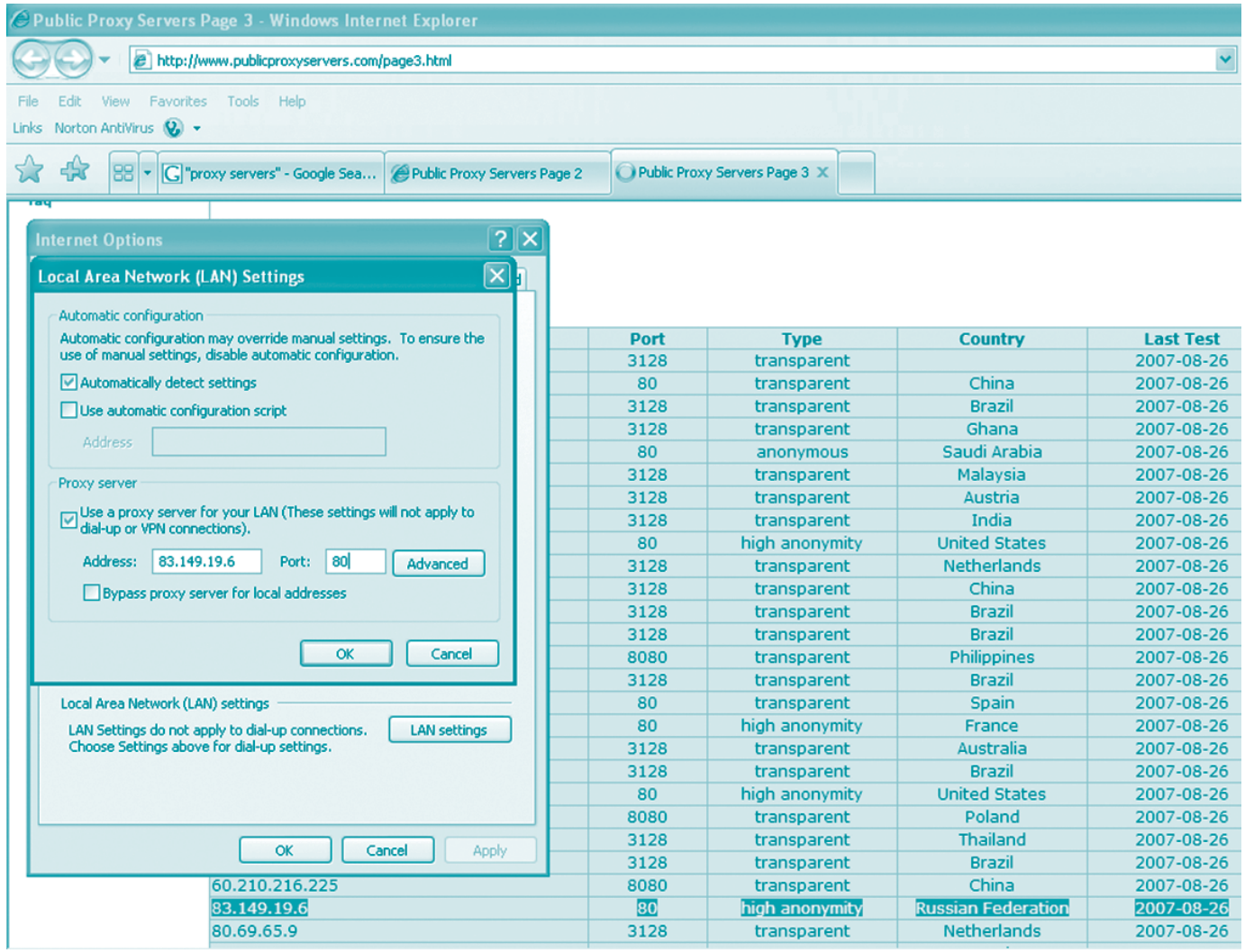
[162] whois.domaintools.com

[163] www.betterwhois.com

[164] www.geektools.com

[165] Effective software is available at no charge on the Internet for cleaning cookies and the cache. See a discussion of cookies, caches, avoiding spyware, maintaining your computer's registry, recommendations for software, and additional useful information at the nonprofit site www.instant-registry-fixes.org.

Figure 11-1: Example of Entering Proxy Server in MS Explorer



	Port	Type	Country	Last Test
	3128	transparent		2007-08-26
	80	transparent	China	2007-08-26
	3128	transparent	Brazil	2007-08-26
	3128	transparent	Ghana	2007-08-26
	80	anonymous	Saudi Arabia	2007-08-26
	3128	transparent	Malaysia	2007-08-26
	3128	transparent	Austria	2007-08-26
	3128	transparent	India	2007-08-26
	80	high anonymity	United States	2007-08-26
	3128	transparent	Netherlands	2007-08-26
	3128	transparent	China	2007-08-26
	3128	transparent	Brazil	2007-08-26
	3128	transparent	Brazil	2007-08-26
	8080	transparent	Philippines	2007-08-26
	3128	transparent	Brazil	2007-08-26
	80	transparent	Spain	2007-08-26
	80	high anonymity	France	2007-08-26
	3128	transparent	Australia	2007-08-26
	3128	transparent	Brazil	2007-08-26
	80	high anonymity	United States	2007-08-26
	8080	transparent	Poland	2007-08-26
	3128	transparent	Thailand	2007-08-26
	3128	transparent	Brazil	2007-08-26
60.210.216.225	8080	transparent	China	2007-08-26
83.149.19.6	80	high anonymity	Russian Federation	2007-08-26
80.69.65.9	3128	transparent	Netherlands	2007-08-26

Information That Can Be Learned From Your Computer's Internet Protocol Address
Information that is useful to law enforcement is also useful to those persons monitoring visitors to their web sites. If a computer's Internet Protocol (IP) address is not made anonymous, the types of information that can be gained from the IP alone include:

- City and state where the computer is accessing the Internet
- Area code
- Longitude and latitude
- ISP
- Last web site visited

See for yourself. Visit these web sites:

- www.zabasearch.com/zabainfo
- www.ip-address.com

The Investment in Critical Thought and Time

Despite the ease and speed of the Internet, two of the most important open source tools are critical thought and time. Both are needed to define search terms and phrases, develop the collection plan, identify critical information needed in an inquiry verify the information, and interpret it. Often, this information will lead to other sources and critical thought is needed to dissect the additional source alternatives, weighing the value of each, and moving the search and collection processes forward.

The process can be laborious, particularly as one sifts through diverse blogs. Reading, consuming, interpreting, and collecting important information from the overwhelming quantity of information is labor-intensive, but valuable for discovering information that can be essential in identifying and preventing threats.

Information collectors and analysts must have the wherewithal to push the process forward, particularly during searches that seem to be unproductive. Managers and administrators must develop the patience to understand these unique performance characteristics when evaluating personnel.

Conclusion

This discussion was an overview of the open source concept, the current philosophy and application of open source information as part of the National Open Source Enterprise, the role of open sources in law enforcement intelligence, and a primer on the use of open source techniques and tools for the intelligence process. The web sites listed in this discussion are intended to serve as illustrations and are not meant to be a comprehensive list nor an endorsement of any particular commercial or open application. They were accurate at the time of publication of this *Guide*.

As the source of first resort, open source information and intelligence provides tremendous potential for law enforcement that should be exploited to increase the efficiency and effectiveness of the intelligence function.

Chapter Annex 11-1: Eclectic Web Sites Sometimes Found Useful for Intelligence

The Intelligence Process sometimes needs information that intuitively would not seem to be part of a law enforcement inquiry. The sites can be accessed at no charge.

- According to the National Counterterrorism Center definition, terrorism occurs when groups or individuals acting on political motivation deliberately or recklessly attack civilians/noncombatants or their property and the attack does not fall into another special category of political violence, such as crime, rioting, or tribal violence. The incidents may be tracked on the Worldwide Incidents Tracking System: wits.nctc.gov.
- The Geographic Names Information System (GNIS), developed by the U.S. Geological Survey in cooperation with the U.S. Board on Geographic Names, contains information about physical and cultural geographic features in the United States and associated areas, both current and historical (not including roads and highways). The database holds the federally recognized name of each feature and defines the location of the feature by state, county, USGS topographic map, and geographic coordinates: nhd.usgs.gov/gnis.html.
- The National Geospatial-Intelligence Agency (NGA) GEOnet Names Server (GNS) provides access to the National Geospatial-Intelligence Agency's (NGA) and the U.S. Board on Geographic Names' (US BGN) database of foreign geographic feature names. The database is the official repository of foreign place-name decisions approved by the US BGN: earth-info.nga.mil/gns/html/index.html.
- The Statistical Abstract of the United States is the authoritative and comprehensive summary of statistics on the social, political, and economic organization of the United States. Sources of data include the Census Bureau, Bureau of Labor Statistics, Bureau of Economic Analysis, and many other federal agencies and private organizations: www.census.gov/compendia/statab.
- The U.S. Census Bureau FactFinder user can obtain comprehensive population, housing, economic, and geographic data in the form of maps, tables, and reports from a variety of Census Bureau sources: factfinder.census.gov.
- Sometimes simple information is needed:
  - The geographic location of an area code: www.areadecoder.com.
  - Social Security numbering scheme: www.ssa.gov/history/ssn/geocard.html.
  - Geographic, social, and economic information about a ZIP Code: www.zipskinny.com.
  - The definition of a word: thesaurus.reference.com.
- A Librarians Internet Index is comprehensive portal of links to web sites on virtually every topic. The unique aspect of this portal is that the web sites which have direct links have been reviewed as being trustworthy sites: www.lii.org.
- The How Stuff Works web site covers a very wide array of topics and explains the components and processes that make the topic functional: www.howstuffworks.com.

- Significant weather events always hold the potential for law enforcement activity. Two good and slightly different sources for weather are:
  - National Weather Service www.nws.noaa.gov.
  - The Weather Channel www.weather.com.
- At times there is a need to convert U.S. dollars to a foreign currency or vice versa. To do this easily at current rates, use the FX Currency Converter: www.oanda.com/convert/classic.
- The need to convert information in a variety of ways often becomes essential, but difficult. Online Conversion has made it simply by providing conversion calculators for length, temperature, speed, volume, weight, cooking, area, fuel economy, clothing, area, angles, frequency, distance, and much more: www.onlineconversion.com.
- Real time tracking of both commercial and private flights: www.flightware.com.
- Scalable satellite imagery can be used to see the layout of a target location (different sites will provide slightly different satellite images):
  - TerraServer www.terraserver.com.
  - Google Maps maps.google.com.
  - Digital Globe www.digitalglobe.com.
- Cyberhomes provides images and/or aerial views and maps of property throughout the U.S., GPS location, legal description of the property, and other information: www.cyberhomes.com.
- Genealogy web sites have become very popular as people seek to learn more about their family tree. Many of these web sites have a surprisingly wide range of information useful for law enforcement: www.ancestry.com.
- In some instances, information such as images, audio, video, word processing, etc., that are in a different format that cannot be opened on the law enforcement computer. These files can be converted online to a different format so they can be opened on your computer at: www.media-convert.com.
- Voicemail menus can often be frustrating, particularly when one needs to talk with a person. The Get Human web site identifies the shortcut codes in a large number of voicemail systems to avoid voice mail prompts and to reach a person: www.gethuman.com.
- A wide range of unique information searches: www.blackbookonline.info.
- Junk science is faulty scientific data and analysis used to advance special and, often, hidden agendas. Junk science is debunked at: www.junkscience.com.
- A guide to medical quackery and health fraud: www.quackwatch.com.

Chapter Annex 11-2: The Pre-Search Development Plan

The Pre-Search Development Plan[154]

1. What unique words, distinctive names, abbreviations, or acronyms are associated with your topic?

   The value of starting with these search elements is that they help define your search parameters. Be certain to include synonyms and professional terminology.

2. Can you think of societies, organizations, or groups that might have information on your subject on their pages?

   Search these as a "phrase in quotes," looking for a home page that might contain links to other pages, journals, discussion groups, or databases on your subject. You may require the phrase in quotes to be in the documents' titles by preceding it by title:[no space]

3. What other words are likely to be in any web documents on your topic?

   You may want to require these by joining them with AND or preceding each by +[no space].

4. Do any of the words in 1, 2, or 3 belong in phrases or strings, together in a certain order, like a cliché?

   Search these as a "phrase in quotes". (e.g., "world jihad" or "Aryan nation").

5. For any of the terms in #4, can you think of synonyms, variant spellings, or equivalent terms you would also accept in relevant documents?

   You may want to allow these terms by joining them by OR and including each set of equivalent terms in ( ). As an example of synonyms: "terrorists" and "jihadis". As an example of alternate spellings: "Osama" and "Usama".

6. Can you think of any extraneous or irrelevant documents these words might pick up?

   You may want to exclude terms or phrases with -[no space] before each term, or and not

7. What broader terms could your topic be covered by?

   When browsing subject categories or searching sites of webliographies or databases on your topic, try broader categories.

[154] Adapted from the Regents of the University of California. Copyright 2004 All Rights Reserved. Created by Joe Barker, Teaching Library, UC Berkeley.

Chapter 12:

Federal and National Law Enforcement Intelligence Resources, Networks, and Systems

Federal and National Law Enforcement Intelligence Resources, Networks, and Systems

Legislation, mission-related responsibilities of federal agencies, and the need to develop programs and products that have interstate utility have led a wide variety of federal agencies to develop resources and systems that support law enforcement intelligence at the state, local, and tribal levels. Some resources are designed to meet specific needs, such as financial crimes investigations, while others are intended to support broad law enforcement needs, such as the FBI's Law Enforcement Online (LEO). Although in most cases, the resources are provided by a federal agency, some resources are national, but are provided by an entity other than the federal government. The value of these diverse resources and systems to state, local, and tribal law enforcement (SLTLE) will vary according to agency size, geographic location in the U.S., and unique crime problems facing a jurisdiction.

This chapter identifies the various resources, giving the greatest attention to those that have the most value for the broadest range of law enforcement agencies. Unlike previous chapters which sought to provide a discussion of integrated issues surrounding the chapter's topical theme, this chapter is more like a catalog. The goal is to identify the most relevant resources for SLTLE and provide insight into what the resources or systems can provide to a law enforcement agency.

Many resources are also available at the state and local levels, but there was no attempt to document them because of their limited national applicability and the volume of information involved. In some instances, the chapter discusses specific state resources for the purpose of illustration. Information about law enforcement intelligence resources within each state can be found at these sources:

1. *National Criminal Intelligence Resource Center* (NCIRC) operated by the Bureau of Justice Assistance, U.S. Department of Justice.[1]
2. Fusion Center Technical Assistance Program of the Lessons Learned Information Sharing (LLIS) online information system operated by the U.S. Department of Homeland Security (DHS).[2]

As will be seen, there is some overlap between resources and systems; nonetheless, exploring the materials in the following pages should provide valuable direction for the law enforcement intelligence consumer.

[1] The public side of this resource is at www.ncirc.gov. The public NCIRC site has a limited amount of information; however, it provides access to the Criminal Intelligence Master Training Calendar. The greatest value of this site is on the secure side of NCIRC that is accessible through the RISS.NET portal and LEO.

[2] Users must first register for access to this web site at www.llis.dhs.gov. After registering, the user must e-mail a request for access to the Fusion Center Technical Assistance Program channel on LLIS.

What Is Needed to Start?

From a basic perspective, certain fundamental elements need to be in place to enable access to, and use many of, these resources and systems.

- Access to the Internet through a security controlled computer(s) designated exclusively for law enforcement use (excluding undercover computers).
- The computer should have a firewall and virus and spyware protections.
- A privacy policy must be in place that is consistent with the federal privacy guidelines.[3]
- A security policy should be in place that is consistent with the Global Justice Information-Sharing Initiative security policy.[4]
- An additional fair use operating policy for the agency's law enforcement computers may be implemented describing both accepted and prohibited use of the law enforcement agency's computers.
- Supervisory accountability should be in place to monitor and supervise access to systems and resources.

Most systems that a user will access will have additional requirements, but they are simply the minimum requirements needed before gaining access to systems and resources.

Federal and National Law Enforcement Intelligence Resources

Many federal agencies have reengineered their intelligence function since 9/11 to make their intelligence products more accessible and useful to SLTLE. Intelligence products have been redesigned or new products developed, dissemination methods have been revised, greater attention has been given to providing critical information that is unclassified for wide consumption by SLTLE, and new offices and initiatives have been developed. More information is being produced and disseminated more widely than in the history of law enforcement. Among the challenges that law enforcement now faces is accessing the needed information and using it with efficacy.

Many federal intelligence resources are in a dynamic state responding to changes in threats as well as changes in policy. It is virtually impossible to provide an exhaustive discussion of them all. This discussion, therefore, will identify the federal intelligence resources that are of greatest use to SLTLE, their intelligence products, and the agencies' contact or access information. In addition, a broader discussion of the FBI than of other agencies will be provided because of the comparatively more frequent interaction on intelligence matters between SLTLE and the FBI.

While federal agencies have attempted to provide more unclassified information to America's law enforcement agencies, a significant amount of classified information remains relating to terrorism. The FBI and the DHS, therefore, have made a commitment to increase security clearances for SLTLE officers. Despite this, controversies and questions remain. Dealing with the issue of classified and sensitive information is the first place to start when discussing federal information sharing.

[3] it.ojp.gov/default.aspx?area=globalJustice&page=1151

[4] it.ojp.gov/global

Terms and Concepts Related to Classified Information

When dealing with classified information, the following terms and concepts are often used as related to SLTLE:

Tear Line or Tear Line Report: The place on an intelligence report (usually denoted by a series of dashes) at which the sanitized version of a more highly classified and/or controlled report begins. The sanitized information below the tear line should contain the substance of the information above the tear line, but without identifying the sensitive sources and methods. This will permit wider dissemination of the information below the tear line, in accordance with the right-to-know and need-to-know principles.

Write for Release (Write for the Consumer): Preparing intelligence reports and products at the unclassified level to the greatest extent possible or using tear line reporting to facilitate the dissemination of releasable information to individuals who do not have a clearance.

Markings. Classified Information and information that has been declassified have an explicit set of comprehensive rules for the proper marking of documents to ensure notice is given about classification and safeguarding. The extensive set of markings guidelines are available from the Office of the Director of National Intelligence in the document entitled *Authorized Classification and Control Markings Register* (available on the Office of the Director of National Intelligence (ODNI) web site in the "Electronic Reading Room" at www.dni.gov/electronic_reading_room.htm).

Sources and Methods: This refers to how information was obtained. "Sources" refers to from whom or where the information was collected (for example, a confidential informant) and "methods" refers to the means used to collect the information (for example, an electronic intercept).

Classified Information

A mystique often surrounds classified information, leading most people to ask, "That's it?" after seeing a collection of classified documents. While a number of explicit elements are required for information to be classified, often the distinction between classified and unclassified information with respect to the law enforcement community is that the classified information contains information about the sources and methods used in the collection of information. Extensive rules and processes are associated with all aspects of classified information. The following discussion addresses only the fundamental issues of classification that are most pertinent to enabling law enforcement intelligence personnel to understand the process.

Some of the rules governing classified information are unique to the specific mission of some federal agencies, their responsibilities, and the types of information they collect and retain. The current discussion is limited to issues and questions that typically arise about classified information specifically related to how SLTLE agencies will most typically interact with the classified information environment.

Table 12-1: Information Categories for Classified Information[5]

Information To Be Classified Must Fall within One or More of the Following Prescribed Categories:
• Military plans, weapons systems, or operations
• Foreign government information
• Intelligence activities (including special activities), intelligence sources or methods, or cryptology
• Foreign relations or foreign activities of the United States, including confidential sources
• Scientific, technological, or economic matters relating to the national security, which includes defense against transnational terrorism
• United States Government programs for safeguarding nuclear materials or facilities
• Vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security, which includes defense against transnational terrorism
• Weapons of mass destruction.

The federal agency responsible for managing the classified information environment is the Information Security Oversight Office[6] (ISOO) of the National Archives and Records Administration (NARA). The ISOO is responsible to the President for policy and oversight of the government-wide security classification system and the National Industrial Security Program. The ISOO receives its authority from *Executive Order 12958, Classified National Security Information*[7] and *Executive Order 12829, National Industrial Security Program*.[8]

The classified information environment is highly controlled. Certain explicit categories of information are subject to classification (see Table 12-1), while other categories of information are subject to prohibitions or limitations concerning classification (see Table 12-2). Despite these regulations, antisecrecy advocates,[9] law enforcement officials, and members of Congress,[10] among others, have expressed concerns that the federal government tends to over classify too much information. Suffice it to note for the current discussion that the debate on over-classification between federal law enforcement and SLTLE is often heated.

[5] www.archives.gov/isoo/pdf/appropriate-classification.pdf

[6] www.archives.gov/isoo

[7] www.archives.gov/isoo/policy-documents/eo-12958-amendment.html

[8] www.archives.gov/isoo/policy-documents/eo-12829.html

[9] See, for example, www.fas.org/blog/secrecy/2007/12/classification_reform_bill_int.html.

[10] For example, in the 110th Session of the United States Congress, Rep. Jane Harmon introduced H.R. 4806 "To require the Secretary of Homeland Security to develop a strategy to prevent the over-classification of homeland security and other information and to promote the sharing of unclassified homeland security and other information, and for other purposes."

Table 12-2: Information Categories Prohibited or Limited for Classification[11]

Information That Is Subject to Prohibitions or Limitations with Respect to Classification:
• Is the information classified to conceal violations of law, inefficiency, or administrative error? • Is the information classified to prevent embarrassment to a person, organization, or agency? • Is the information classified to restrain competition? • Is the information classified to prevent or delay the release of information that does not require protection in the interest of national security? • Does the information relate to basic scientific research not clearly related to national security? • If the information had been declassified, released to the public under proper authority, and then reclassified: » Was the reclassification action taken under the personal authority of the agency head or deputy agency head based on his or her determination that the reclassification was necessary in the interest of the national security? » Was that official's determination in writing? » Was the information reasonably recoverable? » Was the Director of the Information Security Oversight Office notified of the reclassification action? • If the information had not previously been disclosed to the public under proper authority but was classified or reclassified after receipt of an access request: » Does the classification meet the requirements of this order (to include the other elements of this methodology)? » Was it accomplished on a document-by-document basis with the personal participation or under the direction of the agency head, the deputy agency head, or the senior agency official? • If the classification decision addresses items of information that are individually unclassified but have been classified by compilation or aggregation: » Does the compilation reveal an additional association or relationship that meets the standards for classification under this order? » Was such a determination made by an Original Classification Authority in accordance with the other elements of this methodology? » Is the additional association or relationship not otherwise revealed in the individual items of information?

[11] www.archives.gov/isoo/policy-documents/eo-12829.html

According to Executive Order 12958,[12] information at the federal level may be classified at one of three levels:

1. "Top Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe.
2. "Secret" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe.
3. "Confidential" shall be applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe.

Classified information, including computers that contain classified information or are connected to a classified information system, must be located in a Sensitive Compartmented Information Facility (SCIF). A SCIF is an accredited area, room, group of rooms, or installation where Sensitive Compartmented Information (SCI) may be stored, used, discussed, and/or electronically processed. SCIF procedural and physical measures, which are explicitly stipulated in federal government regulations, prevent free access to persons unless they have been authorized with an appropriate security clearance.

Security Clearances for SLTLE Personnel

Before an individual is given access to classified information, he or she must have the appropriate clearance level. Beyond the clearance levels of Top Secret, Secret, and Confidential, "highly sensitive programs" require a clearance addendum to the Top Secret clearance, such as SCI, Special Access Programs, Q Clearances, and other similar programs. Beyond the clearance levels and special conditions that establish a person's right to know, an individual must also have the need to know the classified information. Just because a law enforcement employee has a security clearance does not mean that he or she will be given broad access to classified information.

Beyond access to classified information, security clearances are also often required for access to certain facilities. Employees working in a SCIF must have at least a Secret clearance. Similarly, certain intelligence training programs require people to have clearance before attending the training, either because of the location for the training (i.e., in a secured facility) or content of the training.

A number of federal agencies can authorize clearances. The process begins with the applicant completing a comprehensive questionnaire—Form SF-86 Questionnaire for National Security Positions[13]—wherein he or she must provide extensive information about his or her personal background. The information is used by the federal agency to conduct a comprehensive personal security investigation. Fingerprints must also be submitted and privacy waivers signed. Following the investigation, the findings are adjudicated by a separate body that determines whether to issue a clearance. The adjudication process is an administrative examination of a sufficient period of a person's life to make an

[12] www.archives.gov/isoo/policy-documents/eo-12958-amendment.html amends a previous Executive Order on classified information.

[13] Form SF-86 is available as a form which may be filled out on the computer from the General Services Administration at www.opm.gov/Forms/pdf_fill/sf86.pdf. Applicants should check with the agency from which they are seeking the clearance for special instructions; for example, the SF-86 asks for the applicant's employment history during the past 7 years, while other agencies request the employment history for the past 10 years.

affirmative determination that the individual, based on his or her past behavior and associations, is eligible for a security clearance. The process is the careful weighing of a number of variables. In particular, a person's conduct is reviewed to make a determination that he or she has high integrity and is reliable and trustworthy. When questionable conduct is identified, the adjudication will consider the following factors:

- The nature, extent, and seriousness of the conduct
- The circumstances surrounding the conduct, including knowledgeable participation
- The frequency and how recent the conduct occurred
- The individual's age and maturity at the time of the conduct
- The voluntariness of participation
- The presence or absence of rehabilitation and other pertinent behavioral changes
- The motivation for the conduct
- The potential for pressure, coercion, exploitation, or duress
- The likelihood that the conduct will continue or recur.

The factors are balanced to determine if the clearance should be granted. Once a clearance is issued, the applicant must be briefed on the regulations associated with the clearance and sign a nondisclosure agreement.[14]

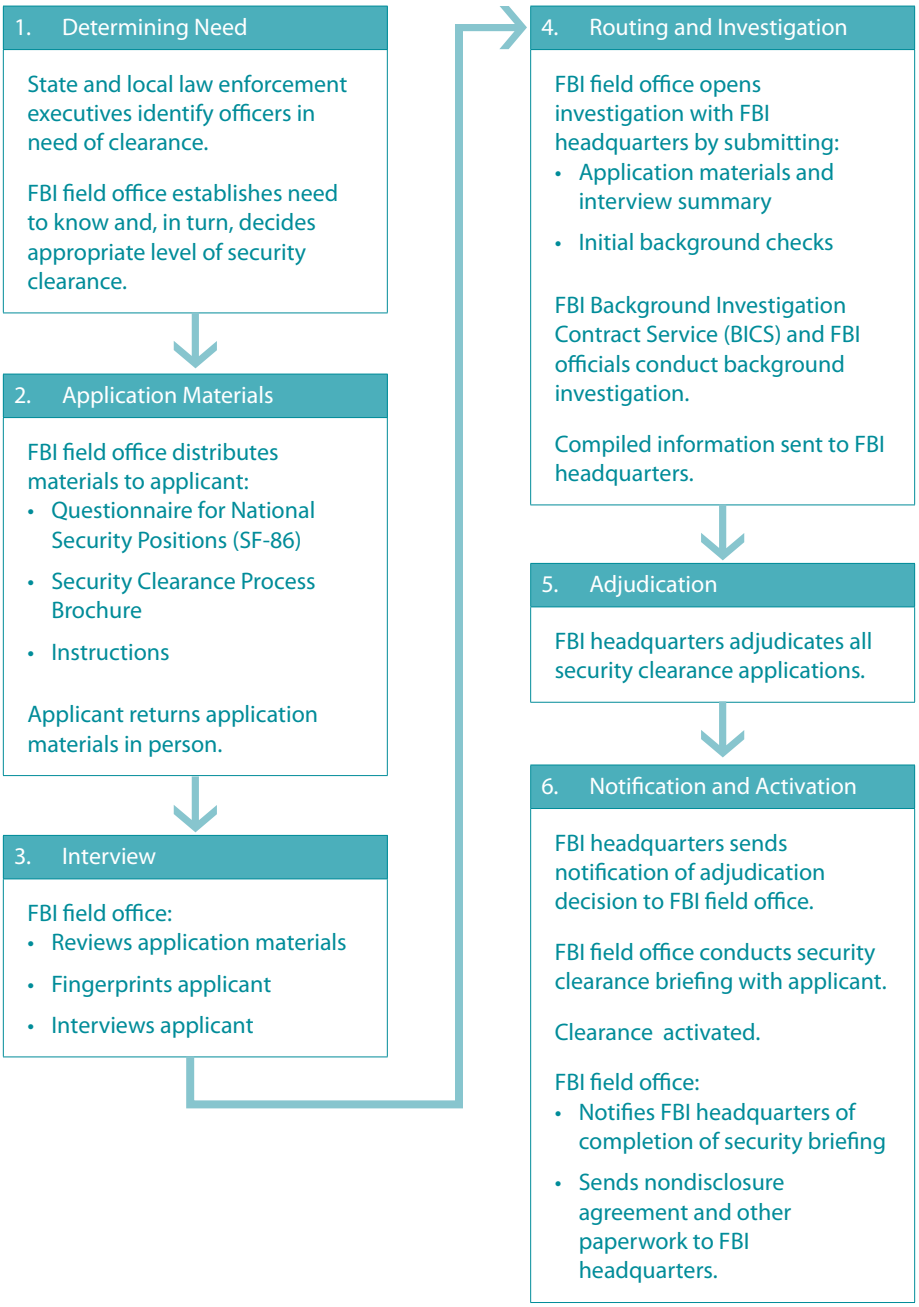
As noted previously, different agencies issue clearances, with some variability in processes. The most common clearances for SLTLE are from the FBI and the DHS. The clearance process is labor-intensive and expensive. For these reasons, as well as some operations security concerns, there must be a substantial reason for issuing a clearance to an SLTLE employee. Moreover, conducting an excess number of clearance investigations slows the process, thereby taking longer to process clearances for those persons who may be in more critical positions. Not all SLTLE requests for clearances will be honored by the federal agency.

In most cases, the FBI will begin consideration of a clearance investigation for an SLTLE officer by examining local issues on a case-by-case basis[15] (See Figure 12-1 for the steps in the FBI process.). For those who seek to apply for a security clearance, the appropriate forms and fingerprint cards can be obtained from the local FBI Field Office.

[14] The general nondisclosure agreement can be found at contacts.gsa.gov/webforms.nsf/0/03A78F16A522716785256A69004E23F6/$file/SF312.pdf.

[15] The FBI provides the following guidance: Most information needed by state or local law enforcement can be shared at an unclassified level. In those instances where it is necessary to share classified information, it can usually be accomplished at the Secret level. Local FBI Field Offices can help determine whether a security clearance is needed, and if so, what level is appropriate.

Figure 12-1: Steps in the FBI Security Clearance Process for SLTLE Personnel[16]



Sensitive but Unclassified and Controlled Unclassified Information

Dissemination refers to the types of information about threats, suspects, and indicators of criminality that a law enforcement agency or government entity wants to purposely share. Because of the sensitivity of the information, controls are put in place to protect the information and prevent inadvertent information sharing with persons who do not have the right to know and need to know.

[16] From: U.S. General Accounting Office. *Security Clearances.* GAO-04-596. Washington, D.C.: U.S. General Accounting Office, 2004, p. 8.

The management of information that is deemed sensitive but does not meet the requirements for classification is going through a significant change process at this writing. The changes are predicated on new initiatives of the Information Sharing Environment (ISE) to be compliant with provisions of the Intelligence Reform and Terrorism Prevention Act of 2004. Because a multiyear transition process is in place transitioning Sensitive But Unclassified (SBU) to Controlled Unclassified Information (CUI), this chapter discuss both.

Sensitive but Unclassified Information

It is not feasible for every law enforcement officer to have a security clearance and not all information meets the standards for classification. A mechanism exists to get critical information into the hands of officers that does not involve the classified information framework. The traditional approach has been to use markings designating the information as SBU. A wide variety of SBU labels are placed on intelligence products and other information by the originator of the information to indicate that the information should not be shared broadly and that dissemination should be limited only to those indicated by the SBU label.

There are no national standards or guidelines for SBU information; rather, each agency has developed its own policies and procedures to identify and safeguard SBU information. Generally, this unclassified information is withheld from the public for a variety of reasons, but has to be accessible to law enforcement, private security, or other persons who have a responsibility to safeguard the public. Agencies have discretion to define SBU in ways that serve their particular needs to safeguard information. Since there is no uniformity in implementing rules throughout the federal government on the use of SBU, the specific meanings of the markings are often unclear.[17] There have been even fewer efforts to define and safeguard the information at the state, local, and tribal levels. There is an intuitive understanding, but no formal process to control the information. Some guidance has been provided by the DHS, which issued a directive in 2004 on "For Official Use Only" information.

For Official Use Only Information

The For Official Use Only (FOUO) label is used within the DHS "…to identify unclassified information of a sensitive nature, not otherwise categorized by statute or regulation, the unauthorized disclosure of which could have an adverse impact on a person's privacy or welfare, the conduct of a federal program, or other programs or operations essential to the national interest."[18] FOUO is not classified information, but information that should be distributed only to persons who need to know the information to be aware of conditions that will help keep the United States and local communities secure. Within DHS, the caveat For Official Use Only will be used to identify SBU information that is not otherwise governed by statue or regulation. In sum, FOUO information may be shared with anyone who has the right to know and need to know the information in the report or product.

Law Enforcement Sensitive Information

The second most common SBU label is Law Enforcement Sensitive (LES). It is more restrictive than FOUO because it limited dissemination to anyone in the

[17] For a detailed review of the SBU meaning and how it is defined and used by different statutes and regulations, see: Knezo, Genevieve J. "*Sensitive But Unclassified" and Other Controls: Policy and Options for Scientific and Technical Information.* Washington, D.C.: Congressional Research Service, 2006.

[18] U.S. Department of Homeland Security, Management Directive System, MD Number: 11042, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information.* May 11, 2004.

law enforcement community who had the right to know and need to know the information. The additional qualifier was that the recipient had to be a law enforcement employee. One of the reasons for the distinction was because some information that contained Personal Identifying Information (PII) had to stay within the law enforcement community for reasons relating to civil rights and privacy.

While these definitions reflect the intent of the FOUO and LES labels—and because there are no national standards or national policies for the explicit types of information of information that is deemed SBU, agencies at all levels of government began making their own rules and adaptations of rules as they labeled SBU information. It is increasingly common to see a document with both the FOUO and LES dissemination labels, which basically eliminates the original distinctions between the labels.

Agencies provide different interpretations to any given SBU label because there are so few uniform national SBU guidelines. There are no sanctions if SBU information is widely distributed, including to the media, and no guidelines to ensure that the information is secured. Nevertheless, and in many ways, particularly for SLTLE agencies, SBU markings reflected a professional agreement to limit the dissemination of certain types of information.

Many of the problems with SBU dissemination labels and procedures are being remedied during a transition away from SBU and into the new method of marking unclassified sensitive data: Controlled Unclassified Information (CUI).

Controlled Unclassified Information

Among the mandates of the Intelligence Reform and Terrorism Prevention Act of 2004 was the development of policies and practices that would enhance the ability of rapid information sharing among the Intelligence Community, law enforcement, the private sector, and foreign partners. One of the information-sharing obstacles, though, was the lack of consistency in policies regulating SBU/CUI. At the federal level alone, the Program Manager for the Information Sharing Environment observed the following:

> Among the twenty departments and agencies we have surveyed, there are at least 107 unique markings and more than 131 different labeling or handling processes and procedures for SBU/CUI. Even when SBU information carries the same label marking (e.g., For Official Use Only), storage and dissemination are inconsistent across Federal agencies and departments. Because such markings are agency-specific, recipients of SBU information in a different agency must understand the processes and procedures of the originating Federal agency for handling the information, even if their agency uses the same marking. The result is an unmanageable collection of policies that leave both the producers and users of SBU information unable to know how a piece of information will be controlled as it moves through the Federal government and therefore reducing information sharing.[19]

[19] McNamara, Ted. *Statement for the Record before the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment of the House Committee on Homeland Security*, April 26, 2007.

These problems were the basis for establishing a common framework for sharing the information under the new label of Controlled Unclassified Information (CUI). After nearly 4 years of work on developing the new framework, the President issued a memorandum to the heads of all executive departments and agencies in the United States Government to implement the CUI framework:

> The global nature of the threats facing the United States requires that (a) our Nation's entire network of defenders be able to share information more rapidly so those who must act have the information they need, and (b) the United States Government protect sensitive information, information privacy, and other legal rights of Americans. A uniform and more standardized government-wide framework for what has previously been known as SBU/CUI information is essential for the ISE to succeed. Accordingly, this memorandum establishes a standardized framework designed to facilitate and enhance the sharing of Controlled Unclassified Information.[20]

The policies set forth in the Presidential Memorandum for the designation, marking, safeguarding, and disseminating of CUI are mandatory for all CUI originated by the Executive Branch of the federal government and shared within the ISE, regardless of the medium used for its display, storage, or transmittal.

It is important to note that the Presidential Memorandum also encourages the adoption of the CUI Framework by state, local, tribal, and private-sector entities. Frequent consultations with individuals and organizations from these entities during the development of this Framework suggest that there is some support for moving in the direction of a common, or mostly common, CUI Framework. As necessary, departments and agencies may agree with foreign partners to ensure that they protect shared CUI in "a like manner," similar to what is now done for sharing classified information. Of course, this provision applies only to the federal government, not to SLTLE. Presidential Guideline 4 activities address foreign government sharing, including sharing of CUI.[21] Additionally, sharing CUI with the private sector will most likely require some change to an agency's contractual policy, which may include mandating the use of the CUI Framework.

The term Controlled Unclassified Information or CUI is a *categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the Federal Government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. Henceforth, the designation CUI replaces Sensitive But Unclassified.*[22] (Emphasis in original.)

[20] www.fas.org/sgp/bush/cui.html

[21] The full text of Presidential Guideline 4 can be found at www.ise.gov/docs/guidance/guideline%204%20-%20sharing%20with%20foreign%20partners.pdf.

[22] Background on the *Controlled Unclassified Information Framework.* (Unpublished background paper.) Washington, D.C.: Executive Office of the President, May 9, 2008, pp. 4–7.

The CUI Executive Agent, based in the National Archives and Records Administration, is responsible for administering all policies and regulations associated with the CUI framework. Among the regulations established thus far are the following:

1. Information shall be designated as CUI if:
    a. A statute so requires or authorizes; or
    b. The head of the originating department or agency, through regulations, directives, or other specific guidance to the agency, determines that the information is CUI. Such determination should be based on mission requirements, business prudence, legal privilege, the protection of personal or commercial rights, or safety or security. Such department or agency directives, regulations, or guidance shall be provided to the CUI Executive Agent for his review.
2. Notwithstanding the above, information shall not be designated as CUI:
    a. To: 1. conceal violations of law, inefficiency, or administrative error; 2. prevent embarrassment to the U.S. Government, any U.S. official, organization, or agency; 3. improperly or unlawfully interfere with competition; or 4. prevent or delay the release of information that does not require such protection;
    b. If it is required by statute or Executive Order to be made available to the public; or
    c. If it has been released to the public under proper authority.[23]

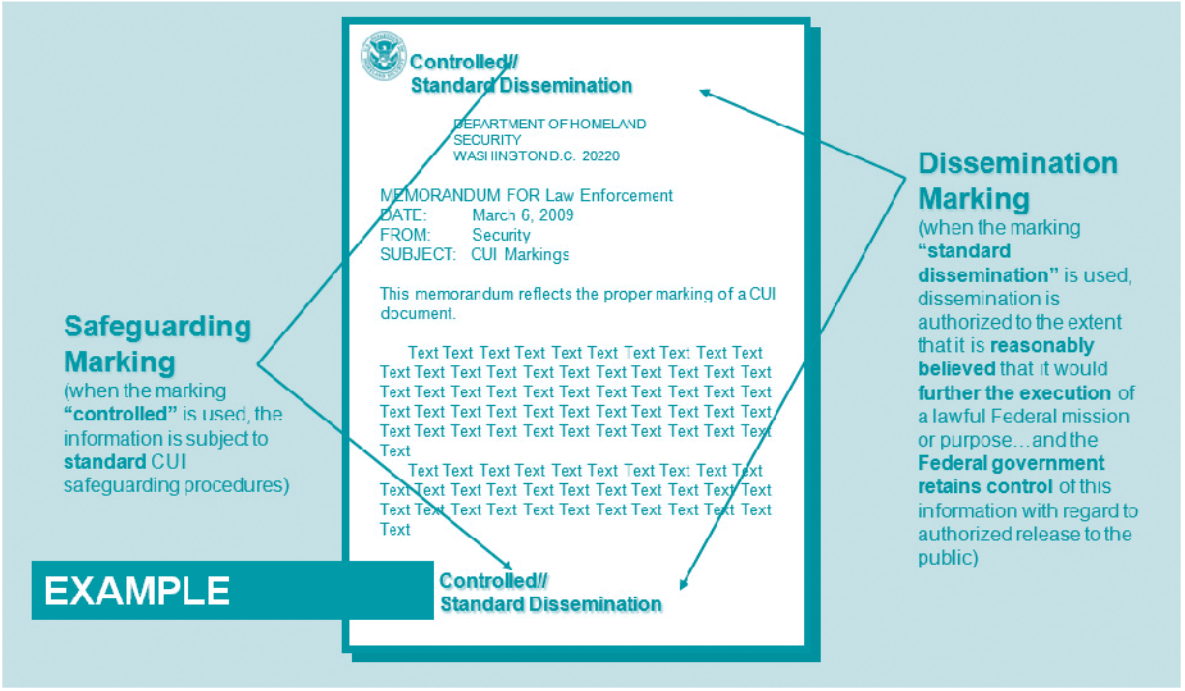
CUI Markings

Marking material as CUI signals that it contains sensitive information and that safeguarding and dissemination controls apply. All CUI will carry one of three markings (See Figure 12-2 for examples).

1. *Controlled with Standard Dissemination:* Information is subject to safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it is reasonably believed that it would further the execution of a lawful or official purpose.
2. *Controlled with Specified Dissemination:* Information is subject to safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Material contains additional instructions on what dissemination is permitted.
3. *Controlled Enhanced with Specified Dissemination:* Information is subject to enhanced safeguarding measures more stringent than those normally required because inadvertent or unauthorized disclosure would create a risk of substantial harm. Material contains additional instructions on what dissemination is permitted.

[23] Ibid.

Figure 12-2: Examples of CUI Document Markings


Safeguarding Marking
(when the marking "controlled" is used, the information is subject to standard CUI safeguarding procedures)
Controlled//
Standard Dissemination
DEPARTMENT OF HOMELAND SECURITY
WASHINGTON D.C. 20220
MEMORANDUM FOR Law Enforcement
DATE: March 6, 2009
FROM: Security
SUBJECT: CUI Markings
This memorandum reflects the proper marking of a CUI document.
Text Text Text

CUI Safeguarding

The CUI background memorandum stated that the marking *Controlled* means that the information is subject to standard CUI safeguarding procedures to reduce the risks of unauthorized or inadvertent disclosure. The marking *Controlled Enhanced* means that enhanced safeguarding is required because inadvertent or unauthorized disclosure would create the risk of substantial harm.

Reasonable safeguarding measures are required for all CUI to protect it from unauthorized or inadvertent release. These measures to will manage the risks associated with the communication, processing, storage, and life cycle of CUI. Defined safeguarding standards will be published in a CUI Framework Standards Registry maintained by the CUI Executive Agents. The guiding principle for these standards is risk management.

The federal government recognizes that it may take some time for state, local, tribal, and private-sector recipients of CUI to implement these safeguarding requirements, particularly the requirements for encryption of CUI during electronic storage and transmission. Because of the importance of promptly sharing CUI, the federal government recommends a phased approach to implementation, which provides the necessary flexibility for transitioning to the new CUI Framework. During this phased approach, federal departments and agencies should be willing to share CUI with state, local, tribal, and private-sector partners that have not fully implemented the encryption aspects of the safeguarding requirements.[24] While encryption may be a challenge for some agencies, access to encrypted e-mail is available through RISS.net, LEO, and HSIN.

Finally, for law enforcement agencies to receive CUI information from a federal agency, they must have a privacy policy in place that meets the ISE *Privacy Guidelines*.[25] Fortunately, creating a privacy policy meeting these standards can be accomplished fairly easily by following the *Privacy Policy Development Guide* that was prepared by the Global Privacy and Information Quality Working Group of the Global Justice Information Sharing Initiative.[26]

Once fully implemented, the framework is intended to end confusion about proper access, handling, and control of unclassified information that needs protection. Moreover, the new system will instill confidence that identical rules apply to everyone using the CUI markings and will provide clear guidance to SLTLE partners who are confused by SBU markings.[27]

Summary

At the time of this writing, the transition from SBU to CUI was just beginning[28] and many legacy markings, for example, LES and FOUO, will continue to be used until new policies are put in place. SLTLE agencies should strongly consider adopting the CUI framework for their own products to aid in simplifying the sharing of sensitive information. Agencies should also monitor the CUI office of the National Archives and Records Administration[29] for changes and developments.

SLTLE agencies will encounter these labels when receiving federal intelligence products and it will be useful to know the framework from which they arise. At a practical level, the rule is for law enforcement officers to use good judgment

[24] Ibid.

[25] For detailed information about the ISE *Privacy Guidelines,* see www.ise.gov/pages/privacy-implementing.html.

[26] The Privacy Policy Development Guide and supporting materials are available at it.ojp.gov/default.aspx?area=globalJustice&page=1151.

[27] McNamara, Thomas E. *Annual Report to the Congress on the Information Sharing Environment,* op cit., 2008, p. 36.

[28] The Office of the CUI Executive Agent in the National Archives and Records Administration is located on the Internet at www.archives.gov/cui.

[29] At the time of this writing, a specific web site for the CUI Executive Agent had not been established. Information can be obtained by going to www.archives.gov and using the site's search utility for CUI.

when handling such materials. This does not mean that SLTLE officers may not disseminate this information further unless prohibited from doing so as indicated on the report; rather, the officer should use the information in a manner that meets community safety needs, including disseminating portions of the information to those segments of the community that would benefit from the data contained in the report.

Federal and National Intelligence Resources and Products

A wide range of information systems is available to law enforcement agencies to aid their intelligence function. Some systems are specifically for intelligence purposes while other systems have a much broader customer base but have applications for intelligence. Some systems are classified, allowing limited access to SLTLE, while other systems are designed specifically for wide use by law enforcement officers. Information systems were designed for diverse purposes; therefore, a brief understanding of these purposes can provide insight into their use and applicability.

Some of the resources described in the following discussion are information systems; others are offices or programs that use or provide services through different information systems. Some resources are federal, meaning that they are provided as part of the mission of a federal agency, and still other resources are national, which means they provide services and resources on a nationwide basis although the organization is not a federal agency and in most cases it receives federal funding to provide its service. Because of rapid growth of many of these resources, poor communication, and different perspectives of what is needed, the reader will find there is some duplication of effort.

As a place to begin, resources and systems may be described in six broad categories. Information actually found in some of the categories will overlap a resource in another category. This typology will help provide a perspective of the different types of resources and systems that are available for SLTLE.[30]

1. *Situational Awareness.* Documents and technologies that provide information on threats, incidents, indicators, and other short-term or real-time information needed for planning or operational responses.
2. *Public Records.* Depending on statutes and policies, various types of information collected or recorded by diverse public agencies may be available. Land transactions, driving records, registered sexual offenders, addresses, telephone numbers, and all types of licenses are illustrations.
3. *Criminal Justice.* Whenever anyone has an encounter with the criminal justice system it is going to be in a record. Computer-aided dispatch calls, arrest records, field interview reports, court records, probation and parole records, and institutional corrections records are examples.
4. *Intelligence.* Any records system or network that is explicitly designated to handle intelligence, such as RISS.net, LEO, and the Homeland Security Data Network. (While many of the networks are not exclusively for intelligence, all contain intelligence products.)

[30] Based on: Shaw, Larry. (Inspector, Florida Department of Law Enforcement Information Systems and Technologies. *Presentation at the Bureau of Justice Assistance-Funded Intelligence Commanders' Course,* Norwalk, California, July 2008.

5. *Resource and Communications Systems.* A number of systems have emerged post-9/11 that are explicitly designed to provide diverse types of intelligence resources and/or provide secure e-mail communications for SLTLE. Examples are the NCIRC, the Automated Trusted Information Exchange, and the Federal Protective Service (FPS) information portal.
6. *Open Sources.* The previous chapter addressed open source information as publicly available information that anyone can lawfully obtain by request, purchase, or observation.

Although many information systems can provide support to the law enforcement intelligence function, it is not feasible to include all of them here. This is particularly true when one considers state and local systems that are in use. Rather, the goal is to provide a snapshot of the systems that SLTLE officers across the United States are most likely to encounter, as well as a brief listing of other federal intelligence information systems that they may encounter occasionally. This discussion will help readers acquire an awareness of the different systems available on a national basis so that law enforcement agencies may develop the access they need to best fulfill their intelligence function.

In most cases, the information from the resources and systems in the following discussions will not be classified, but will be SBU/CUI. In all cases, the sensitivity of the information and appropriate safeguarding of the information will be clearly marked.

Department of Justice— Law Enforcement Information Sharing Program[31]

The L*aw Enforcement Information Sharing Program* (LEISP) is not an information system. It is a program that addresses barriers to information sharing and creates a forum for collaboration on how existing and planned systems will be coordinated and unified for information-sharing purposes. LEISP delineates guiding principles, a policy framework, and functional requirements that are necessary to facilitate multijurisdictional law enforcement information sharing. LEISP establishes the DOJ's commitment to move from a culture of need to know toward a culture of need to share in which information is shared as a matter of standard operating procedure. Through the strategy, the DOJ also commits to participate as a partner to help bring together the law enforcement community in the common cause of achieving multijurisdictional information sharing.

LEISP sets in motion three implementation tracks: Track I is the DOJ's internal reform initiative, OneDOJ, which will closely coordinate information-sharing efforts within the Department, facilitate sharing of DOJ-held information with law enforcement agencies outside the Department, provide connectivity for sharing of information with the DHS, and allow the DOJ to present a single face to its information-sharing partners. Track II will first incorporate quick hits to leverage existing sharing-technology capabilities and then center on building out the services and technology platforms that will enable the Department to share its information seamlessly. In Track III, the Department will work cooperatively

[31] The information in this section is based largely on: *LEISP: United States Department of Justice Law Enforcement Information Sharing Program.* Washington, D.C.: October 2005. Unpublished report available at www.usdoj.gov/jmd/ocio/onedoj_strategy.pdf.

with its federal, state, local, and tribal law enforcement partners to enhance interconnectivity that allows standard, routine information sharing across all jurisdictions on a national basis.

Currently, the LEISP has five major initiatives:

1. OneDOJ System (formerly the Regional Data Exchange – R-DEx).
2. Law Enforcement National Data Exchange (N-DEx).
3. Joint Automated Booking System (JABS).
4. National Virtual Pointer System (NVPS).
5. Federated Identity Management (FIDM) Pilot Program.

The LEISP plans to implement policies, practices, and technologies to ensure that each component of the DOJ shares information as a matter of routine across the entire spectrum of the law enforcement community at all levels of government. The intent of the program is to ensure that law enforcement information-sharing practices in the DOJ are consistent with the national standards and ensure the protection of privacy and civil rights in all systems that contain PII. Moreover, the program should significantly enhance the amount and quality of intelligence that is shared with SLTLE agencies.

One DOJ (formerly the Regional Data Exchange: R-DEx)

The R-DEx system was developed to ensure that DOJ criminal law enforcement information was available for users at all levels of government so that they can more effectively investigate, disrupt, and deter criminal activity, including terrorism, and protect the national security. R-DEx furthered this purpose by consolidating certain law enforcement information from other DOJ systems, as well as certain state and local law enforcement information, so that it may more readily be available for sharing with other law enforcement entities.[32]

Information in R-DEx includes information about individuals who were referred by the Federal Bureau of Prisons (BOP), the United States Marshals Service (USMS), the Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Drug Enforcement Administration (DEA), the Federal Bureau of Investigation (FBI), as well as individuals referred by certain state and local law enforcement agencies that participate in the R-DEx system. All SLTLE agencies participating in R-DEx had to sign a memorandum of understanding (MOU) with the Department of Justice.

Relying on the basic concepts of R-DEx, including its database, the system has evolved into OneDOJ as the current operational information-sharing system for DOJ. It is hosted at the FBI's Criminal Justice Information Services (CJIS) data center and used to achieve the goals of OneDOJ. The OneDOJ system enables DOJ to meet its internal requirements for effective information sharing across its law enforcement agencies; only DOJ users have direct access to the OneDOJ system. External sharing is accomplished through bilateral partnerships with designated regional, state, or federal sharing initiatives. These partnerships allow non-DOJ users to access OneDOJ data from within their own systems and vice-versa.[33]

[32] *Federal Register,* Volume 72, Number 20, January 31, 2007, pp. 4532–4533, edocket.access.gpo.gov/2007/E7-1567.htm.

[33] www.usdoj.gov/jmd/ocio/leisp/initiatives.htm

The system has two primary operational objectives:

1. To serve as DOJ's system for sharing criminal law enforcement information internally across investigative components.
2. To provide regional criminal law enforcement connectivity for authorized users to conduct federated searches of OneDOJ information. This connectivity will also provide authorized DOJ users with the means to query partner law enforcement information as governed by the respective MOU.

OneDOJ is a DOJ repository for law enforcement information shared with other federal, state, local, and tribal law enforcement agencies through connections with regional information-sharing systems. All DOJ law enforcement components— ATF, BOP, DEA, FBI, and USMS—are sharing information under consistent policy and technical standards. Information shared includes open and closed case documents, investigative reports, witness interviews, criminal event data, criminal history and incarceration information, and identifying information about individual offenders.

Information sharing through OneDOJ with law enforcement outside of DOJ is achieved by interconnecting with regional systems to access DOJ information relevant to their users. As one example, the LInX-NW and ARJIS systems are connected with OneDOJ. This allows, for instance, LInX users in Washington state to access shared DEA case files of the Seattle field office from the LInX user interface. Additionally, the bidirectional nature of the connection allows DOJ users to access state and local information in the regional systems from the OneDOJ user interface.

Interconnection with OneDOJ is accomplished through an open, XML-based, NIEM-compliant standard developed by the DOJ LEISP and its partners. The standard, called LEXS-SR (LEISP Exchange Specification–Search and Retrieval), defines the interface between OneDOJ and regional sharing systems.[34]

Law Enforcement National Data Exchange

The Law Enforcement National Data Exchange (N-DEx) system provides SLTLE agencies with a system for collecting, processing, and disseminating criminal and investigative data for use as a pointer system for nationwide information sharing. Data fields within N-DEx include methods of criminal operation, arrestee/indicator information, victim information, suspect information, and other ongoing criminal and investigative information. The system has adopted the National Information Exchange Model to maximize compatibility for information-sharing. At the heart of success for N-DEx is participation by SLTLE agencies in providing data for the system. Federal agencies may also contribute investigative event data.

> All information shared through N-DEx originates from data supplied by data sources from numerous local, state, tribal, and federal systems such as incident reports, arrest reports, case files, booking reports, incarceration records, and criminal histories. These records contain information about entities (people, locations, and items such as weapons and vehicles) and may specify relationships among the entities they contain (e.g., a person lives at a certain address or owns a certain vehicle).[35]

[34] www.usdoj.gov/jmd/ocio/leisp/onedoj.htm

[35] www.fbi.gov/hq/cjisd/ndex/ndex_concept.htm

N-DEx information services correlate data received from data suppliers and apply an analytic process that will proactively notify specific users if certain relationships are discovered. N-DEx data processes will analyze and categorize all information that is entered into the system to address the who, what, when, where, why, and how of law enforcement information nationwide."[36] It will also provide users with a single point of discovery to connect the dots through the N-DEx analytic capabilities. The system's processes will constantly correlate data, even similar data from diverse sources, to provide an ongoing linkage among all known suspects, events, and indicators. When a user conducts a search for a name, for example, the system will automatically link and make available to the user correlations between people, places, and things that he or she did not know.

System development will interconnect the information technology resources housed within the Criminal Justice Information Services (CJIS) Division of the FBI, including the National Crime Information Center (NCIC), Integrated Automated Fingerprint Identification System (IAFIS), and the National Instant Criminal Background Check System's Denial Decision Extract File. It will also define, develop, and connect Federal Crime Reporting data into the N-DEx matrix of information. The system will provide a search capability that will provide law enforcement with a method for querying these repositories in order to link and

Requirements for N-DEx Participation

Who can participate?
- Any law enforcement agency can participate.

What are the requirements?
- Agencies must adhere to national standards for efficient sharing of data.
  - » National Information Exchange Model (NIEM)
  - » Law Enforcement Information Sharing Program (LEISP) Exchange Specification (LEXS)

When can I start?
- Contact the N-DEx program office to develop a strategy for participation. Telephone: 202.324.7126, Fax: 202.324.0920.

How do I start?
- Agencies will:
  - » Sign an operational MOU.
  - » Identify and map incident/case data to the N-DEx Information Exchange Package Documentation (IEPD).
  - » Obtain network connectivity through an existing CJIS wide area network (WAN) or connect over the Law Enforcement Online (LEO.

Why are participation requirements important?
- To provide criminal justice agencies with data standards and suggestions for participation in the N-DEx Program.

Where do I begin?
- The N-DEx IEPD can be downloaded at it.ojp.gov/iepd.

[36] Ibid.

solve crimes as well as the ability to develop crime trend analysis and predictive crime modeling. Connection to the N-DEx System will be accomplished through one of two methods: CJIS WAN or the Law Enforcement Online/Regional Information Sharing System (LEO/RISS).

Joint Automated Booking System

The Joint Automated Booking System (JABS) is an information-sharing initiative for strengthening law enforcement and homeland security activities. The initiative automates the federal booking process and provides a mechanism for rapidly and positively identifying an individual using a fingerprint submission to the FBI's IAFIS. The JABS program is not restricted to DOJ users, but includes other user groups from within the DOJ, DHS, Department of Defense, and the Department of Health and Human Services. JABS added an interagency booking service to provide automated submission of booking packages for federal law enforcement agencies that routinely bring their suspects in for booking. This initiative expanded JABS services to agencies in 11 federal departments outside of DOJ (DHS, Agriculture, Education, Interior, Labor, State, Transportation, Treasury, Veterans Affairs, Housing and Urban Development, and the General Services Administration), as well as the U.S. Postal Service. These agencies can now utilize JABS without having to actually deploy an automated booking station in their offices.[37]

National Virtual Pointer System[36]

For many years, state and local law enforcement envisioned a drug pointer system that would allow them to determine if other law enforcement organizations were investigating the same drug suspect. The DEA was designated by the Office of National Drug Control Policy in 1992 to take the lead in developing a national drug pointer system to assist federal, state, and local law enforcement agencies investigating drug trafficking organizations and to enhance officer safety by preventing duplicate investigations. The DEA drew from the experience of state and local agencies to make certain that their concerns were addressed and that they had extensive input and involvement in the development of the system.

The National Drug Pointer Index (NDPIX) became operational across the United States in October 1997. The National Law Enforcement Telecommunications System (NLETS)—a familiar, fast, and effective network that reaches into almost every police entity in the United States—is the backbone of the NDPIX. Participating agencies are required to submit active case-targeting information to NDPIX to receive pointer information from the NDPIX. The greater the number of data elements entered, the greater the likelihood of identifying possible matches. Designed to be a true pointer system, the NDPIX merely serves as a switchboard that provides a vehicle for timely notification of common investigative targets. The actual case information is shared only when telephonic contact is made between the officers or agents who have been linked by their entries into the NDPIX.

[37] www.usdoj.gov/jmd/ocio/leisp/initiatives.htm

[38] See www.dea.gov/programs/ndpix.htm.

NDPIX was developed for five reasons: 1. To promote information sharing; 2. To facilitate drug-related investigations; 3. To prevent duplicate investigations; 4. To increase coordination among federal, state, and local law enforcement agencies; and 5. To enhance the personal safety of law enforcement officers.

NDPIX has been transitioned and upgraded to the National Virtual Pointer System (NVPS). A steering committee—which included DEA, HIDTA, RISS, the National Drug Intelligence Center (NDIC), the National Institute of Justice, ,the National Sheriffs' Association, the International Association of Chiefs of Police (IACP), and the National Alliance of State Drug Enforcement Agencies—developed the specifications for the system and is overseeing its testing and transition.

Characteristics of the NVPS will include the following:

- Covers all crimes, not just drugs.
- Accepts only targets of open investigations with assigned case numbers.
- Transaction format contains an identifying field for the NVPS Identifier.
- Uses a secure telecommunications network.
- Uses the NDPIX "Mandatory" data elements.
- Single sign-on from any participant allows access to all participating pointer databases.
- Each system provides a user ID and password to its respective users.
- Each system maintains its own data.
- Uniform Crime Reporting or the National Incident-Based Reporting System codes are used to identify type of crime.
- Targets deconfliction for all crimes.
- Will rely on web-based communications.
- Has links with HIDTA and RISS.

This upgrade of the system to the NVPS represents an important development for a comprehensive national pointer system.

Federated Identity Management Pilot

The Federated Identity Management (FIDM) pilot, sometimes known as a single sign-on, now in its second year, is an SBU/CUI initiative funded by the Program Manager's Office of the Information Sharing Environment. The objective is to provide and test an agreed-on standard for authenticating users and remove impediments they may experience while accessing mission-critical data. Benefits include a simpler, more reliable authentication process, thereby providing users with quicker access to data. The U.S. Department of Justice is validating this concept and supporting technologies as they relate to the law enforcement environment and testing specific architecture of the federation believed to be the most appropriate for the LEISP mission.[39]

SLTLE agencies, notably through the Criminal Intelligence Coordinating Council, have been urging adoption of this model. Not only does having an array of different user names and passwords slow the process of seeking information from

[39] www.usdoj.gov/jmd/ocio/leisp/initiatives.htm

different systems, but also users are more likely to use only one or two systems, rather than all that are available because of the cumbersome multiple logons. If users are not fully accessing all available systems, valuable information related to an intelligence inquiry or criminal investigation may not be discovered. While the technology and architecture are in place with the FIDM project, the biggest challenge that remains is related to policy; that is, governing boards of the different systems appear to be reluctant to embrace FIDM as a means of accessing their systems.

Federal Bureau of Investigation Intelligence Initiatives[40]

The Federal Bureau of Investigation (FBI) has stated that to meet its security mission it must gather information and share intelligence with both the domestic law enforcement community and the Intelligence Community concerning all threats, whether from gangs, organized crime, or al Qaeda. As a means to enhance the effectiveness of this responsibility, the FBI developed the Strategic Execution Team (SET).

Through the SET, the FBI is establishing new baseline capabilities for its intelligence process to improve overall performance. The new field intelligence structures and processes have at their foundation the recognition that working seamlessly with SLTLE is essential to protecting America. Law enforcement partners are key customers for FBI intelligence products and the goal is to ensure that those products respond to customer needs.

Integrating Intelligence into the Criminal Programs

After the attacks of September 11, 2001, the FBI shifted resources away from its criminal programs to focus on counterterrorism. During the past few years, as the FBI's counterterrorism capabilities improved and the Bureau grew in size, some resources have been restored to the criminal programs to deal with ongoing threats posed by these groups. During the change process, the FBI recognized the need to develop a capacity to be more predictive and preventive for all crimes within its jurisdiction; that is, in addition to investigating crimes after the fact for prosecution, the Bureau must collect and act on intelligence to detect, disrupt, and dismantle criminal enterprises that pose the greatest threat to society.

While a great deal of progress has been made since 9/11 in developing the FBI's intelligence capabilities, these efforts have focused largely on the national security programs. For many agents working criminal matters, intelligence has been perceived as something done by the other side of the house. A key goal of SET is to change this dynamic to fully integrate intelligence into the criminal programs, to strengthen those programs by making them more intelligence-driven, and ultimately to be one coordinated FBI with a single unified process for intelligence that cuts across all programs.

Impact on Law Enforcement Partners:

- The FBI will provide a more intelligence-driven national and regional approach to criminal investigations.
- There will be an increase in FBI intelligence reports about criminal matters.

[40] The information in this section is based on an internal FBI Report entitled *Implementation of New Field Intelligence Operations: Executive Summary.* April 30, 2008.

Standardize Field Office Structure and Responsibilities

All field offices will be required to have a centralized strategic coordinating component in its Field Intelligence Group (FIG) that will: 1. Help the office fully understand the key threats in their domains and what resources the FBI has to bring to bear on each threat; 2. Ensure that the FBI fully capitalizes on collection capabilities to meet intelligence requirements; and 3. Develop a collection plan to address any gaps.

All field offices will also have a dedicated chief reports officer who will ensure that the office disseminates timely, relevant, and high-quality intelligence to outside partners.

Impact on Law Enforcement Partners:

- There will be uniform structures, positions, and processes across all FBI field offices, making it easier to work with the FBI.

Develop a Domain Management Process

A dedicated Domain Management team on the FIG will pull together information from inside and outside the field office to develop a thorough understanding of the office's territory and the threats and vulnerabilities within. The team will produce the Domain Assessment, a product that takes the synthesized data, adds perspective and context, and recommends specific courses of action. It will answer the fundamental question, "What can we do about it?" The team will also produce a Common Operational Picture, a map representation of the territory, combining open source data on the territory's infrastructure and demographics, and field office data on case subjects, sources, and vulnerabilities.

After creating the initial baseline Domain Assessment and the Common Operational Picture (COP), the team will continuously improve them by identifying what is not known but should be known, i.e., intelligence gaps, and taking action to address them. Domain Management will help FBI managers guide the office's activities and also inform national domain management efforts. It will improve the Bureau's ability to proactively identify threats, manage current investigative activities strategically, and identify new opportunities for information collection and for prosecution.

Impact on Law Enforcement Partners:

- As the FBI develops local, regional, and national pictures of particular threats, particularly criminal threats, the Bureau has committed to share these assessments with law enforcement partners.
- As the domain awareness is developed and continuously improved, the FBI will have better strategic intelligence to share with SLTLE about criminal and national security threats that require attention. If there is the presence of a particular gang or domestic terrorist group, for example, it would benefit local law enforcement to know what trends the FBI is seeing with those groups across the country. It would help local law enforcement know how they are financed, how they recruit, and what their leadership structure looks like. The FBI will develop and share with SLTLE such crime-related assessments.

Develop a Collection Management Process

Collection Management is a formal business process through which the field office's identified intelligence gaps and needs are prioritized into requirements that feed into a comprehensive plan. Elements of that plan are assigned to various squads (and ultimately sources) for resolution. The results are monitored and retasked, as required. Through Collection Management, the FIG will help the field office manage competing demands for intelligence collection, including the need to collect information to further case investigations, to follow threat leads, to conduct liaison and build partnerships, to help meet intelligence requirements from the law enforcement and Intelligence Communities, to complete the COP, to improve the FBI's understanding of a particular issue, and to support regional and national efforts. These requirements will be consolidated and prioritized through a careful balancing of factors, including an analysis of each case, to determine the level of threat represented, national and regional priorities, vulnerabilities and knowledge gaps in the territory and prioritized requirements, and specific requests from SLTLE.

Impact on Law Enforcement Partners:

- Local law enforcement will have a standardized, routine process for submitting, prioritizing, and resolving intelligence requirements.

Enhance Collection

The vast majority of the FBI's intelligence collection occurs in its operational squads. To fully leverage the Bureau's existing source base, the SET plan includes training and information technology tools to increase agents' awareness of priority requirements. Where staffing levels permit, operational squads will be assigned embedded intelligence analysts who will ensure that information collected during the squad's normal course of duties is analyzed and appropriately forwarded to the FIG for dissemination, domain awareness, and/or gap identification.

To further strengthen FBI collection capabilities, all field offices must also have a dedicated team of intelligence special agents assigned to the FIG. These agents will use the full range of appropriate human intelligence (HUMINT) tradecraft and operational skills to develop, recruit, and exploit sources, and leverage relationships with external partners in order to collect information about the most critical gaps. The intelligence special agents will not work on cases for prosecution, but will provide cross-program support, collecting information about counterterrorism, counterintelligence, cyber, and criminal program requirements.

Impact on Law Enforcement Partners:

- Improved information flow between operational squads and the FIG will result in dissemination of more raw intelligence from those squads. The greatest change will be in the criminal programs that historically have not focused on requirements-based intelligence collection.

Enhance Liaison

Recognizing that SLTLE agencies are key eyes and ears in the community, the FBI aslo recognizes that enhanced liaison is a vital component establishing a proactive posture against threats to the U.S. Under the SET plan, the FIG HUMINT squad will

serve as the coordinating hub of all field office liaison activities. It will not absorb relationships established in other squads or programs, but these relationships will be centrally coordinated to ensure common messaging and deconfliction of multiple requests for information from the same entity. Some agents assigned to the FIG will serve in an official liaison role and will coordinate with (and in some cases embed themselves with) federal, state, and local law enforcement agencies. They will work to better understand the intelligence needs of SLTLE, leverage non-FBI sources capable of collecting critical information, and make it easier for SLTLE to leverage FBI resources across the entire FBI and the U.S. Intelligence Community.

Impact on Law Enforcement Partners:

- The standardized liaison program will facilitate the two-way flow of intelligence, allowing the FBI and SLTLE to better leverage each other's domain knowledge, liaison contacts, and sources. Local law enforcement will have a single point of contact that will enable each agency to more easily tap into the FBI knowledge base of criminal and terrorist threats.
- Collectively, the FBI will be better positioned to use mechanisms—without duplication or conflict—that provide early warning on the most critical threats.
- The FBI will continue a high level of participation in fusion centers. The intelligence that is gathered will be shared through these fusion centers, as appropriate.

Improve Production and Dissemination

Field offices will improve the quality of their intelligence products through formal training, including basic and advanced training for reports officers. The chief reports officer will provide the necessary technical expertise and oversight to address content and other measures of quality such as technical tradecraft, standardization, and substantive accuracy.

The timeliness of FBI intelligence products will be improved by streamlining the production and approval process, removing duplicative steps and approvals, and enabling direct dissemination from field offices, where appropriate.

To ensure that intelligence products are relevant to FBI customers' needs, Intelligence Information Reports (IIR) will be tied to specific intelligence requirements from the beginning of the production process. Strong mechanisms for receiving feedback will be implemented. New metrics will also assess each field office's throughput, the ratio of IIRs actually disseminated to the Intelligence Community to the total number of IIRs submitted to FBI headquarters.

Impact on Law Enforcement Partners:

- SLTLE will see improvements in the quality of FBI intelligence products. FBI products from across the field will have a uniform look and feel.
- SLTLE will receive raw intelligence reports more quickly.
- More intelligence will be directly responsive to SLTLE requirements.
- SLTLE will see more intelligence reporting originating from criminal squads.

Terrorist Screening Center[41]

The Terrorist Screen Center (TSC) was created to ensure that government investigators, screeners, agents, and state and local law enforcement officers have ready access to the information and expertise they need to respond quickly when a suspected terrorist is screened or stopped. The TSC consolidates access to terrorist watch lists from multiple agencies and provides 24/7 operational support for thousands of federal screeners and state and local law enforcement officers across the country and around the world. The intent of the TSC is to ensure that federal, state, and local officials are working off the same unified, comprehensive set of antiterrorist information.

Since its implementation on December 1, 2003, the TSC has provided the following:

- A single coordination point for terrorist screening data
- A consolidated 24/7 call center for encounter identification assistance
- A coordinated law enforcement response to federal, state, and local law enforcement
- A formal process for tracking encounters and ensuring that feedback is supplied to the appropriate entities.

The TSC created the terrorist screening database (TSDB), a single, comprehensive source of known or appropriately suspected international and domestic terrorists. These data are available to local, state, and federal law enforcement officers through the NCIC. When a police officer queries the NCIC, he or she may receive a notification that the query resulted in the potential match of a record within the TSDB and directs the officer to contact the TSC to determine if it is an actual match. If it is, the TSC transfers the call to the FBI's CT Watch to provide operational guidance to the officer.

Consolidated Terrorist Screening Database

The TSC receives international and domestic terrorist identity records and maintains them in its consolidated TSDB. The TSC reviews each record to determine which are eligible for entry into the NCIC's Violent Gang and Terrorist Organization File (VGTOF) and once the record is entered into the NCIC, it is accessible by state, local, and federal law enforcement officers. If a query by a law enforcement officer matches a name in the NCIC, the officer will be requested, through the NCIC printout, to contact the TSC. The printout also provides the officer with instructions for arresting, detaining, questioning, or releasing the subject. If the TSC determines that the person encountered by the officer is a match with a person in the NCIC/VGTOF file, the officer is immediately connected to the FBI's CT Watch for operational guidance. Depending on the situation, the CT Watch may dispatch a local Joint Terrorism Task Force (JTTF) agent to assist the law enforcement officer. Information that the officer obtained through the encounter is then sent back to the originating agency.

An example will illustrate the TSC's processes. On August 20, 2004, as two off-duty police officers were traveling across the Chesapeake Bay Bridge between

[41] Information for this section was gained from interviews and reviews of various courses, including testimony and press releases at www.fbi.gov/congress/congress04/bucella012604.htm, www.fbi.gov/pressrel/pressrel03/tscfactsheet091603.htm, and www.cia.gov/news-information/speeches-testimony/2003/wiley-speech-62262003.html.

southeastern Virginia and the Delmarva Peninsula, they observed individuals filming the structure of the bridge. The officers reported the suspicious activity to the Maryland Transportation Authority (MTA) who conducted a traffic stop of the vehicle. The MTA officers ran an NCIC check on one of the occupants of the car and learned that the individual may have a record within the TSDB. At the NCIC's request, the officers contacted the TSC and learned that the individual was the subject of the TSDB record. The TSC transferred the call to the FBI's CT Watch who informed the MTA that the individual was an alleged co-conspirator in a significant terrorism case. The FBI arrested the subject on a material witness warrant, and a search warrant executed at the subject's residence turned up valuable evidence. This new level of information-sharing and cooperation among state, local, and federal law enforcement agencies enhances our ability to prevent a terrorist attack within the United States.

Law Enforcement Online[42]

Law Enforcement Online (LEO) is an online service operated by the FBI for law enforcement, first responders, and criminal justice officials. Law enforcement personnel interested in signing up for LEO simply have to fill out a LEO application and submit it to their local FBI office for approval. The LEO site contains the following resources"

- *Topical Focus Area.* Custom web-type pages that provide a secure community area for general information related to the law enforcement profession using text, graphics, audio, and video.
- *Law Enforcement Special-Interest Groups.* Segmented areas with multilevel controlled access for specialized law enforcement groups that have their own members.
- *E-mail.* Provides the capability to send and receive secure e-mail/messages electronically between LEO users and RISS users.
- *Chat*. The ability to have a real-time discussion among users (through a keyboard) on three levels; one-to-one, groups, and the Electronic Academy for presentations or question-and-answer sessions.
- *Feedback*. The capability to survey users for input on various topics.
- *Electronic Calendar.* Provides national, state, and special-interest calendars for posting upcoming dates of interest for conferences, meetings, training courses, seminars, and other important dates.
- *Topical Electronic Library.* An easily accessed repository of a broad range of publications, documents, studies, research, technical bulletins, and reports of interest to the law enforcement community. The library will provide indexed and full-text retrieval capability. Material for this component is expected to come from the entire law enforcement and education communities.
- *Distance Learning.* Online topical learning modules that can be used any time of the day or night at the user's own pace with instructional feedback

In addition, *FBI Intelligence Assessments, FBI Intelligence Bulletins, and FBI Intelligence Information Reports* are available on the LEO web site, as well as other items of interest related to the FBI intelligence program. To obtain access to LEO, contact the training coordinator at the local FBI field office.[43]

[42] The LEO web page is www.fbi.gov/hq/cjisd/leo.htm.

[43] www.fbi.gov/contact/fo/fo.htm

Guardian and eGuardian

The FBI's Guardian system is a federal classified system restricted for FBI use. The system records suspicious activity that is pre-investigation, pre-case, nonintelligence data with a nexus to terrorism.[44] Because Executive Order 13388 requires federal sharing of terrorist threat information with local law enforcement, the FBI is making portions of the Guardian database visible to law enforcement through LEO. The initiative to allow local law enforcement to have access to the system is called eGuardian. Eventually, the eGuardian project will also include a way for state and local agencies to report suspicious activity in addition to reviewing information gathered by FBI agents.

eGuardian utilizes the existing system and its capabilities by filtering classified information. It facilitates the sharing of critical unclassified data stored within the system and enhances interagency threat assessment and coordination, thereby enabling federal, state, local, and tribal law enforcement to obtain, share, integrate, and use the unclassified threat and incident data from Guardian. It also provides incident capture, searching, reporting, and trend analysis capabilities for these agencies.

eGuardian has a robust incident management system, allowing users to create, update, and search incidents. Any number of people, places, vehicles, weapons, or other pieces of information can be added to an incident. Additionally, the system allows users to attach any kind of file to an incident, including documents, images, videos, and audio clips. In addition to incident management, eGuardian offers other capabilities for data analysis, data optimization, and data segmentation as well as a search capacity similar to that of Internet search engines.

Department of Homeland Security Intelligence and Analysis Directorate

The mission of DHS Office of Intelligence and Analysis (I&A) is to provide homeland security intelligence to the Secretary, the operating components, and headquarters offices as well as to our state, local, tribal, and private-sector partners. I&A, a member of the Intelligence Community, ensures that any information related to protecting the homeland is collected, processed, analyzed, and disseminated to the full spectrum of domestic customers. It provides threat warning, estimative, and alternative analysis. In addition, it also provides intelligence support to infrastructure protection and vulnerability studies. I&A works closely with DHS component intelligence organizations (such as Immigration and Customs Enforcement, Customs and Border Protection [CBP], and others) to ensure that nontraditional streams of domestic information are fused with traditional sources of information from other members of the Intelligence Community to give a complete picture of potential threats to the nation.[45]

DHS has a lead role in providing threat information, situational awareness, and context about nuclear threats to SLTLE as well as private-sector partners. Given the technical nature of nuclear devices and the broad customer base, DHS is providing baseline information on how a field officer might identify components of a nuclear device, differentiate radiological from nuclear devices, training on the

[44] Coleman, Gerry, "Next Generation: CJIS?", *Time System Newsletter* (Wisconsin Department of Justice Crime Information Bureau) 2006-1 (March 2006): p. 1.

[45] Allen, Charles E. *Testimony of the Under Secretary for Intelligence and Analysis before the Senate Committee on Homeland Security and Governmental Affairs: Assessing the Nuclear Attack Threat,* April 2, 2008.

potential effects of a nuclear device, and ensuring that our partners understand the range of effects from a nuclear device. DHS provides this information through unclassified and classified products, as well as secure video teleconferences and in-person threat briefings at state and local fusion centers.

Part of the DHS effort to enhance information-sharing with SLTLE agencies was creation of the Fusion Process Technical Assistance Program Resource Center as a joint initiative between I&A and the DHS Preparedness Directorate. In addition, the program works closely with intelligence and counterterrorism initiatives of the U.S. Bureau of Justice Assistance. The online program serves as a directory of all fusion centers as well as a resource for intelligence-related documents ranging from model policies to lessons learned. It is a dynamic resource available to SLTLE who are registered users of the DHS LLIS web site.[46]

DHS I&A has aggressively developed an intelligence capacity that is consistent with established processes and principles used in the Intelligence Community. Beyond that, I&A has developed new initiatives to increase two-way information-sharing with SLTLE agencies:

- DHS I&A has deployed analysts to many fusion centers at the state and local level across the country. The goal is to have a DHS analyst in all primary state fusion centers. As of this writing, about 35 intelligence analysts had been assigned.
- Trained intelligence reports officers deployed to DHS components provide *Homeland Intelligence Reports* to the rest of the Intelligence Community containing information gleaned from contacts at the borders. I&A has issued nearly 3,000 such reports in the past year, sharing valuable information about transnational threats from the Caribbean and Latin America, sensitive information from ports of entry, and data from people who are given secondary screening or who are denied entry into the United States.
- I&A has raised its visibility with the Intelligence Community, sitting as a full participant in Intelligence Community forums and working hand-in-hand with partners at the Director of National Intelligence, the FBI, and National Counterterrorism Center (NCTC).
    - The I&A has formed the Interagency Threat Assessment and Coordination Group (ITACG) with the FBI, NCTC, and SLTLE. It is located in the NCTC, under NCTC management, but with DHS and FBI senior officers leading it. ITACG officers monitor sensitive databases each day to determine what can be sanitized and sent to state and local partners.
    - I&A contributes to the daily *National Terrorism Bulletin* and *President's Daily Brief* and disseminates joint advisories with the FBI, mostly at the SBU/CUI level, to ensure maximum reach to state, local, and private-sector partners.
    - I&A is establishing a National Applications Office that will use satellite imagery, not only for civil applications, but to support homeland security efforts.[47]

Homeland Security Information Network[48]

The Homeland Security Information Network (HSIN) is a secure, Internet-based system of integrated communication networks designed to facilitate information-sharing between DHS and other federal, state, county, local, tribal, private-sector commercial, and other nongovernmental organizations involved in identifying

[46] Users must first register at www.llis.dhs.gov. Once the user is given access to LLIS, he or she e-mails a request to have access to the Fusion Process Technical Assistance Program Resource Center. www.llis.dhs.gov/channel/channel.do?id=90287.

[47] Allen, Charles E. DHS Under Secretary for Intelligence and Analysis. *Charles E. Allen Address to the Washington Institute for Near East Policy,* Washington, D.C.: May 6, 2008. www.dhs.gov/xnews/speeches/sp_1210107524856.shtm.

[48] Information in this section is based largely on: *Privacy Impact Statement for the Homeland Security Information Network Database.* Unpublished report of the DHS Office of Operations Coordination, April 5, 2006. www.dhs.gov/xlibrary/assets/privacy/privacy_pia_hsind.pdf.

and preventing terrorism and undertaking incident management activities. The mission of HSIN is to enhance the communication of relevant information among all applicable domestic security actors regardless of jurisdictional, geographic, or agency boundaries. Additionally, HSIN enables these organizations to maintain voice and data communications with one another during incident management. The HSIN is managed by the National Operations Center (NOC).

The system supports its user community by enabling approved users to research and analyze information with a nexus to terrorism. The database within HSIN is populated with information from: Suspicious Activity Reports from law enforcement, governmental agency, or private-sector security officials; law enforcement bulletins and reports from federal, state, county, local, and/or tribal law enforcement, and relevant information from approved HSIN user's communications. Prior to inclusion in the HSIN, information will be reviewed by NOC personnel to ensure a nexus to terrorism. After a nexus is established, the information is put into categories according to sector, subject matter, geography, and need to know.

Data collected for HSIN focuses primarily on activities, rather than on individuals. It consists of reports about what individuals, either law enforcement or other persons, have observed that is out of the ordinary based on their judgment, experience, and the circumstance of their observation. In most but not all cases, such observations will not include PII, but instead, the facts of a situation. In instances where the observation or incident led to PII being obtained, the information will be logged into the HSIN database, and additional safeguards will be used, including masking the information. The data that included names would be available only to those whose roles authorize them to access and collect such information, primarily law enforcement personnel and the Intelligence Community. Other users, such as private-sector security managers, would be able to access only the activity-based information; private and other sensitive data would be masked. If they have the need for more information, private-sector users will either contact the source entity (such as another private-sector entity) or look to local law enforcement for additional information that they might be eligible to receive.

The HSIN database will collect relatively raw suspicious activity information, which generally is provided by individuals who observe the activities of others and deem that activity suspicious, based on the totality of observable circumstances. While the primary focus of the information will be on activities, the personally identifiable information accepted for retention as part of a particular submission may include full name, address, date of birth, place of birth, citizenship, physical description (height, weight, eye and hair color), distinguishing scars, marks, or tattoos, automobile registration information, watch list information, intelligence information including links to terrorism, any criminal and/or incident activity, the date information is submitted, and the name of the contributing/submitting organization. The system has the capability to analyze data in a manner that identifies potential threats to the homeland or trends requiring further analysis.

The following are among the other capabilities of HSIN:

Communications
- Low-cost, always-on connectivity
- End-to-end encrypted communications

Collaboration/Analysis
- Secure e-mail
- Interactive collaboration tool (real-time text or voice)
- Supports requests for information, exchange, and cross-reference
- Search and link/timeline analysis, map/imagery displays

Information
- Daily, periodic, and ongoing report sharing.
- Suspicious incident/pre-incident indicator data.
- Media studies and analysis.
- Mapping and imaging (national, state, county, city).
- Critical Infrastructure Protection repository.
- Strategic analysis of terrorist threats, tactics, and weapons

A long-term goal of the HSIN is to have seamless connectivity among the different portals that serve the law enforcement and homeland security communities.

Homeland Security–State and Local Intelligence Community of Interest (HS SLIC)

To foster collaboration and share best practices and lessons learned within the fusion center network, DHS sponsors the Homeland Security State and Local Intelligence Community of Interest (HS SLIC). This is a virtual community of intelligence analysts who not only share threat information but also analytic techniques. Its membership has grown significantly and now has members representing 43 states, the District of Columbia, and seven federal departments. An HS SLIC Advisory Board, which includes state and local intelligence leaders, advises the I&A leadership on issues relating to intelligence collaboration between the federal government and its state, local, and tribal partners. Through the HS SLIC, intelligence analysts across the country collaborate through weekly SBU/CUI threat teleconferences, biweekly Secret-level secure video teleconferences, and in a virtual community of interest within a restricted portion of the HSIN-Intelligence platform, to share sensitive information in an appropriately secure and privacy sensitive environment. Members are thus able to post intelligence products so that there is effective vertical information-sharing between the states and the Intelligence Community and horizontally between the states.[49]

National Counterterrorism Center (NCTC)[50]

In July 2004, the National Commission On Terrorist Attacks Upon the United States recommended the establishment of a National Counterterrorism Center (NCTC)

[49] Allen, Charles E. *Information Sharing at the Federal, State, and Local Levels. Statement for the Record before the United States Senate Committee on Homeland Security and Governmental Affairs,* July 23, 2008.

[50] The public NCTC web site is www.nctc.gov.

to serve as a center for "... joint operational planning and joint intelligence, staffed by personnel from the various agencies...." On August 27, 2004, the President signed *Executive Order 13354, National Counterterrorism Center,* which established the NCTC and stipulated roles for it and its leadership and reporting relationships between NCTC leadership and NCTC member agencies, as well as with the White House. In December 2004, Congress passed the Intelligence Reform and Terrorism Prevention Act and, like the preceding Executive Order, among many other reform initiatives, the act prescribes roles and responsibilities for the NCTC and its leadership.[51]

NCTC operates as a partnership of organizations that include the Intelligence Community, law enforcement, and government agencies representative of the U.S. critical infrastructure. The NCTC is responsible for managing integrated meetings with its partners related to all aspects of terrorists' threats, both domestically and abroad. The ostensible purpose for the creation of intelligence centers, including the NCTC, is to bring together the disparate elements of the Intelligence Community having different intelligence foci and missions in order to achieve common intelligence and national security objectives.

A critical part of the NCTC mission is to develop intelligence products related to terrorism threats, including the following:

- Daily analytic products for senior U.S. government officials and the broader counterterrorism community
- A daily accounting of threat reporting and actions taken
- In-depth analytic assessments of the full range of terrorist topics
- Analysis providing alternative views on terrorism issues
- Situational awareness reports of terrorist threats, incidents, and reported plots worldwide
- Alerts, advisories, warnings, and assessments on topics of interest that are widely disseminated to domestic and overseas operators and analysts
- Strategic operational plans integrated and synchronized across U.S. Government agencies, describing specific objectives, department/agency roles and responsibilities, tasks, and activities for counterterrorism.[52]

Consistent with applicable law and direction from the President, the NCTC may receive intelligence pertaining exclusively to domestic counterterrorism from any federal, state, local, or tribal government, or other source necessary to fulfill its responsibilities and retain and disseminate such intelligence.[53]

The NCTC serves as the central and shared knowledge bank on known and suspected terrorists and international terror groups; ensures that agencies, as appropriate, have access to and receive all-source intelligence support needed to execute their counterterrorism plans or perform independent, alternative analysis; and ensures that such agencies have access to and receive intelligence needed to accomplish their assigned activities. Any agency authorized to conduct counterterrorism activities may request information from the NCTC to assist it in its activities, consistent with applicable law and guidelines provided for the provision of, and access to, intelligence. The NCTC enables the sharing of a wide

[51] Masse, Todd. *The National Counterterrorism Center: Implementation Challenges and Issues for Congress.* Washington, D.C.: Congressional Research Service, 2005, p. ii.

[52] www.nctc.gov/about_us/products.html

[53] Program Manager–Information Sharing Environment. *Information Sharing Environment Implementation Plan.* Washington, D.C.: Office of the Director of National Intelligence, 2006.

spectrum of terrorism intelligence and related information among thousands of users in the federal counterterrorism community through its secure web site that operates in separate security domains.[54] While SLTLE agencies have access to this information, for the most part that access is limited and accessible through the fusion centers.

Regional Information Sharing System

The Regional Information Sharing System® (RISS) has been in operation since 1973 providing services supporting the investigative and prosecution efforts of law enforcement and criminal justice agencies. The network was founded in response to transjurisdictional crime problems and the need for cooperation and secure information-sharing among law enforcement agencies.

Today, RISS is a national network comprising six multistate centers operating regionally.

- **Middle Atlantic-Great Lakes Organized Crime Law Enforcement Network.**[55] Delaware, Indiana, Maryland, Michigan, New Jersey, New York, Ohio, Pennsylvania, and the District of Columbia. The center also has member agencies in England, Australia, the Canadian provinces of Ontario and Quebec.
    - 140 Terry Road, Suite 100
      Newton, PA 18940
      Telephone: 215.504.4910
      E-mail: info@magloclen.riss.net
- **Mid-States Organized Crime Information Center.** Illinois, Iowa, Kansas, Minnesota, Missouri, Nebraska, North Dakota, South Dakota, and Wisconsin. The center also has member agencies in Canada.
    - 1610 E. Sunshine Drive, Suite 100
      Springfield, MO 65804
      Telephone: 417.883.4383
      E-mail: info@mocic.riss.net
- **New England State Police Information Network.** Connecticut, Maine, Massachusetts, New Hampshire, Rhode Island, and Vermont. The center also has member agencies in Canada.
    - 124 Grove Street, Suite 305
      Franklin, MA 02038
      Telephone: 508.528.8200
      E-mail: info@nespin.riss.net
- **Regional Organized Crime Information Center.**[56] Alabama, Arkansas, Florida, Georgia, Kentucky, Louisiana, Mississippi, North Carolina, Oklahoma, South Carolina, Tennessee, Texas, Virginia, and West Virginia, Puerto Rico, and the U.S. Virgin Islands.
    - 545 Marriott Drive, Suite 850
      Nashville, TN 37214
      Telephone: 615.871.0013
      E-mail: info@rocic.riss.net

[54] Ibid.

[55] www.riss.net/centers.aspx?9=MAGLOCLEN

[56] www.rocic.com

- **Rocky Mountain Information Network.**[57] Arizona, Colorado, Idaho, Montana, Nevada, New Mexico, Utah, and Wyoming. The center also has member agencies in Canada.
    - 2828 N. Central Avenue, Suite 1000
      Phoenix, AZ 85004
      Telephone: 602.351.2320
      E-mail: info@rmin.riss.net
- **Western States Information Network.** Alaska, California, Hawaii, Oregon, and Washington. The center also has member agencies in Canada, Australia, and Guam.
    - 1825 Bell Street, Suite 205
      Sacramento, CA 92403
      Telephone: 916.263.1166
      E-mail: info@wsin.riss.net

The regional approach allows each center to offer support services tailored to the needs of member agencies, although the centers also provide services and products that are national in scope and significance. Typical targets of RISS-member agencies' activities are terrorism, drug trafficking, violent crime, cybercrime, gang activity, and organized crime. While the RISS network is funded by the U.S. Bureau of Justice Assistance, it is controlled by its member agencies; therefore, state and local law enforcement agencies establish priorities as well as decisions related to services, such as secure client e-mail systems.

Traditional support services provided to law enforcement member agencies from the RISS centers include the following:

- Information-sharing resources
- Analytical services
- Loan of specialized investigative equipment
- Confidential funds
- Training conferences
- Technical assistance.

RISS.NET

RISS operates a secure intranet, known as RISS.NET, to facilitate law enforcement communications and information-sharing nationwide. RISS local, state, federal, and tribal law enforcement member agency personnel have online access to share intelligence and coordinate efforts against criminal networks that operate in many locations across jurisdictional lines. In September 2002, the FBI LEO system interconnected with RISS. In October 2003, the RISS/LEO interconnection was recommended in the *National Criminal Intelligence Sharing Plan* as the initial SBU/CUI communications backbone for implementation of a nationwide criminal intelligence-sharing capability. The Plan encourages agencies to connect their systems to RISS/LEO.

[57] www.riss.net/Centers.aspx?9=RMIN

Automated Trusted Information Exchange

In April 2003, RISS expanded its services and implemented what was initially called the Anti-Terrorism Information Exchange and later changed to its current name, the Automated Trusted Information Exchange (ATIX) to provide users with access to homeland security, disaster, and terrorist threat information. RISS member agencies, as well as executives and officials from other first-responder agencies and critical infrastructure entities, can access the system. ATIX consists of a web site and connected services hosted on the RISS network. It is designed for use by officials from government and nongovernment organizations who are responsible for planning and implementing prevention, response, mitigation, and recovery efforts for terrorist attacks and disasters. The ATIX program serves state, county, local, and tribal government executives; federal government executives and agencies; regional emergency management; law enforcement and criminal justice organizations; fire departments; agriculture; disaster relief; special rescue units; and telecommunication and transportation.

The web site features secure e-mail and information such as DHS bulletins and advisories, terrorist threat-level alerts, advisories from different government units such as the Department of Transportation, and has areas where users can post and share data specific to their occupational communities (e.g., law enforcement, military, emergency services, etc.).

In each community section on the web site, users can establish collaborative electronic conference services, virtual bulletin boards, and live chat rooms. Member groups also create most of the ATIX site's content and bulletin board posts. Each conference has a live chat feature where users can post conversation threads and discuss topics. An on-screen paging function permits users to notify others if they need to shift a conversation to the telephone or to a face-to-face discussion.

ATIX is informative, user-friendly, and an important resource for law enforcement agencies of any size. The site requires access to the Internet through a secure portal to permit communications. To obtain access to ATIX, the potential user must contact the applicable RISS center and request enrollment from the appropriate state coordinator.

Drug Enforcement Administration[58]

Since it was established in 1973, the Drug Enforcement Administration (DEA), in coordination with other federal, state, local, and foreign law enforcement organizations, has been responsible for the collection, analysis, and dissemination of drug-related intelligence. The role of intelligence in drug law enforcement is critical. The DEA Intelligence Program helps initiate new investigations of major drug organizations, strengthens ongoing investigations and subsequent prosecutions, develops information that leads to seizures and arrests, and provides policymakers with drug trend information on which they can base programmatic decisions. The specific functions of the DEA's intelligence mission are as follows:

- Collect and produce intelligence in support of the administrator and other federal, state, and local agencies
- Establish and maintain close working relationships with all agencies that produce or use narcotics intelligence
- Increase the efficiency in the reporting, analysis, storage, retrieval, and exchange of such information
- Undertake a continuing review of the narcotics intelligence effort to identify and correct deficiencies.

The DEA's Intelligence Program has grown significantly since its inception. From only a handful of intelligence analysts in the domestic offices and Headquarters in 1973, the number of intelligence analysts worldwide is now more than 680. DEA's Intelligence Program consists of several entities that are staffed by both intelligence analysts and special agents: intelligence groups and functions in the domestic field divisions, district, resident, and foreign offices, the El Paso Intelligence Center, and the Intelligence Division at DEA Headquarters. Program responsibility for the DEA's intelligence mission rests with the DEA Assistant Administrator for Intelligence.

Legislation and presidential directives and orders have expanded the role of the Intelligence Community and the Department of Defense in the antidrug effort. DEA interaction with both components occurs daily in the foreign field and at Headquarters. At the strategic intelligence level, the Intelligence Division participates in a wide range of interagency assessment and targeting groups that incorporate drug intelligence from the antidrug community to provide policymakers with all-source drug trend and trafficking reporting.

With analytical support from the Intelligence Program, the DEA has disrupted major trafficking organizations or put them entirely out of business. The DEA Intelligence Division also cooperates a great deal with state and local law enforcement and will soon provide intelligence training for state, local, federal, and foreign agencies. This training will be held at the Justice Training Center in Quantico, Virginia, and will address the full spectrum of drug intelligence training needs. The best practices and theories of all partners involved in the drug issue will be solicited and incorporated into the training. Academic programs, the exchange of federal, state, and local drug experience, and the sharing of, and

[58] A number of DEA strategic intelligence reports are available online at www.dea.gov/pubs/intel.htm. For other intelligence reports and related information, contact your nearest DEA Field Office www.dea.gov/agency/domestic.htm.

exposure to, new ideas will result in more effective application of drug intelligence resources at all levels.

The DEA divides drug intelligence into three broad categories: tactical, investigative, and strategic.

1. Tactical intelligence is evaluated information on which immediate enforcement action—arrests, seizures, and interdictions—can be based.
2. Investigative intelligence provides analytical support to investigations and prosecutions to dismantle criminal organizations and gain resources.
3. Strategic intelligence focuses on the current picture of drug trafficking from cultivation to distribution that can be used for management decision-making, resource deployment, and policy planning.

In February 2006, the DEA's Office of National Security Intelligence officially became the 16th member of the Intelligence Community.[59] The designation was necessary because of the DEA's global presence and the fact that terrorists have financed some operations through illegal drug sales. Intelligence Community responsibilities of the DEA are coordinated through the new DEA National Security Branch which is in the Office of Intelligence.[60]

Intelligence Products. Tactical and investigative intelligence is available to SLTLE agencies through local DEA field offices. In addition, intelligence can be shared with SLTLE agencies through secure e-mail. Many strategic intelligence reports are available on the DEA web site.[61] Reports that are law enforcement sensitive"can be obtained through the local DEA office.

El Paso Intelligence Center[62]

The El Paso Intelligence Center (EPIC) was established in 1974 in response to a Department of Justice study that detailed drug and border enforcement strategy and programs. The study proposed the establishment of a southwest border intelligence service center staffed by representatives of the Immigration and Naturalization Service, the U.S. Customs Service, and the DEA. The original EPIC staff comprised 17 employees from the three founding agencies. Initially, EPIC focused on the U.S.-Mexico border and its primary interest was drug movement and immigration violations.

Today, EPIC still concentrates primarily on drug movement and immigration violations. Because these criminal activities are seldom limited to one geographic area, EPIC's focus has broadened to include all of the United States and the Western Hemisphere where drug and alien movements are directed toward the United States. Staffing at the DEA-led center has increased to more than 300 analysts, agents, and support personnel from 15 federal agencies, the Texas Department of Public Safety, and the Texas Air National Guard. Information-sharing agreements with other federal law enforcement agencies, the Royal Canadian Mounted Police, and each of the 50 states ensure that EPIC support is available to those who need it. A telephone call, fax, or e-mail from any of these agencies provides the requestor with real-time information from different federal databases, plus EPIC's own internal database.

[59] Office of the Director of National Intelligence. *Drug Enforcement Administration Element Becomes 16th Intelligence Community Member.* Press Release #6-06, February 17, 2006.

[60] Office of the Inspector General. Audit Division. *The Drug Enforcement Administration Use of Intelligence Analysts. Audit Report 08-23.* Washington, D.C.: U.S. Department of Justice, May 2008. www.fas.org/irp/agency/doj/oig/dea-intel.pdf.

[61] See www.usdoj.gov/dea/pubs/intel.htm.

[62] See www.dea.gov/programs/epic.htm.

In addition to these services, a number of EPIC programs are dedicated to post-seizure analysis and the establishment of links between recent enforcement actions and ongoing investigations. EPIC also coordinates training for state and local officers in the methods of highway drug and drug currency interdiction through its Operation Pipeline program. In addition, EPIC personnel coordinate and conduct training seminars throughout the United States on such topics as indicators of trafficking and concealment methods used by couriers.

In a continuing effort to stay abreast of changing trends, EPIC has developed the National Clandestine Laboratory Seizure Database. EPIC's future course will be driven by the *General Counterdrug Intelligence Plan,* as well. As a major national center in the new drug intelligence architecture, EPIC will serve as a clearinghouse for the High Intensity Drug Trafficking Area's (HIDTA) Intelligence Centers, gathering state and local law enforcement drug information and providing drug intelligence back to the HIDTA Intelligence Centers.

National Drug Intelligence Center[63]

The National Drug Intelligence Center (NDIC), established in 1993, is a component of the U.S. Department of Justice and a member of the Intelligence Community. The *General Counterdrug Intelligence Plan,* implemented in February 2000, designated NDIC as the nation's principal center for strategic domestic counterdrug intelligence. The intent of NDIC is to meet three fundamental missions:

1. Support national policymakers and law enforcement decision-makers with strategic domestic drug intelligence.
2. Support Intelligence Community counterdrug efforts.
3. Produce national, regional, and state drug threat assessments.

The Intelligence Division consists of six geographic units and four specialized units. The six geographic units correspond to the regions of the Department of Justice Organized Crime Drug Enforcement Task Force (OCDETF)[64] program and concentrate on drug trafficking and abuse. The four specialized units include the Drug Trends Unit, the Organized Crime and Violence Unit, the National Drug Threat Assessment Unit, and the National Interdiction Support Unit.

Within the geographic units, NDIC intelligence analysts cover each state and various U.S. territories. Intelligence analysts maintain extensive contacts with federal, state, and local law enforcement and Intelligence Community personnel in all 50 states, the District of Columbia, Puerto Rico, the Virgin Islands, and the Pacific territories of Guam, American Samoa, and the Northern Mariana Islands. NDIC collaborates with other agencies such as the DEA, FBI, U.S. Coast Guard, Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF), the Bureau of Prisons, and the Office of National Drug Control Policy (ONDCP). NDIC is one of four national intelligence centers including the EPIC, the U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN), and the Director of Central Intelligence Crime and Narcotics Center. NDIC also works closely with the HIDTAs and the OCDETF.

[63] See www.usdoj.gov/ndic.

[64] While the OCDETFs are operational entities, not intelligence entities, they are both consumers of intelligence and sources for information collection. For more information see www.usdoj.gov/dea/programs/ocdetf.htm.

Intelligence Products

Threat assessments, NDIC's primary intelligence products, provide policymakers and counterdrug executives with timely, predictive reports of the threat posed by illicit drugs in the United States.

- The *National Drug Threat Assessment,* NDIC's major intelligence product, is a comprehensive annual report on national drug trafficking and abuse trends within the United States. The assessment identifies the primary drug threat to the nation, monitors fluctuations in consumption levels, tracks drug availability by geographic market, and analyzes trafficking and distribution patterns. The report highlights the most current quantitative and qualitative information about availability, demand, production and cultivation, transportation, and distribution, as well as the effects of a particular drug on abusers and on society as a whole.
- *State Drug Threat Assessment* provides a detailed threat assessment of drug trends within a particular state. Each report identifies the primary drug threat in the state and gives a detailed overview of the most current trends by drug type.
- *Information Bulletins* are developed in response to new trends or high-priority drug issues. They are relayed quickly to the law enforcement and intelligence communities and are intended to warn law enforcement officials of emerging trends.

High Intensity Drug Trafficking Areas[65]

The High Intensity Drug Trafficking Areas (HIDTA) Intelligence System has more than 1,500 law enforcement personnel, mostly criminal intelligence analysts, participating full time in more than 60 intelligence initiatives in the 28 HIDTA designated areas throughout the United States. While HIDTA is a counterdrug program, the intelligence centers operate in a general criminal intelligence environment, thereby leveraging all criminal intelligence information for the program's primary mission.[66]

The HIDTA Intelligence System, a core element in the creation and growth of many SLTLE intelligence programs, largely depends on HIDTA program mandates. Each HIDTA must establish an intelligence center co-managed by both a federal and a state or local law enforcement agency. The core mission of each HIDTA Intelligence Center is to provide tactical, operational, and strategic intelligence support to its HIDTA executive board, a group of participating law enforcement agency principals responsible for the daily management of their respective HIDTAs, HIDTA-funded task forces, and other regional HIDTAs. Developing regional threat assessments and providing event and target deconfliction are also among the centers' core missions. These core functions are critical to building trust and breaking down parochialism between and among the participating local, state, and federal law enforcement agencies.

The plan to connect all HIDTA Intelligence Centers through RISS.net was initiated by the HIDTA Program Office at ONDCP in 1999 and completed in mid-2003. The HIDTA Program Office has commissioned interagency and interdisciplinary working committees to develop a national information-sharing plan, focusing on issues relating to legal, agency policy, privacy, technical, and logistical information-sharing matters. HIDTA program and committee personnel are

[65] See www.whitehousedrugpolicy.gov/hidta for HIDTA points of contact.

[66] policechiefmagazine.org/magazine/index.cfm?fuseaction=display_arch&article_id=139&issue_id=11200

coordinating with, and implementing recommendations made by, other information-sharing initiatives such as the Global Justice Information Sharing Initiative and federally sponsored intelligence programs.[67]

Bureau of Alcohol, Tobacco, Firearms and Explosives[68]

The Intelligence Division of Bureau of Alcohol, Tobacco, Firearms and Explosives (ATF) has evolved rapidly as an important tool for the diverse responsibilities of the bureau. Several activities in particular demonstrate the intelligence capability and resources of the ATF.

The ATF, which is now an agency of the Department of Justice, has developed Field Intelligence Groups at each of its 23 Field Divisions strategically located throughout the United States. These intelligence groups meld the training and experience of special agents, intelligence research specialists, industry operations inspectors, and support staff that focus on providing tactical intelligence support for their respective field divisions and their external law enforcement partners. Each Field Intelligence Group works under the authority of a supervisory special agent. The intelligence group supervisors are coordinated by, and work in conjunction with, the Intelligence Division to form a bureau-wide intelligence infrastructure. The Intelligence Division provides indoctrination and training for all Field Intelligence Group supervisors, intelligence officers, and intelligence research specialists.

The ATF maintains intelligence partnerships with the NDIC, EPIC, FinCEN, INTERPOL, the FBI's Counter Terrorism Center, and other international intelligence sources. Furthermore, the ATF maintains an MOU with the six RISSs that represent thousands of SLTLE agencies, pledging to share unique and vital intelligence resources. These external partners are key components of the ATF's *Strategic Intelligence Plan* and the means by which the ATF ensures a maximum contribution to the nation's law enforcement and intelligence communities.

During FY 2000, the Intelligence Division spearheaded the formulation of an MOU with the FBI to collaborate on investigations conducted by Joint Terrorism Task Forces (JTTF) located throughout the United States. This MOU brings ATF's unique knowledge and skills of explosives and firearms violations to the FBI's expertise in terrorism. Among the resources provided by ATF are the online Arson and Explosives National Registry and the Federal Firearms License (FFL) registry.

The Intelligence Division has implemented a state-of-the-art automated case management/intelligence reporting system called N-FOCIS (National Field Office Case Information System). The system consists of two companion applications: N-FORCE for special agents and N-SPECT for industry operations inspectors. Both eliminate redundant manual data entry on hard copy forms and provide a comprehensive reporting and information management application in a secure electronic environment.

[67] As an illustration of the comprehensive and integrated nature of the HIDTA programs and intelligence centers, see www.ncjrs.gov/ondcppubs/publications/enforce/hidta2001/ca-fs.html.

[68] Contact your local ATF Field Office for intelligence products and resources. Offices and contact information can be found at www.atf.gov/field.

N-FOCIS constitutes an online case-management system and electronic central information repository that allows the ATF to analyze and fully exploit investigative intelligence. N-FOCIS epitomizes the strength and unique value of the ATF's combined criminal and industry operations enforcement missions. The Intelligence Division has provided in-service training to many ATF field division special agents, investigative assistants, and inspectors on the use of the N-FOCIS applications. The ATF is planning to expand the N-FOCIS functionality and to integrate N-FOCIS with several key ATF applications including the National Revenue Center, the National Tracing Center, National Arson and Explosive Repository, and the Intelligence Division's Text Management System. This integration plan establishes N-FOCIS as the bureau's information backbone.

The Intelligence Division prepares a wide range of strategic intelligence reports related to the ATF mission that are available to SLTLE. In addition, intelligence is shared with state and local agencies through RISS and the JTTFs. In addition, ATF will readily respond to inquiries wherein SBU/CUI information may be shared.

ATF has also created a series of Regional Crime Gun Centers. The intent of the centers is to integrate gun tracing with ATF intelligence and with the HIDTA Regional Intelligence Centers to suppress gun-related crime.[69]

Federal Protective Service Secure Portal[70]

The DHS's Federal Protective Service (FPS) provides law enforcement and security services to more than 1 million tenants and daily visitors to federally owned and leased facilities nationwide. The FPS protection services focus directly on the interior security of the nation, and require close coordination and intelligence-sharing with the investigative functions within DHS. FPS is a full-service agency with comprehensive law enforcement, response, and communications components.[71]

To support their broad, nationwide role, FPS saw the need to develop a comprehensive online resource to aid in security, threat assessment, law enforcement, and protection of federal buildings, workers, and visitors. From this need, the FPS developed its Secure Portal. The web-based portal supports inter- and intra-agency secure information sharing and collaboration through compartmentalized collaboration tools, document libraries, secure messaging, and community calendars. Custom plug-ins facilitate geospatial awareness of officer safety, homeland security issues, incident reporting, and management of operations.

SLTLE agencies can gain access to the FPS Secure Portal by contacting a local FPS office or going to fps.esportals.net/signup/index.cfm and e-mailing the help desk link for registration.

Financial Crimes Enforcement Network[72]

The Financial Crimes Enforcement Network (FinCEN) brings agencies, investigators, and information together to fight the complex problem of money laundering. Since its creation in 1990, FinCEN has worked to maximize

[69] As an illustration see www.atf.gov/field/newyork/rcgc/index.htm.

[70] fps.esportals.net (Membership required)

[71] www.dhs.gov/xnews/releases/press_release_0154.shtm

[72] See www.fincen.gov.

information sharing among law enforcement agencies and other partners in the regulatory and financial communities. Through cooperation and partnerships, FinCEN's network approach encourages cost-effective and efficient measures to combat money laundering domestically and internationally.

The network supports federal, state, local, tribal, and international law enforcement by analyzing information required under the Bank Secrecy Act (BSA), one of the nation's most important tools in the fight against money laundering. The BSA's record-keeping and reporting requirements establish a financial trail for investigators to follow as they track criminals, their activities, and their assets. Over the years, FinCEN staff has developed its expertise in adding value to the information collected under the BSA by uncovering leads and exposing unknown information contained in the complexities of money laundering schemes.

Illicit financial transactions can take many routes—some complex, some simple, but all increasingly inventive—with the ultimate goal of disguising its source. The money can move through banks, check cashers, money transmitters, businesses, or casinos, and is often sent overseas to become "clean." The tools of the money launderer can range from complicated financial transactions carried out through webs of wire transfers and networks of shell companies, to old-fashioned currency smuggling.

Intelligence research specialists and law enforcement support staff research and analyze this information and other critical forms of intelligence to support financial criminal investigations. The ability to network with a variety of databases provides FinCEN with one of the largest repositories of information available to law enforcement in the country. Safeguarding the privacy of the data it collects is an overriding responsibility of the agency and its employees—a responsibility that strongly imprints all of its data management functions and operations.

FinCEN's information sources fall into three categories:

1. *Financial Database:* The financial database consists of reports that must be filed with the BSA, such as data on large currency transactions conducted at financial institutions or casinos, suspicious transactions, and international movements of currency or negotiable monetary instruments. This information often provides invaluable assistance for investigators because it is not readily available from any other source and preserves a financial paper trail for investigators to track criminals' proceeds and their assets.
2. *Commercial Databases:* Information from commercially available sources plays an increasingly vital role in criminal investigations. Commercial databases include information such as state, corporation, property, and people-locator records, as well as professional licenses and vehicle registrations.
3. *Law Enforcement Databases:* FinCEN is able to access various law enforcement databases through a written agreement with each agency.

FinCEN works closely with the IACP, National Association of Attorneys General, National White Collar Crime Center, and other organizations to inform law enforcement about the information available at FinCEN and how to use the information to attack criminal proceeds.

High-Risk Money Laundering and Related Financial Crimes Areas[73]

High Intensity Financial Crime Areas (HIFCA) were first announced in the 1999 National Money Laundering Strategy and were conceived in the Money Laundering and Financial Crimes Strategy Act of 1998 as a means of concentrating law enforcement efforts at the federal, state, and local levels in high-intensity money laundering zones. HIFCAs may be defined geographically or they can be created to address money laundering in an industry sector, a financial institution, or group of financial institutions.

To implement the goal of concentrating efforts, a money laundering action team will be created or identified within each HIFCA to spearhead a coordinated federal, state, and local anti-money laundering effort. Each action team will be composed of all relevant federal, state, and local enforcement authorities, prosecutors, and financial regulators who will concentrate on the following:

- Focus on tracing funds to the HIFCA from other areas, and from the HIFCA to other areas so that related investigations can be undertaken
- Focus on collaborative investigative techniques, both within the HIFCA and between the HIFCA and other areas
- Ensure a more systemic exchange of information about money laundering between HIFCA participants
- Include an asset forfeiture component as part of its work.

Gateway

FinCEN's Gateway system enables federal, state, and local law enforcement agencies to access online records filed under the BSA. The system saves investigative time and money by enabling investigators to conduct their own research and analysis of BSA data rather than relying on the resources of an intermediary agency to obtain financial records. A unique feature of Gateway is the "query alert" mechanism that automatically signals FinCEN when two or more agencies have an interest in the same subject. In this way, FinCEN is able to assist participating agencies in coordinating their investigations.

Virtually every criminal enterprise and terrorist organization is involved in some dimension of money laundering. The complexities of forensic accounting, often complicated by jurisdictional barriers, reinforces the need for intelligence personnel to be aware of the resources and expertise available through FinCEN.

Essential to effective intelligence is the ability to access and share information readily. A number of resources and systems are available to SLTLE agencies that permit access to federal intelligence products, regional and local intelligence products, current news and events, and secure e-mail. Many resources are available to law enforcement organizations for a minimal, if any, fee. Regardless of the degree of sophistication of a system, it is essential that a law enforcement organization have some form of secure e-mail and access to an SBU/CUI network to receive current advisories that maximize information sharing

[73] See www.fincen.gov/le_hifcadesign.html.

International Justice and Public Safety Network[74]

The International Justice and Public Safety Network (formerly the National Law Enforcement Telecommunication System [NLETS]) was created by state law enforcement agencies nearly 35 years ago as a primary means of integrating data related to traffic enforcement. Since its founding, the NLETS role has evolved from being primarily an interstate telecommunications service for law enforcement to a more broad-based network servicing the justice community at the local, state, and federal levels. It is now a broad-based interstate law enforcement network for the exchange of law enforcement and related justice information. Its purpose is to provide, within a secure environment, an international criminal justice telecommunications capability that will benefit to the highest degree the safety, security, and preservation of human life and the protection of property. NLETS will assist national and international governmental agencies and other organizations with similar missions who enforce or aid in enforcing local, state, federal, or international laws or ordinances.

NLETS is a nonprofit corporation chartered by the states and funded by user fees collected from the membership and managed by a board of directors consisting of state police executives. Primary services include access to key state databases, particularly drivers' licenses and motor vehicle records, criminal histories, and sex offender registries. The system also has access to special databases such as Canadian files, hazardous materials archives, U.S. General Services Administration fleet, immigration records, FAA registrations, NDPIX,[75] vehicle impounds, and import/export files. The system also includes terminal-to-terminal messaging and broadcast capabilities (such as an Amber Alert).

Accelerated Information Sharing for Law Enforcement

The next generation of NLETS is Accelerated Information Sharing for Law Enforcement (AISLE). The intent of AISLE is to accelerate information sharing for the entire U.S. law enforcement community by adopting and deploying XML[76] Web Services technology for interstate inquiries and responses. Like the Global Justice Information Sharing Initiative, it also seeks to promote the common XML standard for law enforcement information systems. Essentially, AISLE seeks to move NLETS completely into the most advanced realms of networking to enhance information sharing.

Operation Archangel and the Automated Critical Asset Management System

While the discussion of resources and systems has largely been avoided, discussion of state and local systems—the Automated Critical Asset Management System (ACAMS)—is an exception. While locally developed, it is becoming a national system with the support of the DHS.

ACAMS is a component of a broader initiative, Operation Archangel, that was developed by the Los Angeles Police Department. Building on local

[74] For contact information and more details, see www.nlets.org/default.asp.

[75] NDPIX is the National Drug Pointer Index, discussed in detail in Chapter 11.

[76] Internet web pages are typically written in Hypertext Markup Language (HTML) which aids in formatting and integrating diverse resources. The second generation is XML, Extensible Mark-up Language, which has all the features of HTML and provides significantly increased searching and comparison characteristics.

responsibilities for protecting Critical Infrastructure and Key Resources (as discussed in Chapter 9), the intent of Archangel is to identify and protect Critical Infrastructure and Key Resources in the Los Angeles metropolitan area. Its purpose is to defend likely targets against catastrophic terrorist attacks, relying on the guiding principle that local agencies are most knowledgeable about their own critical assets. The system was born out of a need to engender interagency/departmental cooperation and coordination to facilitate the strategic application and management of information and resources for the prevention, deterrence, mitigation, and response to critical incidents, including terrorism. Primarily focused on prevention, Archangel has been designed to identify critical threat locations and plan multiagency/disciplinary prevention, deterrence, mitigation and response efforts.[77]

A number of flexible components of Archangel make it a scalable model that is exportable across the United States. The following are among Archangel's initiatives:

- *Identification and Prioritization of Critical Assets*
- *Critical Asset Assessments* using a three-tiered template:
    1. Conducting appropriate vulnerability assessments to determine and reduce a location's degree of vulnerability.
    2. Harvesting detailed location-specific information (i.e., names, phone numbers, floor plans, site postings, etc.) All for use by pre-incident planners and on-scene incident commanders through web-based delivery during critical incidents.
    3. Drafting site-specific, pre-incident security enhancement plans and post-occurrence action plans designed to provide tactical guidance and insight to planners and/or to incident commanders in the field.
- *Critical Asset Assessment Teams* that conduct an on-site threat and vulnerability assessment.
- *Protective Security Task Force (PSTF),* is a plainclothes, low-profile team of personnel specifically trained and equipped with state-of-the-art technology to provide a comprehensive cloak of security to a threatened asset. Primarily, the PSTF will be deployed when intelligence indicates that a threat may be directed at a critical asset and/or event. In the absence of intelligence, the PSTF will deploy to critical assets throughout the area of responsibility, providing low-key but visible enhancements to the resident security measures.
- *Security Officer Terrorism Awareness Course (SOTAC),* is a 4-hour block of instruction designed specifically for the security industry professional to enhance awareness of current terrorist trends and methodologies for attack.
- *Automated Critical Asset Management System (ACAMS).* Archangel has partnered with U.S. DHS to develop ACAMS, a secure interoperable web-based system to manage critical asset information. ACAMS coordinates the following:
    - Critical Asset Inventory and Prioritization Modeling
    - Asset Manager Questionnaires (promotes public/private partnerships)
    - Critical Asset Assessments

[77] www.lapdonline.org/emergency_services_division/content_basic_view/33044

- Site Specific Pre-Incident Security Enhancement Plans
- Buffer Zone Plans
- Building Inventories
- Site Specific Post-Occurrence/Response Plans.[78]

ACAMS also includes any predeveloped response plans for specific incidents[79] and site-specific pre-incident security enhancement plans for use by strategists to prevent and deter incidents from occurring.[80]

Constellation/Automated Critical Asset Management System

The DHS has embraced the Constellation/Automated Critical Asset Management System (C/ACAMS) that is explicitly intended to support fusion centers and other information-sharing partners in support of the DHS mission of protecting critical infrastructure. C/ACAMS provides state, local, and private-sector partners with a set of resources for collecting and managing information related to critical infrastructures and to inject infrastructure information into fusion center analysis. This information, when combined with terrorism threat streams, provides fusion center analysts and private-sector infrastructure owners and operators with a context for understanding risk and to target protection resources against those assets or systems that have the highest risk profiles. Currently, C/ACAMS is deployed to fusion centers across the United States and is used by more than 2,000 state and local infrastructure protection analysts. The data they have collected on more than 38,000 unique infrastructure assets are vital to the national effort to enable prevention, protection, response, and recovery activities.[81]

Law Enforcement Intelligence Unit[82]

Founded in 1956, the Law Enforcement Intelligence Unit (LEIU) is an independent professional association of U.S. and international law enforcement intelligence professionals who gather, record, and exchange confidential information not available through regular law enforcement channels, concerning organized crime and terrorism. It is an association of U.S. and international law enforcement professionals, similar in many respects to numerous other associations serving professionals. LEIU has no staff, other than an executive director, and no capability as an entity to conduct an investigation or law enforcement activity. Each member agency is bound by, and acts pursuant to, local law and its own agency regulations.

The organization is divided geographically into four zones: Eastern, Central, Northwestern, and Southwestern. Each zone elects a chair and vice chair to serve as zone officers. Internationally, LEIU elects a general chair, vice general chair, and designates a secretary-treasurer and a legal advisor who serve as international officers. The international officers, zone officers, past general chair, and two representatives from the Central Coordinating Agency (i.e., the California Department of Justice which houses LEIU data) make up the executive board. The board is the governing body of LEIU and, as such, establishes policy and passes on the admission of all members, and is governed by a constitution and bylaws.

[78] Ibid.

[79] McCreesh, Patrick and Craig Neuman. *Managing for Counter-Terrorism Success in the Los Angeles Police Department.* New York: The Manhattan Institute and Cambridge, Massachusetts: John F. Kennedy School of Government, Harvard University, 2007, p. 9.

[80] Leson, Joel. *Assessing and Managing the Terrorism Threat.* Washington, D.C.: Bureau of Justice Assistance, U.S. Department of Justice, 2005, p. 19. Also see www.dhs/gov/acams.

[81] Allen, Charles E. *Information Sharing at the Federal, State and Local Levels. Statement for the Record before the United States Senate Committee on Homeland Security and Governmental Affairs,* July 23, 2008, 11.

[82] For more information on LEIU see www.leiu-homepage.org/index.html. For contact information concerning LEIU membership, e-mail leiu@doj.ca.gov. LEIU, California Department of Justice, P.O. Box 163029, Sacramento, CA 95816-3029.

LEIU membership is limited to law enforcement agencies of general jurisdiction having an intelligence function. To become a member, an agency head submits a written application. The applying agencies must be sponsored by an LEIU member. Each member agency head appoints an LEIU representative as the contact for the LEIU.

Virtually any kind of information that may be lawfully retained in law enforcement intelligence records may be exchanged as long as the recipient meets the need-to-know and right-to-know standards. It is important to keep intelligence records consistent with legal standards. LEIU is not a computer system where members can make queries; rather, it is a network where information is exchanged between members, albeit in electronic form.

Information Sharing

To submit an inquiry about a suspected criminal to the LEIU automated system, a member agency enters the subject information through a secure intranet that is stored on RISS.net. The subject information includes, among other items, the person's identity, criminal activity, and criminal associates. All information submitted to the LEIU automated file must meet LEIU File Guidelines (See Appendix C) and comply with 28 CFR, Part 23. The submitting agency must certify that the subject meets established criteria, including criminal predicate. The Central Coordinating Agency manages this automated file.

International Criminal Police Organization[83]

The International Criminal Police Organization (INTERPOL) was founded in 1923 to serve as a clearinghouse for information on transnational criminals. It receives, stores, analyzes, and disseminates criminal data in cooperation with its 181 member countries on a 24/7/365 basis in its four official languages (English, French, Spanish, and Arabic). Interpol deals only with international crimes. Its four core functions are to provide member states with the following:

1. *Secure global police communication services.* INTERPOL runs a global police communications system called I-24/7, which provides police around the world with a common platform through which they can share crucial information about criminals and criminality.
2. *Operational data services and databases for police.* INTERPOL's databases and services ensure that police worldwide have access to the information and services they need to prevent and investigate crimes. Databases include information such as names, fingerprints and DNA profiles, and stolen property such as passports, vehicles, and works of art.
3. *Operational police support services.* INTERPOL supports law enforcement officials in the field with emergency support and operational activities, especially in its priority crime areas of fugitives, public safety and terrorism, drugs and organized crime, trafficking in human beings, and financial and high-tech crime. A Command and Coordination Centre operates 24 hours a day, 7 days a week.
4. *Police training and development.* INTERPOL provides focused police training initiatives for national police forces, and also offers on-demand advice, guidance, and support in building dedicated crime-fighting components. The aim is to enhance the capacity of member countries to effectively combat serious transnational crime and terrorism.[84]

[83] The INTERPOL General Secretariat site is www.interpol.int.

[84] www.interpol.int

Criminal intelligence analysts at INTERPOL are uniquely placed to recognize and detect patterns and criminal trends from a global perspective, and have the resources to assist with specific international crime cases.

In the United States, the contact point for Interpol is the U.S. National Central Bureau (USNCB) which operates within the guidelines prescribed by the Department of Justice, in conjunction with the DHS. The mission of the USNCB is to facilitate international law enforcement cooperation as the United States representative to INTERPOL.

When INTERPOL is seeking specific information or seeking a person, it issues a color-coded notice, with each color representing a different type of action from the recipient agencies. While these notices are rarely encountered by SLTLE officers, it is nonetheless of value to be familiar with them should the issue arise.

U.S. law enforcement officers can gain access to INTERPOL reports and make international inquiries through their state point of contact (usually within the state law enforcement or intelligence agency) who will query the USNCB. The USNCB address and web site are: U.S. Department of Justice, INTERPOL, United States National Central Bureau, Washington, DC 20530 www.usdoj.gov/usncb.

Summary

As demonstrated in this chapter, the amount of information and intelligence being generated by federal law enforcement agencies and national law enforcement entities is significant. If that information is not being used, its value is lost. Not only are these resources responsible for making information available to SLTLE agencies in an accessible and consumable form, nonfederal law enforcement must develop the mechanisms for receiving the information and be good consumers of it.

One of the ongoing controversies is the problem of dealing with classified information. This chapter explained the classification process as well as the initiatives that are being undertaken to deal with this issue. One measure is to increase the number of security clearances for SLTLE personnel. The other measure is for the FBI to write intelligence reports so that they are unclassified, but remain as CUI to give SLTLE personnel access.

By gaining access to secure networking (e.g., LEO, RISS.net, ATIX), interacting on a regular basis with the FBI Field Intelligence Group, and proactively interacting with other federal law enforcement intelligence offices, SLTLE can have access to the types of critical intelligence necessary to protect their communities.

A Summary of Selected Intelligence Networks and Applications

A wide and diverse array of information systems that support the law enforcement intelligence function have been discussed thus far.[85] Many other systems exist at the federal level; however, most law enforcement officers will not have access to them unless they are assigned to a fusion center or major urban area law enforcement intelligence unit. Nevertheless, there is value in having a summary knowledge of some of these systems. Those previously discussed in this chapter are not included in the following summaries.

Classified Networks

- *C Local Area Network (Top Secret Network).* This network, commonly referred to as the C-LAN, is used within DHS to communicate Top Secret information with the Intelligence Community. It provides connectivity to the Department of Defense's Joint Worldwide Intelligence Communications System to access, receive, and share intelligence information.
- *Sensitive Compartmental Information Operational Network (Top Secret Network).* This network, also known as SCION, is used to transport top secret counterterrorism data, including intelligence and warning information. It provides an interface with the Department of Defense's Joint Worldwide Intelligence Communications System that allows FBI agents and analysts to exchange Top Secret intelligence information with other members of the Intelligence Community.
- *Federal Bureau of Investigation Network (Secret Network).* Commonly referred to as the FBINET, it is a global-wide area network used for communicating Secret information, including investigative case files and intelligence pertaining to national security. It also runs administrative applications.
- *Homeland Secure Data Network (Secret Network).* Also known as HSDN, this network transmits homeland security data in support of activities including intelligence, investigations, and inspections that are classified at the Secret level. HSDN provides Secret connectivity to civilian agencies and will provide Secret connectivity in the future for civilian agencies currently using the Department of Defense's Secret Internet Protocol Router Network. It is used, for example, to transmit intelligence summaries, secure messaging, and e-mail correspondence.

SBU/CUI Networks

- *Critical Infrastructure Warning Information Network.* Also known as CWIN, the network is used to transmit voice and data on infrastructure protection, communication and coordination, alert, and notification. In the event that a significant attack disrupts telecommunications networks or the Internet, the CWIN will provide secure capability for communications across key government network operations centers, the private and public sectors, and trusted foreign partners. According to the DHS, the CWIN is the critical, survivable network connecting the DHS with the vital sectors that are essential in restoring the nation's infrastructure during incidents of national significance.

[85]The value, use, and application of many of these systems are discussed in: *Information Technology: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives. A report to the Chairman, Committee on Homeland Security, U.S. House of Representatives.* Washington, D.C.: General Accountability Office, April 2007.

- *Criminal Justice Information Services Wide Area Network*. Also known as the CJIS WAN, it provides secure electronic connectivity to information on individuals, vehicles, and property associated with crimes or terrorist organizations to state, local, tribal, and federal law enforcement agencies. It is also used to identify individuals from submitted fingerprints and to exchange deoxyribonucleic acid (DNA) information, background-check information, and criminal history information.
- *Customs and Border Protection Network*. Commonly referred to as the CBP Network, it is used to transmit SBU/CUI data related to Customs and Border Protection's support of homeland security functions, such as protecting the nation's borders from terrorists and regulating and facilitating the lawful movement of goods and persons across U.S. borders.
- *DHS Core Network*. Also known as the DCN, the network transmits SBU/CUI data related to the DHS homeland security mission in areas such as customs, border patrol, and intelligence.
- *FBI Unclassified Network*. Commonly known as UNet, this is a national wide area network that provides the FBI with access to SBU/CUI intelligence and law-enforcement sensitive information. It provides bureau agents with access to secure mail and LEO.
- *Justice Consolidated Network*. Known as the JCN, this network transmits fingerprint, arrest records, and other data relating to the investigation and prosecution of crimes and terrorist activities among DOJ components.
- *Justice Unified Telecommunications Network*. This network, also known as JUTNet, transmits SBU/CUI information (such as fingerprint and arrest information) pertaining to the investigation and prosecution of crimes and terrorist activities. In addition, it supports video conferencing and certain Voice over Internet Protocol services.
- *Immigration and Customs Enforcement Network*. Also known as ICENet, this network supports the data transmission needs of the DHS Immigration and Customs Enforcement component. Major programs dependent on this network include the Office of Investigations, the Detention and Removal Office, the Federal Protective Services Office, and the Intelligence Office.
- *Secret Service Wide Area Network*. Commonly referred to as the Secret Service WAN, this network supports the homeland security mission by providing security and protection to our nation's leaders and financial systems
- *Transportation Security Administration Network*. This network, also known as TSANet, is a global network used for security operations, intelligence, and law enforcement information-sharing. It is used to transmit alerts, fingerprints, and information from the Transportation Security Administration's mission-critical applications.
- *ONENet*. A single network using dual carriers to support interoperability and data sharing in all DHS mission areas and between all DHS components. The DHS is deploying ONENet to DHS components and it will consolidate the following seven networks: 1. Coast Guard Data Network Plus; 2. Customs and Border Protection Network; 3. DHS Core Network; 4. Federal Emergency Management Agency Switched Network; 5. Immigration and Customs Enforcement Network; 6. Secret Service Wide Area Network; and 7. Transportation Security Administration Network.

SBU/CUI Network Applications

Bomb Arson Tracking System. Commonly referred to as BATS, this application is a partnership among DOJ, the ATF's Bomb Data Center, and members of the nation's fire and post-blast investigative communities. It provides these organizations with a comprehensive incident-based information-sharing system.

eTrace. The eTrace application is a web-based firearm trace submission system and trace analysis module for use by approved law enforcement agencies. The eTrace application improves the efficiency of the firearm tracing process and provides for the secure exchange of firearms trace-related information between the law enforcement community and the ATF.

Federal Emergency Management Agency Switched Network. This network, commonly known as the FEMA Switched Network, provides support for emergency coordination of federal, state, and local operations, disaster assistance, and government recovery efforts. For example, it is used to provide information about disaster victims and logistics for disasters, in addition to normal business.

Conclusion

If effective information sharing is one of the critical goals of contemporary law enforcement intelligence, then networks and systems are the critical tools to reach that goal. As has been seen throughout this chapter, there has been significant growth in the capability of law enforcement agencies to share information. The growth has been a product of new initiatives following 9/11, the availability of new networking technologies that reduce interoperability conflicts, and the commitment of American law enforcement at all levels of government to facilitate information-sharing processes. These factors are in a dynamic state. Systems and networks will change; therefore, it is incumbent on the intelligence manager to carefully monitor trends to stay current.

Chapter 13:

Management and Human Resource Issues for the Intelligence Function

Management and Human Resource Issues for the Intelligence Function

The basic principles and applications of management—leadership, accountability, span of control, chain of command, labor relations, program evaluation, to name a few—apply to the intelligence function in the same manner as they would apply to any other organizational entity. The extensive literature of police administration and management is a solid resource for these issues when managing an intelligence unit. This chapter will focus on selected issues relating to the development and management of the intelligence function.

While most American law enforcement agencies might not have a formal intelligence unit, they still have an intelligence function to manage. With the increasing symbiosis among federal and state, local, and tribal law enforcement (SLTLE), adoption of the *National Criminal Intelligence Sharing Plan* (NCISP), the growth of networked intelligence information systems, and the responsibility of keeping the homeland secure, virtually every law enforcement agency in the country needs to develop some kind of intelligence capacity. That capacity may be a full-scale unit or one person who serves part time as an agency's point of contact for receiving and disseminating critical information. In some form, an intelligence capacity has become a de facto requirement for American law enforcement agencies. As a result, new intelligence processes for law enforcement present challenges such as the following:

- Reengineering some of the organization's structure and processes
- Developing a shared vision of the terrorist or criminal threat within the agency as well as with the broader law enforcement community
- Participating in intelligence processes and following through with information sharing
- Committing resources, time, and energy to the intelligence function
- Developing a proactive spirit and creative thought to identify "what we don't know" about terrorism and international organized crime
- Developing a culture within the law enforcement agency that is able to think globally and act locally
- Developing a culture of information sharing
- Providing vigilance, patience, and entrepreneurial leadership.

To put these components into operation in a functional intelligence mechanism, SLTLE agencies of all sizes need, at a minimum, fundamental operational components, such as these:

- A person designated as the intelligence point of contact to whom external agencies may direct inquiries, warnings, and advisories, and from whom information and questions may be sent. He or she must have sufficient training to understand the language, processes, and regulations incumbent on the law enforcement Intelligence Community.
- A secure electronic communications system for sending and receiving information that is Sensitive But Unclassified/Controlled Unclassified Information (SBU/CUI). Several systems are available, including Law

Enforcement Online (LEO), the Regional Information Sharing System Network (RISS.NET), Automated Trusted information Exchange (ATIX) (originally the Anti-Terrorism Information Exchange)—some of which are available at no charge to the user. With the growth of the Global Justice Extensible Markup Language Data Model (GJXDM) standard[1], access to these systems will be essential for the most accurate information-sharing.

- Established policies for information collection, reporting, and dissemination.
- Established ability to determine the kinds of information and intelligence that is needed to effectively prevent terrorism and disrupt criminal enterprises. This is a difficult challenge requiring a significant labor investment. Understanding the threats and targets within a community and developing responses to neutralize those threats is essential. American law enforcement must discover the evidence of threats that may be in its backyard.

Beyond these factors, a number of management factors may be considered when developing an intelligence capacity. A common question asked by law enforcement executives and those responsible for developing an intelligence capacity, is "Where do I start?" Providing a succinct response is not easy because the starting place will vary depending on agency size, the chief executive's vision, the geographic location of the jurisdiction, the presence of factors that make the jurisdiction a terrorist or criminal target, and other variables unique to the jurisdiction and agency. The first part of the answer is to provide a list of factors to consider when developing or reengineering the intelligence capacity of a law enforcement agency. The second part of the answer is to develop a Concept of Operations (ConOps) for the intelligence unit to refine how the intelligence function is envisioned to integrate it into the agency's other activities. Finally, attention will be given to selected intelligence management issues.

A Checklist of Considerations in Developing or Reengineering the Law Enforcement Intelligence Capacity

The following is a list of questions and variables to consider when developing the intelligence capacity. Not every factor will apply to every agency, although collectively these factors will give a perspective on the intelligence function as it exists within the organizational environment. The list provides a straightforward perspective of the management responsibilities required to accomplish the task. Many of the factors will be discussed in greater detail later in the chapter. (See also Table13-1.)

Administration and Management

- The chief executive must have a vision for the role of the intelligence function.
  - What activities are expected of the intelligence function?
    - Clearinghouse of information?
    - Tactical analysis?
    - Strategic analysis/forecasting?

[1] For information about the Global Justice XML Data Model, see it.ojp.gov/jxdm.

        - Threat assessments?
        - Pointer and deconfliction activities?
        - Other? Make sure this is articulated.
    - Does the chief executive's vision include incorporating the Intelligence-Led Policing (ILP) philosophy throughout the law enforcement agency?
        - If not, what is the envisioned relationship of intelligence to other departmental activities?
            - This should be clearly articulated by the chief executive.
    - If intelligence is one of several responsibilities assigned to one person or unit, what is its priority/relationship to other responsibilities?
    - What crimes are to be the focus (i.e., strategic priorities) of the intelligence function?
    - Will "all hazards" be included?
    - If so, how will it be defined for the intelligence function?
    - What outputs and activities are expected of the intelligence function?
    - Question: Does the chief executive and/or command staff need to be briefed (i.e., trained) on contemporary law enforcement intelligence?
        - If so, how do you propose to suggest or accomplish this?
- The chief executive must demonstrate commitment and support for the intelligence function.
    - This includes allocation of people and adequate resources.
- Obtain budget parameters.
    - How much funding will be available to establish the intelligence unit?
- Will the intelligence supervisor be organizationally responsible directly to the chief executive or to another commander (e.g., the criminal investigations division commander or operations division commander)?
    - There are advantages to both direct reporting to the chief executive and reporting to another commander.
        - If the intelligence unit supervisor answers directly to the chief executive:
            - Advantage: More direct information flow and operational responses regarding threats.
            - Disadvantage: There may be jealousies among those of higher rank with respect to the intelligence supervisor's access to the chief executive.
        - If the unit is assigned under another division commander:
            - Advantage: It helps shield the unit from criticisms of secrecy, which often becomes an issue.
            - Disadvantage: A filtering effect of critical information can occur.
    - While other advantages and disadvantages can occur, they will be dependent on the culture of the law enforcement organization.

Develop the Intelligence Unit's Infrastructure

- Mission, goal(s), and objectives of the intelligence function must be articulated.
- Develop necessary policies and procedures (See Table 13-1 for a list of areas in which to consider developing policy for the intelligence function. The need for policy will be related directly to the mission, goals, and objectives.)
  - Develop a privacy policy that is consistent with federal privacy guidelines.[2]
  - Develop a policy and procedures for your criminal intelligence records system that is 28 CFR Part 23-compliant.
    - The Law Enforcement Intelligence Unit (LEIU) *File Guidelines*[3] serves as a court-tested model.
    - The criminal intelligence records policy should include:
      - Collection standard of a criminal predicate.
      - Retention guidelines.
        - Temporary files should have a time limit for retaining information and standards for review and purging.
      - Review of records in the criminal intelligence records system.
      - Purging requirements and processes.
      - Dissemination criteria.
      - Nondiscrimination statement.
- Select an office location.
  - Will the unit be colocated with CID, narcotics, organized crime, or other unit?
    - If so, be certain that the physical location will be able to meet the security requirements needed for intelligence records.
  - If the intelligence unit is at an off-site location, it is preferable to have a stand-alone office, not with other businesses.
  - Ideally, the intelligence unit's office will be centrally located.
  - Develop your work environment
    - Get access to intelligence products and networks.
    - Lockable filing cabinets.
    - Dedicated computer.
    - All personnel, supplies, and services necessary to fulfill the vision.
- Purchase or obtain the unit's vehicles
  - Undercover vehicles in a variety of styles and colors.

[2] it.ojp.gov/default.aspx?area=globalJustice&page=1151.

[3] it.ojp.gov/documents/LEIU_Crim_Intell_File_Guidelines.pdf.

Table 13-1: Sample Issues for Intelligence Unit Policy Development[4]

- Intelligence unit organization, role, and responsibilities
- Intelligence unit staff position requirements, selection, and training
- Privacy policy (consistent with the federal Information Sharing Environment (ISE) *Privacy Guidelines*)
- Intelligence unit records management
  - 28 CFR Part 23 compliant file guidelines (including standards and processes collection, retention, review, purging, and disseminating)
  - Quality control procedures for data and information accuracy
- Handling of SBU/CUI information
- Access, documentation, dissemination, and of use of information form
  - Intelligence records systems (i.e., RISS.NET, LEO, Homeland Security Information Network [HSIN])
  - Contacting other agencies and jurisdictions (i.e., fusion centers, FBI Field Intelligence Group [FIG], and other law enforcement agencies)
  - Contacting International Criminal Police Organization (INTERPOL)
  - Contacting El Paso Intelligence Center (EPIC)
- Types of intelligence products to be produced
  - Marking and dissemination policy for intelligence products
- Intelligence unit reporting procedures and dissemination
- Suspicious Activity Reporting and field interview procedures and reporting
- Classification and security system for the agency and/or intelligence unit
  - Rules for violations of the security system
- Procedures and accountability when operating under a memorandum of agreement
- Intelligence unit processes and responsibilities during critical incidents
- Surveillance operations (processes, documentation, limitations)
- Access to equipment and resources in support of intelligence activities
- Use of criminal informants
  - Guidelines for payments to criminal informants
- Undercover operations in support of the intelligence function
  - Undercover reporting procedure
  - Investigative and undercover expense fund accountability
  - Consumption of alcoholic beverages during undercover operations and surveillance
  - Narcotic simulation during undercover narcotic investigations
- Information release and media policy
- Intelligence unit performance evaluation and review

[4] A number of sample *Intelligence Policy Manuals* are available online at the DHS Fusion Process Technical Assistance Program at www.llis.dhs.gov. In addition, sample policies are available at the National Criminal intelligence Resource Center web site accessible through the RISS.NET portal and LEO. As will be seen, there is a wide variation of structures and approaches to these manuals. Each needs to be tailored to a specific agency's needs, but the samples provide good guidance. In addition, the International Association of Chiefs of Police prepared a document under BJA funding that provides guidance on developing policies and procedures: Orrick, W. Dwayne. *Best Practices Guide: Developing a Police Department Policy-Procedure Manual.* Alexandria, Virginia: International Association of Chiefs of Police, undated.

Staffing

- Select personnel: Intelligence officers
  - Consider languages and education.
  - Consider how the officers get along with other agencies.
  - Consider a past officer/deputy with undercover experience.
  - Consider policing style.
    - A person who is aggressive in making arrests and kicking in doors typically will not be a good fit in an intelligence unit.
    - Personal characteristics most suited to the intelligence unit include:
      - Maturity.
      - Dependability.
      - Works well without supervision.
      - Self-motivator.
      - A team player.
  - In the selection of officers for the intelligence unit, be certain they are able to obtain a security clearance, if required for the position.
    - For law enforcement officers, one of the more common factors that prohibits them from receiving a clearance is poor credit.
  - Consider knowledge of your special needs, such as gangs, computers, surveillance techniques, tactical surveillance equipment, etc.
- Select personnel: Analysts
  - The analyst's position and role should be viewed as a practicing professional of equal organizational stature to officers, not treated as support staff.
  - Desirable characteristics of an analyst include:
    - Highly motivated.
    - Critical thinker.
    - Strong computer skills.
    - Willing to help all with cases.
    - Ability to obtain a security clearance.
- Once personnel have been selected, contact the local FBI office to apply for security clearances for your new personnel[5]
  - In most cases, a Secret-level clearance will be sufficient. The process takes several months.

Training

- Training
  - Get the added training you need to further your strategic plan.
    - Includes training on your specific policies/procedures.
  - Remember, training includes both the intelligence discipline and training on crimes that are the focus of the intelligence unit.
- Ensure that all training meets the standards of:

[5] See www.fbi.gov/clearance/securityclearance.htm.

- Minimum Criminal Intelligence Training Standards.[6]
- *National Criminal Intelligence Sharing Plan.*[7]

- Conduct a training needs assessment and enroll your personnel in the training they need (Below are examples. Training will be discussed later in the chapter).
  - Training on the discipline and processes of intelligence.
  - Analytic training.
  - Intelligence records management, including 28 CFR Part 23.
  - Analysts will need many other courses to become proficient.
    - Certified Intelligence Analyst certificates.
    - Crime mapping.
    - HIDTA Programs (Analytical Investigative Techniques I and II).
    - FINCEN.
  - Join open-source networks.
- Be certain to monitor the Bureau of Justice Assistance "Criminal Intelligence Master Training Calendar."[8]

Information Management and Information-Sharing

- In light of the chief's vision of intelligence products:
  - Identify the types of intelligence products to produce.
  - Identify the dissemination table of intelligence products.
    - Internal dissemination only?
    - If external dissemination will be included, define:
      - Dissemination criteria (What are the characteristics of recipients who receive the products).
      - Will the Third Agency Rule be applied?
      - Must products be approved for dissemination prior to being sent?
      - What is the mechanism for disseminating products?
      - Will there be an audit trail for disseminated products?
      - What types of products will not be disseminated outside of the agency?
- Select computer databases to store information and intelligence records:
  - Must be kept separate from your agency's regular Records Management System.
  - Must be able to purge records from the system so they are destroyed and not accessible in the future.
  - Secure and audited access to computers and systems.
- Obtain individual computers for your personnel.
  - Analysts need a more powerful and diverse system than needed by officers and deputies.

[6] it.ojp.gov/documents/min_crim_intel_stand.pdf.

[7] it.ojp.gov/documents/NCISP_Plan.pdf.

[8] mastercalendar.ncirc.gov.

- Basic software needs:[9]
  - Word processing program.
  - Spreadsheet program.
  - Relational database.
  - Presentation software.
  - Flowcharting software.
  - Link analysis software.
  - Database reporting/visualization software.
  - Mapping software.
  - Photo enhancement software.
  - Telephone analysis software.
  - Analytic charting.
  - Portable Document Format (PDF) creation software.
  - Security software (virus, adware, spyware software; firewall, and Virtual Private Network [VPN] security).
  - Publication software.
  - Statistical analysis software.
  - Text mining software.
- Budget for analytical tools and commercial databases, including membership in the Regional Information Sharing System (RISS) center and commercial data base search system.
- Full Internet access.
- Stand-alone computer for covert operations.

- Develop a report and intelligence product numbering system.
  - Keep an audit and control log of issued numbers that can be accessed by unit members.
  - Develop a system that easily permits identification of unit, date, and application of the bulletin.
- Organize monthly meetings among all area analysts to discuss and share issues and analytic methods.
- Organize and host a monthly intelligence meeting with other area law enforcement agencies.
  - Meetings should include analysts and officers.
    - Creates a trusting environment with others.
    - Face-to-face contact is critical.
    - Sharing information is critical.
    - Creates a contact list to handle situations quickly.
  - Also invite specific trusted/vetted individuals from appropriate private-sector companies that can assist in your goals, as applicable.
  - Invite federal agencies such as the Joint Terrorism Task Force (JTTF) or Immigration and Customs Enforcement.

[9] Resource: Global Justice Information Sharing Initiative. *Analyst Toolbox. A Toolbox for the Intelligence Analyst.* Washington, D.C.:, U.S. Department of Justice, Global Justice information Sharing Initiative, Intelligence Working Group, November 2006. it.ojp.gov/documents/analyst_toolbox.pdf.

Implementation and Assessment

- Start the process:
  - Test your system and be prepared to adjust it.
  - Identify critical processes and procedures to collect data for assessment.
  - Ask the consumers of the intelligence function if it is working.
  - Seek suggestions for improvement.
- Implement an audit process.
  - Intelligence Guide Audit Model.
  - LEIU Audit Checklist for the Criminal Intelligence Function.
- Strive for continuous quality improvement.

The points in this list are food for thought in developing the agency's intelligence structure. These factors are intended to help identify issues that need to be addressed in planning for the intelligence function. The next step is to integrate these factors into a cohesive vision of how the intelligence structure will actually operate within an agency. The next step, therefore, is to mold these factors into a ConOps.

Developing the Concept of Operations

The Concept of Operations (ConOps) is a user-oriented document that describes the characteristics of a proposed program, initiative, or system from the viewpoints of how staff and users will interact with the proposed initiative.[10] The ConOps is used to communicate overall characteristics of the new organizational entity—in this case, a new intelligence structure—to management, staff, and users. Ideally, the ConOps is prepared in conjunction with a business plan. While the ConOps describes the organization, mission, and organizational objectives from an integrated systems point of view, the business plan describes the proposed system or situation from an investment and process point of view.

The ConOps provides an analysis that bridges the gap between the operational needs and visions and the technical aspects of a functioning organization, in this case, an intelligence unit. The ConOps should also document a program's characteristics and the user's operational needs in a manner that can be confirmed by the user without requiring any technical knowledge beyond that required to perform normal job functions. Management and users, for example, need to understand how the intelligence unit will function and the products it will produce, but do not need to know how to conduct specific types of analysis or access specific systems.

The ConOps documents the visions and expectations of management and users alike without requiring the provision of quantified, testable specifications until later in the system life cycle. The ConOps also provides a mechanism for management and users to express thoughts and concerns about possible issues, strategies, and processes before actual implementation of the system.

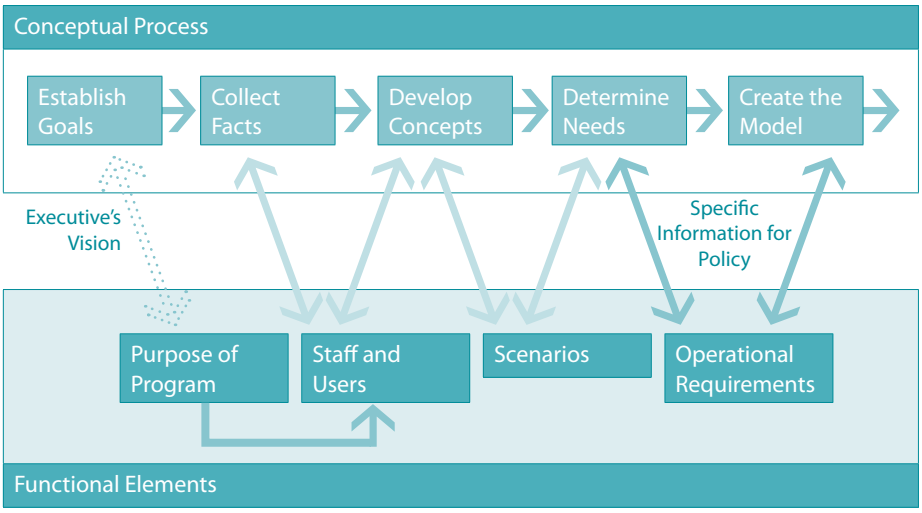
The ConOps represents a process for developing a new functional concept of an organizational activity. It seeks to represent the needs of the organization,

[10] To review different law enforcement agency ConOps, after registering for the DHS Lessons Learned Information Sharing (LLIS) system – www/llis.dhs.gov – go to the Fusion Process Technical Assistance Resource Center and search the "channel" for "ConOps."

needs of the users/consumers of intelligence, and embraces lessons learned or best practices of other organizations, all tailored to meet the needs of the law enforcement agency.

Figure 13-1 illustrates the development process. The series of progressive activities, illustrated on the top row, are intended to clarify the operational concept of a new organizational activity, in this case, a new intelligence structure. The bottom row represents functional components required to develop the concept. More specifically, in order to establish goals, one needs to know the intended purpose of the program, which will be strongly directed by the chief executive's vision of the program. This vision must be shared with the staff who will actually develop and operate the program. Once the goals are clear, the ConOps can move forward to develop an intelligence structure that can accomplish those goals.

Figure 13-1: Process for the Development of a Concept of Operations



The next conceptual step is to gather information related to the goals, for example, national standards (such as the NCISP and *Fusion Center Guidelines)*, lessons learned and best practices from other agencies, legal issues, and other factors that may be specifically idiosyncratic to the jurisdiction. The latter information often has to be gained from staff and potential users of the new (or reengineered) intelligence structure. Based on the collective analysis of these facts, the concept of how the new intelligence structure will work begins to take shape. Once again, two-way discussion with staff and users is essential to ensure that the concept will work. One of the effective mechanisms for testing this is to develop different information-sharing and analytic scenarios to illustrate the concept. For example, if a new Suspicious Activity Reporting mechanism is to be part of the new intelligence structure, different scenarios of how the system would work can be developed with feedback from staff and users on the strengths, weaknesses, and constraints of the system.

Relevant Definitions

- *Concept of Operations:* Articulates the concept and vision of a new organizational entity.
- *Business Plan:* Takes the ConOps to the next step. The business plan establishes functional processes, implementation strategies, and daily operations of the organizational entity.
- *Implementation:* The actual process of making the concept a reality through the use of the business plan.

By developing scenarios for all aspects of the new intelligence enterprise, specific changes to, or needs for, the system can be identified and built into the concept. These needs will help define the operational requirements for the new intelligence structure to be successful—everything from office space to training to new report forms. Once they have been identified, the final model, represented by the ConOps, can be prepared for review and consideration. The culmination of this process needs to be placed in written form to fully communicate the new operational concept.

Contents of a Concept of Operations

There are different models of ConOps, each of which will always need some degree of adaption to meet the unique needs of a given agency or fusion center. The following model, which is broadly based on a model used by the U.S. Department of Health and Human Services,[11] provides a blending of the more common elements found in a ConOps as used by a law enforcement agency.

Title Page
Contents
Figures
Tables

1. *Introduction:* Summarize the purpose of the document, the scope of activities that resulted in its development, its relationship to other relevant plans or standards, the intended audience for the ConOps, and expected evolution of the document. Also describe any security or privacy considerations associated with use of the ConOps.
2. *Referenced Documents:* Provide identifying information for all documents referenced within the ConOps document (e.g., NCISP, *Fusion Center Guidelines*, 28 CFR Part 23, as well as legislation, feasibility studies, or any other relevant documentation.)
3. *Current System or Situation:* Describe the intelligence structure as it currently exists. If there is no current intelligence structure on which to base changes, then describe the situation that motivates development of the proposed intelligence unit.

   3.1 Background, Objectives, and Scope

   Provide an overview of the current intelligence structure including, as applicable, background, mission, goals, objectives, scope, and responsibilities for the current intelligence structure.

[11] www.cms.hhs.gov/SystemLifecycleFramework/Downloads/ConOps.pdf.

3.2 Operational Policies and Constraints

Describe the operational policies and constraints affecting the operations of the current intelligence structure. Operational policies are predetermined management decisions regarding the operations of the current system, normally in the form of general statements or understandings that guide or limit decision-making activities, but allow for some discretion. Operational constraints are limitations placed on the operations of the current system (e.g., available hours of intelligence unit operation, available number of personnel to work in the unit, networking constraints, etc.).

3.3 Description of Current System or Situation

Describe the current intelligence structure or situation that is simple and clear enough that all intended readers of the document can fully understand it. Provide a graphical overview of the current system or situation in the form of a context diagram, a top-level object diagram, or some other kind of diagram that depicts the system and its environment. The description should include the following, as appropriate:

- The operational environment and its characteristics (e.g., facilities, equipment, computing hardware, software, communications links, personnel, and operational procedures used to operate the existing system)
- Major system components and the interconnection among those components
- Interfaces to external systems or procedures
- Capabilities, functions, and features of the current intelligence structure, including types of products that are produced
- Charts and accompanying descriptions depicting inputs, outputs, data flows, control flows, and manual and automated processes sufficient to understand the current system or situation from the user's point of view
- Cost of system operations
- Operational risk factors
- Performance characteristics, such as speed, throughput, volume, frequency
- Quality attributes, such as availability, correctness, efficiency, expandability, flexibility, interoperability, maintainability, portability, reliability, reusability, supportability, survivability, and usability
- Provisions for safety, security, privacy, integrity, and continuity of operations in emergencies that exert influence on the operation or operational environment of the current system.

3.4 Current Modes of Operation

Describe the various modes of operation for the current intelligence structure (e.g., normal, imminent threat, emergency event, natural disaster) including strengths and weaknesses.

3.5 Current Users and Stakeholders

A user class is distinguished by the ways in which users interact with the current intelligence structure. Include descriptions of both internal and external intelligence users, how these users were identified, feedback from the users, and demands from users to which the intelligence structure is currently unable to respond.

3.6 Current Support Environment

Describe the support environment for the current intelligence structure, including support organizations or units; facilities; equipment; support software; and any other aspect of support. For external partners of the intelligence structure, describe the roles, responsibilities, and if a memorandum of understanding (MOU) is in place.

4. *Justification and Description of Changes:* Describe briefly the shortcomings or limitations of the current intelligence structure or the circumstances that motivated development of a new or modified intelligence structure. If there is no current intelligence structure on which to base changes, then so indicate and provide justification for the new structure.

4.1 Justification of Changes

Summarize briefly new or modified aspects of the intelligence unit's operations, including the types of analysis, products, changes, or modified mission and the reasons for those changes. Changes may be based on new national standards, a new MOU, new strategic priorities of the executive, external funding requirements, legislation, or any of a variety of factors.

It is important to articulate the reasons for change to ensure that the explicit conditions or mandates for the change are being met.

4.2 Description of Desired Changes

Summarize the new or modified capabilities, functions, processes, products, and other changes needed to respond to the factors identified in 4.1. Changes should be based on the current intelligence structure described in Section 3. If there is no existing intelligence structure on which to base changes, summarize the capabilities that a new structure will provide. The description should include the following, as appropriate:

- Capability changes
- Information processing changes
- Product changes
- Personnel changes
- Priority changes
- Partnership changes
- Support changes
- Other changes.

4.3 Priorities among Changes

Identify priorities among the desired changes and new features. Each change should be classified as essential, desirable, or optional, and a reason provided for the classification.

4.4 Changes Considered but not Included

Identify desired changes and new features considered but not included in section 4.2, and the rationale for not including them.

5. *Proposed System or Situation:* Describe the concepts for the proposed intelligence structure that results from the desired changes specified in Section 4. The description should be at a high level, indicating the operational features that will be provided without specifying design details. The description should be of sufficient detail to fully explain how the proposed system is envisioned to operate in fulfilling users' needs and the law enforcement agency's business requirements. The ConOps may contain some examples of typical design strategies for the purpose of clarifying operational details of the proposed system, but should not contain design specifications.

   5.1 Background, Objectives, and Scope

   Provide an overview of the proposed intelligence structure including, as applicable, background, mission, goals, objectives, scope, business drivers, and motivation.

   5.2 Operational Policies and Constraints

   Describe the operational policies and constraints affecting the operations of the proposed system. Operational policies are predetermined management decisions regarding the operations of the proposed system, normally in the form of general statements or understandings that guide or limit decision-making activities, but allow for some discretion.

   Operational constraints are limitations placed on the operations of the proposed system (e.g., available hours of system operation, available number of personnel to operate the system, computer hardware, and operational facilities constraints).

   5.3 Description of the Proposed Intelligence Structure

   Describe the proposed intelligence structure that is simple and clear enough that all intended readers of the document can fully understand it. Provide a graphical overview of the proposed structure in the form of a context diagram, a top-level object diagram, relationship to other intelligence entities (particularly as applied to fusion centers), structure within an agency of governmental entity, or some other type of diagram that depicts the structure and its environment. The description should include the following, as appropriate:

   - The intelligence unit's environment and its characteristics (e.g., facilities, equipment, computing hardware, software, communications links, personnel, and operational procedures used for the unit's operations)
   - Major law enforcement intelligence systems for which access is needed (e.g., RISSNET, LEO, HSIN, National Law Enforcement Telecommunication System)
   - Capabilities, functions, and features of the analytic capability including skills of analysts, analytic software, and special skills needed
   - Charts and accompanying descriptions depicting inputs, outputs, data flows, control flows, and manual and automated processes sufficient to understand the two-way information flow for the intelligence structure
   - Cost of the intelligence structure's operations
   - Operational risk factors including civil rights and privacy issues
   - Performance characteristics, such as speed, throughput, volume, frequency

- Quality attributes, such as availability, correctness, efficiency, expandability, flexibility, interoperability, reliability, and usability of intelligence products
- Provisions for security, privacy, integrity, accuracy, and continuity of operations in emergencies for the new intelligence structure.

5.4 Proposed Modes of Operation

Describe the various modes of operation for the proposed intelligence structure (e.g., normal, emergency, special threat). The intelligence structure's processes, procedures, and capabilities or functions should be related to each mode, as appropriate, perhaps using a cross-reference matrix.

5.5 Anticipated Users and Stakeholders

Specify the planned user class for the intelligence structure.

A user class is distinguished by the ways in which users interact with the proposed intelligence structure. Factors that distinguish a user class include common responsibilities, skill levels, work activities, and modes of interaction with the system.

In this context, a user is anyone who interacts with the proposed intelligence structure, including analysts, research specialists, reports officers, investigators, management decision-makers, patrol officers, trainers, and perhaps certain segments of the private sector.

5.6 Proposed Support Environment

Describe the support concepts and support environment for the intelligence structure, including partner organizations, facilities, equipment, support software, and the information-sharing environment of the intelligence structure.

6. *Operational Scenarios:* Provide step-by-step descriptions of how the intelligence structure should operate and interact with its users under a diverse set of circumstances (e.g., development of specific intelligence products as a result of a user's request; how Suspicious Activity Reports are processed through the intelligence structure; how and to whom imminent threat information would be confirmed and disseminated). The scenarios should be described in a manner that will allow readers to walk through them and gain an understanding of how all the various parts of the proposed intelligence structure functions

   The scenarios tie together all parts of the system, the users, and other entities by describing how they interact, and may also be used to describe what the system should not do. The scenarios can be presented in several different ways: for each major intelligence activity or function of the proposed structure; thread-based, where each scenario follows one type of transaction type through the proposed structure, or following the information flow through the system.

7. *Summary of Impacts:* Describe the anticipated operational and organizational impacts of the proposed intelligence structure on the staff, users/consumers, and management. Also describe the temporary impacts on the staff, users/consumers, and management during the time when the new intelligence structure is being conceptualized, during the development of the structure, while the project is being implemented, and when training is being provided. This information will allow all affected organizations and organizational units to prepare for the changes that will be brought about by the new structure and to plan for the impacts during development and transition to the new structure.

7.1 Operational Impacts

Describe the operational impacts of the proposed system on the users, system developers, and the support and maintenance organizations. The impacts to consider include the following:

- Information-sharing with primary or alternative information sources and/or systems
- Changes in procedures
- Use of new analytic methods and resources
- Changes in quantity, type, and timing of data to be entered into the system
- Changes in intelligence requirements
- New modes of operation based on imminent threats and emergencies
- New processes for responding to user analytic requests
- Changes in the operational budget.

7.2. Organizational Impacts

Describe the anticipated organizational impacts of the proposed intelligence structure, compared with current impacts, on staff, management, personnel, partners, and other users of the intelligence structure.

7.3. Impacts During Development

Describe the anticipated impacts on staff, management, personnel, partners, and other users of the intelligence structure during the development of the new intelligence structure. The impacts to consider include the following:

- Involvement in studies, meetings, and discussions prior to implementation of the new structure
- User and support involvement in testing and review of new processes and methods, including training
- Parallel operation of the new and existing structure during transition.

8. *Analysis of the Proposed Intelligence Structure:* Provide an analysis of the benefits, limitations, advantages, disadvantages, and alternatives and trade-offs considered for the proposed intelligence structure.

8.1. Summary of Improvements

Provide a qualitative (and to the extent possible, quantitative) summary of the benefits that the proposed intelligence structure will provide.

8.2. Disadvantages and Limitations

Provide a qualitative (and to the extent possible, quantitative) summary of the disadvantages and/or limitations of the proposed intelligence structure. Disadvantages might include the need to retrain personnel or change to a new style of information-sharing. Limitations might include products and services desired by users but not included as part of the new intelligence structure.

8.3. Alternatives and Trade-Offs Considered

Describe major alternatives considered, the trade-offs among them, and rationale for the decisions reached. In the context of the ConOps, alternatives are operational alternatives. For example, using shared or contract intelligence analysts, limiting the intelligence structure to only strategic or tactical analysis, or colocating the new structure with another agency, etc.

Appendixes

Use appendixes to facilitate ease of use and maintenance of the ConOps document. Each appendix should be referenced in the main body of the document where that information would normally have been provided; for example, samples of new report forms or new policy and procedures.

Glossary

Provide clear and concise definitions for terms used in the ConOps that may be unfamiliar to readers of the document.

The ConOps Next Step

As the name implies, the ConOps is intended to describe how the intelligence vision of the chief executive is conceptualized in an operational form; that is, the ConOps translates the vision into a functional model. The intent is to permit stakeholders—staff, users, management, and relevant external parties—to understand the intended dynamics and comment on different aspects of the envisioned operations. Feedback by stakeholders may be used to fine-tune the concept, as long as it stays true to its vision. The next step is to use the ConOps as a road map to implement the new intelligence structure.

Implementing and Managing the Intelligence Structure

As noted previously, the principles of management apply to the intelligence function of an agency just as they apply to any other organizational entity. The following management discussion focuses on selected elements related to the intelligence function. As will be seen, many of the issues in the following discussions will be applicable to preparing the ConOps.

Establishing an Organizational Framework

Just as any other function in a law enforcement agency, organizational attention must be given to the administrative structure of the intelligence function. Administrators and managers must examine these concerns:

- The need for the intelligence function as it relates to strategic priorities of the agency
- How the intelligence structure functions on a daily basis
- Issues of resource acquisition, deployment, and management
- Future agency requirements for the intelligence function.

Properly organized and staffed, the intelligence function serves as an internal consultant to management for resource deployment. It should be designed as an integrated and organic element of the law enforcement organization, not a distinct function. Indeed, this approach supports the effective implementation of ILP. Intelligence defines the scope and dimensions of complex criminality—including terrorism—facing the jurisdiction and provides alternatives for policy responses to those problems. Also important, it serves as a focal point for information sharing and dissemination to maximize community safety.

Some law enforcement agencies have been reluctant to fully develop an intelligence structure—including both tactical and strategic activities—for several reasons. Perhaps at the top of the list is the past abuses and subsequent lawsuits from poorly organized and managed intelligence activities. In many cases, law enforcement executives eliminated the intelligence function to reduce liability and to minimize criticism from persons in the community who did not understand the intelligence role and/or generally opposed law enforcement intelligence for philosophical reasons. Similarly, the need and value of an intelligence function has not been fully recognized by managers who often do not understand that the intelligence function can be an important resource for agency planning and operations. Intelligence analysts, for example, are frequently assigned clerical tasks such as responding to requests to check names or doing a records search of a person's background, in addition to their analytic duties, largely because the manager does not understand the value that is lost to the organization if the analyst does not have the time to devote to his or her function.

As a consequence of several factors, the zeitgeist—or spirit of the times—is now present for American law enforcement to embrace law enforcement intelligence of the 21st century. Many SLTLE agencies have established a legacy of proactive law enforcement through the use of community policing and its activities of problem solving, CompStat, crime analysis, effective internal and external communications, multidisciplinary responses to crime, and a bottom-up approach to operational direction. Moreover, since 9/11, there has been a greater development of resources and training to make intelligence activities more easily adapted and functional. Finally, the law enforcement intelligence function has become professionalized through greater involvement of academic institutions, federal initiatives, and long-standing activities by groups such as the International Association of Law Enforcement Intelligence Analysts, Inc. (IALEIA) and the LEIU.[12]

Chartering an Intelligence Unit

One of the first steps in creating an intelligence structure is to charter the function through the following steps:

- Determine its organizational structural priority and placement
- Allocate resources
- Define its mission and goals
- Establish the unit's authority and responsibility.

[12] For more information about these organizations, see their respective web pages at www.ialeia.org and www.leiu-homepage.org.

A number of publications describe these processes.[13] The current discussion will identify specific points related to the intelligence function.

The creation of an intelligence function should be based on a needs assessment.[14] This includes identifying current intelligence-related competencies of the law enforcement agency and desired competencies. One of the main outcomes of an effective needs assessment is identifying how an intelligence structure can influence the drive toward greater efficiency and responsiveness. Also important, the needs assessment will define personnel and resource needs.

Resource allocation is always a difficult process because it typically involves diminishing one function to develop another. In most cases, the creation of a new unit will not come with a new appropriation of funding to fully staff and operationalize it; therefore, part of the resource allocation process is to determine where the intelligence function fits in the organizational priorities of the law enforcement agency.

The mission of the intelligence function is the role that the unit fulfills in support of the agency's overall mission. It specifies in general language what the unit is intended to accomplish and establishes the direction and responsibility for the intelligence structure for which all other administrative actions and activities are designed to fulfill. Table 13-2 presents a sample mission statement for a law enforcement agency's intelligence unit.

A goal is the end to which all activity in the unit is directed. It is broad-based, yet functionally oriented. Important, too, the goal must be mission-related, that is, accomplishing goals supports the broader mission of the law enforcement agency. Moreover, the goals will give the unit direction in support of the mission. Since the mission of an intelligence unit will be comprehensive and incorporate diverse functions, several goals will be stipulated. The purpose of goals is to not only provide operational direction but to also serve as performance standards.[15] The environment of the community will change over time as will crime patterns and problems; therefore, the law enforcement agency should review goal statements annually and change or revise them to reflect current issues and trends. (Table 13-2 also includes an illustration of intelligence goals for a law enforcement agency.)

Authority is the right to act or command others to act toward the attainment of organizational goals. Operational authority includes decisions that must be made concerning the degree and type of activities the intelligence function may perform without seeking administrative authorization, financial flexibility of the unit to fulfill its objectives, and the degree of direction or precedence the intelligence structure can exercise over other departmental units. These factors have significant organizational implications and must be developed conceptually and stipulated by policy.

Responsibility reflects how the authority of a unit or individual is used for determining if goals have been accomplished and the mission fulfilled in a manner that is consistent with the defined limits of authority. The unit and its members must be held accountable for its charge and administrative mechanisms must be set in place to assess the degree to which the unit is meeting its responsibilities.

[13] Most police management textbooks describe these processes in detail. Perhaps of particular value are publications available from the International City Management Association bookstore.icma.org.

[14] A good illustration of a law enforcement needs assessment and how it can be performed, which includes multiple applications, is: Healy, J.J. *Needs Assessment in a Multinational Context: A Police Training Program,* Chapter 20. Superintendent, International Training and Peacekeeping Branch, Royal Canadian Mounted Police. www.rcmp-learning.org/docs/ecdd1134.htm.

[15] Performance standards are often characterized as effectiveness and efficiency, wherein effectiveness is "Doing the right job," and efficiency is "Doing the job right."

IACP Model Policy on Criminal Intelligence

The International Association of Chiefs of Police (IACP) has taken a proactive role in all aspects of developing a contemporary intelligence capacity in America's law enforcement agencies. The IACP *Model Policy*[16] on criminal intelligence contains a policy statement and procedures that are of particular benefit to a small agency. As in the case of all models, the language of the IACP policy needs to be adjusted to meet the needs of different jurisdictions. Nonetheless, it provides a sound foundation for starting the process.

Table 13-2: Sample Mission Statement and Goals of an LEI Unit

Sample Intelligence Mission Statement
The mission of the Intelligence Unit of the Hypothetical Police Department is to collect, evaluate, analyze, and disseminate intelligence data regarding criminal activity in this city/county and any criminal activity in other jurisdictions that may have an adverse effect on this city/county. This includes providing processes for collating and analyzing information collected by operational units of the law enforcement agency. The Intelligence Unit will furnish the chief of police with the necessary information so that operations units charged with the arrest responsibility can take the necessary enforcement action.
Sample Intelligence Goals
• The Intelligence Unit shall supply the chief of police with accurate and current strategic intelligence data so that the chief will be kept informed of changing criminal activity in the jurisdiction. • The Intelligence Unit shall provide a descriptive analysis of organized crime systems operating within the jurisdiction to provide operational units with the necessary data to identify organized crime groups and individuals working as criminal enterprises. • The Intelligence Unit will concentrate its expertise on the following crimes: » Islamic extremists in support of terrorism—activities, participants, funding, and logistical support, all of which are of a criminal nature. » Domestic extremists in support of criminal acts— activities, participants, funding, and logistical support, all of which are of a criminal nature. » Labor/strike activity—monitor and gather strategic intelligence to be supplied to the Operations Bureau with regard to this activity. » Organized crime—identify crimes and participants, including new and emerging criminal enterprises. » Major narcotics traffickers—provide tactical intelligence and information analysis to the Operations Bureau on persons identified as being involved in narcotics trafficking enterprises. The Intelligence Unit recognizes the delicate balance between the individual rights of citizens and the legitimate needs of law enforcement. In light of this recognition, the unit will perform its intelligence activities in a manner that is consistent with, and upholds, the civil rights privacy and lawful expressive activity of all persons.

[16] www.cops.usdoj.gov/Files/RIC/CDROMS/LEIntelGuide/pubs/IACP_Criminal_Intel_Model_Policy.pdf.

Auditing the Intelligence Function

An important tool for managing the intelligence function is to perform regular audits. The audit will provide an accountability mechanism that can help maximize efficiency and effectiveness while verifying adherence to policies and procedures. In addition, the audit can serve as a benchmarking tool to measure changes in performance of the intelligence function which, in turn, leads to continuous quality improvement.

The audit is not only an important management tool; it can also serve as a means of demonstrating accountability to the community. It is a structured method for tracking and measuring critical issues related to the intelligence function and provides assurances that the intelligence function is operating in a manner that is consistent with good management practices and within lawful constraints.

There are different kinds of audits, depending on the needs or issues associated with the intelligence function. In all likelihood, a law enforcement agency should perform diverse kinds of audits, such as the following, on a periodic basis.

- *Financial audit*. To ensure that the expenditure of funds is consistent with policy and allowable expenses, including appropriated funds and grant funds. In addition, if there is an undercover/informant budget, this should be audited on a regular basis.
- *Process audit*. To ensure that all intelligence activities are being performed in a manner that is consistent with the law enforcement agency's internal policies and procedures. This includes not only line personnel but also ensuring that supervisors are adequately performing their supervisory function.
- *Compliance audit*. To ensure that intelligence operations are consistent with law and regulations that are external to the organization, such as 28 CFR Part 23, legal mandates, and grant regulations
- *Outcome audit*. To ensure that the intelligence function is accomplishing its goals and objectives.
- *Service audit*. To ensure that the intelligence function is meeting the needs of its consumers.

The person(s) conducting the audit may be somewhat dependent on the nature of the issues associated with the intelligence function, both internal and external to the law enforcement agency. If no controversies are associated with the intelligence function, an audit by a supervisor should suffice, but if controversial issues are related to the intelligence operations, an external auditor would be preferable. Someone who has recognized integrity, such as a retired judge or a recognized business person who is a community leader, would serve well as an auditor. While the intelligence staff will need to provide the raw information to the auditor, an independent party asking questions, making judgments, and drawing conclusions about performance can serve an important role.

Appendix B is an audit checklist developed by the author and used at law enforcement agencies to ensure compliance with court orders. Appendix C is the Audit Checklist developed by the Law Enforcement Intelligence Unit.

Establishing and Managing Partnerships

The nature of the intelligence function requires that a law enforcement agency enter into partnerships. Critical information is shared through collaboration, typically with other law enforcement agencies, but often with other organizations ranging from the private sector (as discussed in Chapter 9) to nonlaw enforcement government agencies, such as public health, the fire service, or emergency operations. These various relationships have different dynamics related to needs, responsibilities, and limitations on access to information. As such, the parameters of each formal partnership should be articulated in a formal partnership agreement.

Broadly speaking, two types of partnerships are related to the intelligence function.

1. *Users.* Organizations and individuals with which information and/or intelligence products are shared. Users are consumers.
2. *Participants.* Organizations and individuals that provide resources and actively contribute to the intelligence activity, such as a regional fusion center. Participants have a shared responsibility for operations.

A formal agreement is simply sound management because it articulates mutually agreed-on operational provisions related to resource management, clear identification of responsibilities and accountability, adherence to legal standards, and conditions associated with liability. Certainly these agreements apply to a wide range of law enforcement activities or services; however, the current discussion is limited to the intelligence function. While the language varies between states, as a general rule there are three forms of written partnerships:

1. *Memorandum of Agreement (MOA).* Users/consumers of an intelligence unit or system, including a records system, that use the system on an ongoing basis would typically sign the MOA. Essentially, the MOA acknowledges that the user will abide by the rules established for the system or activity, aid in cost recovery, and adhere to legal and accountability standards. Obviously, the character of the activity will dictate more detail. As an example, if one agency's intelligence records system can be accessed by another agency, the user may have to agree to pay a monthly fee, adhere to 28 CFR Part 23, and agree to the Third Agency Rule. Failure to meet these standards would result in ending access to the system.
2. *Mutual Aid Pact (MAP).* The MAP is an agreement that is in place to deal with special circumstances, rather than an ongoing service, and establishes the agreed-on conditions when one agency would provide assistance to another. Often, assistance is reciprocal, except for real costs that may be incurred in extended activities. As an intelligence-related example, two law enforcement agencies may agree to aid each other when conducting a surveillance.
3. *Memorandum of Understanding (MOU).* The MOU is more detailed and involves a partnership in an activity. Essentially a contract, the MOU would specify all obligations and responsibilities and typically share liabilities in the endeavor. For example, if multiple agencies agree to develop a fusion center, the MOU may be a fairly detailed document outlining all aspects of governance, management, structure, funding, accountability, and operations of the center.

A key element to understand is that, regardless of the nature of the agreement, its content and detail is to ensure that all parties understand their obligations. Table 13-3 identifies some of the provisions that may be included in a partnership agreement. While not all of these provisions will be required of every agreement, it is important to have a formal document that clearly defines expectations and responsibilities.

Table 13-3: Sample Provisions for a Partnership Agreement

- Activities
- Civil liability/indemnification
- Dispute resolution
- Funding
- Governance
- Information – access and use
- Information – adherence to 28 CFR Part 23
- Information – dissemination to Third Agency
- Information – entry into a system
- Information – ownership
- Location
- Mission, purpose, goals
- Operating procedures
- Payments and costs
- Personnel assignment
- Personnel evaluation
- Personnel removal
- Physical plant considerations
- Property – purchase and maintenance
- Reports to be prepared
- Security clearances of staff
- Security of information
- Security of the facility
- Time limit/term of the agreement

Sources for Intelligence Management and Resource Trends

Effective management of an intelligence unit requires that the manager be constantly informed of emerging issues, technologies, and trends. This is a difficult process; however, one of the more effective methods is to monitor online newsletters of reliable organizations. Topics can range from emerging issues to best practices to new products and new policy and legislation. As an illustration (not an endorsement), some of the more substantive newsletters include (in alphabetical order) the following:

- Center for Digital Government (three newsletters; one specifically on homeland security) www.centerdigitalgov.com.
- *Federal Computer Week* www.fcw.com.
- Federation of American Scientists: Secrecy News www.fas.org/sgp/news/secrecy.
- Foundation for Defense of Democracies: *Weekly Update* www.defenddemocracy.org.
- *Government Computer News* www.gcn.com.
- *Government Computing* www.kable.co.uk.
- *Government Technology* www.govtech.net.
- *Homeland Security Institute Newsletter*: www.homelandsecurity.org.

- *Homeland Security Update* (DFI International) www.dfi-intl.com.
- *Homeland Security Week* www.govexec.com.
- *Homeland Security Weekly Newsletter* www.homelandsecurityweekly.com.
- PoliceOne.com (*Law Enforcement News*) www.policeone.com/policenews.
- U.S. Department of Justice, Justice Technology Information Network www.justnet.org.

As is the case with any information, and as noted in Chapter 11 on open sources, a newsletter will reflect the agenda of its sponsor. Keeping this in mind, valuable information can be gained for an intelligence manager to remain current on the issues for which he or she is responsible.

Human Resource Issues

Who should perform the intelligence function in an SLTLE agency and what qualifications should that person have? This question is impossible to answer conclusively because it depends on myriad variables tied to the attributes of a given law enforcement agency. The agency's size, jurisdiction, geographic location, the priority intelligence is given, resource flexibility, competing crime and calls for service issues and collective bargaining agreements must be calculated into the formula. Rather than provide for the ideal situation, this discussion will present issues, and guidelines that will enable the law enforcement executive to make an informed decision about options available for staffing the intelligence function.

Staffing

Clerical and support staffing decisions can be made for the intelligence function just as for any other assignment in the agency, taking into consideration professional staff workloads, service demands, nonprofessional work activities (e.g., data entry, clerical work), and budget, among others. The key positions are with the professional staff.[17]

The Intelligence Analyst

The intelligence analyst is a professional who collects various facts and documents circumstances, evidence, interviews, and other material related to a crime and places them in a logical, related framework to develop a criminal case, explain a criminal phenomenon, or describe crime and crime trends. The analyst should have at least a baccalaureate degree and receive training in the intelligence process, criminal law and procedure, statistical analysis, and factual and evidentiary analysis. The analyst should be an objective, analytic thinker with good writing and presentation skills. This is a professional position that should be compensated accordingly. Remember: Executives and managers make important operational and resource decisions based on the analysis of issues; therefore, the best qualified and best trained analysts are essential.

An ongoing issue is whether the intelligence analyst will be sworn or nonsworn. Different agencies use different models, each with its advantages and disadvantages.[18] Those who advocate that the intelligence analyst position would

[17] For more detail, see: Wells, Ian, "Staffing the Intelligence Unit," in *Intelligence 2000: Revising the Basic Elements: A Guide for Intelligence Professionals,* ed. Marilyn B. Peterson, Bob Morehouse, and Dick Wright. Lawrenceville, New Jersey: Law Enforcement Intelligence Unit and the International Association of Law Enforcement Intelligence Analysts, 2000: 53–66.

[18] The *General Counterdrug Intelligence Plan* discusses issues related to human resources in *Section E: Analytic Personnel Development and Training.* While not specifically addressing the issues in this discussion, nonetheless it provides some observations and recommendations that are germane to the issues presented herein. See ftp.fas.org/irp/ops/le/docs/gcip/index.html.

What Characteristics Are Desired in a Good Analyst?

- General factors (modified from Frost, C. and J. Morris. *Police Intelligence Reports.* Orangevale, California: Palmer Press, 1983.)
  - » Impeccable standards of honesty and integrity
  - » A thorough understanding of the concepts of :
    - Intelligence
    - Civil liberties
    - Criminal law enforcement
  - » The capacity to think in a logical and rational manner
  - » Capacity to approach situations from broad and divergent perspectives
  - » The ability to comprehend complex masses of data and communicating its contents to others
- Background factors
  - » Broad range of interests
  - » Developed research ability (library, qualitative, quantitative)
  - » Helpful previous experience (law enforcement, military, security)
- Mental traits
  - » Intellectual curiosity
  - » Rapid assimilation of information
  - » Keen recall of information
  - » Tenacity
  - » Willingness and capacity to make judgments
- Communication skills
  - » Developed writing ability
  - » Skill in oral briefing
  - » Interviewing and interrogating skills
  - » Eliciting information from officers
- Liberal arts skills
  - » Good writing ability
  - » Fluency in a second language desirable
  - » Good knowledge of geography
- Work style
  - » Initiative and self-direction
  - » Effective personal interaction
  - » Disciplined intellectual courage

be best served by a nonsworn employee argue that the nonsworn analyst's characteristics and background may provide a more creative and less restrictive view of data when compared to sworn personnel. Further, a sworn employee is likely to be either transferred or promoted out of the intelligence unit, thereby reducing the unit's overall efficiency. Advocates of having a nonsworn employee argue that the position does not require law enforcement authority; therefore

placing a sworn person in an analyst's position may be viewed as an ineffective use of personnel. Finally, the role of an analyst is highly experiential: Over the years, the experienced analysts accumulate a mental repository of names, locations, businesses, and so forth that can be highly useful in an analysis. If this person is a sworn employee who is transferred out of the unit, that accumulated knowledge is lost.

Conversely, opponents argue that nonsworn employees do not have the substantive knowledge and experience for conducting investigations nor do they understand, with the same degree of insight, the life of the street where many intelligence targets live and operate. The analyst builds his or her expertise and knowledge cumulatively throughout his or her work life. Much of this expertise is substantive knowledge and information (persons, crime patterns, locations, and so forth) learned while working on a variety of criminal cases. The analyst needs to view crime problems from the big picture—a picture that is most precisely focused with years of law enforcement street experience.

Other factors not related to the conceptual responsibilities will enter the equation such as the compensation package, collective bargaining agreement provisions, civil service regulations, organizational culture, the candidate pool, and so forth. This is a critical position requiring an effective analytic capability and care should be taken to hire the right person to fit the agency's needs. It should not be, as has too often been the case, an appointment of convenience or a reward appointment to a good clerical person who has worked hard for the department. Professional output from the intelligence unit will occur only if the position is filled by a professional analyst.

Training

The Bureau of Justice Assistance-funded Criminal Intelligence Training Coordination Strategy Working Group conducted a needs assessment of intelligence training in the spring of 2004. Among the findings were the following:

- Training is lacking in all training classifications, but respondents rated intelligence analyst and intelligence manager as the classes most lacking in adequate training. Surprisingly, 62 percent of respondents stated that they are receiving adequate training, but more than one-third (36 percent) indicated that they were not receiving adequate training.
- The majority of respondents cited lack of funding as the primary impediment of training, but respondents also rated as high the difficulty of *finding good trainers, travel and lodging costs,* and *unsure of available training*. Only a handful of respondents selected unsure of appropriate training for personnel as an impediment. *One respondent indicated that, in order to support the tenets of the NCISP, additional training guidelines and opportunities are needed.* Other respondents indicated that training can be sporadic, which dovetails into the need for core minimum standards that can be used consistently nationwide. Other respondents indicated that their agency has not needed intelligence training because they do not have the staff or resources to engage in an intelligence function.[19] (Emphasis in original).

[19] Bureau of Justice Assistance, Criminal Intelligence Training Coordination Strategy Working Group. *Survey of Law Enforcement on Intelligence Training.* Unpublished staff report, 2004.

As a result, the *Minimum Criminal Intelligence Training Standards*[20] were created, and revised in 2007. The standards were designed to "…provide perspective and guidance for the development and delivery of law enforcement intelligence training."[21] The report goes on to note:

> …It is recognized that any type of "standard" can be debated based on an individual's personal philosophy, professional priorities, and life experiences. In order to minimize bias or atypical context, the development process for these standards used a consensual approach reflecting the cumulative judgment of law enforcement intelligence practitioners, managers, executives, trainers, and scholars from all levels of government. The standards reflect the collective judgment of these subject matter experts with respect to the minimum training needed in each noted classification to provide the basic knowledge, skills, and abilities for personnel in each classification in order for them to perform their intelligence duties.[22]

Clearly, intelligence training currently represents the proverbial mixed bag of content, availability, and structure. The content or subject matter of law enforcement intelligence can be divided in two broad categories. The first category is protocols and methodology of the intelligence process. It includes subjects such as information-collection methodologies, laws and regulations associated with intelligence records systems, analytic methods and tools, intelligence reporting structures and processes, and intelligence dissemination. Essentially, these elements constitute the discipline of law enforcement intelligence.

The second category is somewhat more amorphous. Broadly speaking, the category is subject matter expertise. It includes understanding the motives, methods, targets, and/or commodities of criminal intelligence targets. Intelligence researchers and analysts must have subject matter knowledge of the types of enterprises that are being investigated and the context within which these enterprises occur. Whether the target crime is terrorism, drug trafficking, money laundering, or the trafficking of stolen arts and antiquities, the intelligence analyst must be a subject matter expert on the genre of criminality being investigated, both broadly speaking, as well as with the unique facts associated with a specific investigation.

An intelligence analyst working on cases of terrorism by Islamic extremists, for example, needs to substantively understand the distinctions between Shiite and Sunni Muslims, the role of sectarian extremism (notably as related to Palestine), the different Islamic terrorist groups (e.g., al-Qaida, HAMAS, Hezbollah, Islamic Jihad), and their methods, the culture of Muslim nations, different leaders, methods of funding, and so forth. Such substantive knowledge is essential for an analyst to be effective.

[20] it.ojp.gov/documents/min_crim_intel_stand.pdf

[21] Intelligence Training Coordination Working Group. *Minimum Criminal Intelligence Training Standards.* Washington, D.C.: Global Intelligence Working Group, 2007, p. 1.

[22] Ibid.

All training programs currently available contain some aspect of the protocols and methodology of the intelligence process, although most programs for nonanalysts provided an overview of these issues rather than detailed instruction. Fewer programs contained subject matter information for intelligence as part of the training. For those that did provide this information, it was typically because the agency sponsoring the training had a specific jurisdictional responsibility (e.g., the Regional Counterdrug Training Academy's[23] Operational Intelligence course integrates "intelligence concepts" with more specific "drug intelligence indicators").

Training programs continue to emerge on intelligence related topics, most notably funded by the Bureau of Justice Assistance, U.S. Department of Justice, and the Office of Training and Exercise Integration (TEI), Federal Emergency Management Agency, U.S. Department of Homeland Security.[24] Perhaps the best single source for monitoring training programs of all types is through the National Criminal Intelligence Resource Center Master Criminal Intelligence Training Calendar.[25]

[23] www.rcta.org

[24] For example, the Michigan State University School of Criminal Justice has grants from the DHS to offer intelligence training for state, local, and tribal law enforcement agencies nationwide at no cost. For more information see intellprogram.msu.edu.

[25] mastercalendar.ncirc.gov

Table 13-4: Intelligence Training Categories and Descriptions

Training	Description
Awareness	The broadest, most diverse types of intelligence training could best be described as "awareness" training. These programs, which vary in length from 2 hours to 4 days, tend to include information about the intelligence discipline (i.e., definitions, methods, processes, etc.) as integrated with a specific subject matter (e.g., drugs, terrorism, auto theft, etc.). The Bureau of Justice Assistance State and Local Anti-Terrorism Training (SLATT), Federal Law Enforcement Training Center (FLETC), and other groups offer this training throughout the U.S.
Intelligence Analyst	Intelligence analysts training programs have a reasonable degree of consistency in the subject matter topics; however, the hours of training on each topic have more variability. In some cases, the curricula include substantive modules on subject matter: For example, the FBI Center for Intelligence Training program integrates intelligence methods specifically with crimes within FBI jurisdiction. Similarly, Drug Enforcement Administration (DEA) curricula integrates intelligence methods with material on drug trafficking. The most widely used analytic training program is the Foundations of Intelligence Analysis Training offered by the National White Collar Crime Center (NW3C), the International Association of Law Enforcement Intelligence Analysts, and the Law Enforcement Intelligence Unit.
Investigators and Intelligence Unit Researchers	Some intelligence training programs lack the depth of training found in the Analyst curricula, but are more detailed than simply "awareness" training. It appears that the intended audience for these programs is investigators, investigative analysts, or intelligence researchers. In each case, the curricula are similar. Notable among these courses are the 2-week DEA Federal Law Enforcement Analysts Training (FLEAT) course and the FLETC intelligence course.
Executive and Management Issues for Intelligence	Two programs funded by the Bureau of Justice Assistance are in the category: *Criminal Intelligence for the Chief Executive* and the *Intelligence Commanders Course.* In addition, the FLETC offers chief executive training, and an intelligence course at the FBI National Academy is designed for SLTLE enforcement managers.
Specialized Training	This training focuses on a narrow aspect of the entire intelligence process. The best known of these courses is the *Criminal Intelligence Analysis* course offered by Anacapa Sciences, Inc.,[27] that focuses exclusively on the "analysis" component of the intelligence cycle. Other courses that fall into this category are generally software courses such as classes on how to use a particular type of intelligence software (typically either analytic software or databases).

[26] NW3C also offers the course, *Advanced Criminal Intelligence Analysis to Prevent Terrorism*.

[27] Anacapa is a private company. This reference should not be considered an endorsement of the product by the author, the Department of Justice, or any of its components. It is used only as a descriptive illustration.

Categories of Currently Available Intelligence Training Programs

A wide range of programs has been developed on various aspects of law enforcement intelligence. Virtually all were developed before the standards and specifications in the *National Criminal Intelligence Sharing Plan* were established. Table 13-4 describes the five categories of available training programs.

A few law enforcement intelligence training programs serve as core programs because of their consistency and the expertise they offer. A great deal of experience and thought has served as the basis for their development and, as such, they provide models for good practice. For example, the *Intelligence Toolbox* that is offered nationwide by Michigan State University and funded by the Department of Homeland Security, FEMA/TEI, is a comprehensive training program designed to provide a law enforcement agency with all the tools needed to develop a contemporary intelligence capacity that meets all national standards.[28] The following summary descriptions of the most notable programs will provide more insight.

Federal Bureau of Investigation Center for Intelligence Studies[29]

After the terrorists' attacks of 9/11, the Attorney General mandated the FBI to focus on terrorism as its top priority. This necessitated a number of changes in the FBI, including expanding its law enforcement intelligence capability and working closely with state and local law enforcement agencies on terrorism investigations through Joint Terrorism Task Forces (JTTF) and Field Intelligence Groups (FIG). Among the needs precipitated by these changes was a significant broadening of the capacity for intelligence analysis among FBI personnel as well as among state and local JTTF and FIG intelligence staff. The FBI's Center for Intelligence Training, created in 2002 (formerly the College of Analytic Studies) and located at the FBI Academy, offers a range of courses for FBI agents, FBI intelligence analysts, the FBI National Academy, and courses for state, local, and tribal law enforcement.

Drug Enforcement Administration[30]

The DEA has long been recognized for the quality of training it provides through the Intelligence Training Unit of the DEA Academy at Quantico, Virginia. DEA intelligence training focuses on information research and intelligence analysis through the 9-to-10-week (it varies) *Basic Intelligence Research Specialist* (BIRS) program. DEA also offers an advanced intelligence training program as well as specialized programs related to the use of different databases and the classified DEA proprietary intelligence computer system, MERLIN.

Because of the DEA's historic role of working with state and local law enforcement agencies, and the inherent need for intelligence in the Organized Crime Drug Enforcement Task Force and the High Intensity Drug Trafficking Areas (HIDTA), DEA developed its 4-week FLEAT program specifically directed toward state and local law enforcement agencies. The program is offered in different cities throughout the U.S. to enhance the ability of state and local agencies to send intelligence

[28] intellprogram.msu.edu

[29] For enrollment information, contact the training coordinator at your local FBI Field Office. See www.fbi.gov/contact/fo/fo.htm or the FBI Academy www.fbi.gov/hq/td/academy/academy.htm.

[30] For further information on DEA training see www.usdoj.gov/dea/programs/training.htm.

personnel to this tuition-free program. While the program has historically focused exclusively on drug enforcement and money laundering, it is being revised to include a component related to both domestic and international terrorism.

Federal Law Enforcement Training Center[31]

Serving 72 federal law enforcement agencies, FLETC has a massive training responsibility. Predominantly through the Center for State and Local Law Enforcement Training, FLETC offers three courses:

1. *Intelligence Awareness for Law Enforcement Executives Training Program.*
2. *Introductory Intelligence Analyst Training Program.*
3. *Anti-Terrorism Intelligence Awareness Training Program.*

In addition, there is a wide range of other courses related to intelligence and counterterrorism. All information on courses and enrollment is listed on the FLETC web site.[32]

Other Programs and Training Resources

Law enforcement intelligence training continues to evolve, and a number of important initiatives are now underway to deliver improved basic and specialized training at the state and local levels. In addition to the programs described so far, intelligence training initiatives include the National White Collar Crime Center's *Analyst Training Partnership,*[33] HIDTA,[34] and the SLATT[35] program, have both direct and indirect intelligence awareness training.

Beyond these programs, several COPS Office Regional Community Policing Institutes (RCPI) offer a range of counterterrorism training programs, some of which include components of intelligence awareness training. Agencies should contact the RCPI in their region to determine training program offerings.[36]

For a comprehensive view of current intelligence training, including the relationship to the minimum training standards, see *Law Enforcement Intelligence Training: A Mission-Critical Element of Domestic Security* by Merle Manzi.[37]

Intelligence Courses in Higher Education

In recent years, there has been increasing recognition in the academic community of the need for coursework in intelligence that incorporates broad multidisciplinary issues, research, and a philosophical approach to intelligence issues. Increasing numbers of colleges and universities are offering courses and degrees in intelligence studies. Indeed, growth has been so significant that a new organization was formed to represent them, the International Association for Intelligence Education.[38] Most focus on the national security Intelligence Community.

Acknowledging the author's prerogative, there is one higher education program that focuses exclusively on law enforcement intelligence. The nation's oldest criminal justice degree program at Michigan State University (MSU) has offered a cross-listed undergraduate/graduate course entitled *Law Enforcement Intelligence*

[31] FLETC is part of the Department of Homeland Security. For details and contact information see www.fletc.gov/about-fletc.

[32] See www.fletc.gov/training.

[33] This includes the International Association of Law Enforcement Intelligence Analysts, the Law Enforcement Intelligence Unit, and the Regional Information Sharing Systems. For training opportunities see www.nw3c.com/ocr/courses_desc.cfm.

[34] A number of the HIDTA initiatives have intelligence-related training programs. See www.whitehousedrugpolicy.gov/hidta to find an HIDTA office. In addition, the Washington-Baltimore HIDTA often lists a wide range of training programs, including those that are intelligence-related. See www.hidta.org/training/law_enforcement.asp.

[35] See www.iir.com/slatt/training.htm.

[36] To find an RCPI near you, call the COPS Office Response Center at 800.421.6770.

[37] Manzi, Merle. *Law Enforcement Intelligence Training: A Mission-Critical Element of Domestic Security. Intelligence Police Papers Series.* East Lansing, Michigan: Intelligence Program, School of Criminal Justice, Michigan State University, January 2008. intellprogram.msu.edu/resources/policy-papers.php.

[38] www.iafie.org

Operations for approximately 20 years. As a result of a partnership created with DEA, MSU developed a master's degree in law enforcement intelligence and analysis.[39] The degree program, offered completely online, is taught by regular MSU criminal justice faculty members, and is designed as a terminal degree, much like a master of business administration. In addition, MSU offers a certificate program in different aspects of intelligence, many of which are available for academic credit. Clearly, the demand for academic preparation for an intelligence career is a growing market.

Conclusion

This chapter provided an overview of selected issues in the management of the law enforcement intelligence function. As a rule, the application of management principles may be applied generally, regardless of the unit or assignment within a law enforcement agency. The intelligence unit checklist and the ConOps discussion were particularly directed to assist SLTLE agencies to develop or reengineer their intelligence capacity to meet current national standards.

Criminal investigation commanders need to understand caseload differentials for crimes, patrol commanders must know minimum staffing requirements to handle calls for service, and traffic commanders must understand traffic analysis and its application to selective enforcement. It is no different with the intelligence commander. This chapter identified critical substantive elements of the intelligence function that will aid the law enforcement manager to manage this activity more effectively.

[39] www.cj.msu.edu

Chapter Annex 13-1
10 Simple Steps to Help Your Agency Become Part of the National Criminal Intelligence Sharing Plan[40]

1. Recognize your responsibilities and lead by example.

   Recognize the value of sharing intelligence information within your own agency, and encourage the practice of sharing information with other law enforcement and public safety agencies. Use the guidelines and action steps outlined in the *National Criminal Intelligence Sharing Plan* ("Plan") to implement or enhance your organization's intelligence function.

2. Establish a mission statement and a policy to address developing and sharing information and intelligence data within your agency.

   The Plan provides model policies and guidelines for implementing or reviewing an agency's intelligence function. Examples include Criminal Intelligence Systems Operating Policies federal regulation 28 CFR Part 23, the International Association of Chiefs of Police's *Model Policy for Criminal Intelligence*, and the Law Enforcement Intelligence Unit's (LEIU) *Criminal Intelligence File Guidelines.*

3. Connect to your state criminal justice network and regional intelligence databases, and participate in information-sharing initiatives.

   Many states provide access to other government databases, including motor vehicles, corrections, and others. Regional intelligence databases and sharing initiatives promote communication and collaboration by providing access to other agencies' and organizations' investigative and intelligence data.

4. Ensure that privacy issues are protected in policy and practice.

   The protection of individuals' privacy and constitutional rights is an obligation of government officials and is crucial to the long-term success of criminal intelligence sharing. The Plan provides guidelines that support policies which will protect privacy and constitutional rights while not hindering the intelligence process. Implementing and supporting privacy policies and practices within your agency will also reduce your organization's liability concerns.

5. Access law enforcement web sites, subscribe to law enforcement listservs, and use the Internet as an information resource.

   Many web sites on the Internet and others on closed networks provide valuable intelligence assessments and news. Listservs provide instant and widespread communication for investigators, and allow both the receipt and distribution of intelligence information. The Internet provides a wealth of open-source information, including government information and access to private agencies that share with law enforcement.

6. Provide your agency members with appropriate training on the criminal intelligence process.

   Some training models or modules are already found in Internet-based and interactive CD-ROMs, such as the International Association of Law Enforcement Intelligence Analysts (IALEIA), National White Collar Crime Center, and LEIU "Turn Key Intelligence." A listing of available intelligence training sources and specifically scheduled classes is found on the IALEIA Web site: www.ialeia.org. This listing allows individuals to directly contact training source agencies and organizations for more information on classes and schedules.

[40] Bureau of Justice Assistance. *10 Simple Steps to Help your Agency Become Part of the National Criminal Intelligence Sharing Plan.* Washington, D.C.: 2005.

7. Become a member of your in-region Regional Information Sharing Systems® (RISS) center.

   RISS operates the only secure web-based nationwide network for communication and exchange of criminal intelligence information by participating local, state, federal, and tribal law enforcement member agencies. RISS partners with other law enforcement systems to electronically connect them to RISSNET, including High Intensity Drug Trafficking Areas (HIDTA) Investigative Support centers, and other federal and state agency systems.

8. Become a member of the FBI's Law Enforcement Online (LEO) system.

   The FBI's LEO system is a sensitive but unclassified, real-time information-sharing communications system for all levels of the law enforcement community available at no cost to its approximately 40,000 users. LEO provides secure e-mail capability, a national alert mechanism, and access to more than 125 special-interest groups for sharing information by providing access to other networks, systems, databases, and other services.

9. Partner with public and private infrastructure sectors.

   Regular communication with the entities that control America's critical infrastructures such as energy, agriculture, transportation, and shipping is critically important to ensuring the safety and security of the citizens in your community.

10. Participate in local, state, and national intelligence organizations.

    In most areas of the country, there are locally based intelligence organizations that welcome participation from all agencies and are often affiliated with state and national organizations.

Chapter Annex 13-2
Why Law Enforcement Agencies Need an Analytic Function[41]

1. Helps solve criminal investigations.

   The analytical function develops a variety of intelligence products to assist investigators in detecting, preventing, and responding to criminal and terrorism activities. Analytical personnel initiate inquiries, conduct information searches, and act as a central point for information gathered.

2. Increases the ability to prosecute criminals.

   Personnel assigned to the analytical function develop summary tables, charts, maps, and other graphics for use in a grand jury or trial. Analysts provide factual and expert testimony and organize evidence for presentation in court.

3. Supports the chief executive and the agency's mission.

   By maximizing the analytical function, the chief executive can obtain important information and intelligence to possibly prevent future criminal activities. Personnel can prepare materials to assist in allocating resources; developing budget and resource requests; and preparing departmental reports, investigative briefings, and press releases.

4. Proactively informs law enforcement officers of crime trends and develops threat, vulnerability, and risk assessments.

   The analytical function provides support to tactical and strategic operations. Personnel analyze crime reports, identify crime hot spots, develop crime bulletins and summaries, study serial crime data, and forecast future crime. The analytical function develops proactive intelligence products that assess the potential threats of crime groups or criminal activities and recommends methods to intervene in these threats.

5. Trains law enforcement and other intelligence personnel.

   Staff develop course modules on intelligence and analytic methods and provide awareness and methodology training to agency members, executives, and managers.

6. Assists in the development of computerized databases to organize information and intelligence.

   Personnel within the analytical function help in the development and maintenance of systems that collect, collate, retrieve, and disseminate information. Analytical staff participate in departmental testing and acquisition of investigative, intelligence, and analytical software.

7. Fosters meaningful relationships with other law enforcement personnel.

   Analytical staff interact with other law enforcement agencies and build relationships with peers, allowing them to quickly obtain information and efficiently assist in multijurisdictional or complex cases. Through contact with national programs and professional associations, personnel are able to ascertain national issues that may affect local agencies.

[41] Bureau of Justice Assistance. *Why Law Enforcement Agencies Need an Analytical Function.* Washington, D.C.: Bureau of Justice Assistance, October 2005.

8. Ensures compliance with local, state, tribal, and federal laws and regulations.

   Analytical personnel provide expertise and knowledge in the development of protocols to ensure compliance with local, state, tribal, and federal laws and rules that govern intelligence sharing, privacy, and civil liberties.

9. Provides support to fusion centers.

   Personnel provide support to local, state, or regional fusion centers by performing intelligence services such as crime-pattern, association, telephone-toll, and financial analysis. They create intelligence reports, briefs, threat assessments, and other intelligence products to aid in the prevention and deterrence of crime, including terrorism.

Chapter 14:

Summary, Conclusions, and Next Steps

Summary, Conclusions, and Next Steps

Effective law enforcement intelligence operations are sometimes confusing to understand, frequently controversial, and often challenging to implement. Yet, intelligence operations can be an effective tool for community safety.

Intelligence is *confusing* because many people do not make the distinction between law enforcement intelligence and national security intelligence. Moreover, the term is used generically to describe a wide body of activities, thereby contributing to the confusion. Added to this is the development of the Information Sharing Environment, which is not only changing our information-sharing relationships, but also making the demarcation between law enforcement and national security somewhat more difficult to discern on matters of terrorism. One purpose of this guide was to provide consistent and clear definitions and processes that are accepted by law enforcement intelligence professionals and reflect national standards and initiatives in intelligence to help reduce the confusion.

Law enforcement intelligence operations are *controversial* both because of the checkered history of intelligence activities as well as the concern of many today that in the zeal to prevent terrorism, citizens' civil rights will be abridged. There is no doubt that law enforcement suffered setbacks as a result of lawsuits against law enforcement intelligence practices of the 1950s and 1960s. With those setbacks, however, important lessons were learned that not only set the stage for 28 CFR Part 23, but helped lay the foundation for law enforcement intelligence as a profession. Further controversies face law enforcement today as concerned citizens and civil rights groups, who often do not fully understand the intelligence function, fear that law enforcement agencies will gather and keep information about citizens who have not committed crimes but are exercising their constitutional rights on controversial issues. The lessons law enforcement has learned from public education and community policing initiatives can help eliminate these fears—not only through the practice of ethical policing[1] but also by reaching out to diverse communities to explain police practices, responding to questions, and establishing open, trusted lines of communication.[2]

Intelligence operations are *difficult,* as well. It requires changes in processes and changes in interagency relationships to establish links with different law enforcement organizations and groups to maximize effective information sharing. It also requires a redistribution of resources to make the intelligence function perform effectively and to meet operational and training standards set out in the *National Criminal Intelligence Sharing Plan* and the *Minimum Criminal Intelligence Training Standards.* A change in culture is required for Intelligence-Led Policing to become a reality and a realignment of priorities may be needed to accomplish new goals. There is always resistance to change and always legitimate competing interests that must be weighed.

Finally, law enforcement intelligence processes can be *effective*. Intelligence can help identify threats to a community whether from terrorists, organized crime, or even noncriminal hazards. It takes diverse and often disparate information,

[1] The COPS Office Regional Community Policing Institutes (RCPI) have a variety of training curricula for executives and line officers on different aspects of ethical policing. Agencies should contact the RCPI in their region for training opportunities. For more information about an RCPI near you, call the COPS Office Response Center at 800.421.6770.

[2] The COPS Office sponsored an executive session with the Police Executive Research Forum that examined this topic. The resulting document is a valuable resource: Davies, Heather J., Murphy, Gerard R., et al. *Protecting Your Community from Terrorism: Strategies for Local Law Enforcement. Volume 2: Working with Diverse Communities.* Washington, D.C.: U.S. Department of Justice Office of Community Oriented Policing Services and the Police Executive Research Forum, March 2004. www.cops.usdoj.gov/RIC/ResourceDetail.aspx?RID=168.

integrated into a cohesive package, to provide insight that might otherwise be lost. Increasingly, law enforcement intelligence is more thorough, of higher quality, and disseminated more effectively as a result of cooperative initiatives by the Criminal Intelligence Coordinating Council, the Global Intelligence Working Group, and the Counterterrorism Training Coordination Working Group, as well as various cooperative initiatives in the Department of Justice, notably the Office of Community Oriented Policing Services and the Bureau of Justice Assistance, as well as the Department of Homeland Security (DHS) through the Intelligence and Analysis Directorate, and the Federal Emergency Management Agency through its Offices of Training and Exercise Integration/Training Operations. Similarly, there is a greater emphasis on law enforcement intelligence, punctuated by the creation of the fusion centers, and a renewed spirit of partnership between the FBI and state, local, and tribal law enforcement (SLTLE) agencies that is already bearing fruit. FBI and DHS personnel are working side-by-side with SLTLE personnel in many fusion centers to cooperatively resolve criminal threats facing our communities. The end result of all of these initiatives is to make our communities safer. The investment pays important dividends for protecting our citizens.

Challenges for the Future

When examining challenges for the future, the most effective method is to use a strategic approach that takes a macro view of critical trends and determines their impact on the law enforcement environment. An interesting and relevant study comes from the Intelligence Community as a project from the Office of the Director of National Intelligence (ODNI) that seeks to identify trends that threaten U.S. sovereign principles during the coming decade. The report observed the following:

> [m]any drivers and trends are shaping the future global environment in which the Intelligence Community must operate —demographic and social change, increased economic integration and competition, rapid technological innovation and diffusion, environmental pressures and growing energy demand, broad geopolitical changes, and new forms of governance. Each driver and trend independently produces unique changes and challenges; those points where factors intersect often reinforce and amplify the effects of change and create a series of complex and often unpredictable threats and risks that **transcend geographic borders and organizational boundaries.**[3] (Emphasis in original.)

These same trends that have potential effects on national security will also affect our local communities. At the least, they have an impact on public order and most likely influence major crime trends that are diverse and transjurisdictional in nature.

> The ODNI report goes on to observe:
>
> To these persistent threats we add a growing array of emerging missions that expands the list of national security (and hence, intelligence) concerns to include infectious diseases, science and technology surprises,

[3] McConnell, J. M. *Vision 2015: A Globally Networked and Integrated Intelligence Enterprise.* Washington, D.C.: Office of the Director of National Intelligence, 2008, p. 4.

> financial contagions, economic competition, environmental issues, energy interdependence and security, cyber attacks, threats to global commerce, and transnational crime. Foremost among these challenges is the **blurring** of lines that once separated **foreign and domestic intelligence,** and the increased importance of homeland security. By necessity, we must be involved with numerous new partners in interactive relationships, but we must also **respect and maintain the privacy and civil liberties of all Americans.**[4] (Emphasis in original.)

Thus, like the Intelligence Community, law enforcement intelligence will have increasing responsibility to manage all-hazards types of threats while working in a broadened environment of information sharing. The challenges are not only to learn to deal with these new threats and new disciplines but to do so while ensuring the constitutional guarantees of all people.

These are sobering challenges that we must begin to confront now. The safety of American society cannot wait to react; rather, we must be proactive. This, of course, is difficult to do. The challenges of handling current problems on a much broader scale than ever, while at the same time experiencing proportionately smaller budgets, requires creativity and new ways of solving problems.

While law enforcement and the Intelligence Community have made significant, and necessary, investments in technology, success in the production and application of intelligence relies on people. Law enforcement needs to recognize that the creativity to solve the complex problems of the future will require "the best and brightest" to work in government service. Effective and creative analysis of problems can help lead to interventions and solutions. Not only must law enforcement leaders explore the problems of the future, it must also examine the law enforcement culture of today. Analysts must be compensated and treated as equal professionals in law enforcement organizations. The changes that are required to prepare our organizations must begin now, because the process can be long and challenging. One approach is to use a model the author refers to as R-cubed.

Implementing Change: The R-Cubed Approach[5]

Implementing new intelligence initiatives can be difficult. As a road map to accomplish this, the author recommends a process referred to as "R-cubed": Reassessing, Refocusing, and Reallocating (R^3).

The intent of the R^3 exercise is to provide a framework for organizational change as related to intelligence responsibilities. It requires a critical self-assessment of responsibilities and resources, objectivity absent special interests, realistic perspectives, tactical and strategic considerations of traditional and new policing responsibilities, and methods (including financing) of how all police responsibilities will be accomplished. This is a labor-intensive, difficult process that cannot be rushed and should be inclusive; that is, consideration of the inputs of others—employees, community members, elected officials, other agencies—should be included in the process. Final decisions, however, remain with law

[4] Ibid.

[5] Carter, David L. *The Police and Community.* 7th Ed. Englewood Cliffs, New Jersey: Prentice Hall, Inc., 2000.

enforcement executives to make changes as best determined by their collective judgment of responsibilities, priorities, and available resources. A number of factors may be included in each component of the R^3 exercise.

Reassessing

Examine both current priorities and new priorities for intelligence and homeland security to determine what activities need to be continued to maintain community safety and fulfill the law enforcement mission related to crime, order maintenance, and counterterrorism. This assessment should include consideration of a number of variables, such as the following:

- The number of calls for service received by a law enforcement agency and the ability to handle them.
- Specialization currently in the police department, e.g., gangs, narcotics, school programs, initiatives directed toward senior citizens, traffic, etc., and the true demand or need for each specialization.
- Objectivity is critical because special interests can skew priorities.
- Specialization that needs to be developed, e.g., intelligence capacity, first-responder (including weapons of mass destruction), computer crime/cyberterrorism prevention and investigative expertise, investigative capacity for terrorism, obligation to assign personnel to the Joint Terrorism Task Force, and expertise in all-hazards threats that can effect public safety and public order.
- Resources that can be used to help with police responsibilities of all forms, e.g., police reserves, volunteers, expertise in other agencies, community organizations.
- Objective assessment of threats and potential targets within the community and within the region. The latter includes how multijurisdictional crime and terrorist threats would affect an agency directly and indirectly, including mutual aid obligations.
- Current intelligence expertise and practices, including information sharing, and the need to modify these practices, including adding a private-sector component for critical infrastructure.
- Political mandates from elected officials and/or the community that should not be ignored because expectations and concerns of these groups must be taken into account in any assessment process.

Refocusing

Guided by the results of the reassessment, a department must develop a plan of change that incorporates its new priorities, as appropriate. Virtually all of the department's current tasks will continue in some form, but the amount of emphasis and proportion of resources devoted to those tasks will differ, notably in light of added homeland security responsibilities.

Refocusing first requires the department to establish its new priorities by reassessing and evaluating its responsibilities. From there it can it can refocus on its priorities, if needed. While reassessment involves information gathering and analysis, refocusing is the development and implementation of policy steps to make the changes operational.

Second, each area of responsibility must be weighted (i.e., weight constitutes the amount of emphasis given to each broad area of tasks and determines which area receives the greatest amount of attention.) The author does not suggest that intelligence should be the top priority; indeed, in most police agencies managing calls for service will remain the top priority. Instead, this is a realistic expectation that priorities will change with the addition of intelligence/homeland security and that all responsibilities will be affected to some degree. To determine this realignment, responsibilities and weights must be stipulated.

Third, these changes are actually implemented through the issuance of updated (and new, when applicable) policies, procedures, and orders. Implementation also requires communication and, in some cases, in-service training, to explain and clarify the changes.

Reallocating

Once refocusing decisions have been made, the department must reallocate its resources to meet adjusted priorities. This includes personnel, operating expenses, equipment (from cars to radios to computers) and office space, as needed. There is always the possibility that the department will receive an increased appropriation for homeland security in its budget, but it should not be counted on. If so, most likely it will be only a proportion of actual resource needs. The difficult process of reallocation is a necessity that will produce some alienation and, in all likelihood, political rifts within the organization. Reallocation, therefore, also requires effective leadership to guide the organization and motivate personnel to understand the necessity of the changes and the concomitant benefits to the community.

There is no explicit recipe for change in an organization. This is particularly true with intelligence where a renewed emphasis is given to a process that is largely not understood by most personnel. There is little guidance and, despite the best plans, time will be needed for experimentation. Agencies should take the time to carefully consider all new responsibilities, balance them with legitimate competing demands within the agency, and make a clear step toward adjusting the organization.

Conclusion

As demonstrated throughout this guide, America's law enforcement agencies are facing a new challenge. Throughout the history of policing, challenges have been faced, they have been met with resolute determination, and America has been safer as a result. This new challenge is no different. The intent of this *Guide* has been to help America's state, local, and tribal law enforcement agencies make this journey.

Figures/Tables

Figures

Figure 2-1: Classes of Intelligence 10
Figure 2-2: Diverse Information Collected for Intelligence Analysis 11
Figure 2-3: Law Enforcement and National Security Intelligence Authority Comparison 18
Figure 4-1: Intelligence Process, NCISP 58
Figure 4-2: Intelligence Process and Subprocesses 58
Figure 4-3: Threat Assessment Components for Planning and Direction 60
Figure 4-4: Simplified Threat Assessment Illustration 61
Figure 4-5: Processing and Collation Activities 65
Figure 4-6: Example of Reliability and Validity Rating Scales 66
Figure 5-1: Comparison of CompStat and Intelligence-Led Policing 90
Figure 6-1: Three Phases of ILP Development in an SLTLE Organization 99
Figure 6-2: Structure of the Information Management Plan 101
Figure 6-3: Components of ILP 111
Figure 6-4: ILP Continuum of Variables 120
Figure 6-5: ILP Subcontinuums of Variables 121
Figure 7-1: Intelligence Records Submission Decision Tree 152
Figure 7-2: Strategies to Ensure Civil Rights Protections 161
Figure 8-1: Organizational Interrelationships and Responsibilities for the Fusion Process and ISE 181
Figure 8-2: The Fusion Process 182
Figure 9-1: Establishing a Public-Private Partnership for Intelligence 223
Figure 9-2: Nassau County (New York) Police Department SPIN Project Diagram 227
Figure 10-1: Suspicious Activity Reporting Model 241
Figure 10-2: Nationwide Suspicious Activity Reporting Cycle 250
Figure 10-3: Characterizations of Law Enforcement Intelligence Requirements 257
Figure 10-4: The Analytic Process 263
Figure 10-5: Critical Characteristics of Information Quality 266
Figure 10-6: Illustrations of Analytical Charting 269
Figure 10-7: Characteristics of Intelligence Products 275

Figure 10-8: Attributes of Intelligence Products 276

Figure 11-1: Example of Entering Proxy Server in MS Explorer..... 313

Figure 12-1: Steps in the FBI Security Clearance Process for SLTLE Personnel 328

Figure 12-2: Examples of CUI Document Markings..... 333

Figure 13-1: Process for the Development of a Concept of Operations..... 384

Tables

Table 2-1: Comparative Illustrations of Information and Intelligence 12

Table 3-1: National Crime Commissions in the U.S., 1931–2004..... 38

Table 3-2: Significant Post-9/11 Law Enforcement Intelligence Initiatives 44

Table 5-1: Examples of Topics in a Public Education Program 94

Table 5-2: Examples of Actions the Public Can Take 94

Table 6-1: Seven Components of the Information Management Plan 100

Table 6-2: Examples of ILP Strategic Practices 106

Table 6-3: Organizational Self-Assessment Factors of an Intelligence Led-Policing Capacity 123

Table 7-1: Counterpositions on First Amendment Information Collection..... 144

Table 7-2: Questions to Determine if Records Must Comply with 28 CFR Part 23 Regulations 155

Table 8-1: Topics in the *Fusion Center Guidelines* 173

Table 8-2: Analogy of a Crime Lab and a Fusion Center 180

Table: 9-1: Sectors of Private Industry 214

Table 9-2: Sample Components of a Release and Nondisclosure Agreement Regarding Proprietary Information 220

Table 10-1: Interpretation and Illustration of the Rumsfeld Quote 251

Table 10- 2: Traditional Collection versus Requirements-Driven Collection 253

Table 10-3: Differences between Investigation and Intelligence Reports..... 273

Table 10-4: Case Intelligence versus Intelligence Products..... 274

Table 11-1: Comparison of Expressive Statements and Statements with a Criminal Nexus..... 292

Table 11-2: Examples of Information Obtainable from Subscription Database Services..... 298

Table 12-1: Information Categories for Classified Information 324

Table 12-2: Information Categories Prohibited or Limited for Classification 325

Table 13-1: Sample Issues for Intelligence Unit Policy Development..... 379

Table 13-2: Sample Mission Statement and Goals of an LEI Unit 394

Table 13-3: Sample Provisions for a Partnership Agreement..... 397

Table 13-4: Intelligence Training Categories and Descriptions..... 403

Bibliography/Appendixes

Bibliography

Advisory Panel to Assess Domestic Response Capabilities for Terrorism involving Weapons of Mass Destruction. *Implementing the National Strategy.* Washington, D.C.: RAND Corporation, 2002.

Allen, C. E. *Testimony of the Under Secretary for Intelligence and Analysis before the Senate Committee on Homeland Security and Governmental Affairs: Assessing the Nuclear Attack Threat*, April 2, 2008.

Allen, C. E. *Information Sharing at the Federal, State and Local Levels. Statement for the Record before the United States Senate Committee on Homeland Security and Governmental Affairs,* July 23, 2008.

Allen, C. E. DHS Under Secretary for Intelligence and Analysis. *Address to the Washington Institute for Near East Policy.* Washington, D.C.: May 6, 2008.

American Friends Service Committee. *The Police Threat to Political Liberty.* Philadelphia: American Friends Service Committee, 1979.

Attorney General's Report to Congress on the Growth of Violent Street Gangs in Suburban Areas. Washington, D.C.: U.S. Department of Justice, 2008.

Background on the Controlled Unclassified Information Framework. Unpublished background paper. Washington, D.C.: Executive Office of the President, May 9, 2008.

Baginski, M. Remarks in a keynote address at "Community Policing for America's Future: National Community Policing Conference," Office of Community Oriented Policing Services. Washington, D.C.: June 22, 2004.

Best, R. and A. Cumming. *Open Source Intelligence (OSINT): Issues for Congress. CRS Report for Congress.* Washington, D.C.: Congressional Research Service, December 5, 2007.

Best, R. and H. A. Boerstling. *The Intelligence Community in the 21st Century.* House of Representatives 104 Congress, Permanent Select Committee on Intelligence, 1996.

Bhanu, C. and C. Stone. *Public-Private Partnerships for Police Reform.* New York: Vera Institute of Justice, 2004.

Blackstock, N. *COINTELPRO: The FBI's Secret War on Political Freedom.* New York: Vintage Books, 1975.

Boba, R. *Problem Analysis in Policing.* Washington, D.C.: Police Foundation, 2003.

Boba, R. *Crime Analysis and Crime Mapping.* Thousand Oaks, California: SAGE Publications, 2005.

Bureau of Justice Assistance. *10 Simple Steps to Help your Agency Become Part of the National Criminal Intelligence Sharing Plan.* Washington, D.C.: Bureau of Justice Assistance, U.S. Department of Justice, 2005.

Bureau of Justice Assistance. *10 Ways to Integrate Suspicious Activity Reporting into Your Agency's Operations.* Washington, D.C.: Bureau of Justice Assistance, U.S. Department of Justice, 2008.

Bureau of Justice Assistance. Criminal Intelligence Training Coordination Strategy Working Group. *Survey of Law Enforcement on Intelligence Training.* Unpublished staff report, 2004.

Bureau of Justice Assistance. *Why Law Enforcement Agencies Need an Analytical Function.* Washington, D.C., Bureau of Justice Assistance, U.S. Department of Justice, October 2005.

California Peace Officers' Association. *Criminal Intelligence Program for the Smaller Agency.* Sacramento, California: California Peace Officers' Association, 1998.

Calling Time on Crime: A Thematic Inspection on Crime and Disorder. London, U.K.: Her Majesty's Inspectorate of Constabulary, 2004.

Carter, D. L. *The Police and the Community.* 7th ed. Upper Saddle River, New Jersey: Prentice Hall, Inc., 2000

Carter, D. L. *Law Enforcement Intelligence: A Guide for State, Local, and Tribal Law Enforcement Agencies.* Washington, D.C.: Office of Community Oriented Policing Services, U.S. Department of Justice, 2004.

Carter, D. L. *Law Enforcement Intelligence Operations.* 8th ed. Tallahassee, Florida: SMC Sciences, Inc., 2002.

Carter, D. L. and T. Martinelli. "Civil Rights and Law Enforcement Intelligence. " *The Police Chief,* June 2007.

Chevigny, P. G. "National Security and Civil Liberties: Politics and Law in the Control of Local Surveillance." *Cornell Law Review.* 69 (April 1984).

Christopher S., "A Practitioner's Perspective of UK Strategic Intelligence," in *Strategic Thinking in Criminal Intelligence,* ed. J.H. Ratcliffe, Sydney: Federation Press, 2004.

Clarke, R. V. and J. Eck. *Crime Analysis for Problem Solvers in 60 Small Steps.* Washington, D.C.: Office of Community Oriented Policing Services, U.S. Department of Justice, 2005.

Coleman, G. "Next Generation: CJIS?" *TIME System Newsletter.* Wisconsin Department of Justice, Crime Information Bureau. (2006-1) (March 2006).

Collier, P. M., J.S. Edwards, and D. Shaw, D. "Communicating Knowledge about Police Performance." *International Journal of Productivity and Performance Management* 53(5) (2004): 458–467.

Commission on Accreditation of Law Enforcement Agencies. *Standards for Law Enforcement Accreditation.* "Standard 51.1.1 – Criminal Intelligence." Washington, D.C.: Commission on Accreditation of Law Enforcement Agencies, 2002.

Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report.* Washington, D.C.: U.S. Government Printing Office, 2004.

Cowan, P., N. Egleson, and N. Hentoff. *State Secrets: Police Surveillance in America.* New York: Holt, Rinehart and Winston, 1974.

Cryer, D. , Special Assistant to the Director of Central Intelligence for Diversity Management. *Prepared Statement, Hearing before the Permanent Select Committee on Intelligence,* 108th Congress, November 5, 2003.

Department of Homeland Security. Management Directive System, MD Number: 11042, *Safeguarding Sensitive But Unclassified (For Official Use Only) Information.* May 11, 2004.

Department of Homeland Security. National Preparedness Directorate. *Targeted Capabilities List. A Companion to the National Preparedness Guidelines.* Washington, D.C.: U.S. Department of Homeland Security, 2007.

Dillon, D. R. "Breaking Down Intelligence Barriers for Homeland Security." Backgrounder #1536. Washington, D.C.: The Heritage Foundation, 2002.

Dintino, J. and F. Martens. *Police Intelligence in Crime Control.* Springfield, Illinois: Charles C. Thomas, 1983.

Donner, F. J. *Protectors of Privilege: Red Squads and Police Repression in Urban America.* Berkeley, California: University of California Press, 1990.

Elliff, J. T. *Crime, Dissent, and the Attorney General.* Beverly Hills, California: SAGE Publications, 1971.

European Commission. *Report of the Seminar on Public Private Partnerships.* The Hague, Netherlands, 2003.

Federal Bureau of Investigation, Counterterrorism Division. *Terrorism: 2002–2005*. Washington, D.C.: Federal Bureau of Investigation, 2006.

Federal Bureau of Investigation. *The FBI intelligence Cycle: Answering the Questions. A Desk Reference Guide for Law Enforcement*. Washington, D.C.: Federal Bureau of Investigation, July 2004.

Federal Bureau of Investigation. "The FBI's Counterterrorism Program Since September 2001." *A Report to the National Commission on Terrorists Attacks Upon the United States.* Washington, D.C.: Federal Bureau of Investigation, undated.

Fisher, L. E., "Guilt by Expressive Association: Political Profiling, Surveillance and the Privacy of Groups," *Arizona Law Review* 46 (Winter) (2004).

Fourth Annual Report to the President and Congress of the Advisory Panel to Assess Domestic Response Capabilities for Terrorism Involving Weapons of Mass Destruction (Gilmore Commission). IV. Implementing the National Strategy. Arlington, Virginia: Rand Corporation, Research and Development Center, 2002.

Frawley, W., G. Piatetsky-Shapiro, and C. Matheus, "Knowledge Discovery in Databases: An Overview," *Artificial Intelligence Magazine* (Fall 1992).

Friedman, R.S. and F. Peek. "Problem-Based Learning and Problem-Solving Tools: Synthesis and Direction for Distributed Education Environments." *Journal of Interactive Learning Research* 13 (3) (2002) 239–257.

Frost, C. and J. Morris. *Police Intelligence Reports.* Orangevale, California: Palmer Press, 1983.

General Accounting Office. Homeland Security. *Justice Department's Project to Interview Aliens After September 11, 2001. Report to Congressional Committees.* Washington, D.C.: General Accounting Office, Report Number GAO-03-459, 2003.

German, M. and J. Stanley. *Fusion Center Update.* Washington, D.C.: American Civil Liberties Union, 2008.

German, M. and J. Stanley. *What's Wrong With Fusion Centers?* New York: American Civil Liberties Union, 2005.

Global Intelligence Working Group. *Criminal Intelligence for the Chief Executive. A Training Program for the Chief Executive. Glossary.* Washington, D.C.: Global Justice Information Sharing Initiative, U.S. Department of Justice, 2004.

Global Intelligence Working Group. *Fusion Center Guidelines.* Washington, D.C.: U.S. Department of Justice and U.S. Department of Homeland Security, 2006.

Global Intelligence Working Group. *Guidelines for Establishing and Operating Fusion Centers at the Local, State, Tribal and Federal Level.* Washington, D.C.: U.S. Department of Justice and U.S. Department of Homeland Security, 2005.

Global Intelligence Working Group. *Guidelines for Establishing and Operating Gang Intelligence Units and Task Forces.* Washington, D.C.: Bureau of Justice Assistance, U.S. Department of Justice, 2008.

Global Intelligence Working Group. *National Criminal Intelligence Sharing Plan.* Washington, D.C.: U.S. Department of Justice, 2003.

Global Intelligence Working Group. *Privacy Committee Report: Tips and Leads Issues Paper.* Washington, D.C.: Global Justice Information Sharing Initiative, U.S. Department of Justice, 2007.

Global Justice Information Sharing Initiative. *Analyst Toolbox. A Toolbox for the Intelligence Analyst.* Washington, D.C.: U.S. Department of Justice, Global Justice Information Sharing Initiative, Intelligence Working Group, November 2006.

Global Justice Information Sharing Initiative. *Fusion Center Guidelines—Developing and Sharing Information and Intelligence in a New Era.* Washington, D.C.: Bureau of Justice Assistance, 2006.

Global Justice Information Sharing Initiative. *Minimum Criminal Intelligence Training Standards for Law Enforcement and Other Criminal Justice Agencies in the United States. Findings and Recommendations.* Washington, D.C.: U.S. Department of Justice. 2007.

Global Justice Information Sharing Initiative. *Privacy and Civil Liberties Policy Development Guide and Implementation Templates.* Washington, D.C.: Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice, rev. 2008.

Godfrey, E.D. and D. R. Harris. *Basic Elements of Intelligence.* Washington, D.C.: Law Enforcement Assistance Administration, 1971.

Goldstein, H. *Problem-Oriented Policing.* New York: McGraw-Hill, 1990.

Government Accountability Office. *INFORMATION TECHNOLOGY: Numerous Federal Networks Used to Support Homeland Security Need to Be Better Coordinated with Key State and Local Information-Sharing Initiatives. Report to the Chairman, Committee on Homeland Security, House of Representatives.* Washington, D.C.: Government Accountability Office, April 2007.

Government Accountability Office. *Homeland Security: Federal Efforts Are Helping to Alleviate Some Challenges Encountered by State and Local Information Fusion Centers.* Washington, D.C.: Government Accountability Office, GAO-08-35 Homeland Security, October 2007.

Herzog, T. J. *Integrating Correctional Authorities into the Fusion Center Rubric.* Palm Coast, Florida: Corrections Technology Association, 2005.

Homeland Security Advisory Council. *Intelligence and Information Sharing Initiative: Homeland Security Intelligence & Information Fusion.* Washington, D.C.: Department of Homeland Security, 2005.

Homeland Security Council/National Security Council Joint Restricted Deputies Committee Meeting. *Discussion Paper on the Information Sharing Environment*, November 3, 2008.

Information Exchange Package Document (IEPD) for the Suspicious Activity Report of State and Local Entities IEPD. Version 1.01. A joint document of the Program Manager–Information Sharing Environment and the Bureau of Justice Assistance, Office of Justice Programs, U.S. Department of Justice.

International Association of Chiefs of Police. *Criminal Intelligence Sharing: A National Plan for Intelligence-Led Policing at the Local, State and Federal Levels.* Alexandria, Virginia: International Association of Chiefs of Police, 2002.

International Association of Law Enforcement Intelligence Analysts, Inc. *Law Enforcement Analytic Standards.* Washington, D.C.: International Association of Law Enforcement Intelligence Analysts, Inc., and Global Justice Information Sharing Initiative, November 2004.

International Association of Chiefs of Police. *National Summit on Intelligence.* Washington, D.C.: Office of Community Oriented Policing Services, U.S. Department of Justice, 2008.

International Association of Law Enforcement Intelligence Analysts, Inc. *Successful Law Enforcement Using Analytic Methods.* Internet-published document, undated.

Johnson, B. and S. Dorn. "Fusion Centers: New York State Intelligence Strategy Unifies Law Enforcement." *The Police Chief,* February 2008.

Johnson, L. *A Season of Inquiry: The Senate Intelligence Investigation.* Lexington, Kentucky: The University Press of Kentucky, 1985.

Kindsvater, L. C. "The Need to Reorganize the Intelligence Community". *Studies in Intelligence* 47 (1) (2003).

Knezo, G. J. *"Sensitive But Unclassified" Information and Other Controls: Policy and Options for Scientific and Technical Information. CRS Report for Congress.* Washington, D.C.: Congressional Research Service, December 29, 2006.

Koehnlein, B. *The History of the Handschu Decree.* New York: New York Civil Liberties Union, 2003.

Law Enforcement Intelligence Unit. *Criminal Intelligence File Guidelines.* Sacramento, California: Law Enforcement Intelligence Unit, revised March 2002.

Lee, C. "The NYPD Wants to Watch You." *The Village Voice,* December 18–24, 2002.

Leson, J. *Assessing and Managing the Terrorism Threat.* Washington, D.C.: Bureau of Justice Assistance, U.S. Department of Justice, 2003.

Lessons Learned Information Sharing. *Local Anti-Terrorism Information and Intelligence Sharing.* Washington, D.C.: U.S. Department of Homeland Security, 2005.

Lessons Learned Information Sharing. *Best Practices. Homeland Security Intelligence Requirements Process.* Washington, D.C.: U.S. Department of Homeland Security, 2006.

Lilly, J. R. "National Security at What Price?: A Look into Civil Liberty Concerns in the Information Age Under the USA Patriot Act of 2001 and a Proposed Constitutional Test for Future Legislation." *Cornell Journal of Law and Public Policy.* 12(Spring) (2003).

Los Angeles Police Department. *Reporting Incidents Potentially Related to Foreign or Domestic Terrorism. Special Order Number* 11, March 5, 2008.

Loyka, S.A., D.A. Faggiani, and C. Karchmer. *Protecting Your Community from Terrorism: Strategies for Local Law Enforcement, Volume 4: The Production and Sharing of Intelligence.* Washington, D.C.: Office of Community Oriented Policing Services and the Police Executive Research Forum, 2005.

MacLellan, T. *Protecting Privacy in Integrated Justice Systems.* Washington, D.C.: National Governors' Association Center for Best Practices, 2006.

Major Cities Chiefs Association and Major County Sheriffs' Association. *Intelligence and Information Sharing: DHS and law Enforcement.* Unpublished report, 2007.

Martens, F., "The Intelligence Function," in *Major Issues in Organized Crime Control: Symposium Proceedings,* Washington, D.C., September 25–26, 1986, ed. Herbert Edelhertz, Washington, D.C.: U.S. Department of Justice, National Institute of Justice, 1987.

Martinelli, T.J. and J.M. Pollock. "Law Enforcement Ethics, Lawsuits, and Liability: Defusing Deliberate Indifference, " *The Police Chief 67* (October 2000) 10.

Masse, T.M. *The National Counterterrorism Center: Implementation Challenges and Issues for Congress. CRS Report for Congress.* Washington, D.C.: Congressional Research Service, March 24, 2005.

Masse, T. and J. Rollins. *A Summary of Fusion Centers: Core Issues and Options for Congress. CRS Report for Congress.* Washington, D.C.: Congressional Research Service, September 19, 2007.

McConnell, J.M. *Vision 2015: A Globally Networked and Integrated Intelligence Enterprise.* Washington, D.C.: Office of the Director of National Intelligence, 2008.

McCreesh, P. and C. Neuman. *Managing for Counter-Terrorism Success in the Los Angeles Police Department.* New York: The Manhattan Institute, and Cambridge, Massachusetts: John F. Kennedy School of Government, Harvard University, 2007.

McDowell, D. *Strategic Intelligence*: *A Handbook for Practitioners, Managers, and Users.* Cooma, NSW, Australia: Istana Enterprises, Pty., Ltd., 2000.

McKnight, G. D. "A Harvest of Hate: The FBI's War Against Black Youth – Domestic Intelligence in Memphis, Tennessee." *South Atlantic Quarterly* 86 (Winter 1987): 1–21.

McNamara, T. *Annual Report to the Congress on the Information Sharing Environment.* Washington, D.C.: Program Manager-Information Sharing Environment, 2008.

McNamara, T. *Statement for the Record before the Subcommittee on Intelligence, Information Sharing and Terrorism Risk Assessment, House Committee on Homeland Security,* April 26, 2007.

Modafferi, P. and K. Bouche. "Intelligence Sharing: Efforts to Develop Fusion Center Intelligence Standards." *The Police Chief* 73 (2) (February 2005).

Morabito, A. and S. Greenberg. *Engaging the Private Sector to Promote Homeland Security: Law Enforcement-Private Security Partnerships.* Washington, D.C.: Bureau of Justice Assistance, 2005.

Murphy, W. *Statement by the former FBI Assistant Director, Directorate of Intelligence at the 2007 IACP Intelligence Summit,* Washington, D.C.: November 27,2007.

Muslim Public Affairs Council. *A Review of U.S. Counterterrorism Policy: American Muslim Critique and Recommendations.* Washington, D.C.: Muslim Public Affairs Council, 2003.

National Advisory Commission on Civil Disorders. *Summary Report.* Washington, D.C.: U.S. Government Printing Office, 1968.

National Advisory Commission on the Causes and Prevention of Violence. *Law and Order Reconsidered.* Washington, D.C.: U.S. Government Printing Office, 1968.

National Advisory Commission on Criminal Justice Standards and Goals. *Police*. Washington, D.C.: U.S. Government Printing Office, 1973.

National Advisory Committee on Criminal Justice Standards and Goals. *Disorders and Terrorism: Report of the Task Force on Disorders and Terrorism*. Washington D.C.: U.S. Government Printing Office, 1976.

National Advisory Committee on Criminal Justice Standards and Goals. *Organized Crime–Task Force Report on Organized Crime*. Washington, D.C.: U.S. Department of Justice, Law Enforcement Assistance Administration, 1976.

National Alliance of Gang Investigators Associations. *National Gang Threat Assessment*. Washington, D.C.: Bureau of Justice Assistance, U.S. Department of Justice, 2005.

National Centre for Policing Excellence. *Guidance on the National Intelligence Model*. London, UK: Association of Chief Police Officers, 2005.

National Commission on the Causes and Prevention of Violence. *Law and Order Reconsidered*. Washington, D.C.: U.S. Government Printing Office, 1968.

National Commission on Terrorist Attacks Upon the United States. *Staff Statement No. 12: Reforming Law Enforcement, Counterterrorism, and Intelligence Collection in the United States*. Washington, D.C.: National Commission on Terrorist Attacks Upon the United States, 2004.

National Commission on Terrorist Attacks Upon the United States. *The 9/11 Commission Report*. Washington, D.C.: U.S. Government Printing Office, 2004.

National Criminal Justice Association. *Justice Information Privacy Guideline. Developing, Drafting and Assessing Privacy Policy for Justice Information Systems*. Washington, DC: National Criminal Justice Association, 2002.

National Gang Center. *Brief Review of Federal and State Definitions of the Terms "Gang," "Gang Crime," and "Gang Member."* Unpublished web document, undated.

National Governors Association. *Policy Position: EC-05. Homeland Security Policy*. Washington, D.C.: National Governors Association, 2007.

National Strategy for Information Sharing. Washington, D.C.: Executive Office of the President, 2007.

Nenneman, M. *An Examination of State and Local Fusion Centers and Data Collection Methods*. Monterey, California: A thesis prepared for the Naval Post Graduate School, 2008.

NIEM Program Management Office. *Introduction to the National Information Exchange Model (NIEM)*. Washington, D.C.: NIEM Program Management Office, February 12, 2007.

Office of Intelligence and Analysis. *National Strategy for the Fire Service Intelligence Enterprise*. Washington, D.C.: U.S. Department of Homeland Security, 2008.

Office of the Chief Intelligence Officer. *DHS Intelligence Enterprise Strategic Plan*. Washington, D.C.: U.S. Department of Homeland Security, 2006.

Office of the Director of National Intelligence. *Sourcing Requirements for Disseminated Analytic Requirements. Intelligence Community Directive* 206. Washington, D.C.: Office of the Director of National Intelligence, October 17, 2007.

Office of the Director of National Intelligence. *National Open Source Enterprise*. Washington, D.C.: Office of the Director of National Intelligence, 2007.

Office of the Inspector General. Audit Division. *The Drug Enforcement Administration's Use of Intelligence Analysts. Audit Report 08-23*. Washington, D.C.: U.S. Department of Justice, May 2008.

Orrick, W.D. *Best Practices Guide: Developing a Police Department Policy-Procedure Manual.* Alexandria, Virginia: International Association of Chiefs of Police, undated.

Peterson, M. *Intelligence-Led Policing: The New Intelligence Architecture*. Washington, D.C.: Bureau of Justice Assistance, 2005. NCJ 210681.

Peterson, M. *Applications in Criminal Analysis: A Sourcebook*. Westport, Connecticut: Praeger, 1994.

Peterson, M. et al. *Successful Law Enforcement Using Analytic Methods.* South Florida, Florida: International Association of Law Enforcement Intelligence Analysts, Inc., 1996.

Peterson, M., B. Morehouse, and R. Wright, eds. *Intelligence 2000: Revising the Basic Elements. A Guide for Intelligence Professionals.* Sacramento, California: Law Enforcement Intelligence Unit, and Lawrenceville, New Jersey: International Association of Law Enforcement Intelligence Analysts, Inc., 2000.

Pistole, J. S. , Executive Assistant Director, Counterterrorism and Counterintelligence, Federal Bureau of Investigation. *Statement before the House Judiciary Committee Subcommittee on Crime, Terrorism and Homeland Security,* August 23, 2004.

Pitts, D. "Getting the 411." *Fire Chief*. January 1, 2008.

Police Executive Research Forum. *What Is a Fusion Center?* Washington, D.C.: Police Executive Research Forum, 2008.

President's Commission on Law Enforcement and Administration of Justice. T*ask Force Report: Organized Crime*. Washington, D.C.: U.S. Government Printing Office, 1967.

President's Commission on Organized Crime. *Final Report*. Washington, D.C.: U.S. Government Printing Office, 1987.

President's Commission on Organized Crime. *Organized Crime and Money Laundering*. Washington, D.C.: U.S. Government Printing Office, 1984.

Privacy Impact Statement for the Homeland Security Information Network Database. Washington, D.C.: Unpublished report of the DHS Office of Operations Coordination, April 5, 2006.

Program Manager–Information Sharing Environment. *Common Terrorism Information Sharing Standards (CTISS) Program Manual*. Washington, D.C.: Program Manager-Information Sharing Environment, 2007.

Program Manager–Information Sharing Environment. *Guidelines to Ensure That the information Privacy and Other Legal Rights of Americans Are Protected in the Development and Use of the Information Sharing Environment*. Washington, D.C.: Office of the Director of National intelligence, September 4, 2006.

Program Manager–Information Sharing Environment. *Information Sharing Environment Implementation Plan*. Washington, D.C.: Office of the Director of National Intelligence, 2006.

Ramsey, T. *Global Maritime Intelligence Integration (GMII) Enterprise.* PowerPoint Presentation. Washington, D.C.: Office of the Director of National Intelligence, May 9, 2007.

Ratcliffe, J. and R. Guidetti. "State Police Investigative Structure and the Adoption of Intelligence-Led Policing." *Policing: An International Journal of Police Strategies and Management,* 2007.

Ratcliffe, J.H., "The Structure of Strategic Thinking," in *Strategic Thinking in Criminal Intelligence,* ed., J.H. Ratcliffe, Sydney, NSW, Australia: Federation Press, 2004, pp. 1–10.

Ratcliffe, J.H. *Intelligence-Led Policing.* Cullompton, Devon, U.K.: Willan Publishing, 2008.

Ratcliffe, J.H. *Integrated Intelligence and Crime Analysis: Enhanced Information Management for Law Enforcement Leaders.* Washington, D.C.: Office of Community Oriented Policing Services, U.S. Department of Justice, 2007.

Reese, S. *State and Local Homeland Security: Unresolved Issues for the 109th Congress. CRS Report for Congress.* Washington, D.C.: Congressional Research Service, June 9, 2005.

Riley, K. J., G. Treverton, J. Wilson, and L. Davis. *State and Local Intelligence in the War on Terrorism.* Santa Monica, California: RAND Corporation, 2005.

Rossmo, D. K. *Geographic Profiling.* Boca Raton, Florida: CRC Press, 2000.

Sagan, Carl. *Broca's Brain: Reflections on the Romance of Science.* New York: The Ballantine Publishing Group, 1979.

Scheider, M., R. Chapman, and M. Seelman. "Connecting the Dots for a Proactive Approach." *Border and Transportation Security.* Washington, D.C.: Office of Community Oriented Policing Services, 2004.

Scott, M.S. *Problem-Oriented Policing: Reflections on the First 20 Years.* Washington, D.C.: Office of Community Oriented Policing Services, 2000.

Shane, J. "CompStat Process." *FBI Law Enforcement Bulletin* 73 (2) (April 2004).

Shaw, L. *Information Systems and Technologies.* Presentation at the BJA-funded Intelligence Commanders' Course, Norwalk, California, July 2008.

Simeone, M.J. *The Integration of Virtual Public-Private Partnerships in Law Enforcement to Achieve Enhanced Intelligence-Led Policing.* Monterey, California: A thesis prepared for the Naval Postgraduate School, 2007.

Statement by FBI Assistant Director Wayne Murphy, Directorate of Intelligence, at the 2007 IACP Intelligence Summit, Washington, D.C., November 27, 2007.

Steigman, J.L. "Reversing Reform: The Handschu Settlement in Post-September 11 New York City." *Brooklyn Journal of Law and Policy* 11 (2003).

Stone, K. *Deploying and Operating an Effective Regional Fusion System: Lessons Learned from the North Central Texas Fusion System.* Unpublished policy paper prepared by the North Central Texas Fusion System, McKinney, Texas, 2006.

Sullivan, J.P. *Terrorism Early Warning and Co-Production of Counterterrorism Intelligence.* A paper presented at the Canadian Association of Security and Intelligence Studies. Montreal, Canada, 2005.

Suspicious Activity Report Support and Implementation Project. *Final Report*. Washington, D.C.: Major Cities Chiefs Association; U.S. Department of Justice and U.S. Department of Homeland Security, 2008.

The Warren Commission. *Report of the President's Commission on the Assassination of President John F. Kennedy*. New York: Barnes and Noble, Inc., 2003 [Originally published in 1964].

The White House. Executive Office of the President. Office of Homeland Security. *National Strategy for Homeland Security*. Washington, D.C.: 2002.

Tomarchio, J. *Focus on Fusion Centers: A Progress Report*. Prepared Statement Before the Ad Hoc Subcommittee on State, Local and Private Sector Preparedness and Integration, Committee on Homeland Security and Government Affairs, United States Senate, April 17, 2008.

Townsley, M., S. Johnson, and K. Pease. "Problem Orientation, Problem Solving and Organizational Change." *Crime Prevention Studies 15,* Monsey, New York: Criminal Justice Press, 2003.

U.S. General Accounting Office. *Security Clearances*. GAO-04-596. Washington, D.C.: U.S. General Accounting Office, 2004.

United States Senate. Select Committee to Study Governmental Operations. *Intelligence Activities: Final Report*. Washington, D.C.: U.S. Government Printing Office, 1976.

United States Senate. Select Committee to Study Governmental Operations with Respect to Intelligence Activities. *Intelligence Activities and the Rights of Americans: Final Report. Book II*. Washington, D.C.: April 26, 1976.

Weimer, D. R. *The Copyright Doctrine of Fair Use and the Internet: Case Law*. Washington, D.C.: Congressional Research Service, 2005.

Wells, I., "Staffing the Intelligence Unit," in *Intelligence 2000: Revising the Basic Elements, A Guide for Intelligence Professionals,* ed. M. Peterson, B. Morehouse, and R. Wright, Sacramento, California: Law Enforcement Intelligence Unit, and Lawrenceville, New Jersey: International Association of Law Enforcement Intelligence Analysts, 2000.

Wortzel, L. "Creating an Intelligent Department of Homeland Security." *Executive Memorandum 828*. Washington, D.C.: The Heritage Foundation, 2002.

Appendix A: Glossary of Terms for Law Enforcement Intelligence

Law enforcement agencies at all levels are working together more than ever to support information sharing. It is important to note that a tremendous effort is under way to streamline intelligence terms to facilitate information sharing. As a result, criminal intelligence terminology is changing. The definitions contained herein are provided from the perspective of law enforcement/criminal intelligence. Further, some words and phrases will have alternative or additional meanings when used in the context of national security intelligence, the military, or business. The definitions are intended to be merely descriptive of an entity, issue, or process that may be encountered by those working with the criminal intelligence function. Definitions may differ according to state statutes or local rules.

Glossary Of Law Enforcement Intelligence Terms

Actionable: Intelligence and information with sufficient specificity and detail that explicit responses to prevent a crime or terrorist attack can be implemented.

Administrative Analysis: The analysis of economic, geographic, demographic, census, or behavioral data to identify trends and conditions useful to aid administrators in making policy and/or resource allocation decisions.

All-Hazards Intelligence: The collection and analysis of information concerned with noncriminal domestic threats to critical infrastructure, community health, and public safety for the purpose of preventing the threat or mitigating the effects of the threat. (Same as Homeland Security Intelligence).

Allocation: Collection and analysis of information that shows relationships among varied individuals suspected of being involved in criminal activity that may provide insight into the criminal operation and which investigative strategies might work best.

Analysis: That activity whereby meaning, actual or suggested, is derived through organizing and systematically examining diverse information and applying inductive or deductive logic for the purposes of criminal investigation or assessment.

Archiving (Records): The maintenance of records in remote storage after a case has been closed or disposed of, as a matter of contingency, should the records be needed for later reference.

Association Analysis: The entry of critical investigative and/or assessment variables into a two-axis matrix to examine the relationships and patterns that emerge as the variables are correlated in the matrix.

Automated Trusted Information Exchange (ATIX): Operated by the Regional Information Sharing Systems, ATIX is a secure means of disseminating national security or terrorist threat information to law enforcement and other first responders through the ATIX electronic bulletin board, secure web site, and secure e-mail.

Bias/Hate Crime: Any criminal act directed toward a person or group because of that person's race, ethnicity, religious affiliation, or sexual preference.

C3: An intelligence application concept initially used by military intelligence that stands for command, control, and communication as the hallmark for effective intelligence operations.

Clandestine Activity: An activity that is usually extensive and goal-oriented, planned, and executed to conceal the existence of the operation. Only participants and the agency sponsoring the activity are intended to know about the operation. Storefront operations, stings, and certain concentrated undercover investigations (such as ABSCAM) can be classified as clandestine collections.

Classified Information/Intelligence: A uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defense against transnational terrorism, to ensure that certain information is maintained in confidence to protect citizens, U.S. democratic institutions, U.S. homeland security, and U.S. interactions with foreign nations and entities.

- *Top Secret Classification*: Applied to information, the unauthorized disclosure of which reasonably could be expected to cause exceptionally grave damage to the national security that the original classification authority is able to identify or describe (Executive Order 12958, March 25, 2003).
- *Secret Classification*: Applied to information, the unauthorized disclosure of which reasonably could be expected to cause serious damage to the national security that the original classification authority is able to identify or describe (Executive Order 12958, March 25, 2003).
- *Confidential Classification*: Applied to information, the unauthorized disclosure of which reasonably could be expected to cause damage to the national security that the original classification authority is able to identify or describe (Executive Order 12958, March 25, 2003).

Collation (of information): A review of collected and evaluated information to determine its substantive applicability to a case or problem at issue and placement of useful information into a form or system that permits easy and rapid access and retrieval.

Collection (of information): The identification, location, and recording/storing of information, typically from an original source and using both human and technological means, for input into the Intelligence Cycle for the purpose of meeting a defined tactical or strategic intelligence goal.

Collection Plan: The preliminary step toward completing an assessment of intelligence requirements to determine what type of information needs to be collected, alternatives for how to collect the information, and a timeline for collecting the information.

Command and Control: Command and control functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures used by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of a mission.

Commodity (Illegal): Any item or substance that is inherently unlawful to possess (contraband) or materials which, if not contraband, are themselves being distributed, transacted, or marketed in an unlawful manner.

Commodity Flow Analysis: Graphic depictions and descriptions of transactions, shipment, and distribution of contraband goods and money derived from unlawful activities in order to aid in the disruption of the unlawful activities and apprehend those persons involved in all aspects of the unlawful activities.

Communications Intelligence (COMINT): The capture of information, either encrypted or in plaintext, exchanged between intelligence targets or transmitted by a known or suspected intelligence target for the purposes of tracking communications patterns and protocols (traffic analysis), establishing links between intercommunicating parties or groups, and/or analysis of the substantive meaning of the communication.

Conclusion: A definitive statement about a suspect, action, or state of nature based on the analysis of information.

Confidential: *See* Classified Information/Intelligence, Confidential Classification.

Continuing Criminal Enterprise: Any individual, partnership, corporation, association, or other legal entity and any union or group of individuals associated in fact, although not a legal entity, that are involved in a continuing or perpetuating criminal activity.

Controlled Unclassified Information (CUI) : The term Controlled Unclassified Information or CUI is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 12958, as amended, but is (i) pertinent to the national interests of the United States or to the important interests of entities outside the federal government, and (ii) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination. The designation CUI replaces Sensitive But Unclassified (SBU). There are three types of CUI:

- *Controlled with Standard Dissemination:* The information requires standard safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it is reasonably believed that it would further the execution of a lawful or official purpose.
- *Controlled with Specified Dissemination:* The information requires safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Material contains additional instructions on what dissemination is permitted.
- *Controlled Enhanced with Specified Dissemination:* The information requires safeguarding measures more stringent than those normally required because the inadvertent or unauthorized disclosure would create risk of substantial harm. Material contains additional instructions on what dissemination is permitted.

Coordination: The process of interrelating work functions, responsibilities, duties, resources, and initiatives directed toward goal attainment.

Counterintelligence: Information compiled, analyzed, and/or disseminated in an effort to investigate espionage, sedition, or subversion that is related to national security concerns. It also is defined as a national security intelligence activity that involves blocking or developing a strategic response to other groups, governments, or individuals through the identification, neutralization, and manipulation of their intelligence services.

Covert Intelligence: An activity that is planned and executed to conceal the collection of information and/or to conceal the identity of an officer or agent participating in the activity.

Critical Infrastructure: Certain national infrastructures that are so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States. These critical infrastructures are:

- Telecommunications
- Electrical power systems
- Gas and oil storage and transportation
- Banking and finance
- Transportation
- Water supply systems
- Emergency services (including medical, police, fire, and rescue)
- Continuity of government.

Crime Analysis: The process of analyzing information collected about crimes and police service delivery variables in order to give direction for police officer deployment, resource allocation, and policing strategies as a means of maximizing crime-prevention activities and the cost-effective operation of the police department.

Crime-Pattern Analysis: An assessment of the nature, extent, and changes of crime based on the characteristics of the criminal incident, including modus operandi, temporal, and geographic variables.

Criminal History Record Information (CHRI): Information collected by criminal justice agencies on individuals. It consists of identifiable descriptions and notations of arrests, detentions, indictments, information, or other formal criminal charges and any disposition arising from them, including sentencing, correctional supervision, and/or release. The term does not include identification information, such as fingerprint records, to the extent that such information does not indicate involvement of the individual in the criminal justice system.

Criminal Informant: *See* Informant.

Criminal Intelligence: The end product (output) of an analytic process that collects and assesses information about crimes and/or criminal enterprises with the purpose of making judgments and inferences about community conditions, potential problems, and criminal activity with the intent to pursue criminal prosecution or project crime trends or support informed decision-making by management. *Same as* Law Enforcement Intelligence.

Criminal Investigative Analysis: An analytic process that studies serial offenders, victims, and crime scenes in order to assess characteristics and behaviors of offender(s) with the intent to identify or aid in the identification of the offender(s).

Criminal Predicate: Information about an individual or his or her behavior that may be collected and stored in a law enforcement intelligence records system only when there is reasonable suspicion that the individual is involved in criminal conduct or activity and the information is relevant to that criminal conduct or activity.

Cryptanalysis: The process of deciphering encrypted communications of an intelligence target.

Cryptography: The creation of a communications code/encryption system for communication transmission with the intent of precluding the consumption and interpretation of one's own messages.

Cryptology: The study of communications encryption methods that deal with the development of "codes" and the "scrambling" of communications to prevent an unauthorized or unintended party from intercepting the communications.

Data Element: A field within a database that describes or defines a specific characteristic or attribute.

Data Owner: The agency that originally enters information or data into a law enforcement records system.

Data Quality: Controls implemented to ensure that all information in a law enforcement agency's records system is complete, accurate, and secure.

Deconfliction: The process or system used to determine whether multiple law enforcement agencies are investigating the same person or crime. The system provides notification to each agency involved of the shared interest in the case and also provides contact information. This is an information and intelligence sharing process that seeks to minimize conflicts between agencies and maximize the effectiveness of an investigation.

Deductive Logic: The reasoning process of taking information and arriving at conclusions from within that information.

Deployment: The short-term assignment of personnel to address specific crime problems or police service demands.

Designated State and/or Major Urban Area Fusion Center: The fusion center in each state designated as the primary or lead fusion center for the information-sharing environment.

Dissemination (of Intelligence): The process of effectively distributing analyzed intelligence utilizing certain protocols in the most appropriate format to those in need of the information to facilitate their accomplishment of organizational goals.

Due Process: Fundamental fairness during the course of the criminal justice process, including adherence to legal standards and the civil rights of the police constituency; the adherence to principles that are fundamental to justice.

El Paso Intelligence Center (EPIC): A cooperative intelligence center serving as a clearinghouse and intelligence resource for local, state, and federal law enforcement agencies. Primary concern is drug trafficking. EPIC also manages intelligence on other crimes.

Enterprise: Any individual, partnership, corporation, association, or other legal entity and any union or group of individuals associated in fact, although not a legal entity.

Estimate: *See* Intelligence Estimate.

Evaluation (of Information): All information collected for the intelligence cycle is reviewed for its quality, with an assessment of the validity and reliability of the information.

Event Flow Analysis: Graphic depictions and descriptions of incidents, behaviors, and people involved in an unlawful event, intended to help understand how an event occurred as a tool to aid in prosecution as well as prevention of future unlawful events.

Exemptions (to the Freedom of Information Act): Circumstances wherein a law enforcement agency is not required to disclose information from a Freedom of Information Act (FOIA) request.

Field Intelligence Group (FIG): The centralized intelligence component in a Federal Bureau of Investigation (FBI) field office that is responsible for the management, execution, and coordination of intelligence functions within the field office region.

Field Intelligence Report (FIR): An officer-initiated interview of a person believed by the officer to be acting in a suspicious manner that may be indicative of planning or preparing to conduct criminal activity.

Financial Analysis: A review and analysis of financial data to ascertain the presence of criminal activity. It can include bank record analysis, net worth analysis, financial profiles, source and applications of funds, financial statement analysis, and/or Bank Secrecy Act record analysis. It can also show destinations of the proceeds of crime and be used to support prosecutions.

Flow Analysis: The review of raw data to determine the sequence of events or interactions that may reflect criminal activity. It can include timelines, event flow analysis, commodity flow analysis, and activity flow analysis. May show missing actions or events that need further investigation.

For Official Use Only (FOUO): A designation applied to unclassified sensitive information that may be exempt from mandatory release to the public under the FOIA.

Forecast (as related to Criminal Intelligence): The product of an analytic process that provides a probability of future crimes and crime patterns based on a comprehensive, integrated analysis of past, current, and developing trends.

Freedom of Information Act (FOIA): The Freedom of Information Act, 5 U.S.C. 552, enacted in 1966, statutorily provides that any person has a right, enforceable in court, to access federal agency records, except to the extent that such records (or portions thereof) are protected from disclosure by one of nine exemptions.

Fusion Center: The physical location of the law enforcement intelligence fusion process.

Fusion Center Guidelines: A series of nationally recognized standards developed by law enforcement intelligence subject matter experts designed for the good practice of developing and managing an intelligence fusion center.

Fusion Process: The overarching process of managing the flow of information and intelligence across levels and sectors of government.

Granularity: Considers the specific details and pieces of information, including nuances and situational inferences that constitute the elements on which intelligence is developed through analysis.

Guidelines: *See* Intelligence Records Guidelines.

Homeland Security Advisory System: An information and communications structure designed by the U.S. Government for disseminating information to all levels of government and the American people regarding the risk of terrorist attacks and for providing a framework to assess the risk at five levels: Low, Guarded, Elevated, High, and Severe.

Homeland Security Intelligence: The collection and analysis of information concerned with noncriminal domestic threats to critical infrastructure, community health, and public safety for the purpose of preventing the threat or mitigating the effects of the threat. (Same as All Hazards Intelligence).

Human Intelligence (HUMINT): Intelligence-gathering methods that require human interaction or observation of the target or targeted environment. The intelligence is collected through the use of one's direct senses or the optical and/or audio enhancement of the senses.

Hypothesis (from Criminal Intelligence Analysis): An interim conclusion regarding persons, events, and/or commodities based on the accumulation and analysis of intelligence information that is to be proven or disproved by further investigation and analysis.

Imagery: The representation of an object or locale produced on any medium by optical or electronic means. The nature of the image will be dependent on the sensing media and sensing platform.

Indicator: Generally defined and observable actions that, based on an analysis of past known behaviors and characteristics, collectively suggest that a person may be committing, may be preparing to commit, or has committed an unlawful act.

Inductive Logic: The reasoning process of taking diverse pieces of specific information and inferring a broader meaning of the information through the course of hypothesis development.

Inference Development: The creation of a probabilistic conclusion, estimate, or prediction related to an intelligence target based on the use of inductive or deductive logic in the analysis of raw information related to the target.

Informant: An individual not affiliated with a law enforcement agency who provides information about criminal behavior to a law enforcement agency. An informant may be a community member, a businessperson, or a criminal informant who seeks to protect himself or herself from prosecution and/or provide the information in exchange for payment.

Information: Pieces of raw, unanalyzed data that identify persons, evidence, or events, or illustrate processes that indicate the incidence of a criminal event or witnesses or evidence of a criminal event.

Information Classification: *See* Classified Information/Intelligence.

Information Evaluation: *See* Evaluation (of Information).

Information Sharing Environment: A trusted partnership among all levels of government, the private sector, and foreign partners to detect, prevent, preempt, and mitigate the effects of terrorism against the territory, people, and interests of the United States of America. This partnership enables the trusted, secure, and appropriate exchange of terrorism information, in the first instance, across the five federal communities; to and from state, local, and tribal governments, foreign allies, and the private sector; and at all levels of security classifications.

Information Sharing System: An integrated and secure methodology, whether computerized or manual, designed to efficiently and effectively distribute critical information about offenders, crimes, and/or events in order to enhance prevention and apprehension activities by law enforcement.

Information System: An organized means, whether manual or electronic, of collecting, processing, storing, and retrieving information about individual entities for purposes of record and reference.

Intelligence Analyst: A professional position in which the incumbent is responsible for taking the varied facts, documentation of circumstances, evidence, interviews, and any other material related to a crime and organizing them into a logical and related framework for the purposes of developing a criminal case, explaining a criminal phenomenon, describing crime and crime trends, and/or preparing materials for court and prosecution, or arriving at an assessment of a crime problem or crime group.

Intelligence Assessment: A comprehensive report on an intelligence issue related to criminal or national security threats available to local, state, tribal, and federal law enforcement agencies.

Intelligence Bulletins: A finished intelligence product in article format that describes new developments and evolving trends. The bulletins are typically Sensitive But Unclassified (SBU) and available for distribution to local, state, tribal, and federal law enforcement.

Intelligence Community: Agencies of the U.S. government, including the military, that have the responsibility of preventing breeches in U.S. national security and responding to national security threats.

Intelligence Cycle: An organized process by which information is gathered, assessed, and distributed to fulfill the goals of the intelligence function. It is a method of performing analytic activities and placing the analysis in a useable form.

Intelligence Estimate: The appraisal, expressed in writing or orally, of available intelligence relating to a specific situation or condition with a view to determining the courses of action open to criminal offenders and terrorists and the order of probability of their adoption. It includes strategic projections about the economic, human, and/or quantitative criminal impact of the crime or issue that is subject to analysis.

Intelligence Function: The activity within a law enforcement agency responsible for some aspect of law enforcement intelligence, whether collection, analysis, and/or dissemination.

Intelligence Gap: An unanswered question about a cyber, criminal, or national security issue or threat.

Intelligence Information Reports (IIR): Raw, unevaluated intelligence concerning perishable or time-limited information about criminal or national security issues. While the full IIR may be classified, local, state, and tribal law enforcement agencies will have access to SBU information in the report under the tear line.

Intelligence-Led Policing: The dynamic use of intelligence to guide operational law enforcement activities to targets, commodities, or threats for both tactical responses and strategic decision-making for resource allocation and/or strategic responses.

Intelligence Mission: The role that the intelligence function of a law enforcement agency fulfills in support of the overall mission of the agency. It specifies in general language what the function is intended to accomplish.

Intelligence Mutual Aid Pact (IMAP): A formal agreement between law enforcement agencies designed to expedite the process of sharing information in intelligence records.

Intelligence Officer: A law enforcement officer assigned to an agency's intelligence function for purposes of investigation, liaison, or other intelligence-related activity that requires or benefits from having a sworn officer perform the activity.

Intelligence Products: Reports or documents that contain assessments, forecasts, associations, links, and other outputs from the analytic process that may be disseminated for use by law enforcement agencies for prevention of crimes, target hardening, apprehension of offenders, and prosecution.

Intelligence Records (Files): Stored information about the activities and associations of individuals, organizations, businesses, and groups who are suspected (reasonable suspicion) of being involved in the actual or attempted planning, organizing, financing, or commissioning of criminal acts, or are suspected of being or having been involved in criminal activities with known or suspected crime figures.

Intelligence Records Guidelines: Derived from the federal regulation 28 CFR Part 23, these are guidelines/standards for the development of records management policies and procedures used by law enforcement agencies.

International Criminal Police Organization (INTERPOL): INTERPOL is a worldwide law enforcement organization established for mutual assistance in the prevention, detection, and deterrence of international crimes. It houses international police databases, provides secure international communications between member countries for the exchange of routine criminal investigative information, and is an information clearinghouse concerning international criminals/fugitives and stolen properties.

Investigatory Value (of Information): Intelligence or information that is disseminated in the law enforcement community for surveillance, apprehension, or furtherance of an investigation.

Key Resources: Publicly or privately controlled resources essential to the minimal operations of the economy and government.

Key Word In Context (KWIC): An automated system that indexes selected key words that represent the evidence or information being stored.

Law Enforcement Intelligence (LAWINT): The end product (output) of an analytic process that collects and assesses information about crimes and/or criminal enterprises. Its purpose is to make judgments and inferences about community conditions, potential problems, and criminal activity with the intent to pursue criminal prosecution or project crime trends or support informed decision-making by management. Same as Criminal Intelligence.

Law Enforcement Sensitive (LES): Sensitive But Nnclassified information specifically compiled for law enforcement purposes that, if not protected from unauthorized access, could reasonably be expected to 1. Interfere with law enforcement proceedings, 2. Deprive a person of a right to a fair trial or impartial adjudication, 3. Constitute an unwarranted invasion of the personal privacy of others, 4. Disclose the identity of a confidential source, 5. Disclose investigative techniques and procedures, and/or 6. Endanger the life or physical safety of an individual.

Methods: These are the methodologies (e.g., electronic surveillance or undercover operations) by which critical information is obtained and recorded.

Micro-Intelligence: Intelligence activities focusing on current problems and crimes for either case development or resource allocation.

Money Laundering: The practice of using multiple unlawful transactions of money and/or negotiable instruments gained through illegal activities with the intent of hiding the origin of the income, those who have been "paid" from the income, and/or the location of the unlawful income.

National Central Bureau (NCB or USNCB): The United States headquarters of INTERPOL, located in Washington, D.C.

National Criminal Intelligence Resource Center (NCIRC): An Internet web site that contains information regarding law enforcement intelligence operations and practices and provides criminal justice professionals with a centralized resource information bank through which they can access a multitude of criminal intelligence resources to help law enforcement agencies develop, implement, and retain a lawful and effective intelligence capacity.

National Criminal Intelligence Sharing Plan (NCISP): A formal intelligence-sharing initiative, supported by the U.S. Department of Justice, Office of Justice Programs, that securely links local, state, tribal, and federal law enforcement agencies, and facilitates the exchange of critical intelligence information. The NCISP contains model policies and standards and is a blueprint for law enforcement administrators to follow when enhancing or building an intelligence function. It describes a nationwide communications capability that will link all levels of law enforcement personnel, including officers on the street, intelligence analysts, unit commanders, and police executives.

National Security Intelligence: The collection and analysis of information concerned with the relationship and equilibrium of the United States with foreign powers, organizations, and persons with regard to political and economic factors, as well as the maintenance of the United States' sovereign principles.

Need to Know: As a result of jurisdictional, organizational, or operational necessities, intelligence or sensitive information is disseminated to further an investigation.

Network: A structure of interconnecting components designed to communicate with each other and perform a function or functions as a unit in a specified manner.

Open Communications (OPCOM): The collection of open or publicly available communications, broadcasts, audio or video recordings, propaganda, published statements, and other distributed written or recorded material for purposes of analyzing the information.

Open-Source Information (*or* Intelligence): Individual data, records, reports, and assessments that may shed light on an investigatory target or event which do not require any legal process or any type of clandestine collection techniques for a law enforcement agency to obtain. Rather, it is obtained through means that meet copyright and commercial requirements of vendors, as well as being free of legal restrictions to access by anyone who seeks that information.

Operational Analysis: An assessment of the methodology of a criminal enterprise or terrorist organization that depicts how the enterprise performs its activities, including communications, philosophy, compensation, security, and other variables that are essential for the enterprise to exist.

Operational Intelligence: Information is evaluated and systematically organized on an active or potential target, such as groups of or individual criminals, relevant premises, contact points, and methods of communication. This process is developmental in nature wherein there are sufficient articulated reasons to suspect criminal activity. Intelligence activities explore the basis of those reasons and newly developed information in order to develop a case for arrest or indictment.

Outcome Evaluation: The process of determining the value or amount of success in achieving a predetermined objective. This is done by defining the objective in qualitative or quantitative measurable terms, identifying the proper criteria (or variables) used in measuring the success of attaining the objective, determining and explaining the degree of success, and making recommendations for further program actions to attain the desired objectives/outcomes.

Personal Identifying Information: Any information or data from which a reasonable person may identify a specific individual. When Personal Identifying Information is collected, civil rights protections and privacy standards must be afforded to the document or report that contains the information

Planning: The preparation for future situations, estimating organizational demands and resources needed to attend to those situations, and initiating strategies to respond to those situations.

Pointer System or Index: A system that stores information designed to identify individuals, organizations, and/or crime methodologies with the purpose of linking law enforcement agencies that have similar investigative and/or intelligence interests in the entity defined by the system.

Policy: The principles and values that guide the performance of a duty. A policy is not a statement of what must be done in a particular situation; rather, it is a statement of guiding principles that should be followed in activities that are directed toward attaining goals.

Prediction: The projection of future criminal actions or changes in the nature of crime trends or a criminal enterprise based on an analysis of information depicting historical trends from which a forecast is based.

Preventive Intelligence: Intelligence that can be used to interdict or forestall a crime or terrorist attack.

Privacy (Information): The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of personally identifiable information will be adhered to by criminal justice agencies. Use of such information is strictly limited to circumstances in which legal process permits use of the personally identifiable information.

Privacy (Personal): The assurance that legal and constitutional restrictions on the collection, maintenance, use, and disclosure of behaviors of an individual—including his or her communications, associations, and transactions—will be adhered to by criminal justice agencies, with use of such information strictly limited to circumstances in which legal process authorizes surveillance and investigation.

Privacy Act: Legislation that allows an individual to review almost all federal files (and state files under the auspices of the respective state privacy acts) pertaining to him or her, places restrictions on the disclosure of personally identifiable information, specifies that there are no secret records systems about individuals, and compels the government to reveal its information sources.

Proactive: Taking action that anticipates a problem or situation, with the intent to eliminate or mitigate the effect of the incident.

Procedural Due Process: Mandates and guarantees of law that ensure that the procedures employed to deprive a person of life, liberty, or property during the course of the criminal justice process meet constitutional standards.

Procedures: A method of performing an operation or a manner of proceeding on a course of action. It differs from policy by directing action in a particular situation to perform a specific task within the guidelines of policy. Both policies and procedures are goal-oriented, but policy establishes limits to action while procedure directs responses within those limits.

Profile/Criminal Profile: An investigative technique for identifying and defining the major personality and behavioral characteristics of the criminal offender through an analysis of the crime(s) he or she has committed.

Protocol (of Intelligence Collection): Information collection procedures employed for obtaining verbal and written information, including on the actions of people, and physical evidence required for strategic and tactical intelligence analysis.

Public Value (of Information): Intelligence or information can be released to the public when there is a need to know and a right to know the information because of the value that may be derived from public dissemination, to 1. Aid in locating targets/suspects and 2. For public safety purposes (i.e., hardening targets, taking precautions).

Purging (Records): Removing and/or destroying records because they are deemed to be of no further value or that further access to the records would serve no legitimate government interest.

Qualitative (Methods): Research methods that collect and analyze information that is described in narrative or rhetorical form, with conclusions drawn based on the cumulative interpreted meaning of that information.

Quantitative (Methods): Research methods that collect and analyze information that can be counted or placed on a scale of measurement that can be statistically analyzed.

Racketeer Influenced and Corrupt Organizations Act of 1970 (RICO) or similar state statutes: Title IX of the Organized Crime Control Act of 1970 (18 U.S.C. Sections 1961–1968) provides civil and criminal penalties for persons who engage in a pattern of racketeering activity or collection of an unlawful debt that has a specified relationship to an enterprise that affects interstate commerce.

Racketeering Activity: State felonies involving murder, robbery, extortion, and several other serious offenses and more than 30 serious federal offenses, including extortion, interstate theft offenses, narcotics violations, mail fraud, and securities fraud.

Reasonable Suspicion: When information exists that establishes sufficient facts to give a trained law enforcement or criminal investigative agency officer, investigator, or employee a basis for believing that there is a reasonable possibility that an individual or organization is involved in a definable criminal activity or enterprise:.

Recommendations: Suggestions for actions to be taken based on the findings of an analysis.

Records (Intelligence): *See* Intelligence Records (Files).

Records System: A group of records from which information is retrieved by reference to a name or other personal identifier, such as a social security number.

Red Team: A technique for assessing vulnerability that involves viewing a potential target from the perspective of an attacker to identify its hidden vulnerabilities and to anticipate possible modes of attack.

Regional Information Sharing Systems (RISS): RISS is composed of six regional intelligence centers that provide secure communications, information-sharing resources, and investigative support to combat multijurisdictional crime and terrorist threats to more than 8,000 local, state, tribal, and federal member law enforcement agencies in all 50 states, the District of Columbia, U.S. territories, Australia, Canada, and England.

Reliability: Asks the question, "Is the source of the information consistent and dependable?"

Reporting: Depending on the type of intelligence, the process of placing analyzed information into the proper form to ensure the most effective consumption.

Requirements (Intelligence): The types of intelligence that operational law enforcement elements need from the intelligence function within an agency or other intelligence-producing organizations to enable law enforcement officers to maximize protection and preventive efforts as well as identify and arrest persons who are criminally liable.

Responsibility: Responsibility reflects how the authority of a unit or individual is used and determines whether goals have been accomplished and the mission fulfilled in a manner that is consistent with the defined limits of authority.

Right to Know: Based on having legal authority, one's official position, legal mandates, or official agreements, allowing the individual to receive intelligence reports.

Risk Assessment: An analysis of a target, illegal commodity, or victim to identify the probability of being attacked or criminally compromised and to analyze vulnerabilities.

Risk Management-Based Intelligence: An approach to intelligence analysis that has as its object the calculation of the risk attributable to a threat source or acts threatened by a threat source. It is a means of providing strategic intelligence for planning and policymaking, especially regarding vulnerabilities and countermeasures designed to prevent criminal acts and a means of providing tactical or operational intelligence in support of operations against a specific threat source, capability, or modality. It can be quantitative if a proper database exists to measure likelihood and impact and calculate risk; it can be qualitative and subjective and still deliver a reasonably reliable ranking of risk for resource allocation and other decision-making in strategic planning and for operations in tactical situations.

Rules: A specific requirement or prohibition that is stated to prevent deviations from policy or procedure. A violation of a rule typically results in an internal investigation and may result in disciplinary action.

SCI (Sensitive Compartmented Information): Classified information concerning or derived from intelligence sources, methods, or analytical processes that is required to be handled within formal access control systems.

SCIF (Sensitive Compartmented Information Facility): An accredited area, room, group of rooms, buildings, or an installation where SCI may be stored, used, discussed, and/or processed.

Sealing (Records): Records are stored by an agency but cannot be accessed, referenced, or used without a court order or statutory authority based on a showing of evidence that there is a legitimate government interest to review the sealed information.

Security: A series of procedures and measures that, when combined, provide protection of people from harm, information from improper disclosure or alteration, and assets from theft or damage. (Criminal Justice Commission, 1995.).

Sensitive But Unclassified (SBU) Information: Information that has not been classified by a federal law enforcement agency which pertains to significant law enforcement cases under investigation and criminal intelligence reports that require dissemination criteria to only those persons necessary to further the investigation or to prevent a crime or terrorist act.

Sensitive Homeland Security Information (SHSI): Any information created or received by an agency or any local, county, state, or tribal government that the loss, misuse, unauthorized disclosure, modification of, or the unauthorized access to could reasonably be expected to impair significantly the capabilities and/or efforts of agencies and/or local, county, state, and tribal personnel to predict, analyze, investigate, deter, prevent, protect against, mitigate the effects of, or recover from acts of terrorism. SHSI does not include any information that is: 1. Classified as national security information pursuant to Executive Order 12958, as amended, or any successor order; 2. Designated by Executive Order 12951, any successor order, or the Atomic Energy Act of 1954 (42 U.S.C. § 2011), to require protection against unauthorized disclosure; 3. Protected Critical Infrastructure Information (PCII) as defined in 6 Code of Federal Regulations (CFR) § 29.2; 4. Sensitive Security Information (SSI) as defined in 49 CFR Part 1520.

Signal Intelligence (SIGINT): The interception of various radio frequency signals, microwave signals, satellite audio communications, nonimagery infrared and coherent light signals, and transmissions from surreptitiously placed audio microtransmitters in support of the communications intelligence activity.

Sources: From an intelligence perspective, these are persons (human intelligence or HUMINT) who collect or possess critical information needed for intelligence analysis.

Spatial Analysis: The process of using a geographic information system in combination with crime-analysis techniques to assess the geographic context of offenders, crimes, and other law enforcement activity.

Statistical System: An organized means of collecting, processing, storing, and retrieving aggregate information for purposes of analysis, research, and reference. No individual records are stored in a statistical system.

Strategic Intelligence: An assessment of targeted crime patterns, crime trends, criminal organizations, and/or unlawful commodity transactions for purposes of planning, decision-making, and resource allocation; the focused examination of unique, pervasive, and/or complex crime problems.

Substantive Due Process: Guarantees persons against arbitrary, unreasonable, or capricious laws, and it acts as a limitation against arbitrary governmental actions so that no government agency may exercise powers beyond those authorized by the Constitution.

Surveillance: The observation of activities, behaviors, and associations of a LAWINT target (individual or group) with the intent to gather incriminating information, or "lead" information, which is used for the furtherance of a criminal investigation.

Suspicious Activity Report: A report and process wherein criminal indicators and behaviors that appear to have a criminal nexus are documented and processed through a law enforcement organization to determine if a crime is being planned, in the process of being committed or has been committed.

Tactical Intelligence: Evaluated information on which immediate enforcement action can be based; intelligence activity focused specifically on developing an active case.

Target: Any person, organization, group, crime or criminal series, or commodity being subject to investigation and intelligence analysis.

Target Profile: A profile that is person-specific and contains sufficient detail to initiate a target operation or support an ongoing operation against an individual or networked group of individuals.

Targeting: The identification of crimes, crime trends, and crime patterns that have discernable characteristics which make collection and analysis of intelligence information an efficient and effective method for identifying, apprehending, and prosecuting those who are criminally responsible.

Tear-Line Report: A report containing classified intelligence or information that is prepared in such a manner that data relating to intelligence sources and methods are easily removed from the report to protect sources and methods from disclosure. Typically, the information below the "tear line" can be released as Sensitive But Unclassified.

Telemetry: The collection and processing of information derived from noncommunications electromagnetic radiations emitting from sources such as radio navigation systems (e.g., transponders), radar systems, and information/data signals emitted from monitoring equipment in a vehicle or device.

Telephone Record (Toll)/Communications Analysis: An assessment of telephone call activity associated with investigatory targets including telephone numbers called and/or received, the frequency of calls between numbers, the dates of calls, length of calls, and patterns of use.

Third Agency Rule: An agreement wherein a source agency releases information under the condition that the receiving agency does not release the information to any other agency—that is, a third agency.

Threat Assessment: An assessment of a criminal or terrorist presence within a jurisdiction integrated with an assessment of potential targets of that presence and a statement of probability that the criminal or terrorist will commit an unlawful act. The assessment focuses on the criminal's or terrorist's opportunity, capability, and willingness to fulfill the threat.

Threat Inventory: An information and intelligence-based survey within the region of a law enforcement agency to identify potential individuals or groups that pose a criminal or terrorist threat without a judgment of the kind of threat they pose. The inventory is simply to determine their presence.

Undercover Investigation: Active infiltration of or an attempt to infiltrate a group believed to be involved in criminal activity and/or the interaction with a LAWINT target with the intent to gather incriminating information or lead information that is used for the furtherance of a criminal investigation.

Validity: Asks the question, "Does the information actually represent what we believe it represents?"

Variable: Any characteristic on which individuals, groups, items, or incidents differ.

Vet: To subject a proposal, work product, or concept to an appraisal by command personnel and/or experts to ascertain the product's accuracy, consistency with philosophy, and/or feasibility before proceeding.

Violent Criminal Apprehension Program (VICAP): A nationwide data information center operated by the FBI's National Center for the Analysis of Violent Crime, designed to collect, collate, and analyze specific crimes of violence.

Vulnerability Assessment: An assessment of possible criminal or terrorist group targets within a jurisdiction integrated with an assessment of the target's weaknesses, likelihood of being attacked, and ability to withstand an attack.

Warning: To notify in advance of possible harm or victimization as a result of information and intelligence gained concerning the probability of a crime or terrorist attack.

Appendix B: Intelligence Unit Management Audit

These audit criteria focus on the management of the intelligence unit. They were developed by the author for use in auditing a police department for compliance with a settlement agreement in a federal civil rights case.

Audit Criteria for the Law Enforcement Intelligence Function Version 2.0

Section A: Meeting National Standards

1. Does the police department subscribe to the tenets and standards of the Global Justice Information Sharing Initiative?
   ☐ Yes ☐ No
2. Does the police department subscribe to the standards of the National Criminal Intelligence Sharing Plan?
   ☐ Yes ☐ No
3. Does the police department subscribe to the guidelines for information and intelligence sharing of the Office of Domestic Preparedness Guidelines for Homeland Security?
   ☐ Yes ☐ No
4. Does the police department subscribe to the guidelines of the Commission on Accreditation for Law Enforcement Agencies (CALEA) Standard 51.1.1 Criminal Intelligence?
   ☐ Yes ☐ No
5. Does the police department subscribe to the provisions of the International Association of Chiefs of Police (IACP) Model Criminal Intelligence Policy?
   ☐ Yes ☐ No
6. Does the police department subscribe to the standards of the Law Enforcement Intelligence Unit (LEIU) Criminal Intelligence File Guidelines?
7. Does the police department subscribe to the IACP Code of Ethics or have an articulated Code of Ethics?
   ☐ Yes ☐ No
8. Does the police department subscribe to the IACP Code of Conduct[9]or have an articulated Code of Conduct?
   ☐ Yes ☐ No
9. Does the police department have an articulated Statement of Values?
   ☐ Yes ☐ No
10. Does the police department adhere to the regulations of 28 CFR Part 23 for its Criminal Intelligence Records System?
    ☐ Yes ☐ No
    a. Does the police department operate a federally funded multi-jurisdictional criminal intelligence records system?
       ☐ Yes ☐ No
11. Does the police department subscribe to the tenets of the Justice Information Privacy Guidelines?
    ☐ Yes ☐ No
12. Does the police department subscribe to the tenets for information system security defined in the report, Applying Security Practices to Justice Information Sharing?
    ☐ Yes ☐ No

13. Does the law enforcement agency subscribe to the philosophy of Intelligence-Led Policing?
    ☐ Yes ☐ No
14. Are defined activities for the intelligence unit designed exclusively to prevent and control crime with no political, religious or doctrinal purpose?
    ☐ Yes ☐ No

Section B: Management issues

1. Has a mission statement been written for the Intelligence Unit?
   ☐ Yes ☐ No
2. Is the purpose and role of the Unit clearly articulated and related to the Police Department's Mission Statement?
   ☐ Yes ☐ No
3. Have priorities been established for the types of crimes the Unit will address?
   ☐ Yes ☐ No
   a. Is any written rationale provided for these priorities?
      ☐ Yes ☐ No
4. Are expected activities of the unit articulated?
   ☐ Yes ☐ No
5. Does the mission statement express ethical standards?
   ☐ Yes ☐ No
6. Does the mission statement express the importance of protecting citizens' rights?
   ☐ Yes ☐ No

<u>1. Policies and Procedures</u>

1. Are there written and officially articulated policies and procedures for management of the intelligence function?
   ☐ Yes ☐ No
2. Have intelligence policies been formed to minimize the discretion of information collectors?
   ☐ Yes ☐ No If Yes, describe:
3. Is there a policy and procedures on "Information Collection"?
   ☐ Yes ☐ No If Yes, describe:

<u>2. Management of Information: Definitional Standards</u>

1. Are there standard terms used in intelligence activities that have been operationally defined in writing so that all persons in the department know the explicit meaning and implications of the terms?
   ☐ Yes ☐ No
2. What is the source of the definitions?
   ☐ NCISP ☐ Federal Agency
   ☐ Mixed ☐ N/A

3. Has the department articulated standards for classifying information in the Intelligence Unit?[1]
   ☐ Yes ☐ No
4. How are those standards monitored and enforced?
   ☐ Superior ☐ Other
5. Does the department have a system for assessing the reliability of sources that provide information that will be retained in the Intelligence Records System?
   ☐ Yes ☐ No
6. Are there standardized definitions of the reliability scale?
   ☐ Yes ☐ No
7. Does the department have a system for assessing the validity of the information that will be retained in the Intelligence Records System?
   ☐ Yes ☐ No
8. Are there standardized definitions of the validity scale?
   ☐ Yes ☐ No
9. Does the Intelligence Unit have operational definitions that can be applied to a person under investigation or a series of related crimes where the perpetrator is not identifiable in order to classify the case file as either a "permanent file" or a "temporary file"?
   ☐ Yes ☐ No

   If Yes...

   a. Are the types of identifying information that should be placed in the file articulated?
      ☐ Yes ☐ No
   b. Is there a procedure for requiring the articulation of the criminal predicate for the permanent file?
      ☐ Yes ☐ No
   c. Is there a procedure articulating the conditions wherein a temporary file may be created?
      ☐ Yes ☐ No
   d. Does the procedure specify a time limit that the temporary file can be kept?
      ☐ Yes ☐ No

[1]

Priority	Classification	Description	Release Authority
Highest Level	Sensitive	Current corruption case; complex criminality; confidential informants	Deptartment Executive or Intelligence Commander
Medium Level	Confidential	Nonsensitive information through intelligence channels; law enforcement only	Intelligence Unit Commander or Supervisor
Lowest Level	Restricted	LE use but no need for high security	Intell Unit Personnel
Unclassified	Public Access	Information that may be released to public and media	Intell Unit Personnel

e. Is there an operational definition of "Non-Criminal Identifying Information" and procedures for recording and retaining this information?
☐ Yes ☐ No

f. Are there clear procedures that describe the types of information that should not be entered into the Intelligence Records System?
☐ Yes ☐ No

3. Management of Information: Source Documents

1. Does the department have a written directive explaining the different types of source documents that will be entered in the Intelligence Records System?
☐ Yes ☐ No
2. What types of source documents are entered into the Intelligence Records System?
Describe:
3. Does the police department have a written directive that the rationale for each source document entered into the Intelligence Records System must be articulated in a report or notation?
☐ Yes ☐ No

4. Management of Information: Data Entry

1. Who is responsible for entering information into the Intelligence Records System?
Position/Classification:
2. Who supervises the information entry process?
Position/Classification:

5. Management of Information: Accountability

1. Who is the Custodian of the Intelligence Records System that ensures all regulations, law, policy and procedures are being followed?
Position/Classification:
2. Is there a person external to the Intelligence Unit who is designated to monitor the Intelligence Records System and related processes?
☐ Yes ☐ No If Yes, Position/Classification:
3. Does the department have written procedures for the retention of records in the Intelligence Records System?
☐ Yes ☐ No

6. Management of Information: Retention and Purging of Records

1. Does the retention process adhere to the guidelines of 28 CFR Part 23?
☐ Yes ☐ No
2. Does the retention policy and procedure include written criteria for purging information?
☐ Yes ☐ No
3. How often does a review and purge process occur?
Frequency:
4. What is the purge process?
Describe:

5. Does the purge process include a system review of information to confirm its continuing propriety, accuracy, and relevancy?
   □ Yes □ No
6. Does the purge process require destruction of the source document and removal of all references to the document to be purged if the information is no longer appropriate for retention?
   □ Yes □ No
7. What is the destruction process for purged hard copy records?
   Describe:
8. After information has been purged from a computerized Intelligence Records System, is free space on the hard drive and/or specific purged files electronically "wiped"?
   □ Yes □ No
   a. Are backups wiped?
      □ Yes □ No
   b. What is the accountability system for purging backups?
      Describe:
9. Does the purge process require the elimination of partial information that is no longer appropriate if the source document is to be kept because the remaining information in the source documents merits retention?
   □ Yes □ No
10. What is the process for purging partial information from hard copy source documents?
    Describe:
11. Who is responsible for ensuring compliance of the purge process?
    Position/Classification:

7. Management of Information: Personal/Individually-Held Records and Files

1. Is there an intelligence unit policy and procedures concerning the retention of individual notes and records that identifies persons wherein criminality is suspected but is not in either a temporary or permanent file and is not entered into any formal records system or database?
   □ Yes □ No
   a. How is the possession of personal records monitored?
      □ Yes □ No
   b. How is the policy enforced?
      □ Yes □ No

8. Management of Information: Accessing Intelligence Records

1. Is access to the Intelligence Records limited?
   □ Yes □ No
2. If yes, who may access the Intelligence Records System?
   □ Yes □ No
3. What security controls exist for accessing computerized records?
   □ Yes □ No

4. Can the computerized records system be accessed through remote access?
   □ Yes □ No
   a. If so, what security controls exist for remote access?
      Describe:
5. How are physical records stored?
   Describe:
6. Who grants access privileges to Intelligence Records?
   Position/Classification:
7. Who has access to records?
   □ Yes □ No
8. Does the police department apply the Third Agency Rule to information that is shared with other agencies?
   □ Yes □ No
9. What audit process is in place for access to computerized records?
   Describe:
10. What audit process is in place for access to physical records?
    Describe:
11. How are physical records secured?
    Describe:
12. What process is in place to handle unauthorized access to intelligence physical records?
    Describe:
13. What sanctions are in place for a police department employee who accesses and/or disseminates intelligence records without authorization?
    Describe:

<u>9. Physical Location of the Intelligence Unit and Records</u>

1. Sufficiency: Is the Intelligence Unit in a physical location that has sufficient space to perform all of its responsibilities?
   □ Yes □ No
2. Security: Is the Intelligence Unit in a physical location wherein the entire workspace may be completely secured?
   □ Yes □ No
   a. Is there adequate secured storage cabinets (or a vault) for (1) documents classified by the intelligence unit and (2) sensitive records storage within the intelligence unit's physical location?
      □ Yes □ No
   b. Is there adequate security and segregated storage for federally classified documents within the Intelligence Unit?
      □ Yes □ No
      1. Is that storage accessible only by persons with a federal Top Secret security clearance?
         □ Yes □ No
3. Convenience: Is the Intelligence Unit in a physical location that is convenient to the people, equipment, and resources necessary to maximize efficiency and effectiveness of operations?
   □ Yes □ No

10. Tangential Policy Issues: Criminal Informants and Undercover Operations

1. Is there a formally articulated policy and procedures for managing criminal informants?
   ☐ Yes ☐ No
   a. Is a background investigation conducted and a comprehensive descriptive file completed on each confidential informant?
      ☐ Yes ☐ No
   b. Are informant files secured separately from intelligence files?
      ☐ Yes ☐ No
2. Is there a formally articulated policy and procedures concerning undercover operations that apply to members of the Intelligence Unit?
   ☐ Yes ☐ No
3. Does the police department have a policy on alcohol consumption for officers working undercover?
   ☐ Yes ☐ No
   a. Does the police department have a policy requiring designated drivers for undercover officers who have consumed alcohol?
      ☐ Yes ☐ No
4. Does the police department have a "narcotics simulation" policy and training for undercover officers?
   ☐ Yes ☐ No
5. Does the police department have a policy for the issuance of fictitious identification for undercover officers and the proper use of such fictitious identification?
   ☐ Yes ☐ No
6. Do undercover officers receive training specifically related to proper conduct and information collection while working in an undercover capacity?
   ☐ Yes ☐ No
7. With respect to undercover operating funds:
   a. Is there a 1-tier or 2-tier process to approve use of the funds?
      ☐ 1-Tier ☐ 2-Tier
   b. Is a written report required to document expenditure of the funds?
      ☐ Yes ☐ No
   c. What is the maximum time that may pass between the expenditure of funds and personnel accountability for the funds?
      ☐ Yes ☐ No
   d. Is there a regular external audit of undercover funds?
      ☐ Yes (How Often) ☐ No

Section C: Personnel

1. Is a position classification plan in place that provides a clear job description for each position in the Unit?
   ☐ Yes ☐ No
2. Is a position classification plan in place that articulates Knowledge, Skills, and Abilities (KSAs) for each position?
   ☐ Yes ☐ No
3. Is there sufficient hierarchical staff (managers/supervisors) assigned to the Unit to effectively perform supervisory responsibilities?
   ☐ Yes ☐ No

4. Is there sufficient functional staff (analysts and/or investigators) to effectively fulfill defined unit responsibilities?
   ☐ Yes ☐ No
5. Is there sufficient support staff (secretaries, clerks) to effectively support the unit's activities?
   ☐ Yes ☐ No
6. Does the screening process for nonsworn employees of the Intelligence Unit require:
   a. Fingerprint check
      ☐ Yes ☐ No
   b. Background investigation
      ☐ Yes ☐ No
7. If the Intelligence Unit has non-police department employees assigned to it—e.g., National Guard analysts, personnel from the state or local law enforcement agencies—would there be a screening process for those persons?
   ☐ Yes ☐ No If Yes, Describe:

1. Training

1. What types of training do preservice and newly assigned personnel receive?
   ☐ None ☐ Some - Describe:
   a. Are newly assigned sworn employees to the Intelligence Unit required to attend 28 CFR Part 23 training?
      ☐ Yes ☐ No
   b. Are newly hired or assigned nonsworn employees required to attend 28 CFR Part 23 training?
      ☐ Yes ☐ No
2. What types of training do in-service personnel receive?
   ☐ None ☐ Some - Describe:
3. Have members of the Intelligence Unit attended any of the following federal government intelligence training programs which are open to state and local law enforcement officers.
   a. DEA Federal Law Enforcement Analyst Training (FLEAT)
      ☐ Yes ☐ No
   b. FBI College of Analytic Studies
      ☐ Yes ☐ No
   c. Federal Law Enforcement Training Center (FLETC) Criminal Intelligence Analysis Training Course
      ☐ Yes ☐ No
   d. National Drug Intelligence Center Basic Intelligence Analysis Course
      ☐ Yes ☐ No
   e. National White Collar Crime Center Foundations of Intelligence Analysis
      ☐ Yes ☐ No
   f. Regional Counterdrug Training Academy Intelligence Operations Course
      ☐ Yes ☐ No

2. Supervision

1. Does supervision effectively monitor adherence to written procedures?
   ☐ Yes ☐ No
2. Does supervision effectively monitor adherence to guidelines adopted by the department?
   ☐ Yes ☐ No
3. Are performance evaluations tied directly to the job descriptions?
   ☐ Yes ☐ No
4. Does supervision effectively monitor the performance of required duties (Including the quality of performance)?
   ☐ Yes ☐ No
5. Is supervision effectively monitoring personnel to ensure civil rights allegations cannot be made with respect to negligent:
   a. Failure to train
      ☐ Yes ☐ No
   b. Hiring
      ☐ Yes ☐ No
   c. Failure to supervise
      ☐ Yes ☐ No
   d. Assignment
      ☐ Yes ☐ No
   e. Failure to direct
      ☐ Yes ☐ No
   f. Failure to discipline
      ☐ Yes ☐ No
   g. Entrustment
      ☐ Yes ☐ No
6. Is there effective supervision of the Intelligence Unit throughout the chain of command external to the Intelligence Unit?
   ☐ Yes ☐ No

Section D: Fiscal Management

1. Is the budget sufficient to fulfill the stated mission?
   ☐ Yes ☐ No
2. Does the Intelligence Commander have input into the budget planning process?
   ☐ Yes ☐ No
3. Is there over-reliance on "soft money" to operate the Unit?
   ☐ Yes ☐ No
4. Are equipment and personnel line items assigned directly to the Intelligence Unit?
   ☐ Yes ☐ No
5. Is there an established process for reliably monitoring credit cards assigned to personnel?
   ☐ Yes ☐ No

Section E: Unit Evaluation

1. As a whole, is the Unit effective with respect to:

   a. Providing information to prevent crime?
      ☐ Yes ☐ No

   b. Providing information to apprehend criminals?
      ☐ Yes ☐ No

   c. Effectively analyzing information to identify criminal enterprises, crime trends, criminal anomalies, etc.?
      ☐ Yes ☐ No

2. Are data collected on the following factors and reported in an annual report as indicators of the intelligence Unit's productivity as an organizational entity?

   a. Number and type of analytic products delivered for investigative purposes
      ☐ Yes ☐ No ☐ N/A

   b. Number and type of analytic products that led to arrest
      ☐ Yes ☐ No ☐ N/A

   c. Assets seized from illegal activities wherein intelligence contributed to the arrest and/or seizure
      ☐ Yes ☐ No ☐ N/A

   d. Number and types of strategic intelligence products delivered to the command staff
      ☐ Yes ☐ No ☐ N/A

   e. Number of intelligence sharing meeting attended by Unit staff
      ☐ Yes ☐ No ☐ N/A

   f. Number of briefings provided by the intelligence staff
      ☐ Yes ☐ No ☐ N/A

   g. Total number of queries into the intelligence database
      ☐ Yes ☐ No ☐ N/A

   h. Number of permanent files opened
      ☐ Yes ☐ No ☐ N/A

   i. Number of temporary files investigated
      ☐ Yes ☐ No ☐ N/A

   j. Number of requests for information to the unit from outside agencies
      ☐ Yes ☐ No ☐ N/A

3. Are products produced by the Intelligence Unit:

   a. In a consistent format?
      ☐ Yes ☐ No

   b. Easily consumed and used (i.e., understandable and actionable)?
      ☐ Yes ☐ No

   c. Contain timely information and disseminated in a timely manner?
      ☐ Yes ☐ No

   d. Have substantive contact to aid in preventing or controlling crime?
      ☐ Yes ☐ No

4. Given the confidential nature of the information contained in the Intelligence Unit, is there a policy and procedures if a city, county, state, or federal fiscal or program auditor seeks to audit the Intelligence Unit?
   ☐ Yes ☐ No If Yes, Describe:

Section F: Collection

1. Is there an articulated collection plan for the Intelligence Unit?
   ☐ Yes ☐ No
   a. How often and when is the plan updated?
      ☐ Yes ☐ No
2. Have the following activities been performed by the Intelligence Unit:
   a. An inventory of threats in the region posed by criminal enterprises, terrorists, and criminal extremists.
      ☐ Yes ☐ No
   b. An assessment of the threats with respect to their probability of posing a criminal or terrorist threat to the region.
      ☐ Yes ☐ No
   c. A target or criminal commodity analysis of the region.
      ☐ Yes ☐ No
   d. A target or criminal commodity vulnerability assessment in the region.
      ☐ Yes ☐ No
3. For each identified threat, have intelligence requirements been articulated?
   ☐ Yes ☐ No
   a. If Yes, describe the methods of collection that will be used to fulfill those intelligence requirements.
      ☐ Yes ☐ No

Section G: Technology and Networking

1. Are any members of the Intelligence Unit subscribed members of the FBI's secure e-mail system Law Enforcement Online (LEO)?
   ☐ Yes - All ☐ Yes - Some ☐ No
2. Are any members of the Intelligence Unit subscribed members of the secure Regional Information Sharing System (RISS) e-mail system riss.net?
   ☐ Yes - All ☐ Yes - Some ☐ No
   a. If yes, are the RISS databases (e.g., RISS.gang, ATIX, etc.) regularly used?
      ☐ Yes ☐ No
3. Is the police department a member of the Regional Information Sharing System?
   ☐ Yes ☐ No
4. Is a systematic procedure in place to ensure that advisories and notifications transmitted via the National Law Enforcement Teletype System (NLETS) are forwarded to the Intelligence Unit?
   ☐ Yes ☐ No
5. Are you connected to any state-operated intelligence or information networks?
   ☐ Yes ☐ No If Yes, Describe:
6. Are you connected to any regional intelligence or information networks (including HIDTA)?
   ☐ Yes ☐ No
7. Does the intelligence have access and use the National Virtual Pointer System (NVPS)?
   ☐ Yes ☐ No

8. Is there a formal approval process for entering into a Memorandum of Understanding (MOU) for information and intelligence sharing with other law enforcement agencies or law enforcement intelligence entities?
   ☐ Yes ☐ No If Yes, describe the process:
   Who must approve the MOU?

Section H: Legal Issues

1. Is there a designated person in the police department who reviews Freedom of Information Act requests directed to the intelligence unit?
   ☐ Yes ☐ No
2. Is there a designated person in the police department who responds to Privacy Act inquiries directed to the Intelligence Unit?
   ☐ Yes ☐ No
3. Is there a designated person the police department contacts in response to a subpoena for a file in the Intelligence Records System?
   ☐ Yes ☐ No
4. Does the Intelligence Unit Commander have a legal resource for advice to help protect intelligence records from objectionable access?
   ☐ Yes ☐ No
5. Does the Intelligence Unit Commander have a legal resource for advice on matters related to criminal procedure and civil rights?
   ☐ Yes ☐ No
6. Does the Intelligence Unit Commander have a legal resource for advice on matters related to questions of civil liability as it relates to all aspects of the intelligence function?
   ☐ Yes ☐ No
7. Has legal counsel reviewed and approved all policies and procedures of the intelligence unit?
   ☐ Yes ☐ No

Appendix C:
LEIU Audit Checklist for the Criminal Intelligence Function

The Law Enforcement Intelligence Unit (LEIU) is the premier organization for law enforcement intelligence. The organization has established a solid reputation for professionalism, objectivity, and promoting intelligence activities that protect the constitutional rights and privacy of all Americans. This checklist was prepared to aid in the professional management of a state, local, and tribal law enforcement intelligence function. Additional materials, including a description of how the checklist was prepared, are available in the original LEIU Audit Checklist document, it.ojp.gov/documents/LEIU_audit_checklist.pdf.

This checklist provides law enforcement executives and senior- to mid-level law enforcement managers with a tool for conducting an audit or evaluation of their agency's criminal intelligence function. Specifically, this audit tool can help an agency ensure that it is carrying out the criminal intelligence function in accordance with applicable laws, regulations, and guidelines. The principles found in the checklist apply most directly to municipal, county, and state law enforcement agencies. Several introductory comments are appropriate.

This checklist should be applied only to criminal intelligence files, not to other types of law enforcement records. Some law enforcement officials fail to make the distinction between criminal intelligence files and other types of law enforcement records (e.g., investigative files). In the law enforcement context, however, these differences are important and must be recognized.

Investigation generally refers to the systematic examination of facts to determine if a crime has occurred and, if so, develop a case for prosecution. Generally, the term "investigative files" refers to information collected in the course of an investigation where there are reasonable grounds to suspect that a person has committed specific criminal acts.

On the other hand, the criminal intelligence process is an ongoing activity, and is not necessarily triggered by the investigation of any specific offense. While investigation tends to be reactive in nature, criminal intelligence is proactive and used to identify and understand criminals operating in a particular area. Once individuals or groups are identified and their habits known, law enforcement authorities may begin to assess current trends in crime and to forecast, and possibly prevent, future criminal activities. Intelligence provides the knowledge on which to base decisions, and select appropriate targets (subjects, criminal groups or businesses) for investigations. Although criminal intelligence may be used to assist in investigations, surveillance operations, and prosecution of cases, it also provides law enforcement agencies with the ability to effectively manage resources, budget, and meet their responsibility to forecast community threats to prevent crime.

Criminal intelligence consists of pieces of raw information that when collected, evaluated, collated, and analyzed, form meaningful and useful judgments that are both accurate and timely. Taking this raw information and turning it into intelligence can be described as a sequential process with multiple distinct phases. Following appropriate planning, the first phase is collection, when raw information is obtained from various sources. Evaluation then occurs, which determines the reliability of the source and the validity of the information. The third phase is collation and involves indexing, cross-referencing, and filing of information. The fourth phase is analysis, which identifies trends, future developments, and case building. The fifth phase is dissemination, which involves the actual dispensing of the intelligence information. A unit that does not complete each of these phases is not a criminal intelligence unit.

Ideally, this checklist is designed to be utilized by senior law enforcement managers who are not directly involved in the day-to-day operations of the agency's criminal intelligence function. This helps ensure that the audit is objective, and accurately identifies the function's strengths and weaknesses. The checklist can also be used as a self-assessment tool by personnel who are directly involved with the agency's criminal intelligence function. This type of effort will help determine if the unit is acting in accordance with the standard practices and procedures established by LEIU.

Historically, criminal intelligence units have experienced problems in the areas of unit operating procedures, collection, collation, and dissemination; this checklist focuses on these areas.

Unit Operating Procedures

1. Does the criminal intelligence unit have a mission statement? If no, go to question 10.
   ☐ Yes ☐ No
2. Does the mission statement contain a concise, well-defined mandate describing the criminal intelligence unit?
   ☐ Yes ☐ No
3. Does the mission statement describe the use of the intelligence process in support of the criminal intelligence unit?
   ☐ Yes ☐ No
4. Does the statement focus toward criminal predicate?
   ☐ Yes ☐ No
5. Does the statement indicate that the criminal intelligence unit will provide the Chief Executive with criminal information and resulting analysis to counter and control criminal activities?
   ☐ Yes ☐ No
6. Does the statement identify the criminal intelligence unit's expected results?
   ☐ Yes ☐ No
7. Is the criminal intelligence unit staying within its mission?
   ☐ Yes ☐ No
8. Is the criminal intelligence unit assuming work beyond the authorized crime areas?
   ☐ Yes ☐ No
9. Is the statement reviewed on a periodic basis to insure that it is meeting the needs of the agency/organization?
   ☐ Yes ☐ No
10. Does the criminal intelligence unit have policy and procedures guidelines? If no, go to question 18.
    ☐ Yes ☐ No
11. Do the guidelines describe the criminal intelligence unit's operations?
    ☐ Yes ☐ No
12. Do the guidelines provide the criminal intelligence unit's mission statement?
    ☐ Yes ☐ No
13. Do the guidelines detail the criminal intelligence unit's methods of operation?
    ☐ Yes ☐ No
14. Do the guidelines outline the criminal intelligence unit's file guidelines?
    ☐ Yes ☐ No
15. Do the guidelines establish the criminal intelligence unit's security procedures?
    ☐ Yes ☐ No
16. Do the guidelines describe personnel responsibilities and assigned duties?
    ☐ Yes ☐ No
17. Have the guidelines been provided to personnel?
    ☐ Yes ☐ No

18. Are periodic security updates conducted for intelligence personnel on a regular basis?
    ☐ Yes ☐ No
19. Is the criminal intelligence unit located in a physically secure location?
    ☐ Yes ☐ No
20. Are unauthorized persons prevented from accessing the criminal intelligence unit's location?
    ☐ Yes ☐ No
21. Is access terminated when personnel are on leave or cease to work in an intelligence capacity?
    ☐ Yes ☐ No
22. Are there guidelines for transferring material to or from floppy disks?
    ☐ Yes ☐ No
23. Does the criminal intelligence unit have access to the Chief Executive?
    ☐ Yes ☐ No
24. Does the unit provide the Chief Executive with recommendations?
    ☐ Yes ☐ No
25. Does the unit provide the agency with valuable strategic and tactical products?
    ☐ Yes ☐ No
26. Do personnel receive appropriate training?
    ☐ Yes ☐ No
27. Are there clear lines of responsibility and accountability for the functions of the intelligence unit?
28. ☐ Yes ☐ No
29. Is a regular security risk review of the intelligence unit and its systems conducted?
    ☐ Yes ☐ No
30. Are procedures in place governing the criminal intelligence unit's use of special funds?
    ☐ Yes ☐ No
31. Is the criminal intelligence unit's mission achievable with the number of assigned staff?
    ☐ Yes ☐ No

Collection

31. Does a collection effort begin with the development of a written plan?
    ☐ Yes ☐ No
32. Does the collection plan include a set of information requirements that specifies what data are needed by the agency or investigator (s)?
    ☐ Yes ☐ No
33. Does the collection plan comply with applicable local, state, and federal statutes and case law?
    ☐ Yes ☐ No
34. Is the collection plan focused on identifying the nature and extent of criminal activity?
    ☐ Yes ☐ No
35. Does the collection plan utilize all known available sources?
    ☐ Yes ☐ No
36. Are the plan's objectives and requirements communicated to criminal intelligence unit staff?
    ☐ Yes ☐ No
37. Has the Criminal Intelligence Function encouraged the development of a close working relationship between analysts and investigators?
    ☐ Yes ☐ No
38. Have those assigned to the Criminal Intelligence Function received training in the right to privacy?
    ☐ Yes ☐ No

39. Does the state in which your agency resides have laws that address the collection of criminal intelligence data?
    ☐ Yes ☐ No
40. Do the methods used by information collectors fall within legal guidelines?
    ☐ Yes ☐ No
41. Does your agency have informant guidelines in place? If no, go to question 44.
    ☐ Yes ☐ No
42. Do these guidelines address informant control and management?
    ☐ Yes ☐ No
43. Do these guidelines address the maintenance of informant files?
    ☐ Yes ☐ No

Collation

44. Does the unit have criminal intelligence file guidelines?
    ☐ Yes ☐ No
45. Is the criminal intelligence unit operating within the guidelines?
    ☐ Yes ☐ No
46. Are files kept ONLY on individuals who are suspected of being involved in actual or attempted criminal acts; or suspected of being involved in criminal activities with known or suspected crime figures?
    ☐ Yes ☐ No
47. Are files kept ONLY on organizations, businesses, and groups that are suspected of being involved in actual or attempted criminal acts; or are suspected of being operated, controlled, financed, or infiltrated by known or suspected crime figures?
    ☐ Yes ☐ No
48. Do files include information that relates ONLY to a criminal predicate?
    ☐ Yes ☐ No
49. Do the guidelines clearly delineate criteria for determining if information should be entered and retained in the files?
    ☐ Yes ☐ No
50. Is the information stored in criminal intelligence files evaluated according to source reliability and content validity before it is included in a criminal intelligence file?
    ☐ Yes ☐ No
51. Is there a clearly articulated system for assessing source reliability and content validity?
    ☐ Yes ☐ No
52. Is a distinction made between permanent, temporary, and working files along with appropriate retention periods?
    ☐ Yes ☐ No
53. Is the information stored in criminal intelligence files classified in order to protect sources, investigators, and the individual's right to privacy?
    ☐ Yes ☐ No
54. Are files clearly marked with appropriate classification?
    ☐ Yes ☐ No
55. Is information maintained in the criminal intelligence file reviewed for reclassification or purge on a periodic basis to ensure that it is current, accurate, safeguards an individual's right to privacy, and is classified at an appropriate security level?
    ☐ Yes ☐ No

56. Is information maintained in the criminal intelligence file reviewed on a periodic basis for utility, timeliness, appropriateness, accuracy, and completeness?
    ☐ Yes ☐ No
57. Do the criminal intelligence unit's purge policies comply with local, and/or state law regarding records retention?
    ☐ Yes ☐ No
58. Is there a specific staff member(s) who is responsible for purging files?
    ☐ Yes ☐ No
59. Are procedures in place to govern the storage, handling, and security of hard copy source material?
    ☐ Yes ☐ No
60. Does the criminal intelligence unit retain hard copies of source documents? If no, go to question 63.
    ☐ Yes ☐ No
61. Are these documents stored in a safe and secure location?
    ☐ Yes ☐ No
62. Is access to these documents restricted?
    ☐ Yes ☐ No
63. Are procedures in place to govern the storage, handling, and security of source material in an electronic database?
    ☐ Yes ☐ No
64. Is access to the file database restricted?
    ☐ Yes ☐ No
65. Is a specific employee(s) responsible for controlling automated access?
    ☐ Yes ☐ No
66. Are automated access audits conducted periodically?
    ☐ Yes ☐ No
67. Is a record of audits maintained?
    ☐ Yes ☐ No
68. Is automated access immediately deleted when personnel leave or transfer?
    ☐ Yes ☐ No
69. Are files adequately safeguarded through back-up and recovery routines, and off-site storage of critical files, programs, and systems?
    ☐ Yes ☐ No
70. Is the system isolated from other networks or protected by a firewall to restrict unauthorized access?
    ☐ Yes ☐ No
71. Are files (either hard or electronic copy) indexed in an organized fashion?
    ☐ Yes ☐ No
72. Is a file locator system in place?
    ☐ Yes ☐ No
73. Is a particular employee(s) responsible for overseeing the criminal intelligence file system so that it is operating within the guidelines of all applicable laws?
    ☐ Yes ☐ No
74. Are purged documents destroyed in a secure and appropriate manner according to all applicable laws?
    ☐ Yes ☐ No

Dissemination

75. Are procedures in place for responding to requests for information?
    ☐ Yes ☐ No
76. Are records kept of requests for information and responses? If no, go to question 79.
    ☐ Yes ☐ No
77. Are these records audited periodically?
    ☐ Yes ☐ No
78. Are there procedures in place governing the methods of enveloping, dispatching, and recording the dissemination of law enforcement sensitive material?
    ☐ Yes ☐ No
79. Is criminal intelligence information released only to those who have demonstrated a right to know and a need to know?
    ☐ Yes ☐ No
80. Is there an audit trail to determine who has accessed criminal intelligence files?
    ☐ Yes ☐ No
81. Has the criminal intelligence unit established a policy prohibiting third-party dissemination?
    ☐ Yes ☐ No
82. Has the agency identified legal resources that are familiar with criminal intelligence issues and procedures and can adequately represent the agency in legal matters?
    ☐ Yes ☐ No

References

Audit Factors for the Law Enforcement Intelligence Function. David L. Carter, 2004.

Criminal Intelligence File Guidelines. Law Enforcement Intelligence Unit. Revised in March 2002.

Criminal Intelligence Standards and Guidelines. California Peace Officers' Association, July 2003.

Evaluation Checklists for Intelligence Units. Paul R. Roger. *Turn-Key Intelligence: Unlocking Your Agency's Intelligence Capabilities,* IALEIA, LEIU, and NW3C.

Gang File Audit Checklist. California Bureau of Investigation, Division of Law Enforcement, California Department of Justice, May 2001.

Guidelines for the Criminal Intelligence Function. Dick Wright, Simi Valley Police Department, Revised September 1998.

Intelligence 2000: Revising the Basic Elements; A Guide for Intelligence Professionals. LEIU and IALEIA. Managing Editor Marilyn B. Peterson, Editors Bob Morehouse and Dick Wright, 2000.

National Criminal Intelligence Sharing Plan 2003. Office of Justice Programs, U.S. Department of Justice, Award No. 2000-LD-BX-0003, October 2003.

Appendix D: About the Author

David L. Carter, Ph.D.
Professor and Director, Intelligence Program
School of Criminal Justice
560 Baker Hall
Michigan State University
East Lansing, MI 48824-1118
517.355.6649/Fax 517.355.6646
carterd@msu.edu

David L. Carter (Ph.D., Sam Houston State University) is a Professor in the School of Criminal Justice and Director of the Intelligence Program at Michigan State University. A former Kansas City, Missouri, police officer, Dr. Carter was Chairman of the Department of Criminal Justice at the University of Texas-Pan American in Edinburg, Texas, for 9 years prior to his appointment at Michigan State in 1985. He has served as a trainer, consultant, and advisor for many law enforcement agencies throughout the U.S., Europe, and Asia on matters associated with officer behavior, community policing, law enforcement intelligence, and computer crime. In addition, he has presented training sessions at the FBI National Academy, the FBI Law Enforcement Executive Development Seminar (LEEDS), the International Law Enforcement Academy in Budapest, Hungary; the United Nations Asia and Far East Institute (UNAFEI) in Tokyo; police "command colleges" of Texas, Florida, Ohio, Massachusetts, Wisconsin, and Kentucky; and served at the FBI Academy's Behavioral Science Services Unit, the first academic faculty exchange with the Bureau. Dr. Carter is an Instructor in the Bureau of Justice Assistance SLATT program, author of the COPS-funded publication, *Law Enforcement Intelligence: A Guide for State, Local and Tribal Law Enforcement*, and Project Director for three multimillion-dollar intelligence training programs funded by the Department of Homeland Security. He is an Academic Fellow of the Foundation for Defending Democracies wherein he studied terrorism in Israel. Dr. Carter is also a member of the Justice Department's Counterterrorism Training Coordination Working Group and the Intelligence Training Coordination Working Group. In addition to teaching graduate and undergraduate courses at Michigan State, Dr. Carter is Director of the Criminal Justice Overseas Study Program to England. He is the author or coauthor of five books and numerous articles and monographs on policing issues and is a member of the editorial boards of various professional publications. His most recent book is the seventh edition of the widely-used community relations textbook, *The Police and Community*, published by Prentice Hall, Inc.

To obtain details on COPS programs, call the
COPS Office Response Center: 800.421.6770

Visit COPS Online at www.cops.usdoj.gov

May 2009
e050919201

COPS
COMMUNITY ORIENTED POLICING SERVICES
U.S. DEPARTMENT OF JUSTICE

This Page Is Intentionally Left Blank

Additional Reference Information

The Following publications are restricted or have copyright limitations that restricts their distribution.

You can access these publications via the Internet

These publications can be found using a standard web search engine using the following steps:

- Enter the name of the publication.

- Add the file format term **pdf** at the end of the publication search string.

Example

21 st - Century Marine Expeditionary Intelligence Analysis (MEIA-21)
Modernizing Tactical Military Intelligence Analysis **pdf**

Or

The NATO Alternative Analysis Handbook
Second Edition **pdf**

The following is a list of the restricted publications

The National Intelligence Model
National Criminal Intelligence Service
United Kingdom

21 st - Century Marine Expeditionary Intelligence Analysis (MEIA-21)
Modernizing Tactical Military Intelligence Analysis
United States Marine Corps
September 2011

Law Enforcement Intelligence Operations
. CONCEPTS
. ISSUES
. TERMS
David L Carter
School Of Criminal Justice
Michigan State University
East Lansing, MI

Intelligence Analysis In The Knowledge Age
An Analysis of the Challenges facing the Practice of Intelligence Analysis
Magdalena Adriana Duvenage
Stellembpsch University
March 2010

Intelligence Analysis
A Target Centric Approach
Robert M. Clark

Applied Thinking For Intellegence Analysis
A Guide For Practitioners
Charles Vandepeer
Department of Defence
Commonwealth of Australia
2014

The NATO Alternative Analysis Handbook
Second Edition
North Antlantic Treaty Organization
December 2017

Series 1: Research Publications No. 14
Military Intelligence Analysis:
Institutional Influence
Martin Bang
National Defence University
Drottning Kristinas, Stockholm
October 2017

Instructor Materials
Cases in Intelligence Analysis
Structured Analytic Techniques In Action
Second Edition
Sarah Miller Beebe
Randolph H. Pherson
CQ Press, an Imprint of SAGE Publications, Inc.
Thousand Oaks, CA
2015

Criminal Intelligence
Manual for Managers
United Nations
Office On Drugs And Crime
Vienna, Austria
March 2011

DIA Analyst Training Requirements And Competencies
Defense Inteligence Agency
Joint Military Intelligence Training Center
August 2008

Analytic Tradecraft In The U.S. Intelligence Community
John Joseph Borek
Walden University
Minneapolis, MN
2017

Military Peacekeeping
Intelligence Handbook
(MPKI-HB)
United Nations
April 2019

Military Intelligence
Fusion for Complex Operations
A New Paradigm
Ben Connable
RAND National Defense Research Institute
Santa Monica, CA
2012

Assessing the Tradecraft of Intelligence Analysis
Gregory F. Treverton, C. Bryan Gabbard
RAND National Defense Research Institute
Santa Monica, CA
2008

Air Force Pamphlet AFP 14-210
USAF Intelligence Targeting Guide
United States Air Force
February 1998

Training Circular TC 2-50.5
Intelligence Officer’s Handbook
Headquarters, Department of the Army
January 2010

Army Techniques Publication ATP 2-33.4
Intelligence Analysis
Headquarters, Department of the Army
August 2014

Analytical Thinking And Presentation For Intelligence Producers
Analysis Training Handbook
Office Of Training And Education
Central Intelligence Agency

This Page Is Intentionally Left Blank